Safety and Reliability
Methodology and Applications



Editors
Tomasz Nowakowski
Marek Młyńczak
Anna Jodejko-Pietruczuk
Sylwia Werbińska-Wojciechowska

CRC Press
Taylor & Francis Group
A BALKEMA BOOK

This page intentionally left blank

PROCEEDINGS OF THE EUROPEAN SAFETY AND RELIABILITY CONFERENCE, ESREL 2014, WROCŁAW, POLAND, 14–18 SEPTEMBER 2014

Safety and Reliability: Methodology and Applications

Editors

Tomasz Nowakowski, Marek Młyńczak,
Anna Jodejko-Pietruczuk & Sylwia Werbińska-Wojciechowska
Faculty of Mechanical Engineering, Wrocław University of Technology, Wrocław, Poland

CRC Press
Taylor & Francis Group
Boca Raton London New York Leiden

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A BALKEMA BOOK

CRC Press/Balkema is an imprint of the Taylor & Francis Group, an informa business

© 2015 Taylor & Francis Group, London, UK

Typeset by V Publishing Solutions Pvt Ltd., Chennai, India
Printed and bound in Great Britain by CPI Group (UK) Ltd, Croydon, CR0 4YY

All rights reserved. No part of this publication or the information contained herein may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, by photocopying, recording or otherwise, without written prior permission from the publisher.

Although all care is taken to ensure integrity and the quality of this publication and the information herein, no responsibility is assumed by the publishers nor the author for any damage to the property or persons as a result of operation or use of this publication and/or the information contained herein.

Published by: CRC Press/Balkema
P.O. Box 11320, 2301 EH Leiden, The Netherlands
e-mail: Pub.NL@taylorandfrancis.com
www.crcpress.com – www.taylorandfrancis.com

ISBN: 978-1-138-02681-0 (Hbk + CD-ROM)
ISBN: 978-1-315-73697-6 (eBook PDF)

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Table of contents

Preface xxvii

Acknowledgements xxix

Conference organization xxxi

Introduction xxxv

METHODOLOGY AREAS

Accident and incident investigation and modelling

Aeronautics and aerospace

An incident reporting support system for airline cabin crew 3
K. Furuta, K. Okano, T. Kanno, T. Mori & S. Shimizu

Chemical process industry

The effect of the environment conditions on the prediction of flammable cloud dispersion 11
A.M. Schleder, M.R. Martins, E. Pastor & E. Planas

Scenario identification in oil and gas industry: A case in the Middle East 21
Z. Rezvani, P. Swuste & P. Hudson

Civil engineering

Analysis of roadside safety barrier using numerical model 29
P. Hradil, J. Kala & V. Salajka

Critical infrastructure

Developing a framework for characterising cascading failures in past events to inform emergency response decisions 33
H. Hassel, A. Cedergren, L. Svegrup & J. Johansson

A critical evaluation of risk assessment methodology for natural gas pipeline 43
J. Kraus

An ontology-based approach to vulnerability and interdependency modelling for Critical Infrastructure systems 49
P. Trucco & B. Petrenj

Electrical engineering

Renewable sources impact on power system reliability and nuclear safety 57
A. Volkanovski & B. Gjorgiev

Maritime transportation

Titanic viewed from different perspectives on major accidents 65
H. Kim & S. Haugen

Usability of accident and incident reports for evidence-based risk modeling of ship grounding 75
A. Mazaheri & J. Montewka

Winter navigation at the Baltic Sea: An analysis of accidents occurred during winters 2002–2003 & 2009–2013 83
O.A. Valdez Banda, F. Goerlandt, J. Montewka & P. Kujala

Rail transportation

Structuring contributors to successful operation 93
J. Vatn

Road transportation

Country Safety Performance Function and the factors affecting it 101
K. Jamroz

Method of dynamic identification of hazardous driver behaviour by traffic parameters detection 109
M. Sumiła & M. Siergiejczyk

Waterborne transportation

The method of risk management of accidental oil spills at sea 115
K. Łazuga & L. Gucma

Other reliability and safety areas

The impact of new technologies on the safety level of air traffic in Poland 121
K. Krzykowska & M. Siergiejczyk

Black swan accidents: Predicting and preventing the unpredictable 127
D.J. Winfield

Analytical methods in system safety and reliability

Aeronautics and aerospace

Studies of the jet engine control quality based on its response to the disturbance inflicted on the object, designated from its response to the set point inflicted to the controller 137
K. Golak, P. Lindstedt & R. Grądzki

The mathematical formula of safety of aircrafts 141
J. Lewitowicz, S. Rutkowski, R. Tomaska & A. Żyluk

The reliability analysis of the satellite's driving system based on the IABCBLT method 143
W. Peng, J. Zhang & L.J. Kan

The effectiveness of the FMEA technology in the process of the aerospace product development 151
J. Shuyuan, L. Fuqiu, W. Jinjing & L. Meinan

Reliability modeling method of space mechanism considering dynamical cascading effects 155
C.L. Tan, J.G. Zhang, P. Wang & L.J. Kan

Chemical process industry

Comparative analysis of calculation methods of pressure drops for two-phase flow through pipelines 163
G. Boccardi, R. Trinchieri, R. Bubbico & B. Mazzarotta

Critical infrastructure

Empirical Bayes inference with nonlinear homogenizations and correlated intensity functions: Use in asset degradation modelling 171
G. Blair, J. Quigley & L. Walls

Dependence of the gas supply system criticality indicator(s) on the system elements' reliability 181
B. Jokšas, I. Žutautaitė, J. Augutis & T. Rekašius

Comparing societal consequence measures of outages in electrical distribution systems 189
F. Landegren, J. Johansson & O. Samuelsson

On the resilience analysis of interconnected systems by a set-theoretic approach 197
X. Liu, I. Prodan & E. Zio

A brief note on the ratio of the rectilinear and shortest distance between two arbitrary points on the 3-sphere 207
M.A. Odijk & P.H.A.J.M. van Gelder

A game-theoretical model to allocate security resources in a multi-modal transportation system facing adaptive adversaries 211
L. Talarico, K. Sörensen & G. Reniers

Electronic industry

Assessment of the critical events sequences of systems by means of probabilistic languages 217
D. Ionescu, N. Brînzei & J.F. Pétin

Energy production and distribution

RAM analysis applied to decommissioning phase: Comparison and assessment of different methods to predict future failures 225
E. Calixto & Y. Bot

Reliability indices computation for a flow network with a series-parallel-reducible structure 235
J. Malinowski

Information technology and telecommunication

Minimal cut sets and direct partial logic derivatives in reliability analysis 241
M. Kvassay, E. Zaitseva & V. Levashenko

On the probability of escaping a cell—in wireless networks 249
C. Tanguy

Maritime transportation

Reliability analysis of ship-rope transporter with dependent components 255
A. Blokus-Roszkowska & K. Kołowrocki

Maritime traffic flow simulation in the Intelligent Transportation Systems theme 265
A. Blokus-Roszkowska & L. Smolarek

Modeling of event trees for the rapid scenario development 275
M.K. Gerigk

The influence of screw propellers manufacturing accuracy on conditions of the propulsion system operating 281
E. Skupień

Mechanical engineering

Contribution to oil data assessment for system condition determination 287
D. Vališ & L. Žák

Rail transportation

Dependability and safety analysis of ERTMS level 3 using analytic estimation 293
T. Babczyński & J. Magott

Streamlining architectures for integrated safety analysis using Design Structure Matrices (DSMs) 299
K. Höfig, J.Z. Guo & A. Kazeminia

The Markov reliability and safety model of the railway transportation system 303
F.J. Restel

Reliability analysis of rail teleinformation system 313
M. Siergiejczyk

Road transportation

Premises of evaluation of the technical object suitability with including the quality of its maintenance and operation, and their initial conditions 319
R. Grądzki, P. Lindstedt & K. Golak

Bivariate reliability analysis of driving profiles in automobile fleets 327
T. Köttermann, M. Grabert, S. Kempe & S. Bracke

Attempt to apply the theory of reliability to assessment of signalised lane operation 335
K. Ostrowski

Reliability-exploitation analysis of power supply in transport telematics system 343
A. Rosiński

Reliability-maintenance analysis of highway emergency communication systems 349
M. Siergiejczyk, J. Chmiel & A. Rosiński

Hierarchical random models in road transport safety 355
J. Wachnicka, K. Jamroz & L. Smolarek

Other reliability and safety areas

Overall regional risk analysis of four Norwegian municipalities 361
R. Flage, Ø. Amundrud & H.S. Wiencke

Modeling reliability of complex port transportation system 371
K. Kołowrocki & J. Soszyńska-Budny

Reliability optimization of complex port transportation system 385
K. Kołowrocki & J. Soszyńska-Budny

Involvement of expert judgement in dynamic model 393
R. Krikštolaitis, A.E. Lutynska, S. Pečiulytė & I. Žutautaitė

Anthropo-technical systems reliability 399
D. Laskowski, P. Łubkowski, E. Pawlak & P. Stańczyk

Cost-benefit analysis of surveillance technologies 409
P.-H. Lin & C. van Gulijk

Integrated estimation of pipeline failure probability 417
I. Žutautaitė, G. Dundulis, S. Rimkevičius & R. Janulionis

Reliability and safety management

Aeronautics and aerospace

Reliability engineering interactions in aerospace products 425
E.N. Çetin & A.Ş. Temiz

An influence of the lifetime assessment in aviation technology 433
K. Kustroń & J. Lewitowicz

Chemical process industry

How managers should think about risk—a case study from the oil and gas industry 437
T. Bjerga & T. Aven

Balancing safety and performance through QRA and RAM analyses 445
V. Borges & C. Hickey

Public risk perception towards chemical process industry: Comprehension and response planning 453
D. Botheju & K. Abeysinghe

Risk assessment system for verifying the safety guards system based on the HAZOP analysis information 461
A. Nakai, K. Isshiki & K. Suzuki

Development of the Safety Requirements Specification (SRS) in oil and gas industry 467
E.H. Park, K.P. Chang & S.T. Kim

Civil engineering

Development of functional safety standards for civil engineering 475
E. Nachtigall & V. Shcherbina

Mechanism design for risk allocation and benefit sharing in the development of a Geological Disposal Facility for nuclear radioactive waste 481
O. Nieto-Cerezo, E. Patelli, J. Wenzelburger & M. Beer

Optimization of the drinking water coagulation and filtration system as a result of reliability analysis and Life Cycle Costing 487
J. Szymik-Gralewska & I. Zimoch

Critical infrastructure

Methods of visualizing the risk of lack of water supply 497
I. Piegdoń & B. Tchórzewska-Cieślak

Electrical engineering

Concept for development of safety-related filters 507
O. Krini, J. Krini & J. Börcsök

Energy production and distribution

Heat Supply System reliability management 513
B. Babiarz

Uncertainty in the regulation systems of temporary organizations: A challenge for improving the organizational reliability 521
F. Mazzorana-Kremer, C. Martin & J.L. Wybo

Solutions and safety barriers: The holistic approach to risk-reducing measures 531
A. Sevcik & O.T. Gudmestad

A multi-criteria decision model to mitigate the operational risks of offshore wind infrastructures 539
M. Shafiee & A. Kolios

Manufacturing and supply chain/logistic systems

Evaluation of operational reliability of the supply chain in terms of the control and management of logistics processes 549
I. Jacyna-Gołda

Effectiveness of national transport system according to costs of emission of pollutants 559
M. Jacyna, K. Lewczuk, E. Szczepański, P. Gołębiowski, R. Jachimowski, M. Kłodawski, D. Pyza, O. Sivets, M. Wasiak, J. Żak & I. Jacyna-Gołda

Experiments for PHM: Needs, developments and challenges 569
X.-Y. Li, L. Liu, R. Kang, D. Xu, F. Sun & J. Lee

Maritime transportation

Effects of external audits on safety management systems: A case study of the Norwegian-managed maritime industry 577
J.F. Aae, A.K. Sydnes & C. Heggøy

Review of acceptable risk levels of bridge collapse in respect of ships collisions 585
L. Gucma

A new approach for evaluating the disruption risks of a seaport system 591
A. John, R. Riahi, D. Paraskevadakis, A. Bury, Z. Yang & J. Wang

Methodology for evaluation of barriers for rig move operations 599
E. Okstad, S. Hauge, B.A. Mostue & H. Skår

Natural resources and environment

Performance of skimmers in the Arctic offshore oil spills 607
M. Naseri & J. Barabady

Nuclear engineering

Rethinking nuclear safety management: Injunction as a meta-concept 615
S. Agulhon, D. Pécaud & F. Guarnieri

Using IRIDM & VTA to support the risk management of the research reactor Maria 621
M. Borysiewicz, K. Kowal & S. Potempski

Evaluation of risk impact of equipment ageing and asset management for LWR Gen II and III NPPs in the horizon 2020 627
S. Martorell, I. Martón, S. Carlos & A.I. Sánchez

Rail transportation

Safety of the new control command European System 635
M. Siergiejczyk, M. Pawlik & S. Gago

Software systems

All swept up: An initial classification of NSA surveillance technology 643
M. Cayford, C. van Gulijk & P.H.A.J.M. van Gelder

Study of the security of processes running in computer operating systems 651
I.J. Jóźwiak & A. Szleszyński

Control-in-the-loop Model Based Safety Analysis 655
P.-Y. Piriou, J.-M. Faure & J.-J. Lesage

Developing a shared information surface for offshore work permits 663
S. Sarshar, G. Rindahl, C.S. Olsen, J.M. Røsok, M. Eskerud, O.G. Nedrebø, P.J. Berg & G. Misund

Other reliability and safety areas

Graphical technique for practical dependability management 671
L. Barberá, A. Crespo, K. Kobbacy & P. Viveros

A discussion of the risk-management and the rule-compliance regulation regimes in a security context 677
S.H. Jore & A. Moen

Risk management in anchor-handling operations: The balance between control and autonomy 685
J. Røyrvik, K. Skarholt, G.M. Lamvik & J.R. Jonassen

Safety and environmental control of industrial activities in France: A negotiated relationship 695
V. Sanseverino-Godfrin

Risk assessment methods for improving urban security 701
C. Schoppe, J. Zehetner, J. Finger, D. Baumann, U. Siebold & I. Häring

Abstract representation of power system networks as a function of regularity properties 709
A.B. Svendsen, T. Tollefsen, R.F. Pedersen, K.P. Petursson, D. Patel & O.D. Lampe

Drinking water quality aspect in ensuring the safety of water supply systems 717
I. Zimoch, E. Łobos & T. Żaba

Dynamic reliability

Aeronautics and aerospace

Using dynamic risk modelling in Single European Sky Air Traffic Management Research (SESAR) 729
N. Fota, M.H.C. Everdij, S.H. Stroeve, T. Kråkenes, I. Herrera, J. Quiñones, T. Contarino & A. Manzo

Civil engineering

Modification of response spectra by probabilistic approach 739
V. Salajka, J. Kala, Z. Cada & P. Hradil

Maritime transportation

Dynamic Positioning systems with emphasis on harsh climate conditions 743
T. Li, O.T. Gudmestad & A. Barabadi

Mechanical engineering

Wear time-dependent reliability analysis using Bayesian inference 751
J. Feng, J. Zhang, J. Si & P. Wang

Nuclear Engineering

RAVEN and dynamic probabilistic risk assessment: Software overview 759
A. Alfonsi, C. Rabiti, D. Mandelli, J. Cogliati, R. Kinoshita & A. Naviglio

Integrated Deterministic Probabilistic Safety Analysis (IDPSA) of a fire scenario 767
M. Kloos, J. Peschke & B. Forell

Dynamic reliability models for multiple dependent competing degradation processes 775
Y.H. Lin, Y.F. Li & E. Zio

Expert methods in system safety and reliability

Aeronautics and Aerospace

Development of a new algorithm for optimal multi-level redundancy allocation 785
M.A. Farsi

Aircraft crew escape system assistant 791
N. Grzesik & R. Czapla

A fuzzy system for evaluation of baggage screening devices at an airport 797
J. Skorupski & P. Uchroński

Energy production and distribution

Quantification and modelling of epistemic uncertainties for availability risk of future offshore wind farms using expert judgment 805
A. Zitrou, T. Bedford & L. Walls

Maritime transportation

Expert method and real time simulation in navigational safety analysis 813
T. Abramowicz-Gerigk

Mechanical engineering

Causal modeling in industrial Reliability and Maintenance Management 819
Y. Pang & G. Lodewijks

Other reliability and safety areas

The application of risk and reliability techniques to acquire knowledge in the development of expert system for fault diagnosis 825
E.M.P. Hidalgo & G.F.M. de Souza

Failure identification and degradation processes

Aeronautics and aerospace

Life and reliability evaluation of tuner by Constant-Stress Accelerated Degradation Testing method 837
F. Sun, X. Li & T. Jiang

Estimation of lifetimes of components that operate under ageing-attributable wearing conditions 843
H. Tomaszek, M. Zieja & M. Ważny

A Physics-of-Failure-based approach for failure behavior modeling: With a focus on failure collaborations 849
Z. Zeng, R. Kang & Y. Chen

Electrical engineering

Fault diagnosis method for circuit board based on BP neural networks 857
Y. Peng & J. Shi

Electronic industry

Physics of Failures (POF) version B for MTBF prediction 863
Y. Bot & J.B. Bernstein

An adaptive fault detection threshold hardware circuit design to reduce False Alarms 867
Y. Cui, J. Shi, L. Chen, K. Liu & W. An

Energy production and distribution

MUSTADEPT: A tool for the analysis of industrial equipment degradation 873
M. Compare, L. Legnani & E. Zio

Information technology and telecommunication

Provision of the reliable video surveillance services in heterogeneous networks 883
P. Lubkowski, D. Łaskowski & E. Pawlak

Maritime transportation

Identification of degradation processes of seabed protection in ports 889
T. Abramowicz-Gerigk

Mechanical engineering

The use of Self-Organizing Maps for diagnosing faults in motor bearings 895
S. Al-Dahidi

Selected safety aspects of polymer composites with natural fibres 903
A. Krzyżak & D. Vališ

Application of selected diffusion processes on system state assessment 911
D. Vališ & O. Pokora

Nuclear engineering

A modified Auto Associative Kernel Regression method for robust signal reconstruction in Nuclear Power Plant components 917
P. Baraldi, F. Di Maio, P. Turati & E. Zio

Experimental design for the evaluation of Critical Heat Flux of small-scale pressurized nuclear reactors 923
J.P. Duarte, J.R.C. Piqueira & M.E. Taqueda

Road transportation

The stochastic approach in road network vulnerability analysis 929
M. Bíl & R. Vodák

Analysis of brake testing methods in vehicle safety 933
A. Bojko, A.I. Fedotov, W.P. Khalezov & M. Młyńczak

Hilbert-Huang Transforms for fault detection and degradation assessment in electrical motors 939
M. Rigamonti & S. Rantala

Other reliability and safety areas

Volatility regime switching and jump-diffusion process for prognosis: Case of equity price modeling 945
H. Ghamlouch, M. Fouladirad & A. Grall

Performance evaluation of Emergency Response Plans using a Multi-State System approach 953
C. Girard, E. Piatyszek, P. David & J.-M. Flaus

Human factors and human reliability

Aeronautics and aerospace

The model of a pilot competency as a factor influencing the safety of air traffic 963
J. Skorupski & M. Wiktorowski

Human Dependability Model for space application—the HuDeM project 971
T.M. Stene, S.O. Johnsen & S. Ophof

Towards safer air traffic: Optimizing ATC controller workload by simulation with reduced set of parameters 979
B. Számel & G. Szabó

Human reliability test and identification of HCR model basic parameters for multi-factor "Meta-Operation" 989
Y. Yang, X. Chen, J. Zhang & R. Kang

Chemical process industry

Statistical analysis of past accidents and a methodology (MEDIA) for Human and Organizational Factors assessment in process industries 997
M. Ahmad, M. Pontiggia & M. Demichela

Predictive Human Error Analysis in Permit To Work system in a petrochemical plant 1007
M. Jahangiri, F. Zare Derisi & N. Hobobi

Critical infrastructure

Anticipating impacts of change on individual behaviors within a perspective of safety management 1011
T. Côte, E. Rigaud & E. Garbolino

Modeling and assessment of Performance Shaping Factors in construction 1019
Y. Xenidis & K. Giannaris

Energy production and distribution

The impact of the use of subcontracting on organizational reliability and safety 1027
C. Guers, C. Martin & J.L. Wybo

Human error analysis: Review of past accidents and implications for improving robustness of system design 1037
R. Moura, M. Beer, E. Patelli, J. Lewis & F. Knoll

Operational and organizational barriers as means of enhancing safety and learning 1047
T.J. Steiro, E. Hansson Blix, J. Seljelid, T.S. Johansen, R.J. Bye, H.N. Hansen & A. Doumit

Natural resources and environment

Presumptions of culture: Applications and safety implications 1057
F. Størseth

Nuclear engineering

Coding scheme to measure the operator's workload in advanced Main Control Room 1065
S. Kim, Y. Kim & W. Jung

A survey of Bayesian Belief Network Applications in Human Reliability Analysis 1073
L. Mkrtchyan, L. Podofillini & V.N. Dang

Aggregating expert-elicited error probabilities to build HRA models 1083
L. Podofillini, L. Mkrtchyan & V.N. Dang

Other reliability and safety areas

Organizational factor inclusion in Human Reliability Analysis (HRA) tools 1093
N. Balfe & S. Cromie

Design methods of reducing human error in practice 1101
M. Butlewski, M. Jasiulewicz-Kaczmarek, A. Misztal & M. Sławińska

Maintenance modelling and optimisation

Chemical process industry

A hierarchical framework for the measurement of maintenance efficacy and efficiency using performance indicators 1109
G.M. Galante, R. Inghilleri & C.M. La Fata

Civil engineering

State of the art in Operation and Maintenance planning of offshore wind farms 1119
M. Asgarpour & J.D. Sørensen

Critical infrastructure

Maintenance of power systems considering time-dependent uncertainty 1127
T. Iesmantas & R. Alzbutas

Energy production and distribution

Decision-making support for maintenance optimisation of natural gas compressor stations 1133
J. Blondel, L. Marle, O. Mozar, A. Abdesselam & F. Brissaud

Optimization of maintenance and operational policies of an offshore wind farm subject to stochastic wind conditions 1141
B. Castanier, C. Pehlivan & T.G. Yeung

An age-based preventive maintenance for offshore wind turbines 1147
F.P. Santos, A.P. Teixeira & C. Guedes Soares

Availability modelling and analysis of an offshore wind turbine using Extended Coloured Stochastic Petri Nets 1157
P. Zeiler & B. Bertsche

Manufacturing and supply chain/logistic systems

Maintenance in availability of weapon systems under combat operation—optimization possibilities 1167
T. Smal

Maritime transportation

Optimum CTV fleet selection for offshore wind farm O&M activities 1177
Y. Dalgic, I. Dinwoodie, I. Lazakis, D. McMillan & M. Revie

Mechanical engineering

Practical aspects of the application of RCM to select optimal maintenance policy of the production line 1187
M. Jasiulewicz-Kaczmarek

Hidden Markov Models for diagnostics and prognostics of systems under multiple deterioration modes 1197
T.T. Le, F. Chatelain & C. Bérenguer

Nuclear engineering

Application of the Maintenance Rule to Nuclear Power Plant systems through Bayesian Networks 1205
D.P. Dionizio, P.L.C. Saldanha & P.F. Frutuoso e Melo

Experience on risk-informed approach to Allowed Outage Time changes due planned maintenance 1211
P.L.C. Saldanha & P.F. Frutuoso e Melo

Rail transportation

Expert system for means of transport maintenance processes performance. A comparative analysis for various types of rail vehicles 1217
T. Nowakowski & S. Werbińska-Wojciechowska

A Colored Petri Net model for railway track maintenance with two-level inspection 1227
H. Shang & C. Bérenguer

Analysis of the process of unloading containers at the inland container terminal 1237
M. Zając & J. Świeboda

Return logistics/waste management

Reliability based model of the cost effective product reusing policy 1243
A. Jodejko-Pietruczuk & M. Plewa

Other reliability and safety areas

Asset maintenance optimization: The case-study of an offshore wind farm 1249
Y. Bot & D. Azoulay

Maintenance planning for drum shearer machine based on its reliability characteristics and economical sensitivity analysis 1257
S.H. Hoseinie, B. Ghodrati & U. Kumar

A guide for Block Inspection Policy implementation 1263
A. Jodejko-Pietruczuk & S. Werbińska-Wojciechowska

Availability model of technical objects—block inspection policy implementation 1275
A. Jodejko-Pietruczuk & S. Werbińska-Wojciechowska

Condition-based maintenance policies for multi-component systems with Lévy copulas dependence 1281
H. Li, L. Dieulle & E. Deloux

Application of standards in reliability prognosis of braking system of moving walks 1289
E. Rogova, G. Lodewijks & Y. Pang

Occupational safety

Electrical engineering

A Bayesian population variability analysis for estimation of the work time loss distributions due to occupational accidents 1301
M.C. Moura, R. Azevedo, E.L. Droguett, L. Rego, W. Jorge & R. Vilela

Manufacturing and supply chain/logistic systems

Continuous monitoring of at-risk behaviours: A risk-based statistical control method 1311
D. Masi & P. Trucco

Enhancing the implementation of Occupational Health and Safety interventions through a design of the socio-technical interaction 1319
D. Masi, E. Cagno, P. Hasle & S. Farnè

Return logistics/waste management

A risk-based approach to manage the Occupational Hazards in the Arctic drilling waste handling practices 1329
Y.Z. Ayele, A. Barabadi & J. Barabady

Other reliability and safety areas

Estimating individual occupational risk using registration data 1335
P.H.G. Berkhout & M. Damen

Quantification of risk rates of occupational accidents 1345
I.A. Papazoglou, O. Aneziris, L.J. Bellamy, M. Damen, B.J.M. Ale, H.J. Manuel & J.I.H. Oh

Quantitative risk assessment

Aeronautics and aerospace

Reliability assessment method for Ion thruster based on competing failure analysis and performance degradation data 1357
Z. Zheng, S. Dong, L. Zhang, D. Xu, H. Tian & T. Zhang

Chemical process industry

Comparison of risk profiles for chemical process plants using PLATYPUS 1363
C. van Gulijk, B.J.M. Ale, D. Ababei & M. Steenhoek

The use of the combination of indexing and semi-quantitative methods in audits for individual risk assessment in the field of fire and explosion protection 1369
A. Leksin, U. Barth, D. Adeulov & R. Mock

Estimation of the impact probability of fragments produced by explosions of vessels: A case study 1377
M.F. Milazzo, R. Lisi, G. Consolo & G. Maschio

Dynamic risk assessment: Development of a basic structure 1385
N. Paltrinieri & P. Hokstad

Joint applicability test of software for laboratory assessment and risk analysis 1393
D.N. Pluess, Th. Meyer, J. Mašin, P. Mikulášek & M. Ferjenčik

Is a QRA-based method suitable to guide Land Use Planning decisions in India? 1401
A. Sengupta, D. Bandyopadhyay, C.J. van Westen & A. van der Veen

Civil engineering

The effect of maintenance on inflation correction in Dutch PPP projects 1411
D.S. Vervoort

Handling dependencies in Probabilistic Risk Assessments using Evidential Networks 1421
D. Wang, Z.J. Cheng, P. Jiang & B. Guo

Critical infrastructure

The use of geoevents in the risk management of Wastewater Treatments 1431
G. Ancione, M.F. Milazzo & G. Maschio

Utilizing knowledge-to-number-processes in smaller and less resource intensive risk assessments 1439
T. Askeland & R. Flage

Risk assessment of ground water sources for emergency supply 1447
F. Bozek, L. Jesonkova, A. Pawelczyk, Z. Malek & J. Dvorak

Study of volcanic Na-Tech risks in primary Waste Water Treatments 1453
M.F. Milazzo, G. Ancione, E. Salzano & G. Maschio

Optimum concept of management and trade-off with risks 1463
D. Prochazkova

Possibilistic risk analysis of failure in water supply network 1473
B. Tchórzewska-Cieślak, K. Boryczko & I. Piegdoń

Electrical engineering

Multidimensional risk to networks of distributed systems 1481
T.V. Garcez & A.T. de Almeida

Mathematics of PRA applied to Distributed Generation curtailment in saturated grids 1489
P.E. Labeau, F. Faghihi, J.C. Maun, V. De Wilde & A. Vergnol

Energy production and distribution

Priorities assignment for actions in a pipeline: A decision model to evaluate multiple objectives 1497
M.H. Alencar, M.F. Marsaro & A.T. de Almeida

Risk assessment in heat supply system 1501
B. Babiarz

Vulnerability of Energy Infrastructure to intentional attacks—the interplay of resource, conflict and security 1507
P. Burgherr, J. Giroux & M. Spada

Solar storm impact on critical infrastructure 1515
O. Sokolova, P. Burgherr & W. Collenberg

Accident risk assessment for deep geothermal energy systems 1523
M. Spada, E. Sutra, S. Wolf & P. Burgherr

Information technology and telecommunication

Enhancement of IT Risk Assessments by UML 1531
R. Mock, B. Truninger, P. Brunner & T. Hruz

Maritime transportation

Quantitative risk assessment of new ship designs in damage conditions 1539
M.K. Gerigk

Review of risk concepts and perspectives in risk assessment of maritime transportation 1547
F. Goerlandt & J. Montewka

Risk based assessment on increased gas safe machinery spaces of liquefied natural gas fuelled ship 1555
X.J. Li & R.P. Zhou

Semi-qualitative method for ship collision risk assessment 1563
W. Zhang, J. Montewka & F. Goerlandt

Mechanical engineering

RAPP method: Failure analysis and risk determination in automobile fleets within the case study electric actuator 1573
S. Bracke & S. Sochacki

Natural resources and environment

Composite methodology for tsunami vulnerability assessment based on the numerical simulation of 1755 Lisbon tsunami—application on two Portuguese coastal areas 1581
J.L. Barros, A. Emídio, A. Santos & A.O. Tavares

Monte Carlo simulation and Bayesian Evidence Synthesis 1589
U. Sahlin & Y. Jiang

Nuclear engineering

Amendments of the existing guidance on PSA application to nuclear power plants in Germany 1599
H.P. Berg, M. Krauß & M. Röwekamp

Focus areas for a Level 2 PSA that supports a site NPP risk analysis 1605
D.M. Helton, M. Zavisca & M. Khatib-Rahbar

A PSA Level-1 method with repairable components: An application to ASTRID Decay Heat Removal systems 1611
R. Kumar, S. Bechta, P. Kudinov, F. Curnier, M. Marquès & F. Bertrand

Effect of human factor in the analysis of changes to Limiting Conditions for Operation (LCO) applied to Residual Heat Removal System 1619
S. Martorell, I. Martón, P. Martorell & M. Saiz

Application of PSA for design optimization of VVER 440/213 1629
P. Picca, F. Pierro, M. Giovannini, J. Cech, P. Baumeister & J. Prochaska

Rail transportation

Deriving a distribution for accident severity from an F-N curve 1635
J. Braband & H. Schäbe

Geospatial modelling of rail safety hazards 1639
D.J.K. Griffin

Comparing the two methods for judging changes in European railways and in European nuclear safety 1649
N. Petrek & H.P. Berg

Road transportation

Combination of technological and economical risk assessment using the Monte-Carlo-Simulation 1655
F. Plinke, D. Althaus, A. Braasch & A. Meyna

The results of a systematic study of the risks associated with the transportation of hazardous substances 1663
D. Prochazkova, J. Prochazka & H. Patakova

Preference risk assessment of hazardous substances road transportation 1671
D. Rehak, A. Bernatik & P. Novotny

Other reliability and safety areas

Quantifying MSD risks through Job Hazard Analysis 1677
L. Dement

Handling epistemic uncertainty in the Fault Tree Analysis using interval-valued expert information 1683
M. Francese, G.M. Galante, C.M. La Fata & G. Passannanti

Expressing and communicating uncertainty and bias in relation to Quantitative Risk Analysis 1691
F. Goerlandt & J. Montewka

Safety analysis and CFD dispersion simulation of cryogenic release in a deep underground large scale cryogenic installation 1701
E.C. Marcoulaki, A.G. Venetsanos, M. Konstandinidou & I.A. Papazoglou

Reliability and safety based system design

Aeronautics and aerospace

European survey on safety methods application in aeronautic systems engineering 1711
A. Berres, H. Schumann & H. Spangenberg

Semi-formal static and dynamic modeling and categorization of airport checkpoints 1721
P. Renger, U. Siebold, R. Kaufmann & I. Häring

Chemical process industry

Achieving safe designs through evaluation of options at the conceptual level of safety system design 1733
E. Alijagic & V.N. Dang

Civil engineering

Conventional correlation factors in the safety analysis of stochastic systems 1741
O. Lukoševičienė & A. Kudzys

Safety-based approach in multifunctional building design 1749
A. Taraszkiewicz & M.K. Gerigk

Electrical engineering

Management of controls of fire protection systems in Switzerland 1755
E. Nachtigall & S. Metzger

Electronic components with time-dependent failure rates—reasons, values and consequences 1761
P. Zeiler, O. Koller & B. Bertsche

Electronic industry

Availability and reliability evaluation of systems periodically maintained 1771
N. Hu, J. Huang, Ch. Yang, Y. Zheng & O. Dong

Maritime transportation

Reliability and safety based design of lifesaving appliances systems 1777
Z. Burciu

Nuclear engineering

Nuclear power plant safety improvement with new system for safety injection 1783
B. Gjorgiev & A. Volkanovski

Rail transportation

A systematic approach for defense against transient failures 1791
H. Schäbe & I. Shubinski

Reliability allocation for a system with complex redundancy 1797
Z. Vintr & T. Vintr

Other reliability and safety areas

Effective searching process used in obtaining Pareto solutions of two-objective network design problem 1801
N. Takahashi, H. Yamamoto, T. Akiba & K. Shingyochi

Reliability and safety data collection and analysis

Aeronautics and aerospace

SYMBAD—Artificial Neural Networks in furtherance of managing aircraft testing 1811
W. Kosiński, J. Wójcik & M. Zieja

Accelerated Life Test method for satellite electronic instrument 1817
D. Shu, Z. Liang, Z. Zhiteng & M. Haibo

Reliability of the airlines operations system 1823
A. Słodownik & J. Żurek

Quantitative evaluation on storage reliability of pyrotechnics based on thermodynamic characteristic of dynamite and performance degradation data 1829
Z. Wan, W. Hang & C. Hai Long

Agriculture and food industry

Telematics used in the campaigns machinery safety management systems 1833
J. Napiórkowski, P. Szczyglak & K. Kołakowski

Chemical process industry

Collection and analysis of failure data for pressure equipment 1841
P.A. Bragatto, S. Ansaldi, C. Delle Site & P. Agnello

Reliability analysis of prototypes based on small and heterogeneous test data volumes. Case study: Organic fibre prototype analysis 1849
A. Lücker, M. Hinz, S. Bracke & G. Knübel

How to present and understand uncertainty of production assurance analyses with respect to data quality 1857
C. Persskog-Lundtofte, S. Isaksen & L.M. Pedersen

Critical infrastructure

Universal method of battery life prediction 1865
Y. Hanyu, T. Yamamoto, T. Ezawa & A. Itakura

Electronic industry

Reliability prediction of electronic boards by analyzing field return data 1871
S.V. Comert, H. Yadavari, M. Altun & E.N. Erturk

Energy production and distribution

A double-loop Monte Carlo approach for Part Life Data Base reconstruction and scheduled maintenance improvement 1877
F. Di Maio, M. Compare, S. Mattafirri & E. Zio

Using field experience in the treatment of Common Cause Failures in reliability assessment 1885
S. Hauge, S. Håbrekke & M.A. Lundteigen

A geometric test for the analysis of contingency tables 1895
J. Quigley & K.J. Wilson

Assessment of a remaining working life of energetic devices using service data 1903
M. Sykora, M. Holicky, J. Marková & K. Presl

Information technology and telecommunication

Model for Information Quality determination of teleinformation systems of transport 1909
M. Stawowy

Manufacturing and supply chain/logistic systems

A framework proposal to analyse the performance of assets under complex system 1915
T. Grubessich, E. Johns, P. Viveros, R. Stegmaier & F. Kristjanpoller

Proven in use in the machine tool industry for demonstrating the quantitative functional safety according to EN ISO 13849-1 1925
B. Günnel, A. Meyna, M. Schlummer, H. Mödden & A. Broos

Mechanical engineering

Probabilities in safety of machinery—Part 1: Risk profiling and farmer matrix 1933
A. Bornemann, Y. Froese, L. Landi & H. Mödden

Probabilities in safety of machinery—Part 2: Theoretical and practical design 1943
A. Bornemann, Y. Froese, L. Landi & H. Mödden

Research on reliability qualification test design by considering inheritance factor 1951
Y. Wang, D. Xu & L. Liu

Optimal design on Accelerated Degradation Testing with Gamma process for reliability demonstration 1957
C. Zhang, X. Lu, X. Chen & Y. Wang

Road transportation

One producer, two brands: A comparison of car operating conditions 1965
M. Jadwinska, T. Siekierka & M. Zając

Waterborne transportation

Ship voyage characteristics in Wuhan Yangtze River Bridge waterway 1969
Y.-P. Zhou, L.-Z. Sang, Z. Mao & Q. Wu

Other reliability and safety areas

Fleet-level reliability estimation of repairable units 1977
A.H.S. Garmabaki, A. Ahmadi & J. Block

Reliability and safety education and training

Nuclear engineering

Learning from failures: The case of Deepwater Horizon disaster 1985
A.W. Labib

The representation of nuclear power in cinema: The contribution of a filmic analysis to understanding the public debate 1993
A. Portelli, C. Martin & F. Guarnieri

Road transportation

On designing educational aids for users' safety in road tunnels 2001
K. Chatzoglou, E. Rokou, I.P. Tatsiopoulos & K. Kirytopoulos

Other reliability and safety areas

Public buildings safety: Addressing a pilot evacuation exercise 2009
A. Santos & M. Queirós

Simulation methods in system safety and reliability

Aeronautics and aerospace

A safety analysis via minimal path sets detection for object-oriented models 2019
C. Schallert

The use of on-board flight recorder in the modeling process of aircraft landing operations 2029
P. Stańczyk & A. Stelmach

Reliability analysis for Runway Overrun using subset simulation 2035
K. Zwirglmaier, L. Drees, F. Holzapfel & D. Straub

Chemical process industry

A meta model framework for risk analysis, diagnosis and simulation 2043
H. Kanj & J.-M. Flaus

Critical infrastructure

Proposing a multi-layer modeling framework for complex infrastructure systems 2051
C. Nan & G. Sansavini

Hybrid modeling and simulation approach selection to the reliability and vulnerability analysis of Critical Infrastructures 2059
G. Sansavini, C. Nan & W. Kröger

Energy production and distribution

Time dependent gas transmission network probabilistic simulator: Focus on storage discharge modeling 2069
V. Kopustinskas & P. Praks

Information technology and telecommunication

Weekly availability changes of web applications implemented in virtualized environment 2077
T. Walkowiak

Manufacturing and supply chain/logistic systems

Dynamic approach to modeling MTBF/MTTR in industrial and logistics systems 2085
P. Hoffa & P. Pawlewski

Maritime transportation

A new Monte Carlo method for environmental contour estimation 2091
A.B. Huseby, E. Vanem & B. Natvig

On multistate technical system operation process influence on its reliability 2099
K. Kołowrocki, E. Kuligowska & J. Soszyńska-Budny

Mechanical engineering

Uncertainty improving in importance sampling: An integrated approach with fuzzy-cluster sampling 2107
M. Nadjafi, M.A. Farsi & A. Najafi

Medicine and health service

Conversion of a based risk model into a simulation model for simulation and analysis 2113
K. Negrichi, J.-M. Flaus & M. Di Mascolo

Nuclear engineering

Common cause failures modelling by means of Coloured Petri Nets for dependability assessment of a control system of nuclear power plant 2121
N. Brînzei, G. Deleuze, N. Villaume & J.F. Pétin

Propagation of aleatory and epistemic uncertainties in quantification of systems failure probabilities or safety margins 2131
M. Marquès

Road transportation

Safe level of redundancy in Discrete Transportation Systems 2141
D. Caban & T. Walkowiak

Using Petri-Net analysis for advanced reliability analysis of polymer electrolyte membrane fuel cells 2147
M. Whiteley, J. Leigh, A. Fly, L.M. Jackson & S.J. Dunnett

Waterborne transportation

Analysis of ship navigation behaviors in the Wuhan Yangtze River Bridge waterway 2155
X. Chen, L.-Z. Sang, Z. Mao & Q. Wu

Other reliability and safety areas

A novel methodology for availability assessment of complex load sharing systems 2161
F. Kristjanpoller, P. Viveros, A. Crespo, R. Mena & R. Stegmaier

Structural reliability and safety

Aeronautics and aerospace

Life distribution and P-S-N curve analysis of TC21 titanium alloy joint with Electron Beam Welding in ultra-high cycle fatigue regime 2169
Z. Zhiteng, D. Shu, Z. Liang & X. Danjun

Civil engineering

Optimal design of ground-mounted solar systems 2175
R. Boccara, D. Diamantidis & M. Sykora

Approximate quantification of the robustness index of concrete beams subjected to deterioration 2183
W. Botte, R. Caspeele & L. Taerwe

A condition-based deterioration model for the crack propagation in a submerged concrete structure 2193
B. El Hajj, F. Schoefs, B. Castanier & T. Yeung

Reliability assessment of cast-iron heritage structures 2201
J. Marková, M. Holicky, K. Jung, A. Podstawka & V. Bures

Reliability of structures in national codes to Eurocodes 2207
J. Marková & M. Holicky

On climatic actions combinations for probabilistic calibrations 2213
Z. Sadovský

In-plane buckling behaviors of shear-deformable columns with variable cross sections 2219
L. Su & M.M. Attard

Lateral buckling of varying arbitrary cross-section beams with shear effects 2227
L. Su & M.M. Attard

Methodology for the quantitative risk assessment of road bridges exposed to accidental events 2235
M. Sykora, M. Holicky & P. Maňas

Point estimate of dynamic reliability considering parameter uncertainties 2241
Y.G. Zhao & Z.H. Lu

Critical infrastructure

The reliability analysis of welded tanks for oil storage 2249
Z. Kala

Mechanical engineering

Determination of design load for a pile-guide system for large floating installations considering Life-Cycle Cost and probabilistic load distribution 2255
S.-Y. Lee, C. Jo, P. Bergan, D. Chang & B. Pettersen

Road transportation

Analysis of reliability and retaining levels of safety barriers 2261
K. Jung & J. Marková

Other reliability and safety areas

Safe reliability assessment through probabilistic constraint reasoning 2269
E. Carvalho, J. Cruz & P. Barahona

Structural reliability for containment of VVER 440/213 type 2279
J. Králik, P. Picca, F. Pierro, M. Giovannini, N. Zaccari & P. Baumeister

Reliability updating based on monitoring of structural response parameters 2287
B.J. Leira

Uncertainty and sensitivity analysis

Chemical process industry

Comparative analysis of rapid calculation methods for physical explosions of pressure vessels 2299
R. Bubbico & B. Mazzarotta

A study of determination of the design accidental fire load based on the quantitative Fire Risk Assessment with the treatment of uncertainty 2309
B. Chu & D. Chang

Civil engineering

Sobol's sensitivity analysis of stability problems of steel beams 2315
Z. Kala & J. Kala

Energy production and distribution

Quantitative vs. qualitative treatment of uncertain assumptions in risk assessment 2321
C. Berner & R. Flage

Information technology and telecommunication

Comparison of uncertainty models of impact of teleinformation devices reliability on information quality 2329
M. Stawowy

Nuclear engineering

Sensitivity analysis of geological parameters having impact on nuclear waste deep geological repository safety 2335
J. Chudoba

Processes reliability and safety modelling

Aeronautics and Aerospace

An impact of the operators and passengers behavior on the airport's security screening reliability 2345
A. Kierzkowski & T. Kisiel

Risk analysis of the point on aging aircraft structure 2355
M. Woch

Chemical process industry

Risk assessment of a bulk cryogenic tank: Beyond the Leak-Before-Break criterion 2361
M. Compare, L. Legnani, M. Buldrini, G. Sansavini, E. Zio & L. Beretta

Civil engineering

Modeling of a degradation path set with a Gamma process mixture—application to a maintenance decision rule 2369
E. Grall-Maës, A. Grall & P. Beauseroy

Reliability of the delivery in the last 100 meters 2377
K. Lewandowski

Manufacturing and supply chain/logistic systems

Risk analytics within high-precision dental tool manufacturing: Multidimensional failure probabilities and validation 2387
S. Bracke & M. Pospiech

A unified model of systems dependability and process continuity for complex supply chains 2395
L.A. Bukowski & J. Feliks

Using quantitative stochastic model checking tool to increase safety and improve efficiency in production processes 2405
L. Herbert, Z.N.L. Hansen & P. Jacobsen

Research on information system and its impact on distribution process of supply chain 2417
E. Pawlak

Availability and reliability of resources in an agile manufacturing systems 2425
A. Stachowiak

Rail transportation

Initial FMEA analysis of the container transport chain 2433
M. Zając & J. Świeboda

Other reliability and safety areas

On prudent activities in a complex system 2439
I. Årstad & T. Aven

Parallel computing for system availability and applications 2447
R. Briš & S. Domesová

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Preface

Within last fifty years the performance requirements for technical objects and systems were supplemented with: customer expectations (quality), abilities to prevent the loss of the object properties in operation time (reliability and maintainability), protection against the effects of undesirable events (safety and security) and the ability to restore performance (resilience). The high regard that firms and researchers are paying to risk, safety and dependability is probably caused by the intensity of catastrophes that seem to have increased on a global scale. To the most publicized disruptions belong: the terrorist attacks on the World Trade Center on September 11, 2001, the SARS epidemic in South-East Asia in 2003, the natural disaster of Hurricane Katrina in 2005 and Fukushima nuclear power plant disaster in 2011. Thus, the need to adapt the operation of complex systems in such an uncertain and volatile environment has caused the need to formulate new and well established achievements associated with modeling, testing and evaluation of the reliability and maintainability, safety and security, vulnerability and resilience. The concept of a complex system applies not only to the technical systems but also the infrastructure of major importance for social life such as transport and logistics infrastructure, buildings, power systems, water distribution systems or health service. The problem applies to the entire lifetime of the system from the design phase through manufacturing, execution, operations, maintenance and renovation until decommissioning decision. We hope the ESREL 2014 conference will provide an valuable platform for presenting and discussing developments and applications related to indicated problems.

ESREL is a series of annual conferences promoted by the European Safety and Reliability Association ESRA, which dates back to 1989 (in La Baule, France), but was not referred to as an ESREL conference before 1992 (in Lyngby, Denmark). The Conference has become well established in the international community, attracting a good mix of academics and industry participants that present and discuss subjects of interest and application across various industries in the fields of Safety and Reliability. This is the 24th edition of its annual conference that takes place in various countries in Europe. Till now it was organized in: ‘13 Nederland, ‘12 Finland, ‘11 France, ‘10 Greece, ‘09 Czech Republic, ‘08 Spain, ‘07 Norway, ‘06 Portugal, ‘05 Poland, ‘04 Germany, ‘03 Netherlands, ‘02 France, ‘01 Italy, ‘00 United Kingdom, ‘99 Germany, ‘98 Norway, ‘97 Portugal, ‘96 Greece, ‘95 United Kingdom, ‘94 France, ‘93 Germany, ‘92 Denmark, ‘ 91 United Kingdom.

This book contains the proceedings of the ESREL 2014 Conference, held in Wroclaw, Poland and organized by the Wroclaw University of Technology, the Polish Safety and Reliability Association (PSRA) and the European Safety and Reliability Association (ESRA). Originally, approximately 650 abstracts were submitted and following the review by the Technical Programme Committee about 320 full papers in 17 methodological tracks were accepted and are included in the program. The review process was mainly organised by the Technical Area Coordinators and the process was made by a large number of reviewers, which are gratefully acknowledged for their contributions to the improvement of quality of the papers. The review process is an important aspect of the Conference and contributes to the fact that this series of Conferences has been included for the last several years in the ISI citation index, which—at least to academics—is an important feature. This book contains the extended abstracts and a CD with the full electronic text of the papers presented at the ESREL 2014 Conference.

We wish you an interesting and useful reading.

Tomasz Nowakowski
Conference General Chair

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Acknowledgements

The conference is organized jointly by Wroclaw University of Technology, Polish Safety and Reliability Association (PSRA) and European Safety and Reliability Association (ESRA). The Editors would like to thank the many contributors for their active participation, which made the organisation of ESREL 2014 possible.

The joint work of the Technical Area Coordinators, the peers involved in the Technical Programme Committee, the reviewers and the organisers of special sessions have resulted in a number of very interesting meetings. Thanks to all the contributors for the participation and effort in the technical programme setting.

Special thanks are sent to honorary patrons of the Conference: prof. Tadeusz Wieckowski, Ph.D., D.Sc. Rector of Wroclaw University of Technology and Rafał Dutkiewicz, Ph.D. President of Wrocław

We would like to acknowledge specially the conference secretariat, all the administrative and technical support at the Wroclaw University of Technology and the local organising committee. We pass special expressions of gratitude to the website administrators. Their many hours of work are greatly appreciated.

Finally the editors would like to thank the authors, session chairs and conference participants without whom there would not have been any conference.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Conference organization

CONFERENCE GENERAL CHAIR

Tomasz Nowakowski, *Wroclaw University of Technology, Poland*

CONFERENCE GENERAL CO-CHAIRMEN

Enrico Zio, *European Safety and Reliability Association, Italy*
Krzysztof Kołowrocki, *Polish Safety and Reliability Association, Poland*

TECHNICAL PROGRAMME COMMITTEE

Chairman

Marek Młyńczak, *Wroclaw University of Technology, Poland*

Co-Chairmen

Piero Baraldi, *Politecnico di Milano, Italy*
Anna Jodejko-Pietruczuk, *Wroclaw University of Technology, Poland*
Sylwia Werbińska-Wojciechowska, *Wroclaw University of Technology, Poland*

TECHNICAL AREA COORDINATORS

Tim Bedford, *University of Strathclyde, UK*
Christophe Berenguer, *GIPSA-Lab—Grenoble Institute of Technology & CNRS, France*
Emanuele Borgonovo, *Bocconi University, Italy*
Marko Cepin, *University of Ljubljana, Slovenia*
Mohamed Eid, *Commisariat à l'ENergie Atomique et aux Energie, Alternatives, France*
Kazimierz Jamroz, *Gdansk University of Technology, Poland*
Krzysztof Kołowrocki, *Gdynia Maritime University, Poland*
Kazimierz Kosmowski, *Gdansk University of Technology, Poland*
Cezary Madryas, *Wroclaw University of Technology, Poland*
Marek Młyńczak, *Wroclaw University of Technology, Poland*
Tomasz Nowakowski, *Wroclaw University of Technology, Poland*
Daniel Podgórski, *Central Institute for Labour Protection—National Research Institute, Poland*
Luca Podofillini, *Paul Scherrer Institute, Switzerland*
Leszek Smolarek, *Gdynia Maritime University, Poland*
Joanna Soszyńska-Budny, *Gdynia Maritime University, Poland*
Lesley Walls, *University of Strathclyde, UK*
David Valis, *University of Defence, Czech Republic*
Sylwia Werbińska-Wojciechowska, *Wroclaw University of Technology, Poland*
Mateusz Zając, *Wroclaw University of Technology, Poland*
Mariusz Zieja, *Air Force Institute of Technology, Poland*

TECHNICAL PROGRAMME COMMITTEE

Teresa Abramowicz-Gerigk, *Poland*
Mehmood Ahmad, *Italy*
Kerem Akartunali, *UK*
Sameer Al-Dahidi, *Italy*
Adiel Almeida, *Brazil*
Mustafa Altun, *Turkey*
Robertas Alzbutas, *Lithuania*
John Andrews, *UK*
Terje Aven, *Norway*
Morteza Bagherpour, *Iran*
Anne Barros, *Portugal*
Christophe Berenguer, *France*
Peter Berg, *Germany*
Emanuele Borgonovo, *Italy*
Deshai Botheju, *Norway*
Stefan Bracke, *Germany*
Nicalae Brinzei, *France*
Radim Bris, *Czech Republic*
Florent Brissaud, *France*
Zbigniew Burciu, *Poland*
Peter Burgherr, *Switzerland*
Eduardo Calixto, *UK*
Bruno Castanier, *France*
Marko Cepin, *Slovakia*
Alaa Chateauneuf, *France*
Michal Choras, *Poland*
Michele Compare, *Italy*
Roger Cooke, *The Netherlands*
Alfredo Crespo Marquez, *Spain*
Micaela Demichela, *Italy*
Damian Derlukiewicz, *Poland*
Laurence Dieulle, *France*
Mohamed Eid, *France*
Sridevi Emayavaramban, *India*
Mohammad Ali Farsi, *Iran*
Roger Flage, *Norway*
Jean-Marie Flaus, *France*
Knut Fossum, *Norway*
Pavel Fuchs, *Czech Republic*
Thalles v Garcez, *Brazil*
Jim Gaw, *UK*
Miroslaw Gerigk, *Poland*
Adrian Goossens, *The Netherlands*
Antoine Grall, *France*
Justyna Hachoł, *Poland*
Bernhard M. Haemmerli, *Switzerland*
Anca Hanea, *The Netherlands*
Henrik Hassel, *Sweden*
Ivonne Herrera, *Norway*
Mohamed Hibti, *France*
Kai Hofig, *Germany*
Seyed Hadi Hoseinie, *Sweden*
Tomas Iesmantas, *Lithuania*
Benoit Iung, *France*
Lisa M. Jackson, *UK*
Kazimierz Jamroz, *Poland*
Tim Jefferis, *UK*
Stig O. Johnsen, *Norway*
Ireneusz Jóźwiak, *Poland*
Zdenek Kala, *Czech Republic*
Jiri Kala, *Czech Republic*
Jan Kamenicky, *Czech Republic*
Artur Kierzkowski, *Poland*
Seunghwan Kim, *Republic of Korea*
Krzysztof Kołowrocki, *Poland*
Vytis Kopustinskas, *Italy*
Henrik Kortner, *Norway*
Kazimiesz T. Kosmowski, *Poland*
Pierre-Etienne Labeau, *Belgium*
Yves Langeron, *France*
Andre Lannoy, *France*
Eva Lantsoght, *Ecuador*
Bernt Leira, *Norway*
Krzysztof Lewandowski, *Poland*
Peng-Chu Lin, *Taiwan*
Mary Ann Lundteigen, *Norway*
Jan Magott, *Poland*
Jacek Malinowski, *Poland*
Effie Marcoulaki, *Greece*
Jana Markova, *Czech Republic*
Arsham Mazaheri, *Finland*
Maria Francesca Milazzo, *Italy*
Marek Młyńczak, *Poland*
Ralf Mock, *Switzerland*
Heinrich Moedden, *Germany*
Jakub Montewka, *Finland*
Marcio Moura, *Brazil*
Cen Nan, *Switzerland*
Agata Niewczas, *Poland*
Tomasz Nowakowski, *Poland*
Herry Nugraha, *Indonesia*
Ondrej Nyvlt, *Czech Republic*
Eivind Okstad, *Norway*
Christian Paroissin, *France*
Mahdi Parsa, *UK*
Paweł Pawlewski, *Poland*
Francois Peres, *France*
Daniel Pieniak, *Poland*
Katarzyna Pietrucha-Urbanik, *Poland*
Marcin Plewa, *Poland*
Luca Podofillini, *Switzerland*
Erick Portugal Hidalgo, *Brazil*
Darren Prescott, *UK*
Dana Prochazkova, *Czech Republic*
Dirk Proske, *Republic of Austria*
Nagarajan Raghavan, *Singapore*
Matthew Revie, *UK*
Elena Rogova, *The Netherlands*
Vittorio Rosato, *Italy*
Anglea Santos, *Portugal*
Philip Scarf, *UK*
Hartmut Schmaltz, *Germany*

Maria Segovia-Garcia, *UK*
Mahmood Shafiee, *UK*
Jacek Skorupski, *Poland*
Tomasz Smal, *Poland*
Joanna Soszyńska-Budny, *Poland*
Agnieszka Stachowiak, *Poland*
Trine Marie Stene, *Norway*
Zhiqiang Sun, *China*
Miroslav Sykora, *Czech Republic*
Christian Tanguy, *France*
Brabara Tchórzewska-Cieślak, *Poland*
Paolo Trucco, *Italy*
Agnieszka Tubis, *Poland*
David Valis, *Czech Republic*
Pieter Van Gelder, *The Netherlands*
Coen van Gulijk, *The Netherlands*
Jorn Vatn, *Norway*
Michal Vintr, *Czech Republic*
Zdenek Vintr, *Czech Republic*
Sylwia Werbińska-Wojciechowska, *Poland*
Kevin Wilson, *UK*
Yiannis Xenidis, *Greece*
Mateusz Zając, *Poland*
Jaroslav Zajicek, *US*
Zhiguo Zeng, *China*
Mariusz Zieja, *Poland*
Anette Zijderveld, *The Netherlands*
Izabela Zimoch, *Poland*
Enrico Zio, *Italy*
Athena Zitrou, *UK*
Mariusz Żółtowski, *Poland*

LOCAL ORGANIZATION COMMITTEE

Chair

Anna Jodejko-Pietruczuk, *Wroclaw University of Technology, Poland*

Co-Chairmen

Joanna Soszyńska-Budny, *Gdynia Maritime University, Poland*
Franciszek Restel, *Wroclaw University of Technology, Poland*

Members

Krzysztof Bojda
Maciej Chlebus
Piotr Czaja
Izabela Dziaduch
Weronika Huss
Artur Kierzkowski
Tomasz Kisiel
Władysław Kluczkiewicz
Bogumiła Koziar
Mirosław Kwaśniak
Stanisław Kwaśniowski
Krzysztof Lewandowski
Kazimierz Pabisiak
Marcin Plewa
Tomasz Siwulski
Wiktor Stefurak
Sylwia Werbińska–Wojciechowska
Mateusz Zając

Website Administration

Krzysztof Bojda

Organized by

Wroclaw University of Technology, Poland
European Safety and Reliability Association—ESRA
Polish Safety and Reliability Association—PSRA

With the support of the technical and administrative services of Wroclaw University of Technology

Honorary Patronages by
Tadeusz Więckowski, Rector of Wroclaw University of Technology, Poland
Rafał Dutkiewicz, President of Wroclaw, Poland

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Introduction

The *ESREL 2014* conference covers a number of topics within safety and reliability, and provides a forum for presentation and discussion of scientific papers covering both methodology and applications to a wide range of industrial and problem areas.

METHODOLOGY AREAS

M1. Accident and Incident Investigation and Modelling
M2. Analytical Methods in System Safety and Reliability
M3. Reliability and Safety Management
M4. Dynamic Reliability
M5. Expert Methods in System Safety and Reliability
M6. Failure Identification and Degradation Processes
M7. Human Factors and Human Reliability
M8. Maintenance Modelling and Optimisation
M9. Occupational Safety
M10. Quantitative Risk Assessment
M11. Reliability and Safety Based System Design
M12. Reliability and Safety Data Collection and Analysis
M13. Reliability and Safety Education and Training
M14. Simulation Methods in System Safety and Reliability
M15. Structural Reliability and Safety
M16. Uncertainty and Sensitivity Analysis
M17. Processes Reliability and Safety Modelling

APPLICATION AREAS

T1. Aeronautics and Aerospace
T2. Agriculture and Food Industry
T3. Chemical Process Industry
T4. Civil Engineering
T5. Critical Infrastructure
T6. Electrical Engineering
T7. Electronic Industry
T8. Energy Production and Distribution
T9. Information Technology and Telecommunication
T10. Manufacturing and Supply Chain/Logistic Systems
T11. Maritime Transportation
T12. Mechanical Engineering
T13. Medicine and Health Service
T14. Natural Resources and Environment
T15. Nuclear Engineering
T16. Rail Transportation
T17. Return Logistics/Waste Management
T18. Road Transportation
T19. Software Systems
T20. Waterborne Transportation
T21. Other Reliability and Safety Areas

This page intentionally left blank

Methodology areas

Accident and incident investigation and modelling

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An incident reporting support system for airline cabin crew

K. Furuta, K. Okano & T. Kanno
Graduate School of Engineering, The University of Tokyo, Tokyo, Japan

T. Mori & S. Shimizu
ANA Strategic Research Institute Co., Ltd., Tokyo, Japan

ABSTRACT: The objective of this work is to propose a method to provide computer supports to field staff, airline cabin crew as an application domain, in making incident reports. Based on the review of accumulated reports and interview to cabin crew, an ontology of cabin services was constructed, which contains structuralized terms on airplane equipment, cabin and flight crew, cabin crew tasks, causality of unsafe events, and so on. The ontology is used to provide skeletal reporting formats depending on the context of reporting. It has been demonstrated through experimental trials that the reporting support system can contribute to efficiency and ease of reporting, while the improvement of report quality was marginal.

1 INTRODUCTION

Minor human errors and equipment failures that are hidden behind serious accidents are called incidents. Previous works such as (Heinrich 1980) revealed the relation between serious accidents and incidents. Heinrich showed from the statistical records of occupational accidents in US that behind one case of accident, 29 cases of medium-scale accidents with injuries and 300 cases of minor events without any losses occur, which are often called near misses.

Most enterprises and institutions in various industries are enforcing their staff to report and analyze information on background and causal factors of medium-scale accidents and near misses. It is possible to reveal the trends and patterns of incident occurrence and to acquire valuable knowledge for preventing serious accidents by systematically analyzing lots of reports; incident reporting is a key activity for engineering reporting culture, which is a component of a safety culture (Reason 1997).

The most famous incident reporting system in aviation is the Aviation Safety Reporting System (ASRS) of US National Aeronautics and Space Administration (NASA). ASRS is expecting a wide range of reporters including pilots, air traffic controllers, cabin crew, and maintenance staff. It does not seem that ASRS reporting forms have any particular theoretical foundations; it is suited for identifying broad trends of incidents rather than for identifying specific problems (Beaubien & Baker 2002). Accident/Incident Data Reporting Program taxonomy or ADREP 2000 (Cacciabue 2000) is the taxonomy supported by the European Union. The ADREP taxonomy covers an extensive range of incidents, and it focuses on human factors. It was, however, developed to be use by trained analysts rather than pilots.

The Human Factors Analysis and Classification System (HFACS) is a general taxonomy of human errors for identifying causal factors of accidents (Shappell & Wiegmann 2000). It is based on Reason's model of human error (Reason 1990). HFACS was not developed to be used directly by pilots, either. The British Airways Safety Information Systems (BASIS) is a software tool for supporting airlines to collect incident reports from pilots and to manag the data (O'Leary 2002). There is little information available about BASIS, but it does not appear that these is any particular theory behind the BASIS development. The Critical Event Reporting Tool (CERT) was developed for supporting pilots' self-report of relevant information by using a schematic map (Wiegmann & von Thaden, 2003). This work demonstrated that a schematic map is effective for pilots to elicit information about why the incident happened rather than what happened.

A problem in incident reporting is that the quality of reports, which includes both the coverage and the accuracy of reported information, depends on the reporters. If the quality of reports is insufficient, it is impossible to obtain useful outcomes from its analysis. Previous studies, however, primarily focused on the analysis phase by trained analysts but less on how to extract necessary information

from reporters efficiently considering the analysis that follows. The reporting systems usable for field staff rather than analysts were sometimes not powerful enough to extract the causal factors.

The aim of this work is to propose a method to provide computer supports to field staff in making incident reports so that information sufficient for incident analysis can be acquired and the quality of incident reports will be improved. This work adopts incident reporting by airline cabin crew as the application domain. Most previous works are interested in incident reporting from pilots rather than cabin crew. Tasks in a cabin are more influenced by situations than those in a cockpit, because cabin crew have to attend passengers; incident reporting support for cabin crew is particularly focused on in this work.

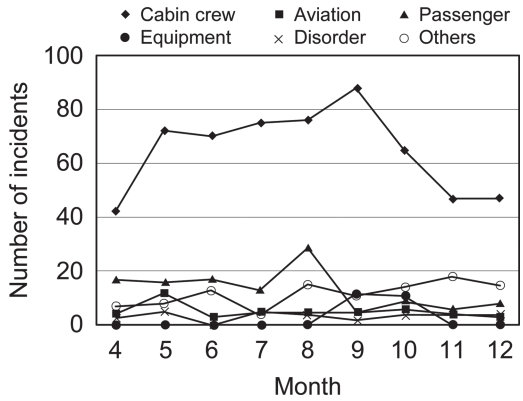


Figure 1. Number of reported incidents for each attribution.

2 ANALYSIS OF APPLICATION DOMAIN

2.1 *Field review*

The role of airline cabin crew as a safety staff is more important than that as a service staff, and the procedures and guidelines as a safety staff are clearly predefined. In order to obtain an overview of cabin services, accumulated incident reports, service manuals, training sessions, briefing about cabin services, and the services during actual flights were reviewed.

An incident that occurred in a cabin is reported following the process below in the target airline company.

1. The crew involved in the incident makes a report using the fixed form after the flight.
2. Another crew who is in charge of checking will supplement the report by interviewing the reporter, if the report submitted is insufficient or ambiguous.
3. The report submitted and checked is proceeded to further analysis.

This work particularly tries to curtail the second step of the above and to make the report quality independent of reporter's skill as much as possible.

The current situation of incident reporting in the field was investigated by reviewing 1,136 cases reported from April to December 2012. The reports are categorized in six classes and the cases that are unrelated to safety issues were omitted from further review here.

Though some reported incidents in cabins are attributable to flight conditions, equipment failures, or passenger behaviors, most of the reviewed cases are related to cabin crew performance, i.e., human errors, regardless of time, crew's experience level, and situation of occurrence. Figure 1 shows the number of reported incidents per month for each attribution.

2.2 *Domain ontology*

Based on the results of field review, an ontology of airline cabin services was constructed. An ontology here means a structured set of concepts and terms that are used by the field staff: cabin crew in this work. The framework of the domain ontology has been chosen so that it matches well incident analysis to be performed using the ontology. The C-mSHELL model, which is obtained from the P-mSHELL model for medical service domains by substituting Customer for the Patient, has been adopted as the framework (Kawano 2002).

The C-mSHELL model consists of six components of Customer, management, Software, Hardware, Environment, and Liveware. In addition to these six components, the tasks allocated to cabin crew and the threats that may disturb cabin services have been added as the top-level nodes of the ontology tree. The ontology will be used for providing various supporting functions to cabin crew in making incident reports.

3 SUPPORTING METHODS

Various methods for incident analysis have been proposed so far, but their basic procedures are similar. The common procedure consists of identification of events that occurred, identification of critical points, analysis of causal factors, proposal of counteractions, and finally assessment of the proposed counteractions.

This work aims to generating high-quality incidents reports uniformly regardless of who made

the reports. The system functions expected from the common procedure of incident analysis are therefore supports for building up event sequences, describing event situations, analyzing causal factors, and proposing counteractions. It is desirable that non-experts of incident analysis can use these functions intuitively, and incident analysis can be applied easily to output data of the system.

Since human errors consist the almost portion of causal factors of incidents in the target domain, the system provides the supports based on the Common Performance Conditions (CPCs), which is the description framework for the context of human performance adopted in the Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel 1998).

3.1 *Common Performance Condition*

It is assumed in CREAM that human reliability depends heavily on the context of human performance described as a combination of three factors: human, technology, and organization. The original CPC consists of nine items, and each item is scored semi-quantitatively and then the results are aggregated to yield a single score that represents the goodness of context. Since it is recommended in CREAM, CPC has been modified referring to the opinions obtained from field staff of the airline so that it matches the application domain. The modified CPC consists of the following ten items:

1. Effects of cabin environment and team configuration,
2. Parallel tasks performed simultaneously,
3. Available time for executing the task,
4. Availability and familiarity of the manuals,
5. Teamwork of the crew,
6. Usability of the equipment,
7. Role assignment and locus of responsibility,
8. Effects of time of day and time difference,
9. Education and training,
10. Knowledge and experience.

3.2 *4STEP/M*

The counteractions for preventing recurrence of similar incidents are proposed using 4STEP/M, which is a method of enumerating countermeasures against human errors (Miura & Harada 2007). The countermeasures are performed by two phases: prevention of errors and mitigation of negative effects. 4STEP/M provides a framework for enumerating the countermeasures in four steps:

Step1 Minimization of the number of tasks,
Step2 Minimization of error probability,
Step3 Multiple detection of errors,
Step4 Minimization of damage.



Figure 2. Example screen shot of event sequence editing.

4 SYSTEM ARCHITECTURE

4.1 *Input of basic data*

The system architecture is explained following the flow of system use.

If the reporter starts the system, the initiating screen appears prompting the reporter to input basic data of the incident. The basic data include report category, reporter's name and ID, date of reporting, flight number, origin and destination, date and time of incident, aircraft type, reporter's position in the crew, the time interval from reporter's last flight on the same type of aircraft, and the category of incident.

If the reporter has chosen the category of incident, the system provides the standard procedure of the task related to the category referring to the information contained in the domain ontology.

4.2 *Description of event sequence*

A screen as shown in Figure 2 is used for editing event sequences for all the staff involved in the incident. Each row of the boxes in the figure shows the event sequence for a separate member of the related staff. Creation, changing the title, and rearrangement of sequence by drag-and-drop are allowed for each box, which corresponds to a unitary cabin crew task. The reporter enters box titles that represent briefly what happened and arrange them in the order of event occurrence. This operation is repeated to describe all the event sequences.

4.3 *Assessment of CPC*

Having described all the event sequences, assessment of CPC follows. If the reporter clicks on a box, a popup window for CPC assessment for the task unit appears. The reporter will assess ten CPC items in a three-grade scale by choosing one radio button as shown in Figure 4. Descriptions of assessment are different for different CPC items, and they have been determined through consultation with airline cabin crew so that they can easily understand the options. Default options are

Effects of cabin environment and team configuration
- ○ Favorable effects
- ◉ Indifferent/Normal effects
- ○ Unfavorable effects

Parallel tasks performed simultaneously
- ◉ None.
- ○ Some but not so many as makes a problem.
- ○ Too many parallel tasks that exceed capability.

Available time for executing the task
- ◉ Enough time was secured.
- ○ The task was finished but done in a hurry.
- ○ Insufficient time was available for finishing the task.

Description of the procedure in CAM
- ◉ The procedure was clearly described.
- ○ Only necessary items were described.
- ○ No descriptions.

Teamwork of the crew
- ◉ Satisfactory.
- ○ Slightly poor.
- ○ Poor.

Usability of the equipment
- ○ Appropriate / Effective for error prevention.
- ◉ No problems.
- ○ Inappropriate / Likely to cause an error.

Role assignment and locus of responsibility
- ◉ Clearly defined.
- ○ Not necessarily clear.
- ○ Ambiguous.

Effects of time of day and time difference
- ◉ None.
- ○ Some but not so much as make a problem.
- ○ Too many parallel tasks that exceed capability.

Education and training
- ◉ Sufficient.
- ○ Not necessarily sufficient.
- ○ Insufficient.

Knowledge and experience
- ◉ Sufficient.
- ○ Not necessarily sufficient.
- ○ Insufficient.

Figure 3. CPC assessment.

preset and the reporter can skip choosing buttons, if there are no unusual situations with CPC. The assessment result for each item is scored [–1, 0, +1] or [–2, –1, 0] depending on whether the best mark for the item is good (favorable) or normal (no problems).

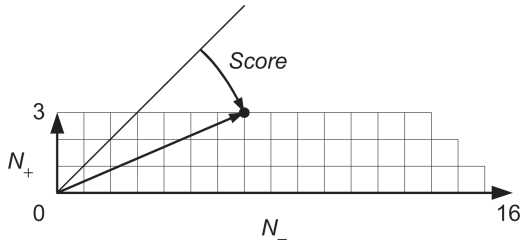


Figure 4. Aggregation scheme of CPC scores.

4.4 *Analysis of causal factors*

After having finished CPC assessment, the system asks the reporter some additional questions for clarifying the context of incident. The system then lists up the candidate factors that may have caused the incident. This judgment is made based on the result of CPC assessment, and the task steps with unfavorable CPC scores are focused on.

CPC scores for different items are aggregated following the work of (Yoshida et al. 2003). Plus scores and minus scores are summed up separately, and then the result is located on the plane as shown in Figure 4, where the horizontal and the vertical axis correspond to the sum of minus scores and that of plus scores respectively. Since the diagonal line represents the neutral situation, the degree of preferable or unpreferable situation is assessed as the deviation from the neutral line, i.e., the arc length normalized by the longest arc. A clockwise deviation corresponds to an unfavorable, and an anticlockwise one to a favorable situation.

The reporter will select some causal factors from the candidates proposed by the system. If the system, however, overlooked any plausible causal factor, the reporter can input an arbitrary causal factor.

4.5 *Proposal of counteractions*

The system asks the reporter some more additional questions, and then it proposes counteractions following the 4STEP/M framework. If the system overlooked any plausible counteraction, the reporter can input an arbitrary counteraction. The system finally prints out the all outcomes of reporting.

5 SYSTEM ASSESSMENT

5.1 *Experimental method*

Two test experiments were conducted, the first experiment for finding out the drawbacks of the original design to improve the system, and the second experiment for assessing usability,

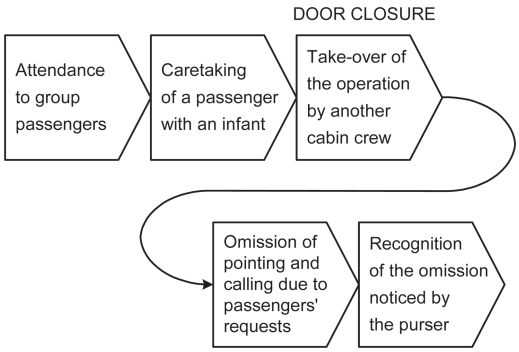


Figure 5. Overview of the test incident scenario.

functionality, effectiveness, and efficiency of the system after modification.

A test incident scenario written in a text was prepared and used in the experiments. The scenario describes a complicated case of omitting a check in door operation that involves more than one cabin crew and passengers. An overview of the scenario is shown in Figure 5. The participants of the experiments read the scenario and then reported the incident in two groups. One group used the support system and then made reports with the current reporting format looking at the outputs of the support system. The other group reported the incident directly without using the support system.

5.2 *Results*

5.2.1 *Usability*

The usability of the system was evaluated by questionnaire to the test users in a five-grade scale, from 1 to five. The average score obtained was 3.2, which means that the participants did not evaluate the system usable. Since the tutorial session for using the system was insufficient, it seems the participants were not accustomed to use the system.

5.2.2 *Functionality*

The radar chart shown in Figure 6 shows the evaluation result of system functionality by questionnaire in a five-grade scale for the following five functions.

1. Describing event sequences in detail,
2. Assessing the context of each step in detail,
3. Proposing the causal factors to be attended,
4. Proposing plausible counteractions,
5. Printing out the results.

The result shows that the participants evaluated the system functionality fairly high except proposing the causal factors to be attended, and printing out the results.

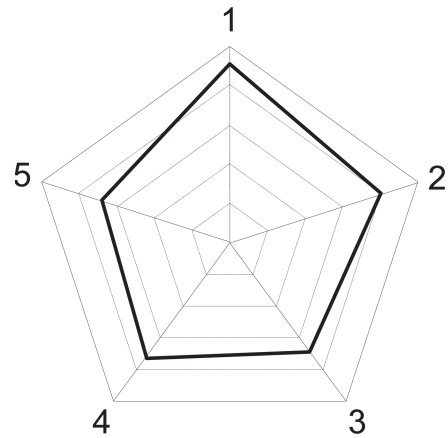


Figure 6. Evaluation result of system functionality.

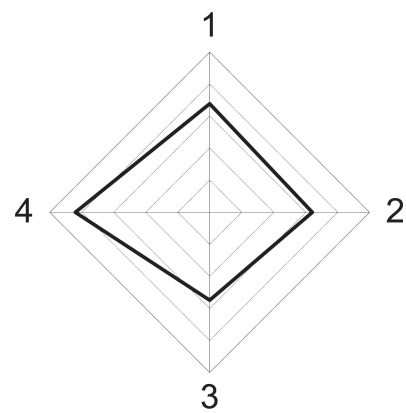


Figure 7. Evaluation result of system effectiveness.

5.2.3 *Effectiveness*

The radar chart shown in Figure 7 shows the evaluation result of system effectiveness by questionnaire in a five-grade scale for the following five aspects.

1. Effectiveness for reporting with ease,
2. Effectiveness for reporting in detail,
3. Effectiveness for reporting in a short time,
4. Effectiveness for clarifying thoughts and analysis.

The participants did not think that the system con tributes to shortening the time of reporting, but they evaluated the system high in terms of clarifying thoughts and analysis.

5.2.4 *Time required for reporting*

The efficiency of the system was assessed by measuring the time required for reporting. Figure 8 compares the time required for reporting between the

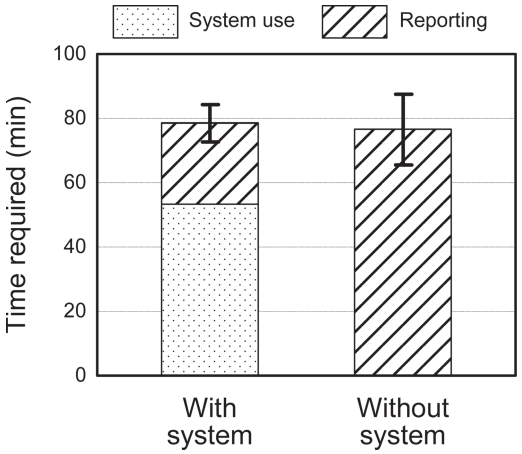


Figure 8. Average time required for reporting.

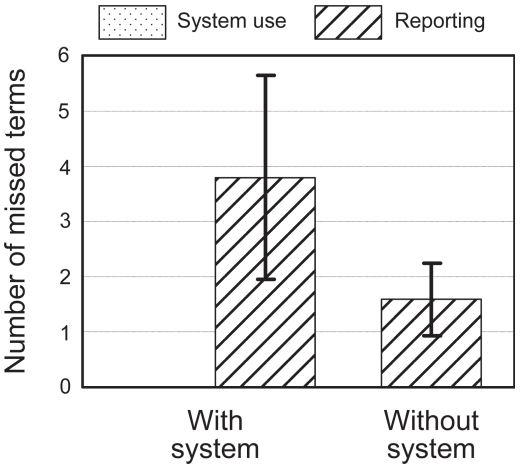


Figure 9. Average number of missed terms.

two groups: with and without using the system. For the group who used the system, the time required for using the system and that for making a report with the fixed format are measured separately.

The average total time for the group with the system was 78.8 ± 5.9 minutes, and it is almost the same as for the group without the system, 76.8 ± 11.1 minutes. If the system can output the results in the fixed reporting format, it is expected that the system will contribute to shortening the time required for reporting considerably.

5.2.5 *Quality of reports*

The quality of the reports that were made with and without using the system was compared. Expert airline staff made an ideal report for the experimental incident scenario and listed up the terms essential for reporting the case. The terms that were missed in the reports generated in the experiment were then counted. For the group who used the system, the count was made both for the system outputs and for the final reports.

Figure 9 shows the result. Those who directly made a report in the fixed format missed some essential terms. Though no missed terms were found in the outputs from the system, those who used the system failed to transcribe some terms into the fixed format of incident reporting. It is expected therefore that such failures can be avoided, if the system can output incident reports in the fixed format directly.

6 DISCUSSION

Extracting relevant information from reporters for incident analysis was achieved by providing guiding frameworks of the information in each step of incident reporting. In particular, since no items for describing context of human performance are given in the present reporting scheme, the analysts have to guess and assess the context from indirect descriptions of the report. The most significant merit of the developed system is that the system can provide a good guiding framework based on CPC for describing and assessing the context.

The time required for using the system alone was cut to one third, though the total time including transcribing the outputs from the system into the present reporting form was almost the same. Direct output in the present reporting form is required for improving thefficiency of reporting with the system. The usability of the system depends highly on users' familiarity to the system and was not necessarily high in the test experiments.

The participants of the experiments made reports reading the written experimental scenario, while they recall their memories in actual reporting. Some of the participants stated that the system will be more useful in the actual than the experimental setting. It is therefore expected that the system can contribute more to improving the efficiency and quality of reporting in actual use.

7 CONCLUSION

A support system of incident reporting for airline cabin crew was developed. The system was assessed by experiments, where the participants read a test incident scenario created from some past cases and made reports with and without using the support system. In addition, the participants answered a questionnaire for subjective assessment. As a

result, it has been demonstrated that the support system can contribute to enhancing the efficiency and ease of reporting, while the improvement of report quality was marginal.

REFERENCES

Beaubien, J.M., Baker, D.P. 2002. *A Review of Selected Aviation Human Factors Taxonomies, Accident/Incidet Reporting Systems, and Data Collection Tools*. Int. J. Applied Aviation Studies, 2(2), 11–36.

Cacciabue, P.C. 2000. *Human Factors Insight and Reliability Data from Accident Reports: The Case of ADREP-2000 for Aviation Safety Assessment*. Proc. 5th Int. Conf. Probabilistic Safety Assessment and Management, 2237–2243.

Heinrich, H.W. 1980. *Industrial accident prevention: A safety management approach*. New York: McGraw-Hill.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method*. Amsterdam: Elsevier.

Kawano, R. 2002. Medical Human Factor Topics. *http://www.medicalsaga.ne.jp/tepsys/MHFT_topics0103.html.*

Miura, T., Harada, E. 2007. *Psychology of Accident and Safety*. Tokyo: Univ. Tokyo Press (Japanese).

National Aeronautics and Space Administration. *Aviation Safety Reporting System*. http://asrs.arc.nasa.gov.

O'Leary, M. 2002. *The British Airways human factors reporting programme*. Reliability Engineering and System Safety, 75(2), 245–255.

Reason, J. 1990. *Human error*. NY: Cambridge Univ. Press.

Reason, J. 1997. *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.

Shappell, S.A., Wiegmann, D.A. 2000. *Human Factors Analysis and Classification System–HFACS*. DOT/FAA/AM-00/7. Washigton DC: Office of Aviation Medicine.

Wiegmann, D.A., von Thaden, T.L. 2003. *Using Schematic Aids to Improve Recall in Incident Reporting: The Critical Event Reporting Tool (CERT)*. Int. J. Aviation Psychology, 13(2), 153–171.

Yoshida, Y., Ohtani, M., Fujita, Y. 2003. *Quantification of a Decision-making Failure Probability of the Accident Management Using Cognitive Analysis Model*. Trans. Atomic Energy Soc. Japan 2, 99–114 (Japanese).

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The effect of the environment conditions on the prediction of flammable cloud dispersion

A.M. Schleder & M.R. Martins
Naval Architecture and Ocean Engineering Department, Risk Assessment Laboratory, University of São Paulo, São Paulo, Brazil

E. Pastor & E. Planas
Department of Chemical Engineering, Centre for Technological Risk Studies, Universitat Politècnica de Catalunya—BarcelonaTech, Barcelona, Spain

ABSTRACT: In order to quantify the damage caused by undesired events involving leakages of flammable materials, specific models are used to analyze the spills or jets of gas and liquid, gas dispersion, explosions and fires. The main step of this analysis is to estimate the concentration, in space and time, of the vapor cloud of hazardous substances released into the atmosphere; the purpose is to determine the area where a fire or explosion might occur and the quantity of flammable material in that area. Recently with the computational advances, CFD tools are used to short and medium range gas dispersion scenarios, especially in scenarios where there is a complex geometry. However, the accuracy of the simulations strongly depends on the boundary conditions. Therefore, this study investigates the sensitivity degree of the prediction of cloud dispersion to changes in values of wind speed, ambient temperature, atmospheric pressure and ground roughness. This paper contributes to an appropriate assessment of the effects of these environment conditions to perform an accurate dispersion simulation using CFD tools and therefore contributes to a more effective analysis of the consequences.

1 INTRODUCTION

Specific models are used to evaluate the release and dispersion of flammable substances when an undesired event occurs; the determination of the dispersion features is essential to model the consequences such as fires and explosions. The consequence analysis is used to define the extent and nature of effects caused by such events and thus is of great help when quantifying the damage caused.

Dispersion models estimate the evolution and the features of the cloud, such as concentration, temperature, velocity and dimensions as a function of time and position. In the case of flammable substances, these models facilitate the prediction of an area where a fire or explosion might occur and the quantity of flammable material in that area.

Nowadays, the use of numerical methods associated with different algorithms of Computational Fluid Dynamics (CFD) to determine the concentration of the vapor cloud of hazardous substances released into the atmosphere, in space and time, has grown considerably (Comier 2008, Middha 2009, Dharmavaram, 2005). CFD is found in some commercial software tools such as CFX, FLACS and FLUENT. The CFD tools transform the governing equations of the fundamental physical principles of fluid flow in discretized algebraic forms, which are solved to find the flow field values in time and space (Anderson, 1995).

CFD tools have proven promising to perform analyzes of consequences in environments with complex geometry, as in the comparative study about the use of integral and CFD tools to evaluate cloud dispersion reported by Schleder & Martins (2013). Nevertheless, as reported by Plasmans et al. (2012), previous studies have shown that consequences analysis using CFD are frequently not easily reproduced and, in many occasions, large differences can arise between the simulation results when working with different tools and/or different CFD analysts to assess the same scenario. These problems stem from the fact that the simulation results can be very sensitive to the wide range of computational parameters that must be set by the user; for a typical simulation, the user needs to select the variables of interest, turbulence models, computational domain, computational mesh, methods of discretization, convergence criteria and boundary conditions among others. The boundary conditions, especially the atmospheric conditions, affect directly the dispersion; however, in most

cases, the conditions are not known and approximate values are used to perform the consequences analyses.

In this context, the study presented here intends to investigate the effects of variations on boundary conditions on the simulation of a cloud dispersion. This study is part of a research project that aims to provide key information for decision making about the use of CFD tools on cloud dispersion evaluation for different scenarios of interest, such as those containing barriers to dispersion; and therefore contributing to optimize the accuracy of the results.

In order to perform this analysis, the same scenarios used in a previous study of grid dependence are used (Schleder et al., 2014) in this case to assess the influence of variations on boundary conditions on the predicted values of the cloud features. The variables of interest have been ambient temperature, atmospheric pressure, wind speed and ground roughness. Two scenarios are presented: a former scenario of a jet release of dense gas in open and flat terrain and a similar release with the presence of a fence.

1.1 *Computational Fluid Dynamics (CFD)*

The physical aspects of any fluid flow are governed by three principles: mass is conserved, Newton's second law is fulfilled (also referred as momentum equation) and energy is conserved; these principles are expressed in integral equations or partial differential equations (continuity, momentum and energy equations), being the most common form the Navier-Stokes equations for viscous flows and the Euler equations for inviscid flows.

The CFD tools transform these governing equations of the fundamental physical principles of fluid flow in discretized algebraic forms, which are solved to find the flow field values in time and/or space. Thus, the results obtained by CFD are a set of data which represent the flow field characteristics at discrete points in time and/or space. The application of CFD tools are related with the computational advances, which explains the growing use of CFD in the recent years (Anderson, 1995).

The boundary and initial conditions of the flow dictate the particular solution obtained from the governing equations, and as such the solution of the governing equations must provide a suitable representation of the boundary conditions.

The software FLACS was used to perform this study (GexCon AS, 2013); FLACS incorporates a water-based model for the simulation of pool spreading and vaporization, and the Reynolds Averaged Navier-Stokes (RANS) equations for the simulation of vapor cloud dispersion.

The pool vaporization is evaluated based on heat transfer from the substrate, solar radiation, convective heat transfer from the air, local wind speed, turbulence levels and local vapor pressure. All these variables are calculated at each time step and locally, for each grid cell (Gavelli et al., 2011). The cloud concentration also will be influenced by atmospheric turbulence, atmospheric stability and density changes. FLACS models flow in the atmospheric boundary layer by profiles of wind, temperature and turbulence parameters on the inlet boundaries (GexCon AS, 2013).

As presented by Gavelli et al. (2011), the model available in FLACS solves Reynolds Averaged Navier-Stokes (RANS) equations based on the standard k-ε model of Launder & Spalding (1974). According to HSE (2010), RANS approach is widely accepted and documented; it is based on the concept of separating the fluid velocity components and scalar quantities (pressure, temperature, concentration) into mean and fluctuating components, then transport equations are used to evaluate the model. The standard k-ε model of Launder & Spalding (1974) presents a turbulence model in which the magnitudes of the two turbulence quantities are evaluated: the turbulence kinetic energy k and its dissipation rate ε, which are calculated from transport equations solved simultaneously with those governing the mean flow behavior (Launder & Spalding 1974).

1.2 *The effects of the atmospheric conditions*

As reported by CCPS (1995), to analyze an accidental release it is necessary to define the governing conditions of the discharge scenario and environment. The items that can define these conditions are source term characteristics, environmental conditions, types of releases, possible source scenarios and possible dispersion mechanisms. The release is usually described separating the region analyzed in three sections: first the discharge section, where the release is almost independent of the environmental conditions and as such the features of the source term define this region; next the intermediary section where both source and environmental conditions are significant in the modeling and the last section, where environmental conditions dominate the process of dispersion. In this paper the focus is on the effects of environmental conditions in the whole dispersion process.

If the substance released presents density higher than air, the first stage of the dispersion will occur as dense gas and when the cloud dilutes enough to its density be equal to the air's, the dispersion will occur as passive or neutral dispersion. In the dense gas dispersion phase, the cloud will be making

descent movements until it reaches the ground and then will spread radially under influence of the gravitational forces, hence having the dense cloud the horizontal dimension greater that the vertical dimension. The vertical dimension will be higher in the extremities of the cloud due to the air resistance (TNO, 2005).

After this stage, when the cloud has density equal to the air's, the passive dispersion occurs which is governed by the environmental conditions, mainly by wind and atmospheric stability (TNO, 2005).

The atmospheric instability occurs because of the wind flow and the air displacement between different layers due to the temperature difference between these layers. This turbulence generates eddies with different sizes; eddies smaller than the cloud disperse the cloud and increase the cloud size (there is no effect on position of the cloud), eddies much bigger than the cloud merely move the cloud (there is no effect on form neither on size) and eddies with the same size of the cloud change the cloud form and increase its contour (TNO, 2005).

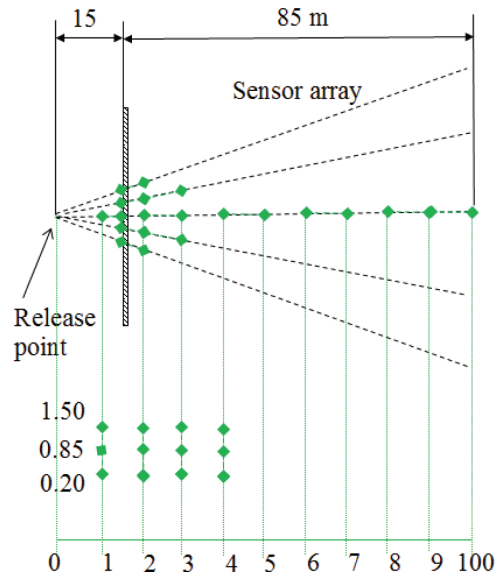


Figure 1. Sensor array.

2 BASELINE SCENARIO

As previously mentioned, the baseline scenario in this study is the same used in a previous study of grid dependence (Schleder et al., 2014) where two trials of the field tests performed by Health and Safety Laboratory (HSL) at the HSL laboratories in Buxton, England (Butler & Royle, 2001) were chosen to perform the sensitivity analysis.

The HSL trials consisted of liquefied propane continuous releases at rates up to 4.9 kg/s, at a height of 1.5 m; during the release a biphasic jet was formed, however there was no pool formation, since the liquid present in the jet evaporated before reaching the ground. The concentration of propane in the resulting vapor cloud was monitored by gas sensors to determine the cloud features at different distances from the release point. The trials set-up involved a liquefied propane storage facility, a release system and a discharge area in which the vapor clouds were produced. The discharge length was aligned with the prevailing wind.

Sensors were placed over a 600 m^2 area (100 m in downwind direction and 6 m in crosswind direction), located within the gas dispersion site; they were located at heights of 0.20, 0.85 or 1.50 m above the ground on the first 40 m of the centerline of the site and at a height of 0.20 m in arcs around the release point, as showed in Figure 1.

In order to investigate the influence of an obstruction, in some of the trials a fence was placed in the cross wind direction in the path of the vapor flow. A 1 m high fence was chosen to be a suitable obstruction; using this height, the top of the fence was approximately in the middle of the gas cloud height, allowing a significant volume of gas to flow unobstructed, whilst at the same time providing an obstruction for the lower part of the cloud. The fence was 20 m long, positioned 15 m from the release nozzle, perpendicular to the centerline of the trials site; it was made by wood and form an impermeable barricade. It was centered so that there was 10 m of fence at either side of the centerline. More details about the field tests are reported in Butler & Royle (2001) and Schleder et al. (2014).

In the previous study (Schleder et al., 2014) trials 8 and 11 of these field tests were selected as baseline scenarios (B1 and B2) to perform the CFD grid dependence analysis. The same trials were selected to perform the sensitivity analysis. The former test (B1 representing test 8) presents an unobstructed scenario while the other (B2 representing test 11) presents the scenario with a fence acting as an obstruction to cloud dispersion. The input parameters used to perform the simulations are presented in Table 1.

The domain and the grid of the baseline scenarios were built according to previous study (Schleder et al., 2014): an orthogonal base X, Y and Z was used, being the X direction horizontal and parallel to wind, the Y direction perpendicular to the wind and horizontal and the Z direction vertical, being the point (0, 0, 1.5) coinciding with the release point.

Table 1. Scenario conditions of baseline scenarios.

Variable	Unit	B1	B2
Ambient temperature	ºC	14.5	17.5
Atmospheric pressure	bar	1	1
Wind speed	m/s	3.0	5.0
Pasquill class	–	D	D
Wind direction	º	195–225	110–225
Relativity humidity	%	63	63
Ground roughness	m	0.03	0.03
Temperature release	ºC	11.96	11.26
Pressure release	bar	7.87	7.58
Discharge rate	kg/s	2.5 ± 0.3	3.4 ± 0.3
Discharge direction	–	Horizontal	Horizontal
Release duration	s	131	141
Discharge height	m	1.5	1.5

The domain was divided in three areas: the first one around the release point (micro grid), formed by the specific and adjacent cells where the leak takes place; the second, the prevailing grid formed by the area where the dispersion is expected (macro grid); and the third, the stretched area in the far field where no relevant concentrations are expected. The transitions among these areas are made gradually in order to obtain stable simulations; the cells are increases gradually from one region to another of the grid such as the maximum ratio between one cell and the next one is two.

The computational domain extended 170 m in the X direction (from 20 m upwind to 150 m downwind from the release point), 30 m in the Y direction (symmetric crosswind plan from the release point) and 10 m in the Z direction; the cells were initially represented by $1\ m \times 1\ m \times 0.5\ m$ cuboids (forming the macro grid).

Concerning the micro grid dimensioning, the guidelines (GexCon AS, 2013) specify that the cross area of the expanded jet must be solved in only one cell and that the area of this cell should be larger than the area of the expanded jet but not larger than twice. Therefore, the jet area expected after the expansion at ambient pressure was estimated and the dimensions of the face cell across the jet defined so that the area fell between these limits. Thus, in B1 scenario, the width and height of the micro grid cells (the release cell and adjacents) were fixed at 0.15 m (as a function of the jet area expected after the expansion at ambient pressure) and, in order to maintain the aspect ratio smaller than 5, the length of the cells was fixed at 0.5 m. In B2 scenario, the width and height of the micro grid cells were fixed at 0.17 m and the length of the cells was fixed at 0.86 m. Once the dimensions of the cells around the leak were defined, cells nearby were smoothly increased to the macro grid resolution: in z direction, the transition zone between the micro grid and the macro grid is from 2 m to 5 m high; in y direction, this region has 12 m in the symmetrical crosswind plan from the release point; and in x direction, the macro grid begins 1 m after the release in downwind direction and 1 m after the release in upwind direction.

Lastly, in both scenarios, the macro grid was stretched in X direction away from the leakage point, (he length of cell growing continuously at a rate of 1.15 to provide a smooth growth with increasing distance from the source. The cells were stretched after 100 m from the leakage point because after this distance significant concentrations of gas are not expected. More details about the grid are reported by Schleder et al. (2014).

Taking into account that the focus of this study is on the dispersion of a cloud the main variable of interest was defined as the concentration of this cloud.

The results of the baseline scenarios are presented in Figures 2 and 3 for scenarios B1 and B2 respectively; the blue lines represent experimental data and the green lines represent the simulated concentrations.

The HSE in the Model Evaluation Protocol (MEP) recommends the use of a factor of 2 range to validation purposes of CFD models, the fraction of predictions should fall within a factor of two of the measurements (Coldrick et al., 2009); in the cases analyzed here, 60% of the simulated values fitted well to this range, the major discrepancies found are related to values of concentration smaller than 2% in scenario B1 that are over simulated by the model. The simulated concentrations concerning to baseline scenarios were reported and discussed in Schleder et al. (2014).

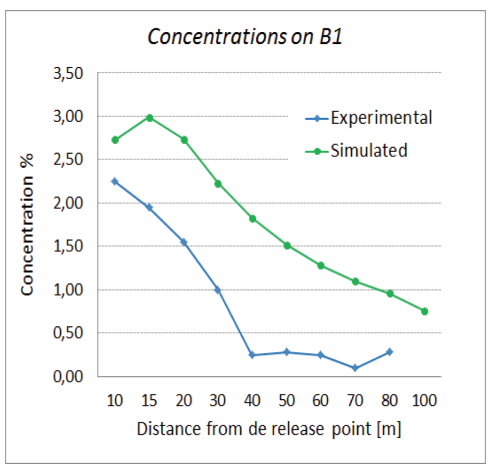


Figure 2. Results of baseline scenario B1.

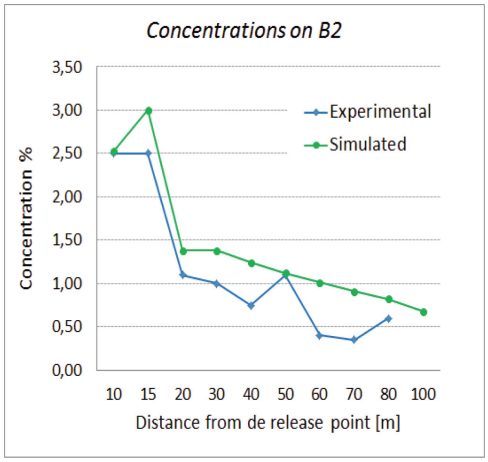


Figure 3. Results of baseline scenario B2.

3 SENSITIVITY ANALYSIS

In CFD modeling, the analyst should choose a large number of parameters and these can affect significantly the results. As reported by Pandya et al. (2012), there are three varieties of sensitivity analysis: local, global and screening methods. The local methods evaluate the effects in the outputs given each input varying one factor at a time around a baseline point; the global methods are more sophisticate and aim to evaluate quantitatively the influence of the entire range of inputs values on the outputs uncertainty. Finally, the screening methods that are based on computing for each input a number of incremental ratios, which are then averaged to assess the importance of the input (Pandya et al., 2012).

The global and screening methods are comprehensive methods that assess the sensitivity of the models in more detail; however, these models deal with the variables as functions, therefore are more time consuming and require more complex tools for their development such as the software's used by Pandya et al. (2012) and Gant et al. (2013). Considering that CFD models are computationally expensive and have a large range of possible inputs, the sensitivity analysis performed here will follow the local approach, which is less time consuming and can be executed with no need of specific software.

The objective of the sensitivity analysis is to verify which inputs affect more the results of the simulation, thus the first step is the choice of the variables subjected to sensitivity analysis. Next, these inputs are varied and the effects on the results regarding to concentration of the cloud are analyzed. Finally the degree of sensitivity is estimated.

As seen, the boundary conditions, especially the atmospheric conditions, affect directly the dispersion; however, in most cases the exact values of the parameters that characterized the conditions are not known and approximate values are used to perform the consequences analyses. In this sensitivity analysis the effects of variations in the wind speed, ambient temperature, atmospheric pressure and ground roughness on predicted concentrations are analyzed.

In order to perform the sensitivity analysis the influence of variations of up to ±10% in the ambient temperature, wind speed, ground roughness and atmospheric pressure values was studied. Each variable was changed independently of the others: for example, when the ambient temperature was decreased by 10%, the other variables remained the same as those defined in the baseline scenario (Table 1).

The same approach was used for both baselines scenarios (B1 and B2); nine simulations were performed for each one: the former using the original values presented on Table 1 and one for each variation presented on Table 2, in which the first column describes the variable of interest, the second is the variation applied over the original value of this variable and the last two the final value of each variable after increasing or decreasing by 10% for scenarios B1 and B2 respectively.

The simulated values for concentration of each simulation were compared with the simulated values of the original baseline scenarios. Monitor points measuring concentration every 10 m following X direction were inserted in the simulations at three heights: 0.2, 0.8 and 1.5 m and thus the comparative analysis between the simulated concentrations of the original baseline scenarios and the simulations after the variation of each parameter was made for each distance and height.

Only the results obtained for the monitor points at 0.2 high are presented here due to space constraint, on Tables 3 and 4. In these tables, the first column reports the distances from the monitor point to the release point, and the other columns

Table 2. Variations in each scenario.

Variable	Variation	Unit	B1	B2
Ambient temperature	–10%	ºC	13.05	15.75
Ambient temperature	+10%	ºC	15.95	19.25
Wind speed	–10%	m/s	2.70	4.50
Wind speed	+10%	m/s	3.30	5.50
Ground roughness	–10%	m	0,027	0,027
Ground roughness	+10%	m	0,033	0,033
Atmospheric pressure	–10%	bar	0,90	0,90
Atmospheric pressure	+10%	bar	1,10	1,10

Table 3. Concentration variation on B1.

Distance [m]	Percentage changes by each parameter on B1			
	Temperature	Wind speed	Ground roughness	Atmospheric pressure
10	–0,7%	–4,4%	0,0%	–2,2%
15	–0,7%	–2,3%	–0,3%	–1,0%
20	–0,4%	+1,8%	–0,4%	+0,7%
30	+0,4%	–0,9%	0,0%	–0,9%
40	–0,5%	–0,5%	–0,5%	–1,1%
50	–0,7%	–0,7%	–0,7%	–2,0%
60	0,0%	+0,8%	0,0%	–1,6%
70	0,0%	+0,9%	0,0%	–1,8%
80	0,0%	–1,0%	–1,0%	–3,1%
100	–1,3%	–1,3%	–1,3%	–3,9%

Table 4. Variation in the estimated values on B2.

Distance [m]	Percentage changes by each parameter on B2			
	Temperature	Wind speed	Ground roughness	Atmospheric pressure
10	+0,8%	+6,3%	0,0%	+4,7%
15	+1,0%	+3,7%	+1,3%	+3,0%
20	+0,7%	+0,7%	0,0%	+1,4%
30	+0,7%	+2,2%	0,0%	+0,7%
40	+0,8%	+3,2%	+0,8%	+2,4%
50	–0,9%	–3,6%	0,0%	+3,6%
60	–1,0%	–5,0%	–1,0%	+5,0%
70	0,0%	–5,5%	0,0%	+5,5%
80	+1,2%	+6,1%	+1,2%	+7,3%
100	+1,5%	+7,4%	+1,5%	+8,8%

report the maximum percentage variation between the simulated concentrations using the original values of the baseline scenario and the concentration simulated after the variation on each particular parameter. The symmetry of the results is analyzed posteriorly. For example, varying the ambient temperature of B1 up to 10%, the estimated concentration in the monitor point at 10 m from the release point at 0.2 high varies at most 0.7%.

The same verification of the previous tables was performed for all monitor points at different heights and the sensitivity degree of each parameter was defined according to the maximum percentage changes in the simulated values of concentration. The variables sensitivity was considered "low" if the maximum percentage changes were less or equal to 2%, "medium" if between 2 and 5% and "high" if greater than 5%, this criteria was applied in order to determine which variables are most sensitive to changes.

Table 5 presents the maximum variation caused on concentration for each input and the variables sensitivity degrees for both scenarios. The changes up to 10% in the temperature cause minor effects in the results, since this variation is not enough to represent a change in the atmospheric stability. However, it is important to note that in different scenarios in which the evaporation process may take longer (such in a case of pool formation), the influence of variations in the ambient temperature may increase, since it will directly affect the vaporization rate.

In addition, from Table 5, it is possible to note that changes up to 10% in the ground roughness do not affect the results significantly. However, in both scenarios, the variations of the wind speed and pressure cause more significant changes in the simulated concentration values.

Figure 4 shows the effect on concentration of varying wind speed in scenario B1. Simulated concentrations in each monitor point at height 0.2 m are plotted: the yellow bars represent the simulated values for the baseline scenario B1 using the initial values of Table 1, the green bars represent the simulated values obtained using the wind speed value decreased by 10% and the blue bars represent the results obtained using the wind speed value increased by 10%.

As can be observed, the effects of variations on wind speed are greater in near field and decrease on far field, being the effect anti-symmetric on near field and tending to a symmetric effect on far field; this occurs because near the source term there is more turbulence due to the jet and therefore there are more eddies generated by this turbulence. The wind contributes to the eddies formation and consequently to the cloud dilution. In far field, there is less turbulence; thus, the wind

Table 5. Sensitivity degree.

	Parameter	Maximum variation on results	Sensitivity degree
B1	Ambient temperature	1.3%	Low
	Wind speed	4.4%	Medium
	Ground roughness	1.3%	Low
	Atmospheric pressure	3.9%	Medium
B2	Ambient temperature	1.5%	Low
	Wind speed	7.4%	High
	Ground roughness	1.5%	Low
	Atmospheric pressure	8.8%	High

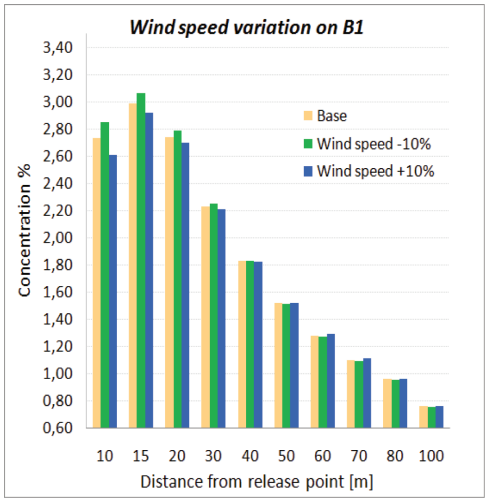


Figure 4. Simulated concentrations varying wind speed on scenario B1.

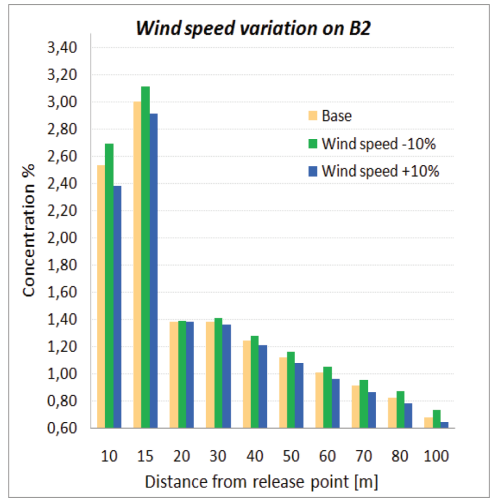


Figure 5. Simulated concentrations varying wind speed on scenario B2.

contributes less to cloud dilution and more to the cloud displacement, moving the entire cloud in the wind direction. This effect would probably be different in a scenario with pool formation; in such a case, there is less turbulence near the source and the wind contributes to cloud displacement and influences the evaporation rate of the pool.

Like Figure 4 for scenario B1, Figure 5 shows the simulated concentrations in each monitor point at height 0.2 m for the baseline scenario B2; it can be observed that the variations in the wind speed cause noticeable effects on the simulated values both on near and far field.

In scenario B2 the variations of wind speed affected the results near the source term, by the same reasons of scenario B1; however, unlike scenario B1, in the far field the results were also significantly affected. In this case, the wind contributes do the cloud dilution in the region near the source, after few meters the turbulence decrease; however, the fence at 15 m blocks partially the cloud and causes turbulence, consequently the results sensitive to variations in wind speed increases. The difference between the results for the baseline scenario and the scenarios with increase and decreased wind speed remains approximately constant from immediately after the fence until the last monitor point.

Concerning to variations in the pressure atmospheric values, Figures 6 and 7 show the simulated concentrations in each monitor point at height 0.2 m for scenarios B1 and B2 respectively: the yellow bars represent the simulated values for the baseline scenario using the initial values of Table 1, the green represents the predict values

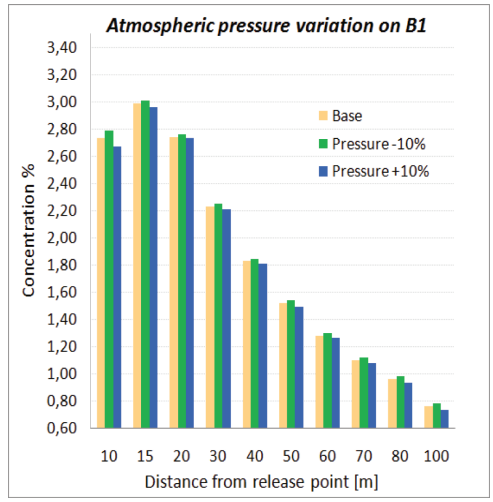


Figure 6. Simulated concentrations varying atmospheric pressure on scenario B1.

obtained using the atmospheric pressure value decreased by 10% and the blue represent the results obtained using the atmospheric pressure value increased by 10%.

When the atmospheric pressure value is increased by 10% the simulated values for concentration for the gas phase decrease and when the atmospheric pressure value is decreased by 10% the simulated values for concentration increase; this probably occurs because with a higher pres-

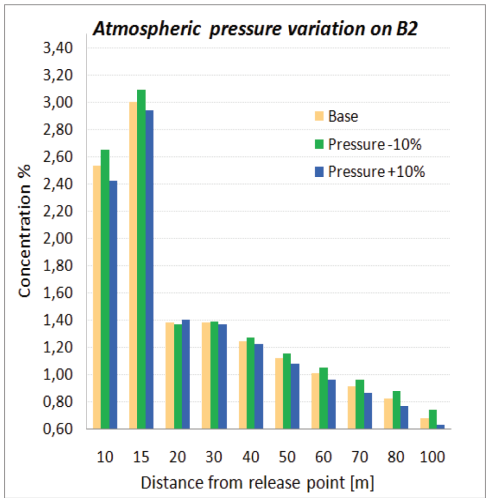


Figure 7. Simulated concentrations varying atmospheric pressure on scenario B2.

sure the liquid fraction into the cloud takes longer to evaporate; from the results of the monitor points at different heights, it is possible to note that the influence of the pressure variations is lowest in the highest part of the cloud, where the liquid fraction is smaller.

4 CONCLUSIONS

This study evaluated the sensitivity analysis of cloud dispersion using a CFD tool; four variables of interest were considered: ambient temperature, wind speed, ground roughness and atmospheric pressure.

In order make the analysis, two trials of the field tests performed by HSL (Butler & Royle, 2001) were chosen; the former presenting an unobstructed scenario and the second with a barrier blocking the spread of the cloud.

In both scenarios the results were more sensitive to changes in the values of the wind speed and atmospheric pressure. The variations on simulated concentrations reach up to 8.8%; however, minor effects on results occurred due to changes in the ambient temperature and ground roughness, in these cases the variations on simulated results reach up to 1.5%.

It is worth noting that the results showed a low sensitivity degree to temperature and roughness variations in the selected scenarios. However, this degree can be higher in other scenarios: for example, in scenarios in which there is pool formation, variations in ambient temperature probably will influence more the results, since this parameter affects the evaporation process.

Moreover, the results were more sensitive to variations in wind speed and atmospheric pressure; it is important to note that the wind variations associated with the presence of the fence affects directly the results, showing that the accuracy of these values is essential to high quality dispersion modeling.

Future research will imply performing a sensitivity analysis of other key parameters on dispersion analysis, especially concerning source term features and other scenarios such as dispersion over water and pool formation. This will allow a better founded decision making process when setting computational parameters in CFD simulations.

ACKNOWLEDGMENTS

The authors gratefully wish to acknowledge the Program for Development of Human Resources (PRH) from Petrobras and Brazilian National Petroleum, Natural Gas and Biofuels Agency (ANP) by the financial support.

REFERENCES

Anderson, J.D. Jr. 1995. Computational Fluid Dynamics—The basics with applications. Maryland: McGraw-Hill. pp. 547.

Butler, C.J. & Royle, M., 2001. Experimental data acquistion for validation of a new Vapour Cloud Fire (VCF) modelling approach. pp. 1–102: Health and Safety Laboratory—HSE.

CCPS—Center for Chemical Process Safety, 1995. Understanding Atmospheric Dispersion of Accidental Releases. New York: Center for Chemical Process Safety.

Coldrick, S., Lea, C.J., & Ivings, M.J., 2009. Validation database for evaluating vapor dispersion model for safety analysis of LNG facilities—Review. The fire protection research foundation. Health and Safety Laboratory—HSE.

Cormier, B.R. 2008. Application of computational fluid dynamics for LNG vapor dispersion. Journal of Loss Prevention in the Process Industries. pp. 332–352.

Dharmavaram, S., Hanna, S.R., & Hansen, O.R. 2005. Consequence Analysis—Using a CFD model for industrial Sites. Process Safety Progress, 24, pp. 316–327.

Gant, S.E., Kelsey, A., McNally, K., Witlox, H. 2013. Sensitivity Analysis of Dispersion Models for Jet Releases of Dense-Phase Carbon Dioxide. Chemical Engineering Transactions, 31, pp. 1–6.

Gavelli, F., Scott, D.G., & Hansen, O.R. 2011. Evaluating the potencial for overpressures from the ignition of a LNG vapor cloud during offloading. Journal of Loss Prevention in the process industries, 24, pp. 908–915.

GexCon AS. 2014. FLACS Software—version 10.1.

HSE—Health and Safety Executive. 2010. Review of FLACS version 9.0—Dispersion modelling capabilities. Available at: http://www.hse.gov.uk/research/rrpdf/rr779.pdf, accessed on January, 2013.

Launder, B.E., & Spalding, D.B. 1974. The numerical computation of turbulent flows., 3, pp. 269–289.

Middha, P. and Hansen, O.R. 2009. Using computational fluid dynamics as a tool for hydrogen safety studies. Journal of Loss Prevention in the Process Industries. Vol. 22, pp. 295–302.

Pandya, N., Gabas, N., Marsden, E. 2012. Sensitivity analysis of Phast's atmospheric dispersion model for three toxic materials (nitric oxide, ammonia, chlorine). Journal of Loss Prevention in the Process Industries (25), pp. 20–32.

Plasmans, J., Donnat, L., Carvalho, E., Debelle, T., Marechal, B., Baillou, F. 2012. Challenges with the use of CFD for major accident dispersion modeling. Process Safety Progress. Vol. 00, pp. 1–5. doi: 10.1002/prs.11571.

Schleder, A.M., Martins, M.R. 2013. The use of Integrals and CFD tools to evaluate the cloud dispersion of flammable and toxic substances leakages. In: European Safety and Reliability Congress—ESREL, 2013, Amsterdã. Proceedings of ESREL 2013—European Safety and Reliability Congress. pp. 1–8.

Schleder, A.M., Martins, M.R., Pastor, E., Planas, E. 2014. The effect of the computational grid size on the prediction of a flammable cloud dispersion. In: International Conference on Ocean, Offshore and Arctic Engineering, 2013, San Francisco, California, USA. Proceedings of the ASME 2014 33th International Conference on Ocean, Offshore and Arctic Engineering, 2014. pp. 1–8.

TNO—The Netherlands Organization of Applied Scientific Research 2005. Methods for the calculation of physical effects due to releases of hazardous materials (liquids and gases)—Yellow Book (Third Edition ed.). Committee for the prevention of disasters.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Scenario identification in oil and gas industry: A case in the Middle East

Zahra Rezvani, Paul Swuste & Patrick Hudson
Safety Science Group, Delft University of Technology, The Netherlands

ABSTRACT: The first element in safety management is the possession of enough knowledge about what and how accidents happen. Evaluation of the layers of protection is important from both retrospective and predictive points of view. This article focuses on incident scenarios and potential causes of incidents in oil and gas plants, based on literature reviews of accident scenarios in one Middle Eastern case and comparing them with world accident scenarios in this sector. The result shows that accident scenarios in this case are similar to accident scenarios in this sector in the world. We argue that this is because they use similar equipment and facilities. Also, loss of containment and fire are the most popular accident in these industries. Finally, there is a repetitive pattern of accidents world-wide.

1 INTRODUCTION

The definition of accident scenarios lies at the heart of the safety management process and the study of safety related decision-making in which individuals in high-hazard industries are engaged. A scenario is a generalized description of the actors, their goals, sequences of actions and events, and background information (Go & Carroll, 2004)—the dynamics of an accident. First (2010) proposed that an accident scenario forms an unplanned event sequence that can result in unwanted consequences. He argued that one or more conditions, besides the immediate sequence of events, are necessary in an accident oe incident scenario. Fecht et al. (1982) added the notions of initiating and intermediate events into the concept of an accident scenario. An initiating event is the first event in an accident scenario but there are also intermediate events that form enabling events, a "condition which does not directly cause the scenario". For example, loss of containment is an accident scenario for major hazards such as gas or liquids. It can be caused by a direct, initiating, event like a rupture in a vessel or by an indirect, intermediate, event such as the occurrence of a runaway reaction that subsequently results in releases through pressure relief devices or can then cause a rupture. In general, initiating events are typically failures that exceed the boundaries of normal process conditions. They can be classified into control (e.g. automation) failures, mechanical integrity failures (e.g., corrosion or erosion of materials ensuring containment) and human error (e.g., inadvertent opening or closing of valves, setting incorrect control values etc.). The operational conditions themselves should be considered as forming a potential for failure (First, 2010).

From a human error perspective, Guerrero et al. (2008) stated that an incident scenario is a composition of actors, objectives, instruments, action sequences, errors, error causes and error consequences, and context elements.

In summary, a scenario provides an analysis tool for strategic planning in safety management. The typical usage of scenarios in safety involves the description and analysis of the current system, the analysis of the problem domain, provision of a model of the real world, envisioning uncertain feature environments, analysis of user tasks, development of a design rationale and finally provision of a communication tool (Go & Carroll 2004). In fact, based on a review of the literature, there is no firm consensus for scenario definition and its application because the range of topics covered is so wide and the concept does not provide much in the way of theoretical focus. It is as a result of a wide range of influencing factors such as a variety of disciplinary backgrounds and various perspectives (retrospective versus predictive). However, this paper focuses on uncovering the actual common accident scenarios in a Middle Eastern oil and gas company based on historical data about what happened in a specific environment, rather than very general considerations of what might be appropriate scenarios. The question is then posed whether there are any differences between such accident scenarios in this Middle Eastern case and accident scenarios in the world's oil and gas companies? What are the main causes of accidents in these industries and do they differ from a potentially unique isolated environment? And, if they

do, does the scenario approach provide a useful basis for improved understanding?

2 METHOD

A documentary analysis was carried out to investigate accident scenarios from both a retrospective and a predictive point of view. In this study, data from cases, published incident reports from the oil and gas industries, were used to first clarify the concept of an accident scenario and then identify the causes of accidents in this sector. Also, risk analyses which have been conducted by researchers and have been documented in this scope were used to fill out the scenarios.

Oil and gas plants and gas industries use the same basic equipments (pumps, tanks, vessels columns etc.) because the basic physics and chemistry of hydrocarbon and gas processing is the same everywhere. Therefore the scenario types for various types of equipment might be categorized by risk analysis, accident history and operational experience. Accidents in oil and gas plants in one oil and gas operating company which includes six oil fields producing more than one million barrels of crude oil, 500 M ft^3 gas, and 6500 barrels of liquified natural gas per day. Over a time period between 1985 to 2009 were assessed. This company has 7 operation units, 4 distillation plants, 10 gas compressor stations, 3 liquified gas plants, a gas refinery, and one water treatment plant.

The accident data was gathered from a book published by the operator (NISOC, 2011). This may not the complete source of data, since usually incident histories are not published publicly as a result of confidentiality issues and it is evident that this document focused on major events, those that caused loss of life, damage to property or harm to the environment. It is, nevertheless, useful for our purpose, which is the identification of the main accident scenarios in this sector because such major incidents can be treated as representative of the major scenarios that are likely. If some minor scenarios are missed they will appear to be either associated with lesser consequences or be much less frequent. We then compared incidents within this specific area with incidents of the same industry in world-wide over the same period (Sam 2005).

The focus was on process incidents which resulted from plant operation and process activities rather than on personal accidents that were unrelated to the process in the plant. Because personal safety incidents are more common the personal scenarios can otherwise easily swamp the less common process scenarios, while the latter will inevitably have much higher potential for disaster involving more people and larger assets.

3 RESULTS

Overall the use of a scenario approach has several advantages. For example, scenarios help to distinguish which are the important events which should be taken into account. Morover, using a scenario approach can clarify the inter-relationship between different aspects such as individual, psychological, social and political factors. From a predictive point of view, structured techniques such as Process Hazard Analysis (PHA), HAZOP and What-If analyses have been used for identification of scenarios in this area and are used world-wide. These methods can find connections between deviations (process upsets), the possible causes (initiating events) and outcomes (consequences). For instance, the principal goal of PHA is to specify scenarios resulting from failures to manage major hazards.

The paper focuses on a list of common incident scenarios in this industry, identifying and using case histories in a Middle-East case in particular and in the world in general. Although the probability of some scenarios are low, certain initiating events and conditions may still happen and cause catastrophic results. Table 1 shows a list of major accidents, scenario types, and initiating events in a Middle East case. It is based on First's classification (First, 2010) who considered 16 scenario types for incidents for various equipment types.

4 DISCUSSION

As can be seen in Table 1 and Figure 1, these findings are similar to findings of other analyses. The similarities are probably the result of using the same basic equipment (pumps, tanks, vessels columns, etc.) and similar processes. So, fires and explosions, including Vapour Cloud Explosions, are the major accidents with which the oil and gas industry are faced. The most common is fire, however explosion has more potential damage in terms of fatalities and loss of property (Khan & Abbasi, 1999).

The main causes of large fires and explosions in oil industries are release or overflow of flammable liquid or gas, overheating or hot surfaces, fitting or pipe failure, electrical breakdown, and overpressure or pressure vessel failure, explosion in equpment chemical reaction, and inappropriate operation (Khan & Abbasi, 1999).

Explosions form the second most important and common incident scenario in this sector and become the most frequent when different types of explosions are combined. Explosions often cause fatalities, damage to property, shutdown of the plant for some days, often months, and serious negative impact on the reputation of the industry.

Table 1. A list of major accidents in a Middle East oil company between 1983 to 2009 (from NISOC, 2011).

Year	Accident type	Unit	Event	Plant/transport	Chemical	Scenario type	Death (d) injuries (i)	Initiating event
1991	Leakage of wellhead separator	Operation	TOX (H_2S)	Well-head separator	Oil–Gas	Leakage of well-head separator	2 d	Failure in control valve, human error
1983	Fire of oil water separator	Operation	Fire	Oil–water separator	Oil	Fuel accumulation,	1 i	Electrical and mechanical control failure of vertical pump, human error
1993	Fire of gas oil tank	Operation	Fire	Gas oil tank	Gasoil	Improper drain	1 d	Drain of gas-oil with gasoline pump
1994	Fire of oil supply tanks	Operation	Fire	Oil supply tanks	Oil	Uncontrolled reaction	–	Control failure
1997	Fire of degassing tank	Operation	Fire	Degassing tank	Oil–Gas	Physical damage of flange	1 d	Control failure, human error
2008	Electrical fire in low voltage switch room	Operation	Fire	Low voltage switch room	–	–	–	Hurricane, control failure
1991	Gas loss (LOCA)	Operation	LOCA	Pipeline	Oil–Gas	LOCA	1 d	Seal leak, human error
1993	LOCA of gas well pipelines	Operation	LOCA	Gas well pipelines	Gas	LOCA	–	Failure in mechanical integrity
1995	Rotation of floating roof of crude oil storage tank	Operation	–	Crude oil storage tank	Oil	Physical damage	–	Control failure
1987	Fire of fuel tanker (oiler)	Operation	Fire	Fuel tanker (oiler)	Oil	Improper drain	1 d	Failure control (drain without bonding fire), human error
1988	LOCA during pigging	Pipeline & maintenance unit	LOCA	Pipeline	Oil	LOCA	1 d	Human error, control failure
1989	LOCA	Pipeline & maintenance unit	LOCA	Pipeline	Gas, H_2S	LOCA	1 d	Control failure
1999	Loss of gas	Pipeline & maintenance	LOCA	Pipeline	Gas	LOCA	1 d, some i	Control failure,
1990	LOCA in 18″ pipeline	Pipeline & maintenance	LOCA	Pipeline	NGL	LOCA	4 i	Human error, physical damage
1996	LOCA	Pipeline & maintenance	Fire, LOCA, fire	Pipeline	Oil, Gas	LOCA	–	Control failure, human error
1989	LOCA	Pipeline & maintenance	Fire	Pipeline	Oil	LOCA	19602 barrel	Control failure, human error
1988	LOCA in 12″ pipeline	Pipeline & maintenance	Oil release Oil discharge	Pipeline	Oil	LOCA	–	Control failure, human error

(*Continued*)

Table 1. (*Continued*)

Year	Accident type	Unit	Event	Plant/transport	Chemical	Scenario type	Death (d) injuries (i)	Initiating event
2008	Sour oil leakage	Pipeline & maintenance	Oil release Oil discharge	Pipeline	Oil, H_2S	Excessive pressure	1 d, >15000 barrel	Control failure, human error
1993	Fire of gasoil tanker	NGL plant	Fire & explosion	Gas-oil tanker	Gasoil	Reaction	–	Human error, control failure
2002	Gas loss in 20″ manifold	NGL plant	Fire & explosion	Manifold	Gas, LPG	Physical damage (corrosion)	1 i	Control failure, human error
1981	Electrical fire in switch room of propane cooling	NGL plant	Fire	Switch room of propane cooling	–	–	2 i	Human failure
1995	Berners fire	NGL plant	Fire	Burners	NGL	Physical damage (corrosion) of burner tubes	–	Failure control
1992	Vapor cloud explosion	NGL plant	VCE	NGL plant	Gas, NGL	Rupture & vent open	2 d	Human failure, mechanical failure
1990	Gas loss	NGL plant	Rupture	NGL plant	Gas, NGL	Loss of containment	1 d	Human error, control failure
1998	Explosion and car fire	NGL plant	Fire, explosion	–	–	Fuel accumulation	7 d	Control failure
2000	Fire and explosion in high gas compression	Gas Compression Station (GCS)	Fire, explosion	High gas compression	Gas	Physical damage, Loss of containment		Control failure
2000	Gas leakage	Gas Compression Station (GCS)	Leakage	Pipeline	Gas	Drain open,	1 d	Human error, mechanical failure
2001	Well Blowout	Drilling	Blowout	Well	Oil, gas	Excessive pressure	1 d	Control Failure, human error
1993	Electrical fire of D.C room	Distillation plant	Fire	Unit	Electrical board	Electrical failure	1 i	Electrical failure, human failure
1991	Electrical fire of high voltage D.C room	Oil booster station	Fire	High voltage D.C room	–	Welding and cutting ignition	–	Human error
1989	Car accident	Transportation	Car accident	–	–	Driving without permission	1	Human error, control failure
1989	Minibus accident	Transportation	Car accident	–	–	Overcome	3	Human failure
1992	Muck trailer accident in well location	Transportation	Car accident	Well	Oil	Parking a muck trailer in sharp ramp	1	Human failure
1993	car accident and fire	Transportation	Car accident, fire	–	–	Deviation to left side	1	Human failure
1985	Fire caused by bulldozer crash with 10″ pipeline	Transportation	Fire	Pipeline	Oil	Physical damage	–	Human failure, control failure

1992	Fire caused by bulldozer crash with 16″ pipeline	Transportation	Fire	Pipeline	Oil	Physical damage	–	Human failure, control failure
1990	rig carrying trunk accident	Transportation	Truck accident	–	–	Deviation	–	Human failure
2000	Coil tubing truck accident	Transportation	Truck accident	–	–	Deviation	–	Human failure
1999	Operation pipeline fire	Transportation	Fire	Pipeline	Oil	Deviation	1 d	Human failure
	Crane boom crash with high voltage wire	Transportation	Crane crash with high voltage wire	–	–	Crash with high voltage wires	1 d	Human failure
1985	Chlorine leakage	Water treatment plant	Chlorine leakage from cylinder	–	–	Seal leak, physical damage	–	Mechanical failure, control failure
1981	Pharmaceutical storage (supply) fire	General accident	Fire	Water treatment plant	Pharmaceutical Chemical	Reaction	–	Control failure, human error
1996	Chemical storage fire	General accident	Fire	Storage	Chemical	Spontaneous ignition, reaction	–	Utility failure and human error
1996	Storage fire	General accident	–	Storage	–	Smoking ignition		Control failure, human

Figure 1. Comparison of major accidents in Middle Eastern case (blue) with world accidents (red) in the oil and gas industry percentages of different scenarios. (LOCA: Loss of containment; F: Fire; EX: Explosion; BLEVE: boiling liquid expanding vapor explosion; IE: internal explosion; TOX: toxic release; VCE: vapor cloud explosion; VCF: vapor cloud fire; VEEB: vapor escape into, and explosion in, building, B: blowout).

It needs to be noted that the conditions may be different in this case as compared to other countries.

Initiating events or major causes in both cases are plant failure e.g. equipment failure, process problems, material movement problems, control failure (ineffective loss prevention program, inadequate material evaluation). Major contributing factors or intermedidate events in this industry are formed by the human element, faulty design, long replacement times and inadequate explosion relief (Sam, 2005).

It is obvious that incidents like pipeline leakage occur more frequently than has been reported.[1] This report contains accidents with consequences being injuries, fatalities, or damage to property, while accident documentation should also include incidents or near-misses without major consequences. Unlike accidents with significant material or personal damage, near misses and smaller incidents are much harder to discover, even though they may be caused by the same conditions and therefore be represented by exactly the same scenarios. Identifying specific holes in barriers requires more details of input rather than was usually reported here.

Loss of containment is the most frequent scenario type in this case. Pipelines have considerable potential for accident in this industry. The frequency of incidents in this part of utility are the highest (Ghazinoory & Kheirkhah, 2008). There

[1]In the personal experience of one author (PH) in another ME country, the difference between the ME and worldwide frequencies of LOCA and fire and explosion may be due to the availability of considerable space on site, resulting in longer lines for leakage exposure, but less chance of ignition or of achieving the critical stochiometric ratio.

are some reasons. Firstly, these cases have very long pipelines as part of their plant. For example, one such oil and gas plant has almost 5000 km of pipeline. Considering 5 similar plants in this region, the total length of pipeline might be as much as 25000 km. Maintaining and repairing such a wide-spread network of pipelines needs considerable effort by operations, plant management and adequate financing. Defects in any one of those factors have the potential for an incident with catastrophic consequences. Secondly, the crude oil in this plant contains H_2S, and CO_2 either of which cause acidity and thereby increase corrosion. Finally, all pipelines have a limited useful life. They should be in limited service but because of a number of limitations, these pipelines were often not replaced and have had to continue in operation after their useful design life.

Sharing of past major incidents with other oil and gas industries provides useful input data for similar process industries in order to identify the most critical barriers and improve their safety processes. One poignant example highlights this matter. In 1998 there was an accident in the gas compression stage of a Middle East oil and gas plant which caused 7 dead as a result of fuel accumulation and vapor cloud explosion which was very similar to the Texas City Refinery disaster on March 23, 2005 in which a distillation tower was overfilled and an uncontrolled release of hydrocarbons led to a major explosion and fires. Fifteen people were killed and 180 were injured in the worst disaster in the United States in a decade. In both incidents, excess hydrocarbons were diverted into a pressure relief system that included a blowdown stack. In the Iranian case, it was equipped with a flare, but one which the operator didn't ignite; in Texas City the blowdown stack was not equipped with a flare to burn off hydrocarbons as they were released. As a result, the flammable overflow from the tower entered the atmosphere. Ignition of the escaped hydrocarbons was enabled by startup of a nearby vehicle resulted in the explosion and subsequent fires (Hopkins, 2008). This example shows the repetitive patterns of accidents, and root causes of events all over the world in this sector. The lesson of this paper is that accidents in one country, where the scenarios are very similar, can and should serve as lessons to prevent the same scenario being actualized in other countries.

5 CONCLUSION

In summary, the existence of scenarios is an aid to the reduction of uncertainty. They provide a way of dealing with different aspects of a problem simultaneously; unlike specifically technical failure analyses, such as FMEA, scenarios allow for a combination of the heterogeneous factors that experience shows actually describe how accidents happen. By using scenarios, the analyst might be able to explore systematically and managers and stakeholders encouraged to think about new possibilities (Wack, 1985).

Oil and gas plants form a major strategic industry all over the world. Every country has confidentiality about public reporting about or even reporting the occurrence of accidents and this is one contributing factor for repeating accidents with the same root or contributing causes in other plants. As Hopkins (2008) mentioned, failure to learn occurs even though there is a "depressing sameness" in the scenarios. It is more unfortunate that this failure continues to happen, even in developed industries which documented and published their earlier failures (Hopkins, 2008). It is better to start to think about accidents in another perspective. Blaming people and considering the technical casues of accidents in isolation is a blind alley for the prevention of accidents. It is necessary to consider the role of other important factors such as culture, organization decision making and management in different level of company. All of these are factors that can be captured in the scenarios that do not necessarily contain specific individuals or machinery, but rather emphasize the overall structure of causal conditions and sequences that lead to incidents or even catastrophes As an example of how to improve matters such as information sharing it is noted that the oil and gas companies has started to have a complete incident database or at least incident investigation reports with more precise and complete information (NISOC, 2011).

REFERENCES

Fecht, B.A., Gates, T., Nelson, K., & Marr, G., 1982. *Comparative safety analysis of LNG storage tanks*. Washington: Richland.

First, K., 2010. Scenario identification and evaluation for layers of protection analysis. *Journal of Loss Prevention in the Process Industries,* 23(6): 705–718.

Ghazinoory, S., & Kheirkhah, A.S., 2008. Transportation of hazardous materials in Iran: A strategic approach for decreasing accidents. *transport*, 23(2), 104–111.

Go, K., & Carroll, J.M., 2004. The blind men and the elephant. *interactions,* 11(6): 44–53.

Guerrero, C.V.S., Vieira, M.F.Q., Mercantini, J.-M., & Santoni, C., 2008. A Process for Human Centered Modelling of Incident Scenarios. In A. Holzinger (Ed.), *HCI and Usability for Education and Work*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Hopkins, A., 2008. *Failure to learn: the BP Texas City Refinery disaster*. CCH Australia Limited.

Khan, F.I., & Abbasi, S.A., 1999. Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries,* 12(5): 361–378.

Mohammadfam, I., Sajedi, A., Mahmoudi, S., & Mohammadfam, F., 2012. Application of Hazard and Operability Study (HAZOP) in Evaluation of Health, Safety and Environmental (HSE) Hazards. *International Journal of Occupational Hygiene,* 4(2): 69–72.

NISOC, 2011. *Survey of Accidents in National South Iranian oil company* Ahwaz, Iran: NISOC.

Sam, M., 2005. *Lees' Loss Prevention in the Process Industries*. Elsevier.

Wack, P., 1985. Scenarios: uncharted waters ahead. *Harvard Business Review,* 63(5): 72–89.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Analysis of roadside safety barrier using numerical model

P. Hradil, J. Kala & V. Salajka
Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT: This paper describes the process by which numeric simulation was recently used to carry out conceptual development of a new temporary protective barrier. An extensive use was made of the non-linear explicit dynamic finite element simulation code LS-DYNA to identify and correct design flaws early in the concept development stage. After arriving at what was considered to be a viable system design, full scale physical crash testing will be carried out to verify the successful performance of the system.

1 INTRODUCTION

Over the past decade, the roadside hardware design process has changed substantially as non-linear dynamic Finite Element Analysis (FEA) has found increasing application. A substantial portion of conceptual design can now be performed using computational simulation rather than experimental testing. The presented paper deals with the analysis of dynamic responses of a noise damping wall to actions of wind as well as to the impact of a vehicle (Hradil et al. 2009). The response to the vehicle impact has been analyzed using a specially elaborated complex computational model, comprising both the nonlinear model of the damping wall and the detailed model of the vehicle (in accordance with EN-1317).

In the past, the development of new roadside safety hardware systems such as railings, barriers, and energy absorbing crash cushions typically required iterative cycles of conceptual design and full scale vehicle crash testing. Much of the conceptual design process was based on sound understanding of engineering and mechanics principles, previous development experience, and intuition. However, with only these tools available, several cycles of concept development and crash testing were usually required to arrive at a successful design. Given the setup time and costs involved in full scale crash testing, and the matrix of testing conditions that must be examined for system approval, this process can be quite costly as well as time consuming. Over the past decade, the roadside hardware design process has changed substantially as non-linear dynamic Finite Element Analysis (FEA) has found increasing application. A substantial portion of conceptual design can now be performed using computational simulation rather than experimental testing (Farnama et al. 2010). Such use of simulation can result in more rapid system development, improved system performance, and reduced development costs. Ultimately, such systems must still be subjected to full scale crash testing to validate and certify their integrity (Consolazio et al. 2003). However, far fewer cycles of development and testing are required if simulation results can be relied upon to identify design flaws that degrade system performance (Adhikary et al. 2012). This paper describes the process by which numeric simulation was recently used to carry out conceptual development of a new temporary protective barrier. An extensive use was made of the non-linear explicit dynamic finite element simulation code LS-DYNA to identify and correct design flaws early in the concept development stage (Kala et al. 2012, Kochavi et al. 2008, Markovich et al. 2011). After arriving at what was considered to be a viable system design, full scale physical crash testing will be carried out to verify the successful performance of the system.

2 DESCRIPTION OF THE DESIGNED MOBILE ANTI-NOISE WALL

The designed mobile antinoise wall system with a length of 36 m involves reinforced concrete anchoring blocks, steel columns with HE 160B cross-sections and antinoise panels of the type SILENT. The anchoring blocks of the designed MAW system have a length of 4 m, see Figure 1.

Both their shape and their in-line arrangement resemble the reinforced concrete crash barrier system. Anchoring blocks are mutually constrained through steel locking pieces, see Figure 3. In the upper part, the anchoring block is provided with a steel clamping piece anchored in the concrete by four shaped steel members, shown in Figure 2.

The clamping piece is designed to fix the steel column HE 160B which (together with the neighboring column) is bearing the antinoise panel. Four bolts are designed to fix the column. The ana-

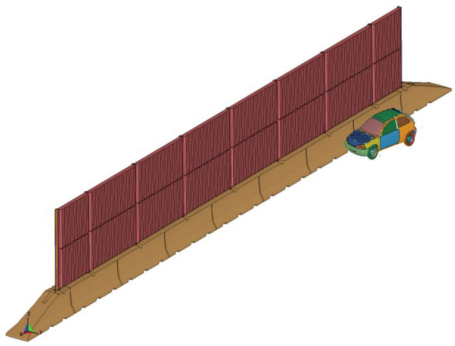


Figure 1. Computation model of the mobile antinoise wall and a vehicle.

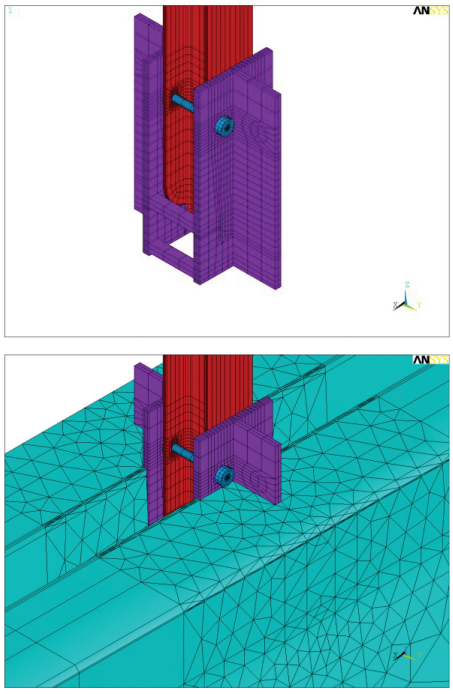


Figure 2. Detail view on designed joint.

lyzed system consists of two terminal anchoring blocks and seven intermediate blocks.

3 CONTINUOUS SURFACE CAP MODEL

The concrete model was primarily developed to simulate the deformation and failure of concrete in roadside safety structures impacted by vehicles. Examples are bridge rails and safety barriers.

The concrete model is commonly referred to as a smooth or continuous surface cap model.

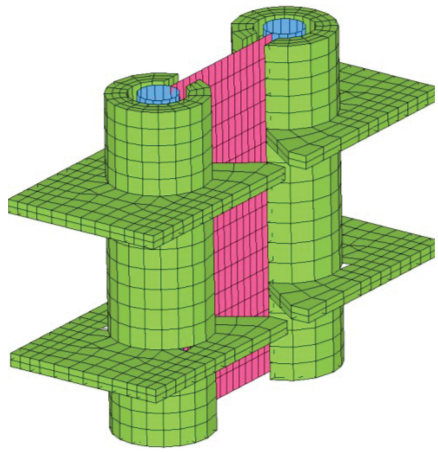


Figure 3. Detail of the block locking piece.

Hence, the 159 model is used for a Continuous Surface Cap Model (Murray 2004, Schwer & Murray 2002). A smooth and continuous intersection is formulated between the failure surface and the hardening cap.

Concrete structures typically contain steel reinforcement. Steel reinforcement exhibits rate effects and yields in a ductile manner until it breaks at an ultimate strain greater than approximately 20 percent. The reinforcement model plays an important role in modeling reinforced concrete behavior (Holomek & Bajer 2012, Jiang et al. 2012). Our approach is to explicitly model the reinforcement (beam elements) separately from the concrete (hex elements) using an elasto-plastic material model with yielding, hardening, rate effects, and plastic strain-based failure.

4 COMPUTATION MODEL OF THE MOBILE ANTINOISE WALL—VEHICLE SYSTEM

The dynamic analysis of the designed mobile antinoise wall has been carried out applying an advanced computation model based on the Finite Element Method. The model has been developed as a spatial non-linear model respecting all substantial structural details of the MAW system. However, various imperfections and gaps due to both manufacturing and assembling process have been neglected. The computation model assumes that anchoring blocks of the MAW system are freely supported on a horizontal plane. Horizontal displacements of blocks are modeled assuming contacts with friction. Non-linear material properties have been considered. Deformation behavior of steel has been described assuming

bilinear kinematic hardening. This concerns structural elements such as block locking pieces, clamping pieces of columns and reinforcing steel bars in blocks. The deformation properties of the concrete of anchoring blocks have been described using a special model developed for the analysis of reinforced concrete crash barriers (Murray 2004). The computation model of the vehicle used in the crash test simulation has been selected from the vehicle database. A light motorcar with the mass of 900 kg has been selected (Sharma et al. 2012).

5 RESULTS OF COMPUTATIONS

The impact of the vehicle on the mobile antinoise wall at the speed of 80 km·h^{-1} under the angle of 15 deg has been analyzed by computer simulation. At the instant of impact, the vehicle contacted the middle of the third anchoring block. The fields of displacements, deformations and stresses of the modeled structures have been computed at discrete time instants. A detailed analysis has been carried out with respect to lateral displacements of anchoring blocks and antinoise panels. The effect of the influence of parameters on the results can be studied by methods of sensitivity analysis (Kala & Kala 2013). Also, a detailed stress analysis of structural elements of joints has been performed.

The analysis has shown that the designed mobile antinoise wall remains stable during and after the vehicle crash.

The maximum stresses appear in the block locking piece elements. Another exposed piece is the connection between steel elements of columns and steel elements anchored in concrete. The stress field in the observed structural elements is displayed in Figure 9. The equivalent stresses attain the level of mean yield stresses, however, the maxima of plastic deformations are well below the allowable limits.

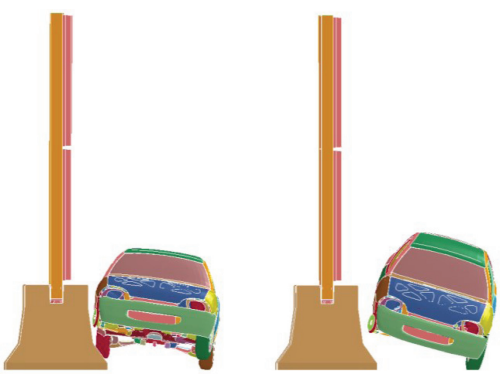


Figure 4. Positions of the vehicle with respect to the mobile antinoise wall (time 0.35 s and 0.60 s).

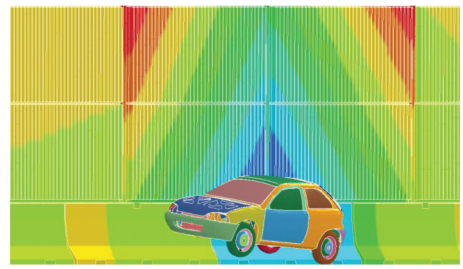


Figure 5. Lateral displacement of the wall, time 0.37 s.

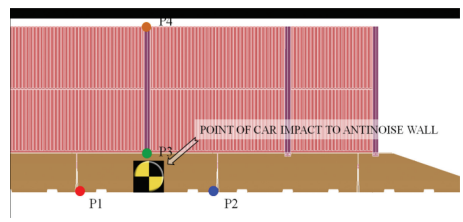


Figure 6. The scheme of simulation configuration.

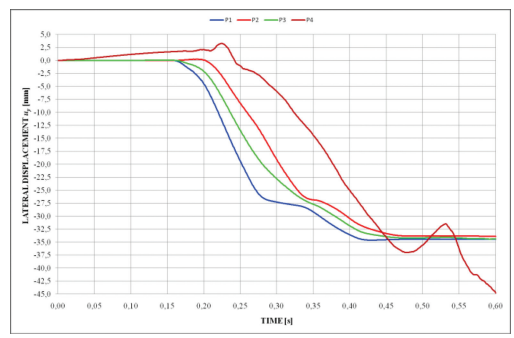


Figure 7. Time history of lateral displacements of points shown in Figure 6.

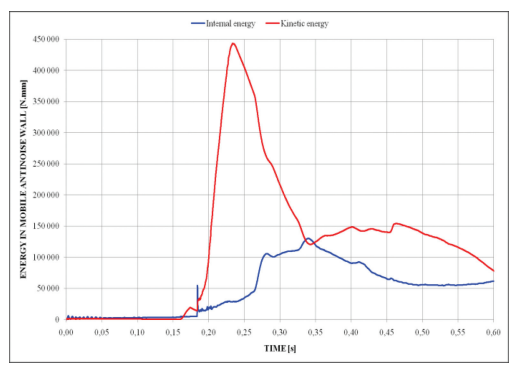


Figure 8. Time history of progression of internal (blue) and kinetic (red line) energy in the mobile antinoise wall.

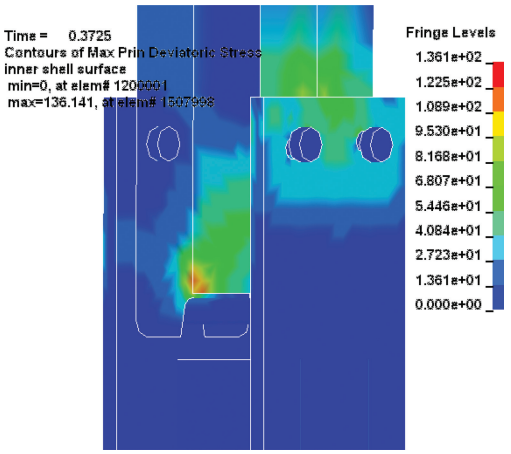


Figure 9. Equivalent stress at the mobile antinoise wall.

Now, the progression of kinetic and internal energy of the vehicle and antinoise wall in time can be determined. The time history of progression of internal and kinetic energy in the antinoise wall is illustrated in the graph in Figure 8. The time of the vehicle impact and the rapid energy change occur in the time of 0.19 s.

6 CONCLUSIONS

An advanced detailed non-linear computation model of the mobile antinoise wall has been used. The computation model of the motorcar has been selected from the database of test vehicle models. The analysis has been carried out using a specially developed procedure. Fulfilling certain specified criteria, the computer analysis substitutes the actual impact test of the vehicle crashing into the restraint system. Following the results of computations, the construction details of the mobile noise damping wall structure have been properly modified. Advanced is a method of global sensitivity analysis that allows us to analyze the higher order interaction effects.

ACKNOWLEDGMENT

This outcome has been achieved with the financial support of the project of GACR 14-25320S “Aspects of the use of complex nonlinear material models”.

REFERENCES

Adhikary, S., Li, B. and Fujikake, K., 2012. Dynamic behavior of reinforced concrete beams under varying rates of concentrated loading, *International Journal of Impact Engineering*, 47, 24–38.

Barnat, J. & Bajer, M. & Vyhnankova, M., 2012. Bond strength of chemical anchor in high-strength concrete, *Procedia Engineering*, 2012(40), 38–43, DOI: 10.1016/j.proeng.2012.07.052.

Consolazio, G.R., Chung, J.H. and Gurley K.R., 2003. Impact simulation and full scale crash testing of a low profile concrete work zone barrier, *Computers and Structures*, 1359–1374.

European Standard EN-1317 Test Vehicle Models, CM/E Group—Politecnico di Milano, Italy.

Farnama, Y., Mohammadib, S. and Shekarchia, M., 2010. Experimental and numerical investigations of low velocity impact behavior of high-performance fiber-reinforced cement based composite, *International Journal of Impact Engineering*, 37(2), 220–229.

Holomek, J. and Bajer, M., 2012. Experimental and Numerical Investigation of Composite Action of Steel Concrete Slab. *Procedia Engineering*. 2012(40), 143–147, ISSN 1877-7058, DOI: 10.1016/j.proeng.2012.07.070.

Hradil, P., Salajka, V. and Vymlátil, P., 2009. Assessment of the stability of the mobile antinoise wall, Technical report.

Jiang, H., Wang, X. and He, S., 2012. Numerical simulation of impact tests on reinforced concrete beams, *Materials & Design*, 39, 111–120.

Kala, J., Salajka, V. and Hradil. P., 2012. Sensitivity Investigation of eigenvalue problem of water tower construction interacting with fluid, *Journal of Vibroengineering*, 14(3): 1151–1159, ISSN 1392-8716.

Kala, Z. and Kala, J., 2013. Uncertainty and sensitivity analysis of beam stability problems using shell finite elements and nonlinear computational approach. *Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures—Proceedings of the 11th International Conference on Structural Safety and Reliability, ICOSSAR 2013; Proc. intern. conf.* New York,16–20 June 2013.

Kochavi, E., Kivity, Y., Anteby, I., Sadot, O. and Ben-Dor, G., 2008. Numerical model of composite concrete walls, in: *Proceedings of the 9th Biennial ASME Conference on Engineering Systems Design & Analysis, ESDA2008*, Haifa, Israel.

LS-Dyna User manual, 2007. Version 971, Livermore Software Tech. Corp., Livermore, California, USA.

Markovich, N., Kochavi, E. and Ben-Dor, G., 2011. An improved calibration of the concrete damage model, *Finite Elements in Analysis and Design*, 47(11), 1280–1290.

Murray, Y.D., 2004. Theory and Evaluation Concrete Model 159, *8th International LS-DYNA Users Conference*, Detroit.

Sahraei, E., Digges, K., Marzougui, D. and Roddis, K., 2014. High strength steels, stiffness of vehicle front-end structure, and risk of injury to rear seat occupants, *Accident Analysis & Prevention*, 66, 43–54.

Schwer, L.E., Murray, Y.D., 2002. Continuous Surface Cap Model for Geomaterial Modeling: A New LS-DYNA Material Type, *8th International LS-DYNA Users Conference*, Detroit.

Sharma, H., Hurlebaus, S. and Gardoni P., 2012. Performance-based response evaluation of reinforced concrete columns subject to vehicle impact, *International Journal of Impact Engineering*, 43, 52–62.

TP 159 Guiding walls. 2003. Technical specifications, classification, requirements and application.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Developing a framework for characterising cascading failures in past events to inform emergency response decisions

H. Hassel, A. Cedergren & L. Svegrup
Division of Risk Management and Societal Safety, Lund University, Sweden
Lund University Centre for Risk Assessment and Management (LUCRAM), Lund University, Sweden
Centre for Societal Resilience, Lund University, Sweden

J. Johansson
Division of Industrial Electrical Engineering and Automation, Lund University, Sweden
Lund University Centre for Risk Assessment and Management (LUCRAM), Lund University, Sweden
Centre for Societal Resilience, Lund University, Sweden

ABSTRACT: Increasing interdependencies between critical infrastructures have made these systems more effective, but also more susceptible to cascading failures. In order to reduce the likelihood and consequences of cascading failures, it is essential to develop tools that support incident commander decisions so that an initial failure does not spread to other infrastructures. Here, a framework for generating knowledge from previous events that can feed in to such a tool is outlined. Design science is used to this end which provides a transparent and systematic approach. Moreover, the paper presents an analysis of existing empirical approaches focusing on identifying methodological aspects that can influence the framework. Although further work is needed, the work presented in this paper shows a promising first step to accomplish such a framework.

1 INTRODUCTION

Critical infrastructures and critical societal functions, such as energy supply, water distribution, and communication services play a key role in forming resilient[1] communities, regions and nations (O'Rourke 2007). By ensuring that infrastructures and societal functions can absorb and withstand hazardous events (including natural, mad-made or intentional) and recover quickly from emergencies and disasters, the societal impacts on communities and regions can be drastically reduced. In several past events damages to critical infrastructure and societal functions have significantly contributed to the negative consequences of those events, such as the WTC attacks in 2001 (Mendonca & Wallace 2006) Hurricane Katrina (Boin & McConnell 2007; Leavitt & Kiefer 2006) and the Canadian ice storm in 1998 (Chang et al. 2007).

Over the last decade there has been a growing realisation of the role played by interdependencies between infrastructures (Aven & Renn 2010; OECD 2003). Interdependencies between infrastructures are currently growing, much due to the technological development that allows for more systems to be interconnected. This generally gives rise to more effective and efficient infrastructures and societies but also opens for more widespread and cascading failures to arise in case of infrastructure breakdowns (Rinaldi et al. 2001; Zimmerman 2001).

Research in the field of infrastructure interdependencies and cascading failures, where a cascading failure is seen as a failure in one infrastructure/societal function[2] that gives rise to a failure in another infrastructure/societal function, is currently growing.[3] A large part of this research is devoted to developing new methods

[1]There are different accounts on what constitute resilience but at the least it constitutes the robustness, i.e. the ability to absorb and withstand shocks, and recovery or rapidity, i.e. the ability to quickly restore any disruptions in the functions and services that a system provide (McDaniels et al. 2008).

[2]Although the concept of critical infrastructure often is broadly defined to include both physical networks, e.g. transportation, and more social/societal functions, e.g. emergency services and governmental services, the term to is more commonly associated to physical assets or systems in practice. Therefore, this paper also uses the term critical societal functions to emphasize that the interest here is not only on the more physically-related systems.

[3]A search, dated 2014-02-17, on the online database Scopus (www.scopus.com) on the keywords "infrastructure*" AND "interdependenc*" gives 965 hits. From 1997–2002 the hit rate is about 10–15 per year whereas since then it has gradually increased to around 100–120 hits per year.

and approaches for analysing infrastructure interdependencies in order to better understand cascading failures and their effects, and to increase the ability to estimate societal impacts. The reviews presented by Ouyang (2013), Satumtira & Duenas-Osorio (2010), Griot (2010), Pederson et al. (2006) and Johansson et al. (2013) show that there are several different types of approaches available in the literature. Most of the approaches are forward-looking in the sense that hypothetical scenarios are modelled using e.g. economic (Rose & Liao 2005; Haimes et al. 2005), system dynamics (Stapleberg 2008; Min et al. 2007), agent-based (North 2001; Dudenhoeffer et al. 2006.), expert-based (Chang et al. 2013) or hybrid models (MaKenzie et al. 2012; Johansson et al. 2013).

Another group of approaches is the empirical ones where the focus is to analyse past events in order to identify and characterise interdependencies. These approaches are either those where methodological frameworks for analysing past events are presented (e.g. McDaniels et al. 2007) or those that are restricted to analysis of a single or a few past events (Chang 2000; Bigger et al. 2009).

Surprisingly, analyses of past events to find out the frequency and characteristics of cascading failures are scarce, as pointed out by van Eeten et al. (2011). However, insights about past events can lay a foundation for a better understanding of infrastructure interdependencies and likely future cascading failures. This kind of knowledge has many benefits. First, it is crucial in a proactive perspective in order to design-in or increase the resilience of a community or a region. Without accounting for possible cascading failures any resources devoted to increasing resilience, e.g. by increasing the resilience of a specific infrastructure, would be sub-optimal. Second, knowledge about likely cascading failures is very useful in the emergency response phase or a disaster, since this knowledge can be used to inform emergency response decisions of how to effectively mitigate the consequences of an ongoing event. Such decisions could for example concern which, of many, infrastructure services to protect; with the purpose of stopping downstream effects of service disruptions. The decisions made by the emergency responder are likely to have a greater chance of success, in terms of stopping or limiting the cascading failures and/or their societal effects, if they are well informed.

The research presented in this paper addresses the latter perspective, i.e. informing decisions in the response phase. More specifically, this paper aims to develop a framework that can be used to study past events with the purpose of identifying and characterising cascading failures as well as the effects of contextual factors on such failures. Such knowledge should then for example be possible to use in an incident decision support tool[4] in order to inform and therefore hopefully improve the decisions taken by emergency responders so that the risks of cascading failures are reduced.

2 A DESIGN SCIENCE APPROACH

Development of a framework for characterising cascading failures constitutes a design science activity. Hevner et al. (2004) argue that design science is composed of two consecutive activities: Construct and Evaluate. Construct refers the development of an artefact (such as a framework) and Evaluate refers to finding out, preferably through practical applications, whether the constructed artefact has the intended effect (i.e. fulfils its purpose). Typically, the Construct and Evaluate activities are performed in several loops in order to refine the artefact. This paper will mainly be limited to the Construct step and leave the full scale practical applications and systematic evaluations for future research.

The Construct step will be performed by adopting the design hierarchy proposed by Rasmussen (1985) and applied in e.g. Cedergren & Tehler (in press) Palmqvist & Tehler (2014), Abrahamsson & Tehler (2013). This design hierarchy describes artefacts on three levels of abstraction, which in the next sections will be used as a point of departure for constructing the framework. On the first level the *Purpose* of the framework will be described which is a statement of *why it exists/is needed*. This also includes what the framework should be used for and as such any user requirement or constraints should also be specified. On the second level the *Functions* of the framework should be specified which are statements of *what it should be able to do* in order to fulfil the purpose. Finally, the third level constitutes the *Form* of the framework which is simply *how it is actually designed*.

Typically, developing a concrete form of an artefact is facilitated by good knowledge of existing similar artefacts as the one to be developed (Tehler & Brehmer 2013). Therefore, this paper will also make a systematic analysis of the existing empirical methods and frameworks for characterising and analysing cascading failures. This will be done by first analysing whether the existing methods contain or address the functions specified for the framework; and in case they do, consideration

[4]Note that the framework developed here is part of an EU research project called CascEff, which has as an overall aim to develop an Incident Evolution tool that can be used proactively for increasing emergency preparedness and during emergency response as a decision support tool.

of whether these methodological features can be used or influence the design of the framework.

By making sure there is a logical chain from purpose to function to form the likelihood of successfully developing a framework is likely to increase. However, at the same time, it is important that the framework is systematically evaluated though practical applications so that it is ensured that it actually fulfils its purpose (has the intended effect). But, as mentioned previously, the full scale application and evaluation will be addressed in research to come.

3 PURPOSE OF THE FRAMEWORK

The overall purpose of the framework proposed in this paper is that it should generate generalised knowledge about cascading failures that can be used to inform decisions made in the response phase of an emergency. Such knowledge would enable the emergency responders to take actions that account for likely cascading failures and their effects, and hence, increase their potential to interrupt or alleviate them and thus mitigating the societal consequences.

The knowledge about cascading failures should be generated based on past events. However, since each emergency is unique it must be possible to extrapolate the findings concerning a cascading failure from one context, i.e. the one defined by the context of the past event, to another context, i.e. the one defined by an ongoing or hypothetical future event. Finally, the framework should be general, in terms of being applicable independent on the event type, and practical in terms of being able to generate knowledge with limited time and resources.

4 FUNCTIONS OF THE FRAMEWORK

Based on the purpose and constraints described above the following functions can be defined which specifies that the framework *should be able to support* the:

1. *Selection of initiating event*[5] *types to consider*—this is important since what types of events to consider will affect the types of cascading failures and contexts that will be covered, which in turn will affect which decision contexts the generated knowledge can be used in.
2. *Selection of initiating events that includes cascading failures*—this is important since the specific initiating events of interest here are those where cascading failures played a major role.
3. *Identification of cascading failures to include*—this is important since a prerequisite for learning from a cascading failure is to identify and find necessary information about them. Also some cascading failures may not be relevant to include e.g. due to their insignificance, or that they are irrelevant to emergency response decisions.
4. *Characterisation of cascading failures*—this is important since information about characteristics of cascading failures, e.g. severity of societal impacts, rapidity of effects, are necessary to provide a sensible decision support, e.g. to enable ranking of decision alternatives.
5. *Characterisation of contextual factors*—this is important since information about context is necessary to enable extrapolation of the findings from one context to another, i.e. whether a particular observed cascading failure would occur in another context.
6. *Inferences about the significance of the cascading failures*—this is important since in order provide sensible decision support in emergency response, collected data must be analysed so that inferences regarding the significance or criticality of cascading failures and/or infrastructures/societal functions can be made.
7. *Inferences about the effect of contextual factors on cascading failures*—this is important since being able to extrapolate from one context to another requires an understanding of how changing contexts are likely to affect the characteristics of cascading failures.

5 ANALYSIS OF EMPIRICAL APPROACHES

In this section, existing empirical approaches will be analyses from the perspective of identifying whether they address the functions described in the previous section; and if that is the case, a brief description of how this function is designed (the form) will be made. This will then be used as input when discussing the form of the framework developed in this paper (see section 6).

In Table 1 the analysis of existing approaches is presented. The empirical approaches addressed here are the following:

1. The framework for characterising Infrastructure Failure Interdependencies, IFI, suggested by a research group at the University of British Columbia (McDaniels et al. 2007; Chang et al. 2007; Chang et al. 2009). The intention of this

[5]An initiating event is seen as the starting point for possible downstream cascading failures, either an external events, such as ice storms, tsunamis, and earthquakes, or internal events, such as electric power blackout or rupture of a water main.

Table 1. Analysis of whether and how the seven functions have been addressed in existing empirical approaches.

	Function						
Approach	1. Selection of initiating event types to consider	2. Selection of events that include cascades	3. Identification of cascading failures	4. Characterisation of cascading effects	5. Characterisation of contextual factors	6. Inferences about significance of cascades	7. Inferences about the effect of context
McDaniels et al., 2007; Chang et al., 2007; Chang et al. 2009	No explicit guidance, but primarily restricted to large-scale power outages	No explicit guidance, limited number of events have been analysed—chosen based on their large-scale consequences.	Keyword search in media accounts, within three months, inclusion/exclusion criteria in manual reading.	Impacted system, type of interdependency, type of failure, order, Societal consequences: e.g. severity, spatial extent, no. of people affected.	Primary power outage: date, description of event, initiating event type, spatial extent, duration, weather conditions, and temperature.	Aggregation over events: e.g. 1) differences in societal impacts in different events. 2) Relative freq. of cascades between sectors	Comparative studies where differences in cascades and societal impacts are compared to differences in context—qualitative arguments.
Rahman et al. (2009)	No explicit guidance. Wide range of computer related failure reports were used, but not sorted on the basis of initiating events.	347 of 10 000 cases selected, where failure originated from, or affected, Communication and Information Infrastructure (CITI)	See 2. Failures originated from, or affected, Communication and Information sector were chosen.	Scale and degree of impact, fault intent, duration, financial impact, public safety, affected sites, description, source/affected infrastr.,	Date and country	Percentages e.g.: per fault type, intention, impact distribution, failure leading to CITI failures infrastructures affected by CITI failures.	Statistical analysis (see 6)
Zimmerman, Restreop et al. (2006)	No explicit guidance, but electric power outages are in focus.	No explicit guidance. Uses a database with no reference on how the events were selected.	Initiators and targets of failures counted as pairwise infrastructure coupling.	Metrics for characterisation of 1) Coupling 2) Cascades as sequence of failures over time	No explicit guidance	Ratios of caused vs. affected infrastr. and durations of outages for initiated/affected infrastr.	No explicit guidance
Van Eeten et al. (2009)	No explicit guidance	No explicit guidance	Google news search and official governmental or sector reports. Number of people affected more than 10 000.	Events that initiate cascades. Events that are result of a cascade. Independent events. An indication of the consequences and impact.	Several factors, e.g.: Affected CI, sector, and organisation init. event, start/end time, spatial extent, duration/progress of recovery.	Number of events, percentage of cascade initiating, cascade resulting, and independent for each sector. Directionality of cascades.	No explicit guidance

Mendonca et al. (2004)	No explicit guidance	No explicit guidance	No explicit guidance	From media reports: Type of interdependency. Number of cascades in different time phases.	No explicit guidance	Number and the percentage of infrastructure disruptions in the time phases. Number of interdep. disruptions.	No explicit guidance
Tsuruta et al. (2008)	No explicit guidance, earthquakes are addressed but approach is general	No explicit guidance, two events chosen based on their large-scale consequences	Based on literature, hearings and visits, but no details are given	Classification of terminal and origin infrastructures; in three time phases: immediate, response, restoration	No description	Number of cases where failures has cascaded between different sectors, also for different time phases	No explicit guidance
Bigger et al. (2009)	No explicit guidance, hurricanes hitting Florida during 2004 selected.	No explicit guidance, Selection of events was made beforehand.	All intra-dependencies within a CI, and interdependencies between and among CIs. Based on interviews with utilities.	First to higher-order dependencies, hurricane impact, event sequences, upstream/down-stream dependencies, recovery and restoration.	Operations during emergency, priorities for service restoration. General information about each of the studied hurricanes.	"Sample matrices", e.g. some analyses of closed-loop interdependencies presented.	Factors influ-encing recovery: 1) limited knowledge about dependence on suppliers 2) analysis of equipment pre-position-ing sites.
Dueñas-Osorio and Kwasinski (2012)	No explicit guidance. Case study of 2010 Chile earthquake.	No explicit guidance.	No guidance. Based on data availability from TCLEE: power, potable water, telecommunication.	Time lag analysis of restoration processes (autocorrelations and cross-correlations of restoration curves)	Claims anecdotal data should be considered. Contextual factor described. No guidance regarding their effect.	No, only one case study.	No explicit guidance.

framework is to enable the identification of empirical patterns of infrastructure interdependencies primarily related to electric power-related failures.
2. The framework for studying interdependencies in the communication and information infrastructures domain suggested by Rahman et al. (2009).
3. The approach suggested by Zimmerman and colleagues where quantitative metrics are suggested to characterise interdependencies (Zimmerman & Restrepo 2006; Restrepo et al. 2006).
4. The approach suggested Van Eeten et al. (2009) in their systematic review of cascading failures, primarily focusing on the Netherlands.
5. The approach used by Mendonca et al. (2004) where the focus was on the assessment of infrastructure disruptions following the WTC attack.
6. The approach used by Tsuruta et al. (2008) where the focus was on the Kobe and the Mid Niigata earthquakes in Japan.
7. The approach used by Bigger et al. (2009) who studied the effect of interdependencies in a number of U.S. Hurricanes.
8. The approach used by Dueñas-Osorio & Kwasinski (2012) who conducted a case study on an earthquake in Chile using a statistical approach.

In summary, the approaches vary in their focus and how they treat the different functions. Few approaches support the choice of type and specific events to address, rather this is typically chosen ad hoc with no "higher goal" in mind (such as generalisability). All approaches identify cascading failures, often based on media accounts, but the characterisation varies greatly from description of a large range of factors to just logging originating and affected infrastructure/function. A few approaches consider contextual factors, but without any explicit account of the reason for choosing a particular set of factors. All approaches do something to draw conclusions regarding significance but this varies from accounting for societal impacts to counting number of times an infrastructure/societal function has been involved in a cascading failure. Finally, none of the approaches perform any systematic assessment concerning how the context affects the characteristics of cascading failures.

6 DISCUSSION ON THE FORM OF THE FRAMEWORK

In this section we discuss and reflect on different ways of designing the form of the seven functions specified for the framework. Whenever possible, this discussion draws on the ways these functions have been addressed in the empirical approaches analysed in the previous section.

6.1 *Selection of initiating event types to consider*

Typically the existing approaches do not provide any support for this function. Rather, the initiating events to consider are either given on beforehand, where only one or a few initiating events are assessed (such as in e.g. Mendonca et al. (2004) or Bigger et al. (2009)) or the initiating events are not distinguished (such as in e.g. Van Eeten (2009)).

In the present framework a number of criteria can be defined that can be used as a point of departure for selection of initial event types to consider. These include the following:

1. All events included must have occurred fairly recently so that the information can be seen as valid for contemporary conditions.
2. Information of the event must be easily retrievable, preferably written in English, to enable a feasible data collection process.
3. The full set of initiating events included must have a large diversity, in order to support decision in a broad range of emergencies.
4. The events must include an active role of emergency responders, since the decision support should enable choices between different action alternatives.

6.2 *Selection of initiating events that include cascading failures*

Based on the selection of initiating event types outlined in previous section, a selection of specific events should be made. With few exceptions, the existing frameworks do not address this function in great detail. In the present framework the following criteria are suggested for the selection of events:

1. The societal consequences should be significant in the event.
2. The events where cascading failures have significantly contributed to the societal consequences are selected. Those where this is not the case are logged so that e.g. inferences about probabilities of cascading failures can be made (in function 6).

These criteria will be evaluated based on reading overall accounts of the events. The overall accounts are judged to be enough to read at this stage since if it is not clear that the criteria are fulfilled based on them it is not likely the event will be relevant. Also, the set of selected events should collectively cover cascading failures occurring in all

critical infrastructures/societal sectors. These critical infrastructures/societal sectors can either be the originating or the affected infrastructure/sector.

6.3 *Identification of cascading failures to include*

This function is something all the existing approaches, as described in Section 5, deal with. Several of the approaches use media accounts to identify information about cascading failures due to the easy access of information. That of course enables a broader range of failures to be included, than if primary data would have been used, but it is somewhat unclear to what extent media provide accurate accounts. In the present framework any written material (media accounts, official investigations, previous research, etc.) will be used to find information about cascading failures. All cascading failures that are described will be selected, except those which do not *directly* give rise to significant societal impacts, and at the same time do not *indirectly* give rise to significant societal impact through a sequence of cascading failures. The following steps will be conducted:

1. First, automatic database searches will be conducted to find written accounts that are relevant for the particular event.
2. Each account will be manually read, focusing on title and abstract/summaries to identify those that potentially include information about cascading failures, which e.g. are those that primarily focus on consequences rather than causes of the events.
3. Detailed manual review of chosen accounts with the purpose of identifying cascading failures.
4. If a large number of accounts is still included after step 2, a stop criteria will be used which essentially states that when no or very few additional cascading failures are identified, then no additional accounts will be read.

6.4 *Characterisation of cascading failures*

The characterisations performed in the empirical approaches (described in Section 5) varies; some simply only describe the originating system and the affected system, some also describe in which time phase the cascading failure occurs, whereas some provide a fuller account of the cascading failure, including societal impacts (using various dimensions), type of interdependency and order of the dependency.

In the present framework the following characteristics of the cascading failures are suggested, which are chosen keeping in mind that the characterisation should be relevant for an emergency responder in the response phase:

1. Originating system
2. Affected system
3. Interdependency type
4. Time lag—i.e. time difference between failure in originating system and failure in affected system or time for restoration in originating system and affected system
5. Spatial lag—i.e. geographical distance between failure in originating system and failure in affected system
6. Duration—duration of failure in originating system, duration of failure in affected system
7. Service reductions—severity of service reduction in originating system, severity of service reduction in affected system
8. Societal effects—type and severity of societal effects due to service reduction in affected system.

These characteristics are chosen based on them being particularly relevant for decisions in the emergency response phase, e.g. when it comes to prioritisations.

6.5 *Characterisation of contextual factors*

Few of the empirical approaches (see Section 5) describe the contextual factors surrounding the initiating event or particular cascading failure. When this is done the focus is on describing the initiating event characteristics, weather conditions, etc. In the present framework, those characteristics that are possible for emergency responders to attain information about during the actual response phase should be described. A tentative list of what characteristics that are included in the present framework include, but is not limited to:

1. Weather conditions
2. Time of the year
3. Country
4. Urban/rural area
5. Available resources for response and restoration.

These contextual factors should be seen as a first suggestion that need to be further addressed. They are chosen based on them being relevant for and possible to characterise in the response phase of an accident.

6.6 *Inferences of about the significance of different cascading failures*

In the existing empirical approaches there is a large variation in the way that inferences have been drawn about cascading failures, but several of these have influenced the suggestion of how to design the present framework. More specifically,

the following types of analyses and result presentations will be made:

1. Relative frequency of an infrastructure/societal function being affected by another one (van Eeten 2011).
2. Relative frequency of an infrastructure/societal function affecting another one (van Eeten 2011).
3. Analysis/Aggregation of several cascading failures into chains and feedback loops (Bigger et al. 2009).
4. Probability of a particular cascading failure (also information about initiating events where cascading failures have not occurred, see 6.2).

6.7 *Inferences about the effect of contextual factors on cascading failures*

None of the existing frameworks do a systematic attempt to find out how the context will affect the characteristics of the cascading failure. Here two possible approaches will be considered and possibly adopted in a complementary way: a statistical approach and an expert-based approach.

In the statistical approach one would look at a rather large number of events to see whether it is possible to find statistically significant correlations between contextual factors and some cascading failure characteristics.

In the expert-based approach contrafactual reasoning is used to identify contextual factors of importance. Contrafactual reasoning has been employed in e.g. accident investigations (Snook 2002), in investigations of emergency response (Abrahamsson et al. 2010) and restoration (Wilhelmsson & Johansson 2009) and is about asking hypothetical questions such as "what if a the event occurred in the summer rather than the winter—how would that affect the characteristics of the cascading failures?". Obviously, this requires good knowledge about the systems of interest, why it is called an expert-based approach.

7 CONCLUDING REMARKS

In order to reduce the likelihood and consequences of cascading failures, it is essential to develop decision support for emergency responders to enable them to make informed decisions. The framework outlined in this paper will serve the purpose of identifying and analysing previous cascading failures that can feed in to such a decision support. In the development of this framework, significant inspiration has been drawn from design science. In particular, the concepts of Purpose, Function, and Form have been used to provide a structured approach to the process of setting up desired requirements and designing the framework. At this stage, the framework is still in its early stage of development, and further work is thus necessary. As a first step, the form of the framework needs further specification, e.g. by operationalising the different selection criteria suggested in the paper. This would for example include how to measure the significance of a cascading failure and the threshold for including a cascading failure in the analysis. In the next step, the framework will be tested on a smaller sample of events, which subsequently will be evaluated in relation to the way the purpose is fulfilled.

A challenge that is foreseen when applying the framework relates to handling situations where complete information about the characteristics of the cascading failure and the context is not available. In such situations other data sources may become necessary, e.g. conducting complementary interviews. Another challenge relates to using or developing a consistent terminology throughout the data extraction and classification process. As a starting point, though, it would be reasonable to adopt the terminology from the European Programme for Critical Infrastructure Protection (EPCIP).

Despite these remaining steps and challenges, the combination of the structured approach offered by design science and the valuable contributions from previous empirical research initiatives addressing cascading failures, the framework outlined in this paper points at a promising route towards generation of new generalised knowledge of cascading failures. This knowledge has a great potential for improving emergency responders' ability to manage emergencies that include the potential for cascading failures if they occur.

ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant agreement n° 607665.

REFERENCES

Abrahamsson, M., Hassel, H., & Tehler, H. 2010. Towards a System-Oriented Framework for Analysing and Evaluating Emergency Response. *Journal of Contingencies and Crisis Management* 18(1), 14–25.

Aven, T. & Renn, O. 2010. *Risk Management and Governance: Concepts, Guidelines and Applications*. Heidelberg: Springer.

Bigger, J.E., Willingham, M.G., Krimgold, F. & Mili, L. 2009. Consequences of critical infrastructure interdependencies: lessons from the 2004 hurricane season in Florida. *International Journal of Critical Infrastructures* 5(3): 199–219.

Boin, A. & McConnell, A. 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management* 15(1): 50–59.

Cedergren, A. & Tehler, H. in press. Stuyding Risk Governance using a Design Perspective. *Safety Science.*

Chang, S.E. 2000. Disasters and transport systems: loss, recovery and competition at the Port of Kobe after the 1995 earthquake. *Journal of Transport Geography* 8: 53–65.

Chang, S.E., McDaniels, T.L., Fox, J., Dhariwal, R., & Longstaff, H. (2013). Towards Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgements. *Risk Analysis* 34(3): 416–434.

Chang, S.E, McDaniels, T.L., Mikawoz, J. & Peterson, K. 2007. Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. *Natural Hazards* 41(2): 337–358.

Chang, S.E, McDaniels, T.L & Beaubien, C. (009. Societal Impacts of Infrastructure Failure Interdependencies: Building an Empirical Knowledge Base. *In Proceedings of TCLEE, Oakland, June 28–July 1, 2009.*

Dudenhoeffer, D.D., Permann, M.R. & Manic, M. (2006). CIMS: a framework for infrastructure interdependency modeling and analysis. *In Proceedings of the 2006 winter simulation conference*, *Perrone.*

Dueñas-Osorio, L. & Kwasinski, A. 2012. Quantification of Lifeline System Interdependencies after the 27 February 2010 Mw 8.8 Offshore Maule, Chile, Earthquake. *Earthquake Spectra* 28(1): 581–603.

Griot, C. 2010. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterization. *International Journal of Critical Infrastructures* 6(4): 363–379.

Haimes, Y.Y., Asce, F., Horowitz, B.M., Lambert, J.H., Asce, M., Santos, J. & Crowther, K. 2005. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. *Journal of Infrastructure Systems* 11(2): 67–79.

Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. *Management Information Systems* 28(1): 75–105.

Johansson, J., Svegrup, L. & Hassel, H. 2013. Societal consequences of critical infrastructure vulnerabilities: integrating power system and regional inoperability input-output models. *In Proceedings of European Safety and Reliability, ESREL 2013, Amsterdam.*

Johansson, J., Svegrup, L. & Hassel, H. 2013. *Studie och översiktlig utvärdering kring applicerbara metoder för komplex beroendeanalys på såväl sektoriell som tvärsektoriell nivå, Report 3177*. Lund: Lund University Center for Risk Assessment and Management (LUCRAM), Lund University.

Leavitt, W.M. & Kiefer, J.J. 2006. Infrastructure Interdependency and the Creation of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans. *Public Works Management & Policy* 10(4): 304–314.

MacKenzie C.A., Barker K., & Grant F.H. 2012. Evaluating the Consequences of an Inland Waterway Port Closure with a Dynamic Multiregional Interdependency Model. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans* 42(2): 359–370.

McDaniels, T., Chang, S., Cole, D., Mikawoz, J. & Longstaff, H. 2008. Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change* 18: 310–318.

McDaniels, T., Chang, S., Peterson, K., Mikawoz, J. & Reed, D. 2007. Empirical Framework for Characterizing Infrastructure Failure Interdependencies. *Journal of Infrastructure Systems* 13(3): 175–184.

Mendonca, D. & Wallace, W. A. 2006. Impacts of the 2001 World Trade Center attack on New York City critical infrastructures. *Journal of Infrastructure Systems* 12: 260–270.

Min, H.J., Beyeler, W., Brown, T., Son, Y.J. & Jones, A.T. 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IEEE Transactions* 39: 57–71.

North, M.J. 2001. Smart II: The spot market agent research tool version 2.0. *Natural Resources and Environmental Issues* 8(1): 69–72.

OECD 2003. *Emerging Systemic Risks in the 21st Century: An Agenda for Action*. Paris: Organisation for Economic Co-operation and Development.

O'Rourke, T.D. 2007. Critical Infrastructure, Interdependencies, and Resilience. *The Bridge* 37(1): 22–29.

Ouyang, M. 2013. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety* 121: 43–60.

Palmqvist, H. & Tehler, H. 2014. How is capability assessment related to risk assessment? Evaluating existing research and current application from a design science perspective. S*ubmitted to 12th International Probabilistic Safety Assessment and Management.*

Pederson, P., Dudenhoeffer, D.D., Hartley, S. & Permann, M. 2006. *Critical Infrastructure Modeling: A Survey of U.S. and International Research*. Idaho Falls: Idaho National Laboratory.

Rahman, H.A., Beznosov, K. & Martí J.R. 2009. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. *International Journal of Critical Infrastructures* 5(3): 220–244.

Rasmussen, J. 1985. The role of hierarchical knowledge representation in decisionmaking and system management. *IEEE Transactions on Systems, Man, & Cybernetics* 15(2): 234–243.

Rinaldi S.M., Peerenboom J.P., Kelley T.K. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, 21(6): 11–25.

Rose A. & Liao S. 2005. Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science* 45: 75–112.

Satumtira, G. & Duenas-Osorio L. 2010. Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research. In Gopalakrishnan K., Peeta S. (Eds.), *Sustainable and Resilient Critical Infrastructure Systems*, Berlin: Springer.

Snook, S. 2002. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Princeton: Princeton University Press.

Stapelberg, R.F. 2008. Infrastructure systems interdependencies and risk informed decision making (RIDM): impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards. *Journal of Systemics, Cybernetics and Informatics* 6(5): 21–7.

Tehler, H. & Brehmer, B. 2013. Design inom olycks—och krishanteringsområdet med fokus på ledning. Lund: Lund University Center for Risk Assessment and Management (LUCRAM), Lund University.

Tehler, H., Brehmer, B. & Jensen, E. 2012. Designing societal safety: A study of the Swedish crisis management system. In *proceedings of the 11th International Probabilistic Safety Assessment and Management Conference And The Annual European Safety and Reliability Conference 2012, PSAM 11 ESREL 2012* 25–29 June 2012 5: 4239–4248.

Tsuruta, M., Goto, Y., Shoji, Y. & Kataoka, S. 2008. Damage propagation caused by interdependency among critical infrastructures, *The 14th World Conference on Earthquake Engineering, Beijing, Oct 12–17. 2008.*

Van Eeten, M., Nieuwenhuijs, A. Luiijf, E., Klaver, M. & Cruz, E. 2011. The state and the threat of cascading failures across critical infrastructures: the implications of empirical evidence from media reports. *Public Administration* 89(2): 381–400.

Wilhelmsson, A. & Johansson, J. 2009. Assessing Response System Capabilities of Socio-technical Systems, *ESREL 2009, Istanbul, Turkey, 6–11 June, 2009.*

Zimmerman, R. (2001). Social Implications of Infrastructure Interactions. *Journal of Urban Technology* 8(3): 97–119.

Zimmerman, R. & Restrepo, C.E. 2006. The next step: quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures* 2(2/3): 215–230.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A critical evaluation of risk assessment methodology for natural gas pipeline

J. Kraus
Technical University of Liberec, Liberec, Czech Republic

ABSTRACT: A new methodology for the quantitative risk assessment in the vicinity of high pressure natural gas pipelines has been recently adopted in the Czech Republic. A major objective of this methodology is to determine the minimum distances between gas pipelines and buildings and it can be used during a process of planning the route of new pipelines as well as for a risk assessment in individual cases when it is not possible to keep the minimum distance. Since the outputs of proposed methodology are used for a land planning, it is appropriate to examine the quality of methodology. This is done by identification and evaluation of uncertainties in individual steps of risk assessment. The purpose of the evaluation is to get the information on uncertainties of risk assessment and limits of usability of the methodology.

1 INTRODUCTION

A Quantitative Risk Assessment (QRA) is always performed on one or more models of a real world, a system or an event. The model never contains all information on modeled system and this state of deficiency of information related to understanding or knowledge of a system or an event is called uncertainty. The necessity of identifying and expressing the uncertainty is widely recognized (Helton & Burmaster, 1996) and this need is even more important when there is an intention to use the QRA as a tool in more cases. As the outputs of the QRA methodology for gas pipelines (CGA, 2013a) are currently used in valid codes of practice of Czech gas industry (CGA, 2013b), the need of uncertainty evaluation is clear.

There are a lot of different uncertainty categories and no generally accepted uncertainty taxonomy exists (Nøkland & Aven, 2009). The similar statement can be made about ways in which the uncertainty is expressed. For a purpose of evaluation of the QRA methodology for gas pipelines a semi-quantitative method of expressing uncertainty originally presented by Aven (2008) is applied. Following degrees of uncertainty are defined and used for evaluation.

1.1 *Minor uncertainty*

All of the following conditions are met:

- The phenomena involved are well understood; the models used are known to give predictions with the required accuracy.
- The assumptions made are seen as very reasonable.
- Much reliable data are available.
- There is broad agreement among experts.

1.2 *Major uncertainty*

One or more of the following conditions are met:

- The phenomena involved are not well understood; models are non-existent or known to give poor predictions.
- The assumptions made represent strong simplifications.
- Data are not available, or are unreliable.
- There is lack of agreement among experts.

1.3 *Moderate uncertainty*

Conditions are between those characterising minor and major uncertainty.

2 QRA METHODOLOGY FOR GAS PIPELINES

A detailed description of evaluated QRA methodology is given in CGA (2013a). Due to the fact that so far the methodology is available in Czech only, it is appropriate to outline the process of QRA here. The process of QRA involves steps listed below with defined inputs, outputs and activities within every single step.

2.1 *Scenarios selection*

The process of risk assessment begins with a selection of events representing disruption of gas pipeline and a natural gas leak. A set of scenarios of possible gas pipeline damages and following physical effects

has been selected by a group of experts from gas industry. Every scenario is given by nominal pipe size, pressure of natural gas, extent of damage and physical effect following the gas leak. Only two extents of damage are included in scenarios—hole in the pipeline and rupture of the pipeline. The hole is defined as damage with the diameter of the hole larger than 2 cm and smaller than or equal to the diameter of the pipe, while rupture is damage with the diameter of the hole larger than the pipeline diameter. Pipe sizes include those used in the Czech Republic with nominal diameters from 100 mm to 1000 mm for transportation of natural gas with nominal pressure from 4 MPa to 10 MPa. Physical effects cover the gas leak and fire of released gas. Three possible types of fire (fire ball, jet fire, flash fire) are considered in the QRA.

2.2 *Determining the frequency of gas leaks*

The basic information on frequency of gas pipeline incidents is taken from EGIG (2011). This database covers a period of 1970 to 2010 and contains data from fifteen European countries on more than 135,000 km of pipelines. Based on these data the frequencies of two considered pipeline damages (hole and rupture) are determined for different pipe sizes. Then the reduction factors are introduced to reflect current technologies used in construction and operation of gas pipelines and their influence to possible causes of gas pipeline damages. These reduction factors are determined using expert judgements on all measures applied against manufacturing defects, construction defects and negative influence of third parties as well as measures for ensuring the appropriate preventive maintenance of gas pipeline. Reduced frequencies of pipeline damages are used for calculations of the individual risk. Table 1 shows reduced frequencies for different pipe sizes and both considered damages of pipeline.

2.3 *Fire ball modelling*

Algorithms for the calculation of the mass of released gas, mass of gas within flammability limits, dimensions of the fire ball and heat flux from the fire ball have been taken from CPR (2005). The meteorological conditions are not taken into account for this type of fire. From computed heat flux and exposure time the thermal dose is determined. Then the probability of death is assigned to the thermal dose. Finally the individual risk for fire ball is computed as a product of the probability of death, the probability of fire ball and the frequency of disruption of gas pipeline.

Table 1. Reduced frequencies of pipeline damages.

Pipeline diameter (m)	Frequency of damage ($km^{-1} \times year^{-1}$)		
	Hole	Rupture	Total
80	5.94×10^{-5}	2.36×10^{-5}	8.30×10^{-5}
100	5.37×10^{-5}	2.20×10^{-5}	7.57×10^{-5}
300	1.99×10^{-5}	1.09×10^{-5}	3.08×10^{-5}
500	7.30×10^{-6}	5.40×10^{-6}	1.27×10^{-5}
700	2.70×10^{-6}	2.70×10^{-6}	5.40×10^{-6}
1000	6.00×10^{-7}	9.00×10^{-7}	1.50×10^{-6}

2.4 *Jet fire modelling*

A simplified Chamberlain model is used for modelling the jet fire. Contrary to the fire ball modelling, the meteorological conditions are considered in this case and the computation of flame shape and heat flux is done for different directions and speeds of wind. Determination of the thermal dose takes into account the exposure time which limited by duration of gas leak (upper limit) and the time necessary to escape from the area affected by the jet fire (lower limit). The individual risk is computed for weighted combination of different meteorological conditions.

2.5 *Flash fire modelling*

The flash fire can occur as a result of delayed ignition of a cloud of gas. In this case a time-limited steady release of gas is simulated as series of puffs, each of which is considered as a separate release described by Pasquill-Gifford model. Both atmosphere stability and direction and speed of wind are taken into account, as the gas dispersion depends on these factors. The computation of individual risk for flash fire reflects the fact that the heat flux, the probability of ignition of dispersed gas and exposure time vary in time and space.

2.6 *Calculation of individual risk*

The QRA methodology covers only risk to human health and lives. Other possible categories of risk such as environmental damage or economic losses are not addressed. The individual risk coming from a single gas leak is computed as a weighted combination of a risk for every type of fire. The weights are given by probabilities of occurrence of different types of fire. Then the individual risk in particular location is determined by integration of risk from individual segments of gas pipeline. Total individual risk is obtained by combining the individual risk from two different extents of gas pipeline damage (hole and rupture). This individual risk is determined for an unprotected person permanently present in a given position. Because these conditions (no protection and permanent presence of a person) do not reflect reality, two reduction factors are introduced and used to obtain reduced total individual risk.

Table 2. Reduced individual risk—pipeline DN 700, type B2.

Distance (m)	Class of building			
	1	2	3	4
20	4.52×10^{-8}	4.05×10^{-8}	3.40×10^{-8}	2.47×10^{-8}
40	4.26×10^{-8}	3.82×10^{-8}	3.19×10^{-8}	2.32×10^{-8}
60	3.69×10^{-8}	3.32×10^{-8}	2.76×10^{-8}	2.01×10^{-8}
80	2.85×10^{-8}	2.56×10^{-8}	2.12×10^{-8}	1.54×10^{-8}
100	1.90×10^{-8}	1.71×10^{-8}	1.40×10^{-8}	1.01×10^{-8}
120	1.06×10^{-8}	9.50×10^{-9}	7.64×10^{-9}	5.38×10^{-9}
140	5.07×10^{-9}	4.53×10^{-9}	3.54×10^{-9}	2.47×10^{-9}
160	1.58×10^{-9}	1.43×10^{-9}	1.09×10^{-9}	7.99×10^{-10}

The degree of protection is specified individually for every type of fire and for four different classes of buildings defined as follows: Class 1—buildings where more than 500 people but less than 1000 people can gather, Class 2—buildings where less than 500 people can gather, Class 3—residential buildings for more than 50 people, Class 4—individual buildings for living and recreation occupied by 50 people or less. The presence of a person in the affected area is reflected by a specified fraction of time the person spent here. Both reduction factors are set according to recommendations published in Bumba et al. (2005) and CPR (1999). Example of calculated reduced individual risk in different distances from the pipeline of construction type B2 with nominal diameter of 700 mm is in Table 2.

2.7 *Calculation of societal risk*

The societal risk is given by the product of reduced individual risk and number of affected people. The QRA methodology allows calculating the societal risk for three different tasks:

- Determining the risk for a group of people inside individual objects.
- Determining the risk for a people on the roads.
- Determining the risk alongside the section of gas pipeline.

The map of individual risk in given area is created for the purpose of determining the societal risk for people inside buildings. Based on this map and number of people inside individual buildings it is possible to compute the societal risk. When determining the risk for a people on the roads, the exposure times and degree of protection are different from those used for people inside buildings. The number of affected people on the road depends on the traffic load and length of road segment affected by the fire. Once these input parameters are determined (or estimated), the societal risk is computed. In case of determining the risk alongside the section of gas pipeline the societal risk is computed as a sum of risk for all affected objects.

Table 3. Minimum distances between gas pipelines of construction type B2 and buildings.

Pipeline diameter (mm)	Class of building			
	1	2	3	4
Up to 100 incl.	–	–	–	–
100 to 300 incl.	–	–	–	–
300 to 500 incl.	70	–	–	–
500 to 700 incl.	110	90	70	–
Over 700	160	140	100	–

2.8 *Acceptability of risk*

Currently no binding limit of acceptable risk is defined here in the Czech Republic, but according to existing recommendations for the risk assessment, the individual risk higher than 10^{-5} is unacceptable while the individual risk lower than 10^{-6} is acceptable. This implies that the individual risk within these limits is considered tolerable. Similar limits for the societal risk are 10^{-3} for unacceptable risk, 10^{-5} for acceptable risk and the interval between 10^{-3} and 10^{-5} for tolerable risk. The authors of the methodology have chosen the middle of this interval, i.e. 10^{-4} as a limit value for acceptable societal risk. Based on calculated societal risk and limit of acceptable risk the minimum distances between gas pipelines and buildings are specified for every construction type of high pressure gas pipelines and four previously defined classes of buildings. As example of minimum distances the results for gas pipelines of type B2 are in Table 3. Missing values mean that for given combination of pipeline diameter and class of building no minimum distance between the pipeline and buildings is necessary to ensure acceptable level of risk.

3 EVALUATION OF QRA METHODOLOGY

The evaluation of QRA methodology for gas pipelines begins with the identification of uncertainty in every of the QRA steps. Identified uncertainties cover uncertainty in models used in individual QRA steps, uncertainty in input data and parameters and their variability, disagreement among experts and completeness of the QRA process. Once the identification of uncertainties is finished, degree of uncertainty is assigned to every identified uncertainty. During the evaluation of QRA methodology, following uncertainties were identified.

3.1 *Uncertainty in scenarios selection*

Scenarios included in evaluated QRA methodology cover only the risk from fire following the gas leaks. Other possible consequences of gas pipeline disruption (e.g. blast) are not mentioned nor discussed and neither the risk from effects other than fire and its share in total level of risk is determined. This restriction of events further examined was identified as a main source of uncertainty in the QRA process.

3.2 *Uncertainty in frequency of gas leaks*

Determination of frequency of gas pipeline incidents is based on data published in EGIG (2011). Authors of the QRA methodology argue that these data do not fully reflect technological improvements applied on construction and operation of gas pipelines in recent years and for this reason the correction coefficients are implemented. A group of 28 experts from gas industry was formed with the task to assess the influence of individual technological measures to frequency of gas pipeline incidents. Disagreement in expert judgements constitutes an uncertainty in estimation of the frequency of gas leaks.

3.3 *Uncertainty in fire modelling*

Various models are used for computing the heat flux of individual types of fire. In general, every model contains calculation of following quantities: mass flow, duration of the gas release, shape of the gas cloud, heat generated due to combustion, heat flux. Meteorological conditions are taken into account in limited extent in models of jet fire and flash fire. Uncertainty in calculation of heat flux, selection of particular meteorological conditions and their influence on distribution of heat flux in time and space are main uncertainties of this part of the QRA.

3.4 *Uncertainty in calculation of individual risk*

Calculation of individual risk from a fire adopts a lot of assumptions regarding exposure time,

Table 4. Summary of uncertainties identified in the QRA methodology.

		Degree of uncertainty		
Step of QRA	Uncertainty	Minor	Moderate	Major
Scenarios selection	Completeness of scenarios		X	
Frequency of gas leaks	Historical data on incidents	X		
	Correction coefficients			X
Fire modelling—fire ball	Mass flow		X	
	Duration of the gas leak		X	
	Heat flux		X	
	Meteorological conditions	X		
Fire modelling—jet fire	Mass flow		X	
	Duration of the gas leak		X	
	Heat flux	X		
	Meteorological conditions		X	
Fire modelling—flash fire	Mass flow		X	
	Duration of the gas leak		X	
	Heat flux			X
	Meteorological conditions		X	
Calculation of individual risk	Exposure time		X	
	Thermal dose		X	
	Probability of death	X		
	Probability of fire occurrence		X	
	Personal protection			X
	Time spent in affected area		X	
	Influence of terrain			X
Calculation of societal risk	Number of affected people		X	
	Personal protection			X

thermal dose, probability of death, probability of ignition and probability of occurrence of individual types of fire. Obtained individual risk is corrected with respect to degree of personal protection and to the time spent in affected area. Mentioned assumptions and correction coefficients present the main uncertainty in calculation of individual risk. Another uncertainty is introduced by fact than land relief and terrain obstacles are not taken into account in any of used models.

3.5 *Uncertainty in calculation of societal risk*

The main uncertainty in determining the societal risk is limited knowledge regarding the number of people affected by events following disruption of the gas pipeline. Also the estimated degree of protection of people inside the buildings and vehicles is uncertain. These factors become even more important when the calculated societal risk is close to the limit of acceptable risk.

Identified uncertainties in individual steps of QRA are summarized in Table 4. A degree of uncertainty is assigned to every uncertainty using the semi-quantitative method presented in Introduction. This way of mapping the uncertainty allows highlighting those uncertainties which deserves further examination and helps to establish a risk picture covering not only the level of risk but also the uncertainty inevitably associated with the risk.

3.6 *Verification*

According to authors of the QRA methodology, historical data on gas pipeline accidents were used for verification of the methodology in terms of scenarios selection and physical effects following the gas leak. One of accidents used for verification was a gas release and subsequent fire which happened in Tresana, Italy in January 2012. The incident happened on the pipeline with diameter of 762 mm (30 inches) and operating pressure of 5.9 MPa. The release and ignition of gas led to a jet fire with flames about 200 high and creation of a crater 20 meters wide and 7 meters deep. Ten people were injured and one of them died after a month due to severe burns. Although the authors of the QRA methodology state there is a good compliance between results of physical effects modelling and historical data, no details are given.

4 CONCLUSIONS

A semi-quantitative approach of expressing the uncertainties has been used to evaluate the quality of QRA methodology for gas pipeline. The evaluation shows a number of uncertainties in the methodology and although assigning the degree of uncertainty is partly subjective, it provides general information on quality of evaluated methodology and can be used as a base for further examination of uncertainties and their importance for results of risk assessment. If the methodology should be used as a tool in a process of land planning, it is necessary to know its weak points and limitations. Uncertainty identification and evaluation helps to get a better picture of a risk and to realize that the methodology can provide only estimation of the level of existing risk. The evaluation also showed that the semi-quantitative method of classification and expressing of uncertainties can be used in the first round of evaluation of the QRA methodology. However for further examination of identified uncertainties it is necessary to use methods other than simple semi-quantitative expression of uncertainties. Identification and semi-quantitative expression of uncertainties in the QRA methodology for gas pipeline together with verification of practical applicability of semi-quantitative approach of expressing the uncertainties are the main findings of this research.

REFERENCES

Aven T. 2008. A semi-quantitative approach to risk analysis, as an alternative to QRAs. *Reliability Engineering and System Safety* 93(6): 790–797.

Bumba J. et al. 2005. *The procedures and methods of analysis and risk assessment for the purposes of the Act on the prevention of major accidents* (in Czech). Prague: Occupational Safety Research Institute.

CGA 2013a. *The methodology for determining the risk in the vicinity of natural gas pipeline* (in Czech). Prague: Czech Gas Association.

CGA 2013b. *TPG 702 04 Gas mains and service pipelines of steel for maximum operating pressure up to 100 bar included* (in Czech). Prague: Czech Gas Association.

CPR 1999. *Guidelines for quantitative risk assessment CPR 18E.* The Hague: Committee for the Prevention of Disasters.

CPR 2005. *Methods for the calculation of Physical Effects due to releases of hazardous materials (liquids and gases) CPR 14E*. The Hague: Committee for the Prevention of Disasters.

EGIG 2011. *8th Report of the European Gas Pipeline Incident Data Group.* Groningen: European Gas Pipeline Incident Data Group.

Helton, J.C. & Burmaster, D.E. 1996. Guest editorial: treatment of aleatory and epistemic uncertainty in performance assessments for complex systems. *Reliability Engineering and System Safety* 54(1–2): 91–94.

Nøkland, T.E. & Aven, T. 2009. Review and discussion of uncertainty taxonomies used in risk analysis. In S. Martorell et al. (eds.), *Safety, Reliability and Risk Analysis; Proceedings of the European Safety and Reliability Conference 2008 (ESREL 2008)*, London: Taylor & Francis.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An ontology-based approach to vulnerability and interdependency modelling for Critical Infrastructure systems

P. Trucco & B. Petrenj
Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy

ABSTRACT: The systematic and complete identification of meaningful accident scenarios for Critical Infrastructure is still one of the major challenges to achieve higher resilience performance. THREVI2 project has been designed to answer this need by developing a comprehensive and multi-dimensional all-hazards catalogue for CI. Specific objectives are: to develop and elaborate three coordinated ontologies (Hazards & Threats, CIs topologies, CIs Interdependencies); to merge them by existing vulnerability models; and to develop a dedicated software tool for scenarios generation to support different end-users (e.g. authorities and operators). THREVI2 ontologies have been developed by a joint implementation of different methodologies: literature review, experts' review, basic ontology development methodology, and a final pilot testing of the tool. The main results achieved are generalised and standardised: i) specification framework for CIs and services; ii) all-hazards catalogue for CI. The developed SW tool offers an improved scenario generation process to support CI risk assessment.

1 INTRODUCTION

Critical Infrastructures (CIs) are exposed to a wide spectrum of hazards and threats which vary in nature (natural, technological, human-intentional or non-intentional) and, that can be internal (e.g. technical failure, sabotage, human error) or external to the infrastructure (e.g. flood, chemical explosion, terrorist attack). As such, hazard and threat assessment is a key element within CIP strategies and CI risk assessment. However, it is difficult for Authorities or Operators to get comprehensive information of all potential disruption scenarios relevant for CIP, since:

– hazard, threat and vulnerability assessments are often very specific in nature and related to different disciplinary fields;
– existing information most often focuses only on one type of hazard or on the vulnerability of one type of target (a single infrastructure or asset).

This is why the systematic and complete identification of meaningful accident scenarios for Critical Infrastructure is still one of the major challenges to achieve higher resilience performance. At European/National level it is a part of the CI identification process, since the EC Directive 2008/114/EC requires to develop "worst case scenarios", to simulate the failure of a potential ECI, in order to assess the transboundary impacts on other Member States. At infrastructure level, vulnerability and risk assessment needs to be applied to define appropriate protection and resilience measures (e.g. European CI operators have to include in the Operator Security Plan "a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impacts").

THREVI2 project has been designed to answer to the Authorities' and Operators' need to get comprehensive information of all potential disruption scenarios relevant for CIP/R by developing a comprehensive and multi-dimensional all-hazards catalogue for critical infrastructures. Specific objectives are:

– to elaborate three coordinated ontologies (Hazards and Threats, CI topologies, CI Interdependencies);
– to merge them by existing vulnerability models;
– to develop a dedicated software tool for scenarios generation to support different end-users in specifying the overall "system of systems" and generating a set of relevant disruption scenarios.

To this end, an ontology-based approach has been implemented and two interconnected ontologies have been developed:

– an ontology of physical and functional topologies of Critical Infrastructure systems;
– an ontology of Hazard & Threat (H&T) affecting CIs

They have been then merged through specific vulnerability and dependency entities.

In a preceding paper (Trucco et al., 2014) the ontology development process adopted in the project and the main features of the final integrated set of ontologies was presented. In this paper we briefly recall on the main results regarding CI and H&T ontologies and build upon the previous work. The advancements include modelling of vulnerabilities and interdependencies and progress in the development of the supporting software tool (PATHFINDER).

2 ONTOLOGICAL APPROACH TO SCENARIO GENERATION

An ontology can be defined as '*a formal description of entities and their properties, relationships, constraints, behaviours*' (Grüninger and Fox, 1995), or simpler as '*a specification of a conceptualization*' (Gruber, 1993).

Ontology deals with questions concerning what entities exist or can be said to exist, and how such entities can be grouped, related within a hierarchy, and subdivided according to similarities and differences. It is used to describe the concepts and relationships that are important in a particular domain, providing a vocabulary for that domain as well as a computerized specification of the meaning of terms used in the vocabulary. Ontologies are used to capture and share knowledge about some domain of interest, organising elements within the domain by using *classes*, *properties* and *instances*. Ontologies range from taxonomies and classifications, database schemas, to fully axiomatized theories. An ontology together with a set of individual *instances* of classes constitutes a *knowledge base* (Noy & McGuinness, 2001).

In recent years, ontologies have been adopted in many business and scientific communities as a way to share, reuse and process domain knowledge. Ontologies are now central to many applications such as scientific knowledge portals, information management and integration systems, electronic commerce, and semantic web services. From the perspective of Lacy & Gerber (2004) ontologies are beneficial in simulation and modelling through the formalization of semantics, the ability to query and inference, and the sharing and reuse of developed models.

2.1 *Overview of ontologies for CI and emergency management*

Liu et al. (2013) conducted a thorough review of the ontologies for the field of Crisis Management (CM). They have identified a set of critical subject areas that cover the information concepts dealt with in CM. Among the ontologies designed originally for these areas of CM, very few are formally represented and publicly accessible (Liu et al., 2013). Regarding the CI area, existing ontologies represent:

- the domain simulators (used for observing and analysing the behaviours of a system), such as PSCAD—for conceptualising power system simulators and EPANET for representing water distribution simulators (Grolinger et al., 2011):
- geographic information in infrastructure systems, such as OTN (Lorenz et al., 2005)—a formal description of the Geographic Data Files (GDF) ontology (GDF is an ISO standard for specifying how to store geographic information for intelligent transport systems).

Other contributions include:

- ENISA's ontologies of resilience and threats in cyber domain (Vlacheas et al., 2011);
- DISASTER (2014) project—developed an integrative and modular ontology for establishing a common knowledge structure between all the first responders involved in an emergency;
- Emergency Information Sharing Protocols among the operators of CIs and first responders—e.g. *Emergency Information Interoperability Frameworks (EIIF)* for emergency management, through which critical requirements and candidate ontology components are introduced (W3C, 2009), or *Tactical Situation Object (TSO)*—a message structure to record a view of a situation as seen by a particular observer at a particular time (OASIS, 2009);
- HLA (High Level Architecture) standard (by IEEE) and MSI (Multi-Simulator Interface) program (Rubin et al., 2006) focused on modelling of system interdependencies to enable federated simulations. However, environments based on these approaches are not suitable to simulating CIs (Tofani et al., 2012; Masucci et al., 2009);
- The DIESIS project (Design of an Interoperable European federated Simulation network for Critical Infrastructures) aims to establish a basis for the modelling and simulation of CI based upon open standards (Rome et al., 2009). Still, domain ontologies express concepts in a highly specialized manner and are often very detailed, making it difficult to merge ontologies into a general representation (Masucci et al., 2009);
- The Infrastructure Interdependency Simulator (I2Sim) uses a cell-channel model to represent the physical elements of CI and their interdependencies (Rahman et al., 2008). It enables the modelling of interdependencies without modelling the details of involved entities;
- The Meta-Knowledge Infrastructure Ontology (MKIONT) defines a general template for expressing the basic concepts and relationships of CIs and their interconnections. In short, the MKIONT provides: (i) a CI template that

captures basic concepts and relationships pertaining to a CI; and (ii) an interconnection template that represents CI interconnections and their relative semantics (Masucci et al., 2009);
– Tofani et al. (2010) use the ontology framework to model the interdependencies among CIs. Their proposed framework consists of three ontologies: WONT (World ONTology) contains concepts and relations that are common across CI domains; IONT (Infrastructure ONTology) extends WONT to represent the knowledge of specific CIs and FONT (Federation ONTology) enables modeling relations among different infrastructures;
– GenOM (Generic Object Model), represents and organizes the knowledge about CI interdependencies through a three-leveled hierarchy of object classes (Lee & Yavagal, 2004);

A standardized and comprehensive ontology regarding infrastructure's assets, functions and interdependencies is not documented in the extant literature.

2.2 *Study methodology*

We use taxonomies to describe how different classes are related by organising them into groups and/or hierarchies (according to level of detail). Adopting a standardised description is also important for systematic connection between the taxonomies to the other parts of the ontology.

In the first place we have to organise knowledge in specific domain using scattered data and various sources. For the two main domains (Critical Infrastructures and Hazards & Threats) it is necessary to determine what concepts exist and to describe and classify them within the domain in a systematic way. THREVI2 ontologies have been developed by a joint implementation of different methodologies:

– literature review covering scientific, technical and regulatory documentation;
– experts review, to complement incomplete documentation, to validate and harmonise the proposed ontologies;
– basic ontology theory and development methodology;
– pilot testing of the SW tool in two different contexts, respectively at national and regional scale.

3 ONTOLOGICAL SPECIFICATION OF CI AND RELATED THREATS

3.1 *Critical infrastructure ontology*

For the CI System Ontology, the sectors covered include *Energy*, *Transport*, *Water* and *Telecommunications,* for a total of 11 different infrastructure subsectors (Fig. 1).

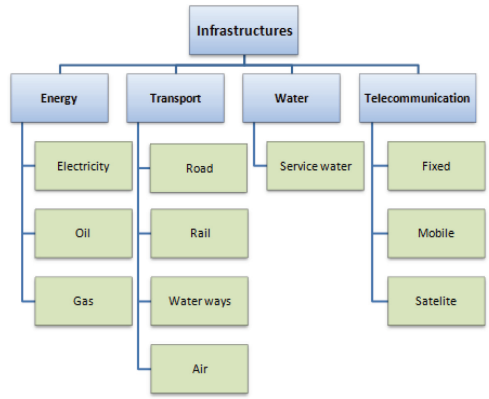


Figure 1. Covered infrastructure sectors and subsectors.

The ontology has been developed using various data sources. Globally, more than 100 references, of *scientific*, *technical* and *regulatory* nature, have been identified and systematically reviewed. After analysis, a portion of the sources turned out not to be useful for the ontology description. At the end 62 documents have been used to develop the final 22 sub-ontologies (reference list available inside the project deliverable).

Each CI is described by means of two interconnected sub-ontologies, one for the physical and the other for the functional specification. The overall infrastructure ontology framework is organized in three parts—assets, functions and services that were subsequently linked within the service delivery process.

3.2 *Hazards & threats ontology*

Hazard and Threats (H&T) Ontology aims at characterising different typologies of events, in a systematic way, to be merged in a federation of ontologies enabling a first-order recognition of:

– all the possible hazards and threats that can affect or destroy a generic CI;
– all the possible infrastructure that can be affected by a specific hazard or threat.

The H&T ontology is based on a hierarchical structure (classes and sub-classes), and is developed considering the possibility to reuse available literature on threat classification. For each class, a set of features (duration, impacted area, etc.) is assigned to better characterize the classes and to allow flexible navigation of the user within the ontology.

In literature, threat is sometimes used as a synonym of hazard, e.g. "threat: a person or

thing likely to cause damage or danger (Oxford Dictionary, 2012). However, some definitions show a distinction between both concepts. The first difference between a hazard and a threat is related to the probability of occurrence and the magnitude of the potential event. A threat is a very low-probability but serious event—to which analysts may be unable to assign a probability in a risk assessment because it has never occurred. The difference is clearly illustrated by the precautionary principle, which seeks to reduce potential threats to a set of well-defined risks before an action, project, innovation or experiment is allowed to proceed (European Commission, 2000). A threat is therefore associated with a high range of uncertainty (RGS, 2013).

The second difference is that a threat is the result of intent: "a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not" (Oxford Dictionary, 2012). The US Presidential Commission on Critical Infrastructure Protection (PCCIP), for example, defines "threat" as a "foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defence or economic security. A threat may be an individual, an organization, or a "nation" (PCCIP, 1997) but a threat-source does not present a risk when there is no vulnerability that can be exercised (Stoneburner et al., 2002). Threats do not necessarily need to originate from human sources, but can be natural, human, or environmental (RGS, 2013).

"*Natural or technological threats*" is therefore used to define low-probability but serious events (compared to natural or technological hazards), while human threats (e.g. cyber or terrorist threats) refer to the intent of creating harm or damage (RGS, 2013).

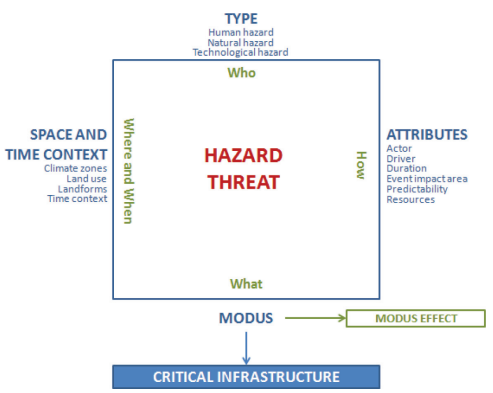


Figure 2. Hazard & threat ontology.

To be helpful in understanding hazards and threats in light of vulnerabilities and risk, need to be characterised in some detail (Fig. 2). In addition to the common attributes, *Modus* has been introduced as a feature to define and simplify in which way a given event occurs and can affect the CI. Modus has been used as the link between the ontologies of the CI and H&T, defining CI assets vulnerabilities.

4 MODELLING VULNERABILITIES & INTERDEPENDENCIES

4.1 *Vulnerability modelling*

Having developed CI assets and H&T ontologies, the following step consisted of connecting the two ontologies. It was done by assessment of actual and potential vulnerabilities of CI assets to specific hazards and threats. Vulnerability can be understood as '*the susceptibility of the infrastructure to threat scenarios*' (Ezell, 2007).

For instance (Fig. 3), **Snow Avalanche** can affect an infrastructure in different ways—either through direct impact on it, the subsequent static pressure and/or because by producing an obstruction (so it has *Static Pressure*, *Kinetic Energy* and *Obstruction Modus*).

Moduses affect (are linked to) exclusively CI assets, while impact of modus on CI functions is taken into account through possible unavailability of asset needed to execute the function.

The links have been mapped within a matrix indicating connections where modus affects an asset (Annex A contains the first assumption to be validated). In cases where modus affects an assets conditionally (e.g. depending on the asset material or position), asset has been characterised by additional attributes which define if the modus will affect the specific asset type. The typical examples of attributes are ***position*** of an asset (buried/superficial/above ground) for different types of

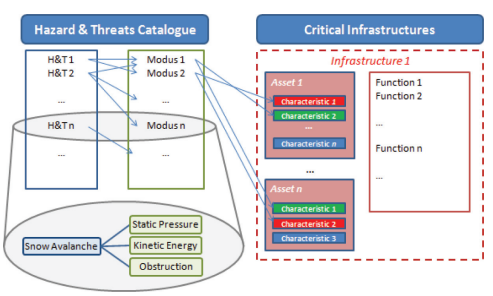


Figure 3. Impact/vulnerability modelling (links between H&T and infrastructure assets).

pipelines, or asset ***material*** (steel/concrete) in case of a bridge.

4.2 *Interdependencies modelling*

The main concepts and definitions related to critical infrastructure interdependencies are widely accepted (see, e.g., Rinaldi et al., 2001). A proper modelling of all types of interdependencies is needed to comprehensively cover all the possible vulnerabilities and risks affecting CI.

Geographic interdependency occurs if a local environmental event creates state changes in infrastructures (Rinaldi et al., 2001). For example, a disrupted asset (impacted by a hazard and/or threat) can behave as a source of a new hazard causing cascading effects through different interdependency mechanisms (Fig. 4).

Functional (or Physical) interdependency is a physical reliance on material flow from one infrastructure to another (Rinaldi et al., 2001). Within CI topologies (service delivery process) mechanism, control and material/resource inputs have been defined for each single function, as well as material flow between related functions—covering both dependencies within and between infrastructure sectors (e.g. see Fig. 5). The relations (links) between Assets and/or Functions have been defined adopting the Integration Definition Function Modeling (IDEF∅) standard, generally used for developing structured representations of a system or enterprise (Colquhoun & Baines, 1991). It relates classes to its **inputs** (e.g. requirements, materials) and **outputs** (e.g. functions, services)—white boxes; **mechanisms** (e.g. resources, assets)—blue boxes; and **controls** (e.g. plans, legislations, monitoring)—red boxes. Bold circles represent connections between different phases of service delivery process.

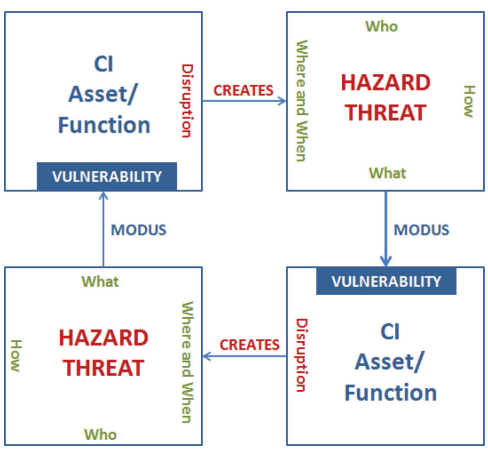


Figure 4. Modelling of geographical interdependency.

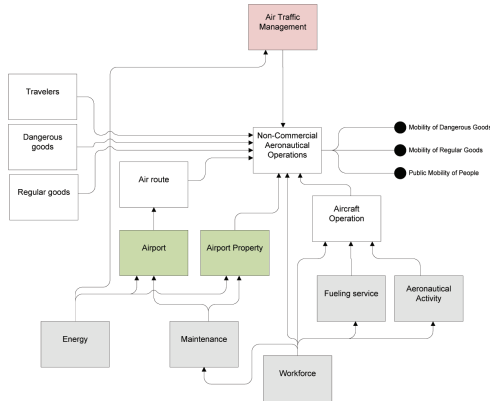


Figure 5. Service generation stage in air transport sector.

Cyber interdependency occurs if the state of an infrastructure depends on information transfer between infrastructures (e.g. SCADA, communications, monitoring, controlling) (Rinaldi et al., 2001). The information is normally transmitted through the information infrastructure. Cyber interdependencies have been modelled by connecting information (a common resource that has been identified as an input to functions) and telecommunication assets.

4.3 *Validation*

In the first phase, about 25 experts have been invited to review the Critical Infrastructure ontologies on assets and functions. Experts have been provided with an evaluation template (available on request) where they have been able to propose:

- doubts on the clarity of, or different nomenclature and description for assets/functions;
- missing relevant assets and/or functions;
- not relevant assets and/or functions (candidates to be removed);

They have also reviewed the service delivery process and validated connections (and their types) between assets and/or functions, indicating missing or wrong links.

Based on the comments and recommendations received by the experts, some of the assets and functions have not been used in the final integration of CI sub-ontologies. It is either due to a high level of detail—assumed not to be relevant to describe the effects of threats to service delivery process—, or to an activity that is not being carried out on regular bases (and thus not relevant in the standard service delivery process). However, we decided to keep these assets/functions inside the catalogue

in order to assure the completeness of the ontology and a comprehensive description of CI.

In the subsequent phase, experts are requested to validate the integration of CIs and H&T ontologies that are connected through different types of interdependencies. This part of the validation has been carried out through face-to-face interviews with technical managers and experts along with the pilot application of the PATHFINDER tool.

5 PATHFINDER SOFTWARE TOOL

The main output of the project is the PATHFINDER tool, principally planned for two types of users—*Critical Infrastructures managers/operators* and *National/Local Authorities* (*Civil Protection operators*). The general approach for identifying vulnerability paths is given in Figure 6, but may vary according to different users' needs.

It will be possible to use the tool in two main modes (Fig. 7):

- *WIZARD mode*—the order of setting the criteria (filters) necessary to delineate paths is defined. Under this mode, a minimal cut set of selection criteria is defined. The user browses through the pages in an established order that will be different according to the user type.
- *FREE mode*—the user can browse through the pages in free order without limitation (for expert users).

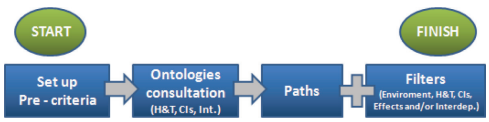


Figure 6. PATHFINDER tool utilization process.

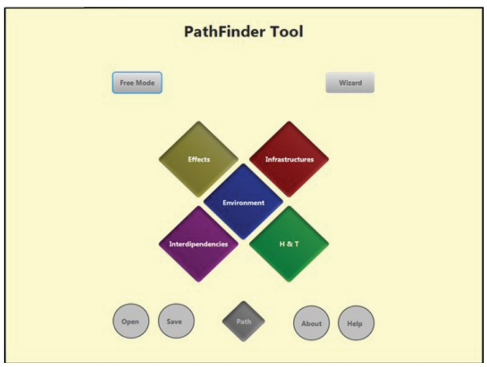


Figure 7. PATHFINDER tool: main window.

Other controls include (Fig. 7):

- *Setup pages* (middle part of the screen) that contain all the set-up options.
- *Path Button* that launches the final query, and will remain disabled until a minimal set-up will be done. Effects are the impact modes through which the hazards hit the infrastructures. In Infrastructures page the user can set one or more infrastructure he is interested in. In Environments page the user can set one or more environments, which can be associated with infrastructure or used for hazards screening. In Hazards and Threat page the user can define screening criteria for hazards and their attributes. Selection list is available within each of the sub-ontologies.

Standard options—enabling user to save on his computer the file containing the current set-up, open an existing file or use the guide.

The PATHFINDER tool has been tested in two pilot applications in collaboration with one EU Member State and one relevant CI operator.

6 CONCLUSIONS

Two main results have been achieved by the present study: a generalised and standardised specification framework for CI and services; a generalised and standardised all-hazards catalogue for CI.

By developing of a multidimensional ontology-based model it is possible to generate and document a larger set of plausible accident scenarios, fully exploiting the existing knowledge on CIP as well as all the specific knowledge on the system under analysis and its external environment. Thus, by integrating CI, Hazards & Threats and vulnerabilities, the PATHFINDER tool enables an effective risk assessment and prioritisation of activities and resources.

Indirect benefits are also expected, in terms of quality of shared information among actors, thanks to a standardised nomenclature and modelling of CI assets, functions and vulnerabilities. The contribution of the study to the general body of knowledge consists of a publicly available integrated ontology covering relevant domains when it comes to scenario identification. It enables an easy description of CI systems and their behaviour in face of H&T and under influence of interdependencies. Integration of this work with ontologies for inter-organisational information sharing presents a good opportunity for the development of a comprehensive Emergency Management ontology for CI.

However, the proposed integrated ontology suffers from some limitations. The main one is the

modelling of logical interdependencies as a further level of integration between CI sub-ontologies. Two or more infrastructures are logically interdependent if the state of each depends upon the state of the other via some mechanism that is not a physical, cyber, or geographic connection (Rinaldi et al., 2001). This category may contain policy, legal or regulatory regimes, economic systems and trends, social and human factors etc., making it very complex and uneasy to be properly addressed via ontology development.

Future planned activities include integration of Geographic Information System (GIS) that will enable visualisation as well as spatial representation of assets, systems and threats.

ACKNOWLEDGMENT

THREVI2 research project has been co-funded by DG Home Affairs of the European Commission, under CIPS/ISEC Work Programme. The financial support is gratefully acknowledged

REFERENCES

Colquhoun, G.J., & Baines, R.W. 1991. A generic IDEFO model of process planning. *The International Journal of Production Research*, 29(11), 2239–2257.

Dictionary, O.E. 2012. Oxford dictionary of English. online version.

DISASTER project website 2014 http://disaster-fp7.eu/node/21.

European Commission 2000. Communication from the Commission on the precautionary principle (COM/2000/0001).

Ezell, B.C. 2007. Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, *27*(3), 571–583.

Grolinger, K., Capretz, M.A.M., Shypanski, A. & Gill, G.S. 2011 Federated critical infrastructure simulators: Towards ontologies for support of collaboration, *2011 24th CCECE conference*, Niagara Falls, ON, 001503–001506.

Gruber. T.R. 1993 "*A translation approach to portable ontologies*" Knowledge Acquisition, 5(2):199–220. http://www-ksl.stanford.edu/kst/what-is-an-ontology.html.

Grüninger, M. & Fox. M.S. 1995 "*Methodology for the design and evaluation of ontologies*", Technical Report, University of Toronto, Toronto, Canada.

Lacy, L., & Gerber, W. 2004, December. Potential modeling and simulation applications of the web ontology language-OWL. In *Proceedings of the 2004 Winter Simulation Conference,* (Vol. 1). IEEE.

Lee, S.W. & Yavagal, D., "GenOM User's Guide," Technical Report TR-SIS-NISE-04-01, Knowledge Intensive Software Engineering Research Group, Dept. of Software and Information Systems, UNC Charlotte, 2004.

Liu, S., Shaw, D., & Brewster, C. 2013, May. Ontologies for Crisis Management: A Review of State of the Art in Ontology Design and Usability. In *Proceedings of the ISCRAM 2013 conference, 12–15 May, 2013*.

Lorenz, B., Ohlbach, H.J., & Yang, L. 2005. Ontology of transportation networks.

Masucci, V., Adinolfi, F., Servillo, P., Dipoppa, G., & Tofani, A. 2009. Ontology-based critical infrastructure modeling and simulation. In *Critical Infrastructure Protection III* (pp. 229–242). Springer Berlin Heidelberg.

Noy, N.F., & McGuinness, D.L. 2001. Ontology development 101: A guide to creating your first ontology.

OASIS 2009. Disaster and emergency management—Shared situation awareness. www.oasis-open.org.

President's Commission on Critical Infrastructure Protection—PCCIP 1997, *Critical Foundations: Protecting America's Infrastructure*.

Rahman, H.A., Armstrong, M., Mao, D., & Marti, J.R. 2008, October. I2Sim: a matrix-partition based framework for critical infrastructure interdependencies simulation. In *Electric Power Conference, 2008*. Canada (pp. 1–8). IEEE.

Rinaldi, S.M. Peerenboom, J.P. & Kelly, T.K. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Mag. 21: 11–25.

Risk Gov. Solutions (RGS) 2013. THREVI2 Project—Deliverable 2.1. "*Hazard and Threat Taxonomy and Ontology*".

Rome, E., Bologna, S., Gelenbe, E., Luiijf, E.H., & Masucci, V. 2009, July. DIESIS: an interoperable European federated simulation network for critical infrastructures. In *Proceedings of the 2009 SISO European Simulation Interoperability Workshop* (pp. 139–146). Society for Modeling & Simulation International.

Rubin, A., Hein, C., & Prasad, G. 2006. Multi-Simulation Interface (MSI) for Complex Simulations.

Stoneburner, G., Goguen, A., & Feringa, A. 2002. Risk management guide for information technology systems. *Nist special publication*, *800*(30).

Tofani, A., Castorini, E., Palazzari, P., Usov, A., Beyel, C., Rome, E., & Servillo, P. 2010. An ontological approach to simulate critical infrastructures. *Journal of computational science*, 1(4), 221–228.

Trucco, P., Petrenj, B. & De Ambroggi, M. 2014 "Ontology-based Disruption Scenario Generation for Critical Infrastructure", *Proceedings of PSAM12*, June 2014, Honolulu.

Vlacheas, P.T., Stavroulaki, V., Demestichas, P., Cadzowm S., Gorniak, S. & Ikonomou, D. (2011, December). *Ontology and taxonomies of resilience.* The European Network and Information Security Agency (ENISA).

W3C 2009. http://www.w3.org/2005/Incubator/eiif/XGR-Framework-20090806/.

ANNEX A: Links between Assets and Modus.

X—Modus affects Asset

C—Modus affects Asset conditionally (attribute required)

			MODUS																														
			Data alteration				Ground deformation		Contamination			Energy variation				Mechanical action						Environmental variation							Unavailability of resources
																Wearing		Pressure											
			Data corruption	Data destruction	Data breach	Data theft	Transient ground deformation	Permanent ground deformation	Air contamination	Water contamination	Food contamination	Electrical discharge	Ionizing radiation	Thermal energy	Electromagnetical diturbance	Corrosion	Abrasion	Static pressure	Overpressure peak	Kinetic energy	Dynamic pressure	Temperature variation	Degradation of visibility	Degradation of air quality	Degradation of soil quality	Obstruction/ occupation		
ASSET	COMMON ASSETS AND RESOURCES	SCADA	X	X								X			X							X							X
		TRAVELERS							X	X	X																			X
		WORKFORCE							X	X	X																			X
		ENERGY																												X
		REGULAR GOODS												X								X							X
		DANGEROUS GOODS										X	X	X				X	X	X	X	X							X
		INFORMATION	X	X	X	X									X															X
ASSET	ENERGY	Electricity	Power Generation Plant	X	X			X	X						X	X	X	X	X	X	X	X						X	
			Transmission Grid	X	X			X	X				X				X	C	C	C	C	C								
			Distribution System	X	X			X	X				C			X	X	C	C	C	C	C								
			Smart Grid	X	X											X														
			Meter	X	X								X		X	X	X	C	C	C	C	C								
		Oil	Oil plant and equipment	X	X			X	X						X	X	X	X	X	X	X	X						X	
			Oilholder station	X	X			X	X						X	X	X	X	X	X	X	X								
			Pressure Regulating Installation (PRI) station	X	X			X	X						X	X	X	X	X	X	X	X								
			Oil system	X	X			X	X						C	X	X	C	C	C	C	C								
		Gas	Gas plant and equipment	X	X			X	X						X	X	X	X	X	X	X	X						X	
			Gasholder station	X	X			X	X						X	X	X	X	X	X	X	X								
			Pressure Regulating Installation (PRI) station	X	X			X	X						X	X	X	X	X	X	X	X								
			Gas system	X	X			X	X						C	X	X	C	C	C	C	C								
	TRANSPORT	Road	Surface Road					X	X						X		X	X			X							X	
			Road Bridge					X	X						C		C	C		X	X	X						X	
			Road Tunnel					X	X						X		X	X		X	X							X	
			Toll Booth					X	X				X		X	X	X	X		X	X							X	
		Rail	Rail Station					X	X																			X	
			Surface rail					X	X																			X	
			Rail bridge					X	X						C		C	C	X	X	X	X						X	
			Rail tunnel					X	X						X		X	X		X	X							X	
			Operating property					X	X						X		X	X		X	X	X						X	
			Non-operating property					X	X						X		X	X		X	X							X	
			Train														X		X	X	X	X						X	
		Air	Airport	X	X			X	X				X	X	X	X							X	X				X	
			Airport Property					X	X																			X	
			Aircraft														X		X	X	X	X						X	
		Water	Port					X	X						X	X			X	X	X	X						X	
			Ship														X		X	X	X	X						X	
	SERVICE WATER		Gaging station	X	X			X	X						X	X	X	X	X	X	X	X							
			Water abstraction and raw water transfer system	X	X			X	X						C	X	X	C	C	C	C	C						C	
			Water-Treatment system	X	X			X	X						X	X	X	X	X	X	X	X	X					X	
			Water main pipeline	X	X			X	X						C		X	C	C	C	C	C							

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Renewable sources impact on power system reliability and nuclear safety

A. Volkanovski & B. Gjorgiev
Reactor Engineering Division, Jožef Stefan Institute, Ljubljana, Slovenia

ABSTRACT: The introduction of the renewable energy sources in power system result in multiple and complex challenges considering continuous and reliable operation of the power grid. One of the main challenges is intermittent power production from some renewable power sources requiring compensation of the power by the remaining power plants in the given system.

This paper presents the results of the analysis of a power system generation availability considering introduction of wind generating power units. The power system reliability is assessed by the Loss of load probability evaluated from the cumulative outage probability table. The analysis considers the uncertainty of the available power from the wind genera-tors and uncertainty of the peak load in the analyzed system. Weibull distribution is used for the characterization of the wind speed in the developed method. The consequences of the substitution of the nuclear power plants with the wind generators on the safety of the remaining operating nuclear power plants are analyzed. The core damage frequency obtained from the probabilistic safety assessment model of the nuclear power plant is used to evaluate the safety of the nuclear power plants.

Obtained results show that introduction of wind generating units in the power system results in increase of the Loss of load probability. The obtained Loss of load probability depends on uncertainty of the peak load size and shape parameters of the wind speed in the model. Increase share of wind generation in overall power system generation results in increased Loss of load probability. Substitution of the nuclear power plants with wind generation results in small decrease of the overall core damage frequency in the given system. The decrease of the overall core damage frequency depends on the characteristics of the substituted nuclear power plants and share of nuclear and wind generation in the analyzed system.

1 INTRODUCTION

The main function of the power system is to provide electrical energy to the customers as economically as possible with an acceptable degree of continuity and quality, known as reliability. The two constraints of economics and reliability are competitive since increased reliability of supply generally requires increased capital investment. These two constraints are balanced in many different ways in different countries and by different utilities, although generally they are all based on various sets of deterministic criteria.

A wide range of power system reliability indices are determined using probability theory (Billinton and Allan, 1984). The approach used and the resulting formulas depend on the problem and the assumptions utilized.

In general the two main categories of the power system reliability evaluation techniques are analytical and simulation. Analytical techniques represent the system by a mathematical model and evaluate the indices using mathematical solutions. Monte Carlo simulation methods estimate the indices by simulating the actual process and random behavior of the system. Generally Monte Carlo simulation requires a large amount of computing time and is not used extensively if alternative analytical methods are available. The obtained indices are only as good as the model derived for the system, the appropriateness of the evaluation technique and the quality of the input data used in the models and techniques.

The most important aspect in power system reliability evaluations is to have a complete understanding of the engineering implications of the system (Volkanovski et al., 2009).

The Loss of Load Probability (LOLP) or Expectation (LOLE) method is the most widely used probabilistic technique for evaluating the adequacy of a given generation configuration (Volkanovski et al., 2008, Daemi et al., 2012, Sanghvi and Shavel, 1984, Celik, 2007, Lucio et al., 2012).

Loss of load probability consists of two segments in which the generating unit unavailability is characterized by random outage rate (forced)

and scheduled outage rate. The effect of random outages is evaluated probabilistically, while that of scheduled outages is evaluated deterministically.

In power system analysis the application of LOLP is limited to the estimation of generation adequacy without consideration of the transmission system capacity or reliability.

The EU directive on the promotion of renewable energy sources sets the share of renewable energy in final energy consumption to 20% by 2020 (EC, 2009). This overall target is broken down into binding national targets for all EU member states (Klessmann et al., 2013). This target for the renewable sources together with the liberalization of the electricity market (Karova, 2011) is policy driven.

The goal of this paper is to analyze and assess implications of the introduction of the intermittent power sources on the overall reliability of the power system. In addition the implications of substitution of nuclear power plants with such sources on safety of the nuclear power plants are analyzed. The Monte Carlo sampling approach is applied for assessment of the implications of uncertainties of wind generation and peak load on the obtained results. The Probabilistic Safety Assessment (PSA) model of the nuclear power plant is used for assessment of the implications on nuclear safety.

2 METHOD DESCRIPTION

The LOLP assessment method is given in Section 2.1. Models of wind generator output power and load uncertainties are given in Section 2.2. Description of the Monte Carlo sampling and integration in the developed method is given in Section 2.3.

2.1 *LOLP assessment*

The probability of finding the generator in the forced outage at distant time in the future represents the basic parameter used in static capacity evaluation for modelling of generating unit reliability. This probability is defined as unit Unavailability (U) and in power system applications it is known as the unit Forced Outage Rate (FOR), defined as:

$$U = FOR = \frac{\lambda}{\lambda + \mu} \tag{1}$$

where λ = the expected failure rate; μ = the expected repair rate.

The unavailability (FOR) calculated with equation (1), for generating unit with relatively long operating cycles, is an adequate estimator of the probability that the unit under similar conditions will not be available for service in the future (Volkanovski et al., 2008).

Capacity outage probability table is an array of the capacity levels, or corresponding capacity out of service and the associated probabilities of existence. The associated probability of existence is the probability of the indicated amount of capacity being out of service. For capacity model is used the cumulative probability of existence and it is equal to the sum of probabilities corresponding to capacity on outage equal to or greater than the indicated amount.

Capacity model can be created using a convolution algorithm (Volkanovski et al., 2008, Billinton, 1970, Allan, 1996), which is a recursive algorithm of adding or removing units in the model and calculating the cumulative probability of a particular capacity outage state.

In case of two state units, cumulative probability of a particular capacity outage state of X (MW), after a unit of capacity C (MW) and forced outage rate U is added, is given by:

$$P(X) = (1-U)P'(X) + (U)P'(X-C) \tag{2}$$

where $P'(X)$ = the cumulative probability of the capacity outage state of X (MW) before unit is added; $P(X)$ the cumulative probability of the capacity outage state of X (MW) after the unit is added.

The equation (2) is initialized by setting $P'(X = 1.0$ for $X \leq C$ and $P'(X) = 0$ otherwise and $P'(X\text{-}C) = 1.0$ for $X \leq C$.

Generating units that are removed from system for scheduled maintenance are not available for service. New capacity model of system is created using recursive algorithm for unit removal:

$$P'(X) = \frac{P(X) - (U)P'(X-C)}{(1-U)} \tag{3}$$

where $P'(X\text{-}C) = 0$ for $X \leq C$.

The recursive algorithm given by equation (3) allows modification of the capacity outage probability table when units are taken out from system.

The load model can either be the daily peak load variation curve, which only includes the peak loads of each day, or the Load Duration Curve (LDC), which represents the hourly variation of the load. The LOLP is evaluated by convolution of the capacity and load model, obtaining the expected time interval in the specified period in which the peak load will exceed the available capacity:

$$LOLP_p = \sum_{i=1}^{n} P_i(C_i < L_i)\ time/period \tag{4}$$

where $LOLP_p$ = value of LOLP in period p with n time units; C_i = the available capacity on time i; L_i = the forecast load on time i; $P_i(C_i < L_i)$ = the

probability of loss of load on time i, obtained directly from the capacity outage cumulative probability table. In the developed method, the value of daily $LOLP_p$ is calculated using equation (4) and $n = 24$, and those values are summed to calculate the daily $LOLP_p$.

The LDC is used to evaluate the LOLP giving a risk expressed in number of hours during the day when the load will exceed available capacity (Volkanovski et al., 2008).

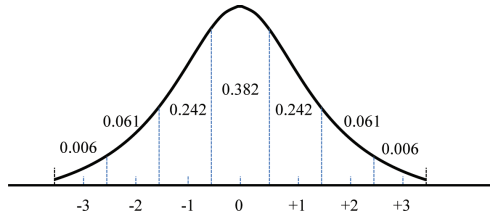


Figure 1. Seven-step approximation of the normal distribution.

2.2 *Wind power and load uncertainties*

The Weibull distribution adequately represents (Li et al., 2014, Liu, 2012) the wind speed probability distribution for most sampling times. Wind speed v is a variable generated at random (for a given time interval of one hour) with a Weibull distribution given by the following Probability Density Function (PDF):

$$f(v,c,k) = \frac{k}{c}\left(\frac{v}{c}\right)^{k-1} e^{-\left(\frac{v}{c}\right)^{k}} \tag{5}$$

where c = scale factor; k = shape factor.

The power output P of a single Wind Turbine Generator (WTG) is determined by applying a simplified input–output function:

$$P_{WTG} = \begin{cases} 0, & v < v_{ci} \quad or \quad v > v_{co} \\ \dfrac{v - v_{ci}}{v_r - v_{ci}} P_r, & v_{ci} \le v \le v_r \\ P_r, & v_r \le v \le v_{co} \end{cases} \tag{6}$$

where P_r = the rated power output; v_{ci} = the cut-in wind speed; v_r = the rated wind speed; v_{co} = the cut-out wind speed of the WTG.

The uncertainty in load forecasting can be included in the LOLP calculations by dividing the load forecast probability distribution into class intervals (Allan, 1996). The area of each class interval represents the probability that the load is the class interval mid-value. The LOLP is calculated for each load represented by the class interval multiplied by the probability of the given load.

The load forecast uncertainty was modeled using a normal distribution divided into seven discrete intervals. The probability of each area is given on Figure 1.

2.3 *Monte Carlo sampling*

Uncertainty of the wind power production is analyzed by a computerized Monte Carlo technique (Han and Lim, 2012, Tewari et al., 2011). The wind speed is sampled from probability distributions given by equation (5) used to assess power generation of single wind generator given by equation (6). The capacity outage probability table is updated considering the wind generators power obtained from the simulation. The LOLP is calculated from updated capacity outage probability table for seven different load sizes for each hour in the day. Overall LOOP for given day is calculated and stored.

High performance computer compiler (INTEL, 2013) and corresponding library (Software, 2013) were used in the computer code developed for analysis of the LOLP within this study.

3 TEST SYSTEM

The main parameters of the wind turbine generators, given in reference (Li et al., 2014) are shown in Table 1.

Peak Load of Ppeak = 9000 [MW] is used in the analysis, with Hourly Peak Load as percentage of Daily Peak Load given in reference (Grigg et al., 1999) are shown in Table 2.

The standard deviation of $\sigma = 5\%$ of peak load was used in Base model. The standard deviations of $\sigma = 2\%$ and $\sigma = 10\%$ were also analyzed. Value of $c = 7.65$ and $k = 2.06$ are used for scale and shape factors of wind speed.

Parameters of the generating units in the Base model with 5% share of the wind power in the total installed power are given in Table 3.

Table 3 shows that in Base model the installed power is for 10% larger than the peak load Ppeak. It is assumed that all units are scheduled for operation during all hours of the analyzed period.

Three case scenarios were developed and analyzed from the Base model.

First case scenario CASE1 has increased 10% share of wind power in the model. One NPP from base model is shutdown as shown on Table 4.

Second case scenario CASE2 has increased 15% share of wind power in the model. The power from

Table 1. Test system main parameters.

	Pr [MW]	v_{ci} [m/s]	v_r [m/s]	v_{co} [m/s]
Value	3	3	11.7447	25

Table 2. Hourly peak load in percent of daily peak.

Hour	Load [%]
12–1 am	67
1–2	63
2–3	60
3–4	59
4–5	59
5–6	60
6–7	74
7–8	86
8–9	95
9–10	96
10–11	96
11-noon	95
Noon-1 pm	95
1–2	95
2–3	93
3–4	94
4–5	99
5–6	100
6–7	100
7–8	96
8–9	91
9–10	83
10–11	73
11–12	63

Table 3. Parameters of generators in Base model.

Unit	Power [MW]	Number of units	FOR
Wind	3	166	0.07
Nuclear	1000	3	0.04
Coal	200	20	0.06
Water	100	25	0.05

nuclear power plants is decreased as shown on Table 5.

Third case scenario CASE3 has 20% share of wind power and two NPP shutdown as shown on Table 6.

Equal number of simulations N_{sim} = 10000 is used in Monte Carlo sampling in all analyzed models. The Probability Density Function (PDF) is assessed for N_{int} = 500 intervals between smallest and largest obtained value of LOLP from the sampling.

Table 4. Parameters of generators in CASE1.

Unit	Power [MW]	Number units	FOR
Wind	3	**333**	0.07
Nuclear	1000	**2**	0.04
Coal	200	20	0.06
Water	100	**30**	0.05

Table 5. Parameters of generators in CASE2.

Unit	Power [MW]	Number units	FOR
Wind	3	**500**	0.07
Nuclear	1000	**2**	0.04
Coal	200	20	0.06
Water	100	25	0.05

Table 6. Parameters of generators in CASE3.

Unit	Power [MW]	Number units	FOR
Wind	3	**667**	0.07
Nuclear	1000	**1**	0.04
Coal	200	**22**	0.06
Water	100	**26**	0.05

4 REFERENCE NPP MODEL

The PSA model of the NPP is developed on the basis of the plant model and Level 1 PSA analysis given in the corresponding references (NRC, 1990).

The PSA model includes 14 Event trees, 168 Fault trees and 576 Basic events.

The contribution of the Accident Groups to Core Damage Frequency (CDF) obtained for the NPP model is given in Table 7.

The LOOP Accident group, as shown on Table 7, have largest share in the overall plant CDF.

The frequency of the Loss of Offsite Power (LOOP) initiating event in reference model is LOOP = 7.7E-2 [/yr]. The share of each LOOP data category into overall LOOP with mean frequencies are given in Table 8.

In this study it is assumed that Grid related LOOP will change proportionally with the change of LOLP. The share of the CDF from the LOOP accident group will change proportionally with the change of LOOP frequency (Volkanovski et al., 2009).

Change of the frequency of other initiating events resulting from the changes in the power system is not considered in this study. The increase of the number of transients and corresponding initiating event frequency is expected in case of the NPP that are utilized for load following.

Table 7. Share of accident sequences in CDF.

No.	Accident group	Mean CDF [/yr]	Share [%]
1.	All LOOP	9.63E-06	44.9
2.	All LOCA	6.31E-06	29.4
3.	Int. LOCA	1.60E-06	7.5
4.	All transient	1.52E-06	7.1
5.	ATWS	1.99E-06	9.3
6.	SGTR	4.03E-07	1.9
Total CDF		2.15E-05	100

Table 8. Share of each LOOP data category into overall LOOP.

LOOP data category	Mean frequency [/yr]	Share [%]
Plant centered	4.44E-03	5.7
Switchyard centered	2.23E-02	28.9
Grid related	3.99E-02	51.8
Weather related	1.04E-02	13.4
All	7.70E-02	100

5 RESULTS

Obtained Probability Density Function (PDF) of the LOLP for Base model and different standard deviations of the peak load σ are given on Figure 2. Mean LOLP for analyzed Base models is given in Table 9.

Results on Figure 2 and Table 9 show that increase of the peak load standard deviation σ results in increase of the LOLP.

Obtained results for Case 1 and different load deviations are given on Figure 3 and Table 10.

Figure 3 and Table 10 show that increased peak load uncertainty results in larger LOLP but relative increase is smaller compared to the Base model.

Impact of wind speed parameters on the obtained results were analyzed on Case 1 model for different shape factor *k* values. Obtained results are given in Table 11 and Figure 4.

Figure 4 and Table 11 shows that decrease of the wind speed shape factor k results in change of the LOLP PDF and increase of the mean LOLP.

Figure 5 shows obtained LOLP PDF for all analyzed models and equal load standard deviation σ = 5%. Table 12 shows obtained mean LOLP for analyzed case scenarios.

Figure 5 and Table 12 shows that increase of the share of wind generation in the system results in large increase of the mean LOLP.

Figure 5 shows that LOLP PDF has increased range with the increase of the wind generation share.

The recommended annual LOLP for given power system (Billinton and Allan, 1988) is in range of

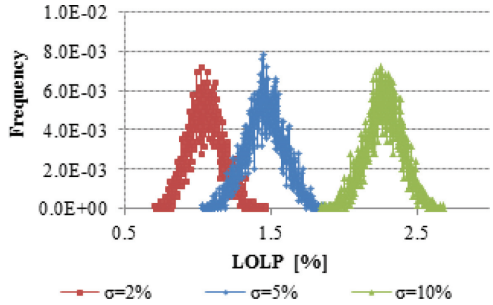


Figure 2. Obtained LOLP for Base model.

Table 9. Mean LOLP for Base model.

	σ = 2%	σ = 5%	σ = 10%
LOLP [hr/day]	1.05E-02	1.46E-02	2.28E-02

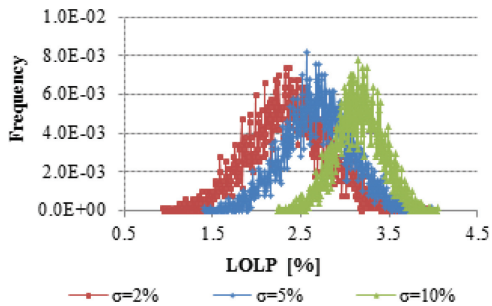


Figure 3. Obtained LOLP for Case 1.

Table 10. Mean LOLP for Case 1.

	σ = 2%	σ = 5%	σ = 10%
LOLP [hr/day]	2.35E-02	2.68E-02	3.16E-02

Table 11. Mean LOLP for different shape factor k.

	k = 2.05	k = 1.56	k = 1.06
LOLP [hr/day]	2.68E-02	2.78E-02	3.01E-02

0.1–1 days/year that is equal to 6.5E-3–6.5E-2 hr/day. Comparison with values in Table 7 shows that obtained values for analyzed scenarios are in this range. The mean LOLP for Case 3 is near the largest recommended value.

In analyzed case scenarios it is assumed closure of single (Case 1 and Case 2) or two NPP (Case 3). The closure of the NPPs results in change of the

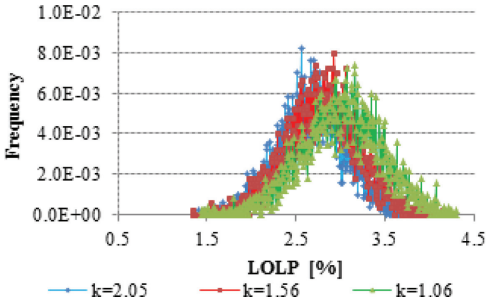


Figure 4. Obtained LOLP for different shape factors *k*.

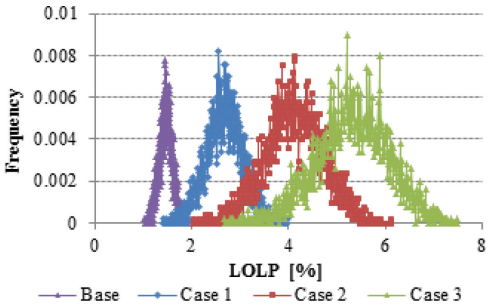


Figure 5. Obtained LOLP for analyzed case scenarios.

Table 12. Mean LOLP for analyzed case scenarios.

	Base	Case 1	Case 2	Case 3
LOLP [hr/yr]	1.46E-02	2.68E-02	4.10E-02	5.32E-02

Table 13. Change of CDF in analyzed systems.

	Case 1	Case 2	Case 3
ΔCDF+ [/yr]	8,33E-06	1,80E-05	1,32E-05
ΔCDF– [/yr]	2,15E-05	2,15E-05	4,29E-05
ΣCDF [/yr]	–1,31E-05	–3,44E-06	–2,97E-05

sum of the CDF of the NPPs in given power system ΣCDF. This decrease ΔCDF—is equal to the sum of the CDF of the closed NPPs.

Obtained results from the analysis show that introduction and increase of the share of the wind generation in the power system results in increased LOLP. The consequence is increased grid related LOOP initiating event frequency. This results in increase of the CDF of the reaming units in the system ΔCDF+.

Table 13 summarizes the changes of the CDF in the analyzed systems.

Table 13 shows that shutdown of the nuclear power plants results in decrease of the overall sum of CDF of NPP in the system indicated by negative ΣCDF and corresponding risk. Table 13 shows that obtained decrease of overall CDF and corresponding risk is small if analysis considers the increase of the CDF of the remaining NPP in the system.

6 CONCLUSIONS

Implications of introduction of wind generation on power system reliability and NPP safety was analyzed. The LOLP was used as a measure of the generation adequacy of the system. The core damage frequency was used as a measure of the NPP safety.

Obtained results show that increase uncertainty of the peak load size results in larger mean LOLP. The mean LOLP depends on the parameters of the distribution used for characterization of the wind speed. Increase of the share of the wind generation results in increased LOLP. The change of the wind generation share modifies the probability density function of the LOLP.

Analysis of the substitution of the NPP with wind generation shows that overall decrease of the CDF in the analyzed system depends on the share of the wind generation and number and characteristics of the NPP that are shutdown. Obtained results show that overall decrease of the CDF is smaller than the sum of the CDF of the NPP that are shutdown.

ACKNOWLEDGMENTS

This research was partly supported by the Slovenian Research Agency (research program P2-0026) and partly by the European Atomic Energy Community's (Euratom) Seventh Framework Programme FP7/2007-2011 under Grant agreement no. 605001.

REFERENCES

Allan, R.N. (1996). Reliability Evaluation of Power Systems, *Springer*.

Billinton, R. (1970). Power System Reliability Evaluation. *International Journal of Electrical Engineering Education,* 8(6): 467.

Billinton, R. & Allan, R.N. (1984). Reliability evaluation of power systems, *Pitman Advanced Publishing Program.*

Billinton, R. & Allan, R.N. (1988). Reliability Assessment of Large Electric Power Systems, *Springer*.

Celik, A.N. (2007). Effect of different load profiles on the loss-of-load probability of stand-alone photovoltaic systems. Renewable Energy, 32(12): 2096–2115.

Daemi, T., Ebrahimi, A. & Fotuhi-Firuzabad, M. (2012). Constructing the Bayesian Network for components reliability importance ranking in composite power systems. *International Journal of Electrical Power & Energy Systems,* 43(1): 474–480.

EC (2009). Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing Directives 2001/77/EC and 2003/30/EC. *Official Journal of the European Union*.

Grigg, C., Wong, P., Albrecht, P., Allan, R., Bhavaraju, M., Billinton, R., Chen, Q., Fong, C., Haddad, S., Kuruganty, S., Li, W., Mukerji, R., Patton, D., Rau, N., Reppen, D., Schneider, A., Shahidehpour, M., Singh, C. & Force, R.T.S.T. (1999). *The IEEE reliability test system—1996. Ieee Transactions on Power Systems,* 14(3): 1010–1018.

Han, S.H. & Lim, H.-G. (2012). Top event probability evaluation of a fault tree having circular logics by using Monte Carlo method. *Nuclear Engineering and Design,* 243(0): 336–340.

Intel. (2013). Intel® Visual Fortran Composer XE 2013 SP1.

Karova, R. (2011). Regional electricity markets in Europe: Focus on the Energy Community. Utilities Policy, 19(2): 80–86.

Klessmann, C., Rathmann, M., De Jager, D., Gazzo, A., Resch, G., Busch, S. & Ragwitz, M. (2013). Policy options for reducing the costs of reaching the European renewables target. Renewable Energy, 57(0): 390–403.

Li, G., Yue, H., Zhou, M. & Wei, J. (2014). Probabilistic assessment of oscillatory stability margin of power systems incorporating wind farms. *International Journal of Electrical Power & Energy Systems,* 58(0): 47–56.

Liu, X. (2012). Optimization of a combined heat and power system with wind turbines. International Journal of Electrical Power & Energy Systems, 43(1): 1421–1426.

Lucio, J.H., Valdés, R. & Rodrı´Guez, L.R. (2012). Loss-of-load probability model for stand-alone photovoltaic systems in Europe. *Solar Energy,* 86(9): 2515–2535.

NRC, U.S. (1990). Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events. *NUREG/CR-4550, SAND86-2084.* Washington.

Sanghvi, A.P. & Shavel, I.H. (1984). Incorporating explicit loss-of-load probability constraints in mathematical programming models for power system capacity planning. *International Journal of Electrical Power & Energy Systems,* 6(4): 239–247.

Software, R.W. (2013). IMSL Fortran Numerical Library 6.0.

Tewari, P., Vinod, G., Sanyasi Rao, V.V.S., Munshi, P. & Kalra, M.S. (2011). Uncertainty evaluation of blackout initiated accident sequences of a typical PHWR. *Nuclear Engineering and Design,* 241(12): 5251–5262.

Volkanovski, A., Cepin, M. & Mavko, B. (2009). Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety,* 94(6): 1116–1127.

Volkanovski, A., Mavko, B., Boševski, T., Čauševski, A. & Čepin, M. (2008). Genetic algorithm optimisation of the maintenance scheduling of generating units in a power system. *Reliability Engineering & System Safety,* 93(6): 779–789.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Titanic viewed from different perspectives on major accidents

H. Kim & S. Haugen
Department of Production and Quality Engineering NTNU, Trondheim, Norway

ABSTRACT: Several perspectives on major accidents have evolved over the last four decades to explain why accidents occur and how to prevent them. Each perspective looks at the causes of an accident in its own particular way, and may draw different conclusions about the causes of the same accident. In the paper, we have taken a look at an accident that occurred about a century ago, the sinking of the Titanic. The paper summarizes the accident using modern accident investigation techniques. Subsequently, six perspectives on major accidents are applied to identify how the accident causes can be related to the perspectives.

The result shows that none of the perspectives cover all the accident causes alone, and a combination of the perspectives can help the overall understanding of the accident. Based on this, some reflections are made on the similarities and differences between the different perspectives.

1 INTRODUCTION

Several perspectives on major accidents have evolved over the last four decades to explain why accidents occur and how to prevent them. Key are the energy-barrier model (Gibson, 1961, Haddon, 1970, Haddon, 1980), Turner's Man-Made Disasters (MMD) model (Turner and Pidgeon, 1978, Pidgeon and O'Leary, 2000), Perrow's Normal Accident Theory (NAT) (Perrow, 1984), High Reliability Organizations (HRO) theory (Rochlin et al., 1987, LaPorte and Consolini, 1991), Rasmussen's conflicting objectives perspective (Rasmussen, 1997), and resilience engineering (Hollnagel, 2004, Hollnagel, 2008). Each looks at the causes of an accident in its own particular way, and the perspectives therefore focus on different causes of the same accident.

The main objective of the paper is to study how each major accident perspective can be applied to an actual accident and to emphasize the importance of using several accident perspectives. For this purpose, the paper investigates the Titanic accident using a modern accident investigation technique, and six perspectives on major accidents are applied to identify how the accident causes can be related to the perspectives. Subsequently, the paper argues for the necessity of integrating the accident perspectives and suggests one possible approach which is based on the energy-barrier model.

The topics we cover in the paper are as follows:

1. What are the causes of the Titanic accident and how can we structure them? (Section 2)
2. What is the main idea of each accident perspective? (Section 3)
3. How can we apply each accident perspective to the causes of the Titanic accident? (Section 4)
4. Why do we need an integrated accident perspective and how can we integrate them? (Section 5 and 6)

Finally, some concluding remarks are given in Section 7.

2 INVESTIGATION INTO TITANIC ACCIDENT

2.1 *Event tree analysis*

The story of the Titanic is well-known, and the causes of the disaster have been well investigated over several decades. There were unusual amounts of icebergs, ice warnings were ignored, the Titanic made maximum speed in an ice field, and the lookout spotted the iceberg too late. After spotting the iceberg, there was a frantic manoeuver, serious hull damage due to the collision, and failure of rescue and evacuation. The combination of these events caused the disaster of the Titanic (Smith and Rayner, 1912, Eaton and Haas, 1996, Rapport, 2004, Beesley, 2008, Foecke, 2008, Lightoller, 2010, BBC, 2011, BBC, 2012, Compton, 2012, History, 2012, NationalGeographic, 2012, Ward, 2012). They are structured as an event tree given in Figure 1.

2.2 *MTO analysis*

Man, Technology and Organization (MTO) analysis has been widely used the last decade for

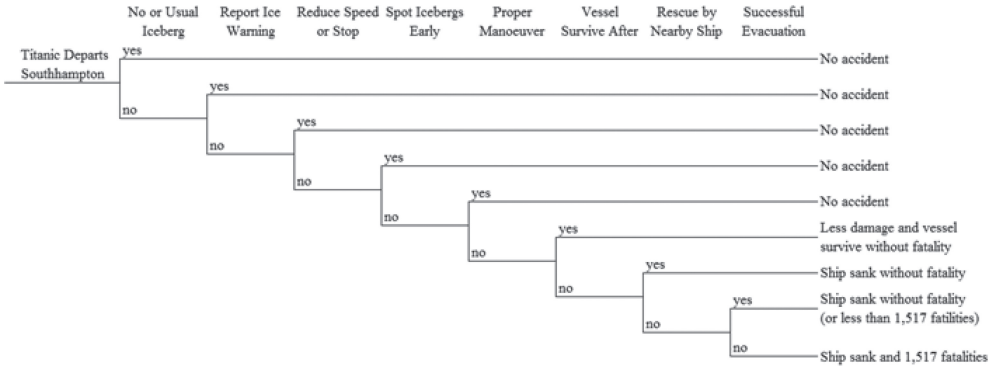


Figure 1. Event tree analysis for the Titanic accident.

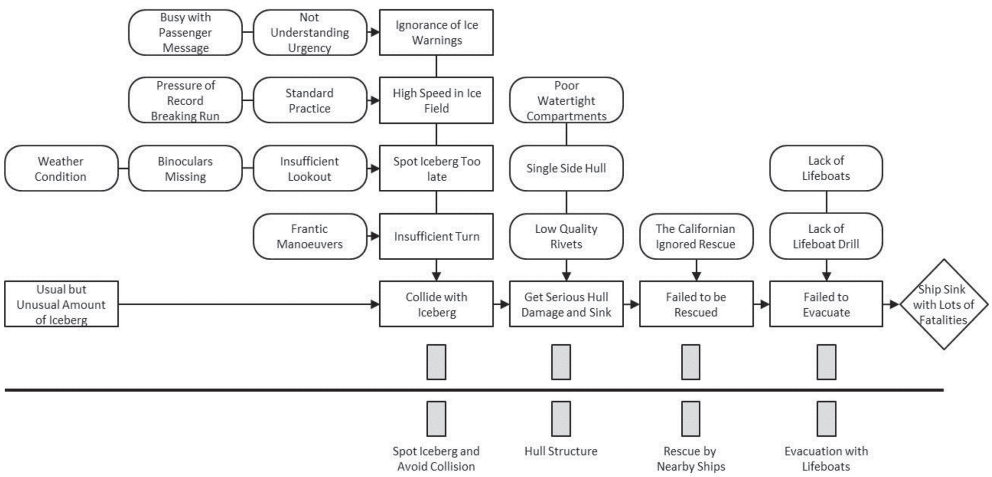


Figure 2. MTO analysis for the Titanic accident.

investigating accidents in the Norwegian offshore industry. The basis for the MTO analysis is that human, organizational and technical factors should be focused equally in an accident investigation. The analysis is based on using three methods: (Rollenhagen, 1995, Bento, 1999, Sklet, 2004)

– Structured analysis by use of event and cause diagrams
– Change analysis by describing how events have deviated from earlier events or common practice
– Barrier analysis by identifying technological and administrative barriers which have failed or are missing.

The main purpose of MTO analysis in the paper is not to investigate the accident in every detail, but to illustrate events, causes and conditions of the accident with a whole picture, and show the structure and relation of them. Thus, details of how the MTO analysis has been performed are not covered in the study.

Event and cause analysis and barrier analysis are illustrated into a single picture as shown in Figure 2. Based on this chart, the study investigates major accident perspectives in the accident of the Titanic. The change analysis is not included in Figure 2 because it has not so much relevance to this study.

3 SIX MAJOR ACCIDENT PERSPECTIVES

The paper focuses on six major accident perspectives: the energy-barrier model, MMD model, NAT,

Table 1. Comparison of six major accident perspectives.

Accident perspective	Why accidents occur?	How to prevent them?
Energy-barrier	Failure to establish and maintain adequate barrier functions	Include barrier functions in the design of the system and maintain barrier functions throughout system life
MMD	Lack of information flow and misperceptions with incubation period	Make systematic efforts to collect information about hazards and build culture for active search for signals of danger
NAT	Mismatch between complexity and coupling	Reduce complexity or loose couplings and discard high-risk systems that are both complex and tightly coupled
HRO	Not discussed explicitly but there seems to be an implicit understanding that accidents are caused by un-recovered errors	Build organizational redundancy and cultures that combines requirement for fault-free performance with openness to the fact that errors do occur (mindfulness)
Conflicting objectives	Distributed decision making in dynamic and opaque systems with invisible and untouchable boundaries	Establish counter pressures that favor safe performance and make boundaries to unacceptable performance visible and touchable
Resilience engineering	A mismatch between the coping capacity of the organization and the emerging dangerous interactive patterns	Build and maintain the abilities to anticipate, monitor, respond, and learn

HRO theory, conflicting objectives perspective, and resilience engineering. The main ideas of each accident perspective are very briefly summarized in Table 1 (Rosness et al., 2010).

4 MAJOR ACCIDENT PERSPECTIVES AND TITANIC ACCIDENT

This section applies the six major accident perspectives to the 23 causes of the Titanic accident. Each of the causes is briefly introduced and studied with regard to the six perspectives on major accidents.

4.1 *Usual but unusual amount of icebergs*

The Captain and crew of the Titanic did not pay much attention to general ice warnings because icebergs were common at that time of the year on the route of the Titanic (Lightoller, 2010, Ward, 2012). The "usual icebergs" caused the crew to be stuck in outdated behaviors which did not work in a changed situation, and therefore it is relevant to the ability to anticipate from resilience engineering. It can also be explained by mindfulness of HRO theory whose idea is to survey the existing situation based on expectations and contain unexpected events. Unusual amount of icebergs increased the hazard of iceberg. This cause is therefore related to the energy-barrier model, HRO theory and resilience engineering.

4.2 *Wireless operator busy with passenger messages*

The main role of the wireless operators was not to receive ice warnings, but to provide a luxury message service for passengers. Moreover, one day before the disaster, the transmitter broke down altogether, and it took two wireless operators seven hours to dismantle the entire system which caused a lot of backlog of messages from passengers. By the night of the disaster, both wireless operators were exhausted and could not even consider delivering the ice warnings forty feet forward to the bridge (Ward, 2012). This is relevant to the energy-barrier model, HRO theory, conflicting objectives perspective and resilience engineering. The HROs build organizational redundancy and operate in "high tempo mode" in such circumstance. It can also be explained by resilience engineering. The Titanic did not anticipate this high demand situation of wireless operators, and the Captain failed to monitor the stress and overload of the wireless operators. The conflicting role between sending passenger messages and reporting ice warnings is relevant to the conflicting objectives perspective. Lastly, it contributed to "ignorance of ice warnings" which weakened the barrier of "spot iceberg and avoid collision".

4.3 *Wireless operator not understanding the urgency of warnings*

The wireless operators knew nothing about navigation, and therefore latitude and longitude meant nothing to them. Even in the face of explicit ice warnings, they would not have known the extreme urgency (Ward, 2012). It is relevant to information flow of MMD theory, ability to monitor of resilience engineering, and mindfulness of HRO theory. It also affected "ignorance of ice warnings" and therefore influenced the barrier of "spot iceberg and avoid collision".

4.4 *Ignorance of ice warnings*

The Titanic received seven ice warnings from nearby ships on the day of the disaster (Ward, 2012). The two ice warnings from the Mesaba and the Californian were critical reports with great urgency. However, the wireless operator just put the message from the Mesaba under a paper weight (Lightoller, 2010), and replied to the Californian that "shut up, shut up, I am busy; I am working Cape Race" (Compton, 2012). It is a result of the previous two conditions: "wireless operator busy with passenger messages" and "wireless operator not understanding the urgency of warnings". It is therefore applicable to the energy-barrier model, MMD theory, HRO theory, conflicting objectives perspective and resilience engineering.

4.5 *Pressure of record breaking run*

The Titanic seemed to try to beat the time set by the Olympic on its own maiden voyage and the following three facts support it: i) Ismay, Chairman of White Star Line, repeatedly stated that "we will beat the Olympic and get in to New York on Tuesday", ii) the Titanic held a thousand ton more coal than the Olympic took on its own maiden voyage, iii) on the morning of the disaster, the Titanic seemed certain to make a record breaking trip (Ward, 2012). It is relevant to the energy-barrier model and conflicting objectives perspective. The pressure of record breaking run drove the Titanic towards the boundary of a safe performance, and it influenced the barrier of "spot iceberg and avoid collision" by encouraging "high speed in ice field".

4.6 *Standard practice*

Maintaining the speed in ice field at night was a standard practice of steamship liners using the North Atlantic track at that time (Beesley, 2008), and no captain would dream of slowing down even in the vicinity of ice at night (Ward, 2012). It is applicable to the energy-barrier model, HRO theory, and resilience engineering. The Captain was getting stuck in outdated behaviors, which is a failure of ability to anticipate in resilience engineering. It can also be explained by mindfulness of HRO theory because it is a lack of preoccupation with failure. Lastly, it promoted "high speed in ice field" and therefore weakened the barrier of "spot iceberg and avoid collision".

4.7 *High speed in ice field*

The Titanic was making its maximum speed just prior to the collision, and it was a result of the previous two conditions: "pressure of record breaking run" and "standard practice". Thus, "high speed in ice field" is relevant to the energy-barrier model, HRO theory, conflicting objectives perspective, and resilience engineering.

4.8 *Weather condition*

On the day of the disaster, the weather was calm and the sea was smooth. There was no moon, no wind, and no swell. These weather conditions precluded the lookout from spotting iceberg. If there had been either wind or swell, the outline of the iceberg would have been more visible, through the water breaking at the base, and the Titanic could avoid it (Lightoller, 2010). "Weather condition" made it difficult to spot iceberg, which influenced the barrier of "spot iceberg and avoid collision".

4.9 *Missing binoculars*

The Titanic lookouts were supposed to have binoculars, and the lookout testified to the US inquiry that if he had had binoculars to scan the horizon ahead, he would have seen the iceberg early enough for the Titanic to avoid it. However, the binoculars had accidentally been locked away because there was an unexpected reshuffle of its senior officers. (Ward, 2012). It influenced the performance of lookout, and therefore weakened the barrier of "spot iceberg and avoid collision".

4.10 *Insufficient lookout*

The weather was against the Titanic, and binoculars were missing in ice field at night. Under these circumstances, an extra lookout should have been placed at the stemhead, and a sharp lookout should have been kept from both sides of the bridge by an officer (Compton, 2012). It is applicable to the energy-barrier model, HRO theory, and resilience engineering. The Titanic should have been operated in "high tempo mode" with organizational redundancy of HRO theory. It is also relevant to

the ability to anticipate and respond of resilience engineering. It contributed to "spot iceberg too late" which weakened the barrier of "spot iceberg and avoid collision".

4.11 *Spot iceberg too late*

At 11.40 pm, the lookout of the Titanic saw the iceberg, and the original distance from the iceberg at that time was only between 600 yards and half a mile (Ward, 2012). It is a result of the combination of the above three conditions (Section 4.8–4.10), and therefore it contains the energy-barrier model, HRO theory and resilience engineering. It is also related to NAT. Spotting iceberg late decreased the buffer for preventing collision; in other word, it increased tightness of coupling.

4.12 *Frantic manoeuver and insufficient turn*

The First Officer of the Titanic ordered "Hard a-starboard" right after he was informed of the iceberg which ran completely contrary to accepted procedure. The action was much more likely to cause collisions than to prevent them (Ward, 2012). It is relevant to the energy-barrier model, HRO theory and resilience engineering. The frantic action of the First Officer can be explained by the ability to respond in resilience engineering and preoccupation with failure and sensitivity to operations of mindfulness in HRO theory. It influenced and weakened the barrier of "spot iceberg and avoid collision".

"Insufficient turn" is a result of "frantic manoeuvers", and therefore the former has the same accident perspectives with the latter.

4.13 *Collide with iceberg*

As a result of Section 4.2 to Section 4.12, the Titanic failed to spot the iceberg early and collided with it. In other words, the barrier of "spot iceberg and avoid collision" failed to maintain its function. It is caused by neither a single event nor a single condition, but by a combination of all of the above conditions and events. The event of "collide with iceberg" is therefore applicable to all of accident perspectives which are relevant to Section 4.2 to Section 4.12: the energy-barrier model, MMD model, NAT, HRO theory, conflicting objectives perspective and resilience engineering.

4.14 *Poor watertight compartment*

The Titanic was divided into 16 main watertight compartments, but only one watertight bulkhead extended to the upper most continuous deck C. The flooding over deck E contributed largely to the sinking of the Titanic (Smith and Rayner, 1912). The prime motivation for making the Titanic less safe was to increase the convenience and overall satisfaction of its passengers like huge dining rooms and saloons (Ward, 2012). It is relevant to the energy-barrier model and conflicting objectives perspective. Establishing passenger convenience is a kind of organizational pressure which resulted in imperfect watertight compartments. It also weakened the barrier of "hull structure".

4.15 *Single side hull*

The sides of the ship were just a single hull under the waterline. In the event of a glancing blow, the watertight compartment would be rendered absolutely useless, owing to the fact that there was no side protection (Compton, 2012). The weight and the cost for double side hull was so great that it was abandoned by the ship owner of the Titanic (Beesley, 2008). It is applicable to the energy-barrier model, and conflicting objectives perspective. The pressure of cost and weight exacted single side hull which weakened the barrier of "hull structure".

4.16 *Low quality of rivets*

Using sub-surface sonar, the iceberg damage has been mapped and it was found that the hull was not severely deformed, which implies that there was a failure of the riveted seams. Analysis of the wrought iron rivets has shown that they contained an average of three times more slag than optimal levels. It was seen that pressure to finish Titanic caused the company to order wrought iron that was one level below that generally specified for rivets. (Foecke, 2008). It is related to the energy-barrier model and conflicting objectives perspective. The pressure of the schedule forced the Titanic to use low quality rivets, which weakened the barrier of "hull structure".

4.17 *Get serious hull damage and sink*

As a result of the above three conditions (Section 4.14–4.16), the Titanic got serious hull damage and sank after the collision. Therefore, "get serious hull damage and sink" is applicable to the energy-barrier model and conflicting objectives perspective.

4.18 *The Californian ignored rescue signal and failed to be rescued*

The Californian was the nearest ship to the Titanic when it sank on the day of the disaster. The lookouts of the Californian saw several rockets from the Titanic and reported them to the Captain.

However, he ignored their reports because of the color and time intervals of the rockets. A distress signal should have fired at precise one-minute intervals, but the Titanic did not. Almost five hours after they saw the first rocket, they learned that the Titanic had sunk during the night. If the Carpathia had gone to the rescue of the Titanic immediately, most of the people aboard could have been rescued and survived. (Ward, 2012). This is related to the energy-barrier model and MMD model. Ignorance of the distress signal is a lack of information flow, and firing rockets at precise one minute intervals is a fantasy plan for a sinking ship. It also influenced the barrier of "rescue by nearby ships".

"Failed to be rescued" is a result of "the Californian ignored rescue signal" and therefore, the former has the same accident perspectives with the latter.

4.19 *Lack of lifeboats*

The Titanic was provided with 16 lifeboats and 4 collapsible, and total capacity of lifeboats was 1,176 persons (Smith and Rayner, 1912). Even though the Titanic was only equipped with enough lifeboats to save half the people aboard, that was still more than were required by law at that time. The Board of Trade specified required number of lifeboats, but the number of passengers and crew was not considered relevant (Ward, 2012). In 1911, a year before the Titanic sank, Alexander Carlisle, an expert witness, argued that the vessels should carry far more lifeboats for passenger safety. However, the committee actually recommended fewer lifeboats than before. In fact, the Titanic was capable of carrying sixty four lifeboats to be prepared for any change in the regulations. However, the White Star Line wanted to leave as much deck space as possible free for passengers and equipped only 20 lifeboats (Ward, 2012). This is relevant to the energy-barrier model, MMD model and conflicting objectives perspective. The Board of Trade committee tried to change their requirement, because someone knew that there was a problem in the regulation. However, the organizational pressure forced the committee to ignore the consideration and made the Titanic carry only 20 lifeboats. Lastly, it contributed to "failed to evacuate" and weakened the barrier of "evacuation with lifeboats".

4.20 *Lack of lifeboat drill*

Not only were the Titanic's lifeboats too few to save all its passengers and crew, but they were not even used to their full capacity. Total capacity of lifeboats was 1,176 persons but only 706 persons were saved. Almost five hundred of those who died could have been saved, if all the boats had departed fully laden (Ward, 2012, Smith and Rayner, 1912). The major reason affecting it was the lack of lifeboat drill. There had been no proper boat drill, nor a muster, and many of the crew did not join the ship until a few hours before sailing (Compton, 2012). As a result, the crew of the Titanic were not prepared at all when disaster hit. This is applicable to the energy-barrier model, HRO theory and resilience engineering. The crews of the Titanic were not prepared for the evacuation and failed to respond. It is a failure of ability to respond in resilience engineering and a failure of anticipation of the unexpected and contain the unexpected in HRO theory (Weick and Sutcliffe, 2001, Rosness et al., 2010). This led to "failed to evacuate" and weakened the barrier of "evacuation with lifeboats".

4.21 *Failed to evacuate*

It is a result of the above two conditions (Section 4.19 and 4.20), and therefore "failed to evacuate" is applicable to the energy-barrier model, MMD model, HRO theory, conflicting objectives perspective and resilience engineering.

5 RESULT

The relations between the 23 causes of the Titanic accident and the six accident perspectives have been discussed in Section 4, and the result is summarized in Table 2.

The result shows that the accident of the Titanic consists of causes from different accident perspectives, and none of them can explain the entire conditions and events alone, except for the energy-barrier model. MMD model and NAT are applicable to only small part of the accident. The conflicting objective perspective, HRO theory and resilience engineering are related to nearly half of the accident causes only. It means that focusing on only one perspective may narrow our viewpoint and make us omit other important causes. For example, regarding the MMD model, the disaster of the Titanic occurred because of lack of information flow. Someone in the rule making committee knew the problem of lifeboat requirements and several crew knew that something was wrong during navigation. However, they are not the only causes of the accident, but only a small part of it. There were other important causes like "pressure of record breaking run", "insufficient lookout", "low quality rivets", and so on.

NAT, HRO theory, and resilience engineering are only relevant to operational causes, while the other perspectives are applicable to both operational

Table 2. Titanic accident and six major accident perspectives.

No.	Events and conditions	Energy-barrier	MMD theory	NAT	HRO theory	CO perspective	RE
1	Usual but unusual amount of icebergs	x			x		x
2	Wireless operator busy	x			x	x	x
3	Not understanding urgency	x	x		x		x
4	Ignorance of ice warnings	x	x		x	x	x
5	Pressure of record breaking run	x				x	
6	Standard practice	x			x		x
7	High speed in ice field	x			x	x	x
8	Weather conditions	x					
9	Missing binoculars	x					
10	Insufficient lookout	x			x		x
11	Spot iceberg too late	x		x	x		x
12	Frantic manoeuver	x			x		x
13	Insufficient turn	x			x		x
14	Collide with iceberg	x	x	x	x	x	x
15	Poor watertight compartments	x				x	
16	Single side hull	x				x	
17	Low quality rivets	x				x	
18	Get serious hull damage and sink	x				x	
19	Californian ignored rescue signal	x	x				
20	Failed to be rescued	x	x				
21	Lack of lifeboats	x	x			x	
22	Lack of lifeboat drill	x			x		x
23	Failed to evacuate	x	x		x	x	x

and design matters. Too much attention to those perspectives may lead us to overlook design and installation problems.

The energy-barrier model is related to all causes of the disaster of the Titanic, but it cannot explain the reason why those causes had occurred. Details of each cause can be supported by other perspectives. For instance, "lack of lifeboats" weakened the barrier of "evacuation with lifeboats" but the energy-barrier model cannot explain why there were not enough lifeboats on the Titanic. With MMD model, we can find that there was an insufficient information flow in rule making process, and conflicting objectives perspective can point out that enough lifeboats were not equipped because the owner wanted much more free space.

6 DISCUSSION

Focusing on only one accident perspective is not enough to understand entire accident causes. All of the perspective are correct but the reason every perspective is describing it differently is because they view the accident from different viewpoints. An integrated accident model is therefore necessary for an overall understanding of an accident. The basis can be the energy-barrier model because it can provide an explicit and overall view on the causes of an accident (Rosness et al., 2010), and it has been shown that all of the causes, in the Titanic accident, are directly or indirectly relevant to the energy-barrier model. The other five perspectives can support the energy-barrier model and explain why weakening or strengthening of barriers occurs. The integrated accident model for the Titanic is given in Figure 3. The integrated accident model can help us explain the whole accident causes, and therefore we can distribute our limited resources efficiently to maintain barrier functions. For instance, the first barrier, "spot iceberg and avoid collision" is relevant to all five accident perspectives, while the second one, "hull structure", is related to only one perspective. This means that the first barrier may be influenced by much more factors than the second one, and therefore we need to pay more attention to the first barrier to maintain the entire barrier of the vessel with limited resources.

Another interesting point is that HRO theory and resilience engineering show exactly identical aspect on the result. If one is relevant to HRO theory, then it is always related to resilience engineering, and vice versa. In fact, there are many

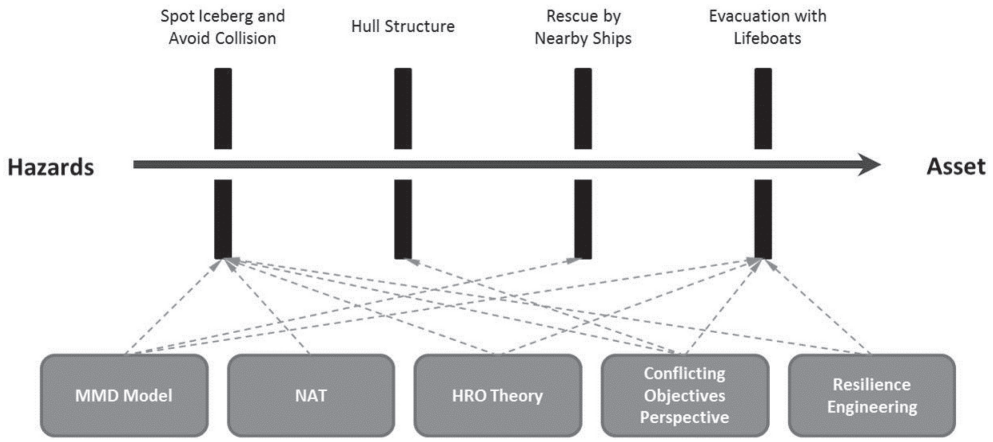


Figure 3. Integrated accident model and Titanic accident.

similarities between the two perspectives. Both of them deal with operational factors mainly and focus on successes instead of failures. Five elements of mindfulness of HRO theory resemble four abilities to succeed of resilience engineering. Comparing those two perspectives and investigating differences in actual accident cases can be an interesting future work.

Lastly, the result of applying accident perspectives to the Titanic accident has shown that all of the conditions and events are, directly or indirectly, relevant to the energy-barrier model. The reason for this may be that the paper applied MTO analysis to accident investigation, which is basically founded on the energy-barrier model. We may find other factors which are not related to the energy-barrier model if we analyze the accident with other methods like the Functional Resonance Analysis Method (FRAM) or Systems-Theoretic Accident Modelling and Process (STAMP). Applying those methods and comparing the differences can be the subject for a future study.

7 CONCLUDING REMARKS

The paper has investigated the accident of the Titanic and applied six accident perspectives to the causes. It has been found that there were a total of 23 contributed to the disaster. Some of them were related to all of the six perspectives, while the others were relevant to only small part of them. It is concluded that a single accident perspective cannot explain entire accident causes and sequences, but combination of the perspectives can help overall understanding of the accident of the Titanic. Based on this result, the paper has suggested a concept of an integrated accident model which includes every accident perspective based on the energy-barrier model. Through this integrated accident model, we can understand an accident in overall point of view and distribute limited resources to each barrier in effective way.

ACKNOWLEDGEMENTS

The authors with to thank Ann Britt Miberg Skjerve from IFE in Norway for giving us the idea to use the Titanic as a case for this paper.

REFERENCES

BBC. 2011. *Titanic: How can a disastrous ship be celebrated?* [Online]. Available: http://www.bbc.co.uk/news/magazine-13593391 [Accessed 15/12 2013].

BBC. 2012. *Titanic—Southampton Remembers* [Online]. Available: http://www.bbc.co.uk/programmes/b01flx8k [Accessed 15.12 2012].

Beesley, L. 2008. *The Loss of the S.S. Titanic*, Forgotten Books.

Bento, J. 1999. Human–Technology–Organisation; MTO-analysis of event reports. OD-00-2. (In Swedish). Restricted.

Compton, N. 2012. *Titanic on Trial: The Night the Titanic Sank, Told Through the Testimonies of Her Passengers and Crew,* Bloomsbury Academic.

Eaton, J.P. & Haas, C.A. 1996. *Titanic: Destination Disaster: the Legends and the Reality,* Norton.

Foecke, T. 2008. What really sank the Titanic? *Materials Today*, 11, 48.

Gibson, J.J. 1961. The contribution of experimental psychology to the formulation of the problem of safety–a brief for basic research. *Behavioral approaches to accident research*, 77–89.

Haddon, W. 1970. On the escape of tigers: an ecologic note. *American Journal of Public Health and the NATIONS HEALTH*, 60, 2229–2234.
Haddon, W. 1980. The basic strategies for reducing damage from hazards of all kinds. *Hazard prevention*, 16, 8–12.
History. 2012. *Titanic* [Online]. Available: http://www.history.com/topics/titanic [Accessed 15.12 2012].
Hollnagel, E. 2004. *Barriers and accident prevention*, Ashgate Publishing, Ltd.
Hollnagel, E. 2008. Risk+ barriers = safety? *Safety Science*, 46, 221–229.
Laporte, T.R. & Consolini, P.M. 1991. Working in practice but not in theory: theoretical challenges of "high-reliability organizations". *Journal of Public Administration Research and Theory: J-PART*, 1, 19–48.
Lightoller, C.H. 2010. *Titanic and Other Ships*, Lulu Enterprises Incorporated.
Nationalgeographic. 2012. *Titanic 100 Years* [Online]. Available: http://channel.nationalgeographic.com/channel/titanic-100-years/ [Accessed 15.12 2012].
Perrow, C. 1984. Normal accidents: Living with high risk systems. New York: Basic Books.
Pidgeon, N. & O'leary, M. 2000. Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science*, 34, 15–30.
Rapport, N.B. 2004. Enron, Titanic, and the Perfect Storm. Scholary Works.
Rasmussen, J. 1997. Risk management in a dynamic society: a modelling problem. *Safety science*, 27, 183–213.
Rochlin, G.I., La Porte, T.R. & Roberts, K.H. 1987. The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review*, 40, 76–90.
Rollenhagen, C. 1995. *MTO: en introduktion: sambandet människa, teknik och organisation,* Studentlitteratur.
Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K. & Herrera, I.A. 2010. Organisational Accidents and Resilient Organisations: Six Perspectives Revision. *Trondheim: SINTEF Industrial Management*.
Sklet, S. 2004. Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials*, 111, 29–37.
Smith, W.A. & Rayner, I. 1912. "Titanic" Disaster Report Washington: Committe on Commerce United States Senate.
Turner, B.A. & Pidgeon, N.F. 1978. *Man-made disasters*, Wykeham Publications (London).
Ward, G. 2012. *The Rough Guide to the Titanic*, Rough Guides, Limited.
Weick, K.E. & Sutcliffe, K.M. 2001. *Managing the unexpected*, Jossey-Bass San Francisco.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Usability of accident and incident reports for evidence-based risk modeling of ship grounding

A. Mazaheri & J. Montewka
Department of Applied Mechanics, Marine Technology, Research Group on Maritime Risk and Safety, Aalto University, Espoo, Finland
Kotka Maritime Research Center, Kotka, Finland

ABSTRACT: This paper presents study of 22 grounding accident reports by the Finnish Accident Investigation Board and 73 voluntary near-miss grounding reports from the ForeSea® incident database. The objective was to find out the usability of accident and incident reports for evidence-based risk modeling of ship grounding accidents. A version of Human Factors Analysis and Classification System (HFACS) suitable for grounding accident analysis is introduced as a framework to review the accident reports. Accident reports are shown as a reliable source of evidence to extract the most significant contributing factors in grounding accidents. However, the credibility of voluntary incident reports is considered low at their current form, and their usability for the evidence-based risk modeling is questionable.

1 INTRODUCTION

Risk managers should usually use risk models to understand the behavior of a system and its components in order to mitigate the involved risks by implementing proper control measures (IMO, 2002). In this regard, a suitable model for risk management purposes should reflect the available background knowledge on the system and its components (Aven, 2013, Montewka et al., 2014). Currently available risk models for maritime risk analysis are not proper enough for risk management purposes as they are mostly based on the intuition of the developers rather than the evidence; thus they may not necessarily presenting the true available knowledge of the system. For the review of the risk models of ship grounding, the reader is referred to (Mazaheri et al., 2013b). The lack of knowledge about the underlying causes of accidents leads to the evidential uncertainty of any model attempting to describe this type of accident, (Aven and Zio, 2011). To decrease this uncertainty, evidence-based modeling that addresses real accident scenarios is encouraged, as opposed to development of imaginary scenarios, (e.g. Kristiansen, 2010, IMO, 2012).

One of the main sources of the evidence that is available and can be used for risk modeling is accident reports that are prepared by expert accident investigators (Schröder-Hinrichs et al., 2011). Since obtaining primary data about an accident that has happened in the past is nearly impossible, using accident reports as a secondary source of data is unavoidable (Mazaheri et al., 2013c). There are some concerns regarding using only accident reports for modeling, though. One is that the accidents are scarce in frequency, thus the number of scenarios that can be analyzed is limited (Ladan and Hänninen, 2012). To overcome this imperfection, one of the suggested solutions is to utilize incident reports, as incidents occur much more frequently than accidents (Bole et al., 1987). Besides, since incidents are governed by the similar mechanism and underlying factors that cause accidents (Ladan and Hänninen, 2012) but they did not end in actual accidents, analyzing the incidents may likely give insights about the in-placed risk control options that stopped the incident to become an accident. Here, an incident or near-miss refers to an individual or a series of mishaps that did not result in a serious accident like ship grounding.

Accident and incident reports are useful for uncovering the factors that have contributed to the occurrence of a mishap as well as the level of importance of each factor. Besides, the way that the contributing factors are linked together may be understood from such reports. In this regard, the aim of this paper is to study the usability of the accident and incident reports for evidence-based modeling by assessing the type of knowledge that one can extract from these reports. As Lundberg et al. (2009) highlighted, in practice the result of an accident analysis depends on two issues namely the causes and the causality. The causes are the contributing factors that their presence in the accident is observed, and the causality is related

to the mechanism that the causes are connected and cause the accident at the end. In this paper, we merely look for the presence of different causes in the causal networks of grounding accidents based on the reviewed reports, and the causality relation analysis is left for further studies.

The paper is organized as follows: Section 2 introduces the accident and incident reports that are used for the study. The applied methodology for reviewing the reports for evidence-based modeling is presented in section 3. Section 4 presents the obtained results, whereas Section 5 discusses them. Section 6 concludes the paper.

2 REVIEWED REPORTS

2.1 *Accident reports*

Accident reports are categorized as a secondary source of data, in which the reports are prepared from the primary data that the investigator obtained first-hand by interviewing the operators and analyzing the evidence after an accident (Mazaheri et al., 2013c). In maritime safety analysis, the official accident reports that are prepared by the accident investigation boards normally present valuable information and knowledge regarding why and how an accident happens. For this study, we have utilized the accident reports of the grounding accidents prepared by Accident Investigation Board of Finland (AIB). AIB has the policy to run investigations on: 1) marine accidents that happen in the Finnish water territories no matter which flag vessels are involved; 2) marine accidents that happen outside the Finnish water territories if at least one involved ship flies the Finnish flag. However, not all of the accidents falling in the above criterion will be investigated, rather only those accidents that the acquired knowledge can enhance the safety awareness in marine traffic, (AIB, 2012). In the publicly available database of AIB, there exist 77 reports of grounding accidents that happened between the years 1995–2012. The majority of the reports are written in Finnish language and few reports are also prepared in Swedish language. From among the available reports, 22 reports have English translations and they used in this study.

Although more systematic analysis and attention towards the organizational contribution factors can be seen in the recent reports of AIB, the structures of the reports have more or less the same over the last two decades. They are all started with a summary, which briefly explains the event and the findings of the investigators. The reports continue with general description of the vessel, external condition at the time of the accident, and then the accident and the possible performed rescue operations. These are followed by the analysis of the accident and the causes. At the end, the report is concluded by presenting the causal chain of events and the underlying factors in the accident, as well as some recommendations to improve maritime safety. The parts that are fully reviewed for this study are *summaries*, *analyses*, and the *conclusions*. However, for some of the reports, other parts are also browsed in order to better understand the accident and the sequence of the causal events.

2.2 *Incident reports*

On the contrary to the accidents, there is almost no available systematic reporting system for incidents. Currently, there are quite few available sources that can be used for obtaining the near-miss data, of which not all are available for public use, see for example (Ladan and Hänninen, 2012). For this study, we have used the incident reports available in the ForeSea® database, which is an anonymous, voluntary, and feed-by-users database that was initiated by Finnish and Swedish government agencies. The database was created in order to collect the hazardous conditions that are not normally reported to authorities (ForeSea, 2014). Reporting to ForeSea® can be performed only by registered users and by filling a form with four questions. The parties need to answer the questions in their own words as clearly as possible. The questions are: *What did happen?; What did cause the event?; What were the consequences of the event?; What measures were taken?* The answers are then first handled by a third party, in which the parts that can jeopardize the anonymity will be removed and some key words are assigned to each case to make it searchable, and finally it is added to the database.

In the database of ForeSea®, there exist 3046 reports (accessed on 10.05.2014), of which 1715 of them are categorized as near-misses or non-conformity. For the purpose of this study, we use 73 cases, which are returned as connected to grounding.

3 METHODOLOGY

3.1 *Accident reports*

Since the accident reports were prepared in a systematic way by expert accident investigators, in order to uniformly extract the knowledge from all the reports, a framework is needed for reviewing the reports. There are a handful of tools and frameworks available for accident and incident analyzing and reporting (Johnson, 2003), which are mostly based on linear or non-linear accident theories that deal with complex socio-technical systems.

From the way AIB reported the investigation, it is understood that a complex linear accident theory has been utilized for investigating the accidents. Therefore, we have utilized a redefined version of the well established Human Factors Analysis and Classification System (HFACS) framework to review these reports.

HFACS is based in the "Swiss Cheese" model of human error, (Reason, 1990), which looks at four levels of active errors and latent failures, including 1) unsafe acts, 2) preconditions for unsafe acts, 3) unsafe supervision, 4) organizational influences. It was initially developed to study the contribution of human elements in military aviation accidents (Shappell and Wiegmann, 1997, Shappell and Wiegmann, 2000). However, the framework has been developed further to cover environmental factors (machinery failures) and meteorological conditions (Wiegmann et al., 2005). The success of the method in detecting the contributing latent and active failures in the accident analysis made the method popular in the field of accident analysis. It is vastly used in analysis of civil aviation accidents (Shappell et al., 2007), railroad (Reinach and Viale, 2006) and maritime (Chen and Chou, 2012, Chen et al., 2013). Reinach and Viale (2006) have developed the method by adding the fifth level, namely "external factors", to the initial four levels in order to cover the latent failures, which are believed to be specific for a particular domain under study. The same practice is followed by recent studies that used HFACS; (e.g. Schröder-Hinrichs et al., 2011, Chauvin et al., 2013, Chen et al., 2013).

Since an accident is unique from its own perspective, frameworks like HFACS try to assign the unique causes of an accident into more global factors to give better understanding of the phenomena by cumulating the causes into frequent factors. In this regard, having a specific framework with more specialized global factors for each domain and purposes seems beneficial. The different versions of HFACS that are recently introduced in the maritime domain support this belief, for example HFACS-MA (Chen et al., 2013) for general maritime accidents, HFACS-Coll for collision accidents (Chauvin et al., 2013), and HFACS-MSS for machinery space accidents (Schröder-Hinrichs et al., 2011). Therefore, we have revised HFACS to a specific version suitable for grounding accidents analysis (HFACS-Ground; see Fig. 1) by implementing factors that are more related to grounding accidents. HFACS-Ground is also built as a five-level framework and has many similarities with HFACS-Coll and HFACS-MA. However, in addition to the factors that cover traffic control and piloting services as affecting factors on grounding accident, "infrastructure" is added as a latent failure subcategory to the "environmental factors" in order to cover the issues related to the complexity of waterway, like waterway design and markings, which are believed to have effect on the frequency of grounding accidents (Mazaheri et al., 2013a). The accident reports in this study were then reviewed using HFACS-Ground framework.

In order to avoid subjective interpretations of the reports, only the factors that were explicitly mentioned in the reports were extracted and classified based on the HFACS-Ground. This basically means that the reviewers avoided further investigating the causality of the mentioned causes in the reports up to the higher levels. In total, HFACS-Ground contains 147 factors. Each factor is assigned a nanocode, which are used to catch the frequency of the causal factors mentioned in the reports.

3.2 *Incident reports*

In contrary to the accident reports that were prepared in a systematic analytical way by expert accident investigators, the incident reports suffer from the lack of a systematic view of the event. The reports are short (from few sentences to maximum of half a page) and have been reported by people of different expertise. This has resulted that the reports have different qualities with regard to the provided data and information. Most of the reports have reported only what have been seen, and merely few have tried to hypothesize the possible causes of the events. Even those few reports lack the evidence to support the provided hypotheses. Therefore, using HFACS-Ground for analyzing incident reports is not practical; rather it might be misleading as normally active failures are the only causes that are reported in the incident reports. Therefore, another approach has been followed in this study for reviewing the incident reports. The incident reports were read through and the explanatory phrases from the texts were extracted as the mishaps that caused the incident. Thereafter, in order to catch more frequent causes, the extracted phrases from all the reports were grouped into 22 more general categories, see Table 2.

3.3 *Statistical analysis*

To identify any significant link between the extracted contributing factors from both types of the reports, the statistical dependencies of the factors are studied two-by-two using Pearson correlation coefficient (r). The reliabilities of the studies are tested using χ^2-goodness-of-fit test. The Spearman rank correlation coefficient (ρ) is also used to study the rank relation between the frequencies of

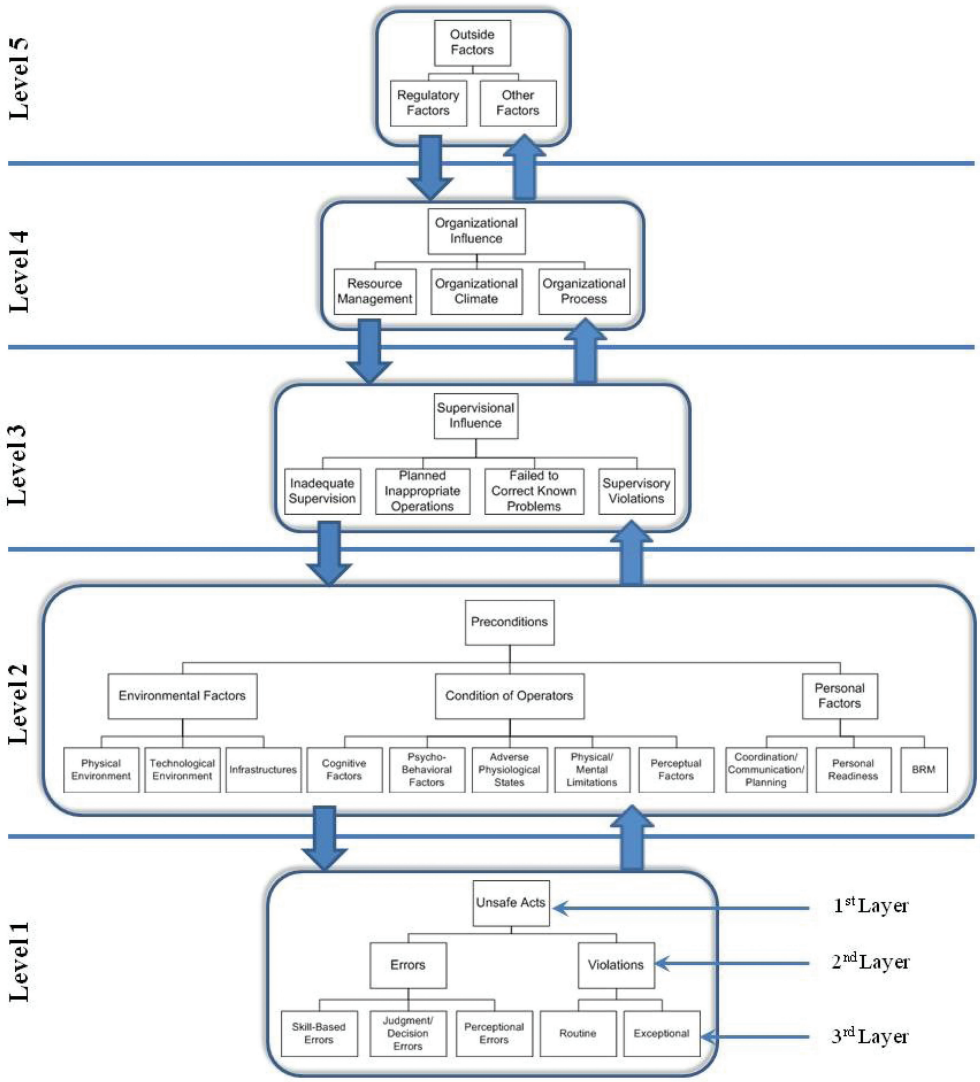


Figure 1. Human factors analysis and classification system for grounding (HFACS-Ground).

the extracted contributing factors from the accident and incident reports.

4 RESULTS

4.1 *Accident reports*

Table 1 shows the results of the reviewing of the accident reports as the relative frequency of each class of factors. The relative frequency expresses the number of a specific class of factors in the reports in relation to the number of all the other factors in each level (see Fig. 1). It is seen that levels 1 and 2 of the failures as *unsafe acts* and *preconditions* are seen more frequently in the accident reports. Level 5 of failure as the *external factors* has the smallest frequency. Level 2 of failure as *preconditions* has the highest frequency among other levels of failures, which may be the result of having the largest coverage of the factors.

Out of 147 causal factors, covered by HFACS-Ground, 88 factors belong to this level. Table 1 shows that "*judgment/decision errors*" is the most frequent active failure. When this is seen together with the most frequent latent failure, as issues related to *communication/cooperation/planning*,

Table 1. Analyzing the accident reports using HFACS-Ground.

Level		1st Layer	%	2nd Layer	%	3rd Layer	%	Rank
Active Failure	1	Unsafe Acts	16.8	Error	95.6	Skill-Based	22.7	9
						Judgment/Decision	68.2	2
						Perceptional	9.1	11
				Violation	4.4	Routine	50	13
						Exceptional	50	13
Latent Failure/Condition	2	Preconditions	55.5	Environmental Factors	33.6	Physical Environment	33.3	5
						Technological Environment	45.1	3
						Infrastructures	21.6	6
				Condition of Operator	26.3	Cognitive Factors	21.5	10
						Psycho-Behavioral Factors	57.5	4
						Adverse Physiological Sates	25	8
						Physical/Mental Limitations	7.5	12
						Perceptual Factors	2.5	15
				Personal Factors	40.1	Coordination/Communication/Planning	83.6	1
						Personal Readiness	0	25
						SRM (incl. BRM)	16.4	7
	3	Unsafe Supervision	12.8	Inadequate Supervision			51.4	16
				Planned Inappropriate Operations			11.4	22
				Failed to Correct Known Problems			17.2	20
				Supervisory Violations			20	19
	4	Organizational Influence	13.9	Resource Management			42.1	17
				Organizational Climate			15.8	21
				Organizational Process			42.1	17
	5	External Factors	1.1	Regulation Gaps			33.3	24
				Other Factors			66.7	23

one may see the importance of the proper planning and communication, since most of the errors may be avoided as a result of that. Nevertheless, this is a causality issue that needs to be further studied. Table 1 also shows that the most frequent failures are among the two first levels of failures in HFACS-Ground framework. Since these two first levels of failures are mostly related to the failures of the frontline operators, this shows that: either the reviewed accident reports somehow failed to further investigate the top tier causes as *organizational*, *supervisional*, and *external* factors; or those preconditions may have been less involved in the causality network of the accidents. If the first conclusion is true, then there is the risk that the recommendations that are made based on these investigations may not be able to tackle the actual problem.

4.2 *Incident reports*

Table 2 shows the results of the reviewing of the incident reports as the relative and observational frequencies. The relative frequency of a category is in relation to all the categories. The observational frequency puts a specific category in relation to all reviewed reports.

It can be seen that *mechanical failure or unexpected behavior* of equipment by far is the most frequent mishap category that is reported by the incident reports (74%). The next category in the list is *errors*, which stands second to mechanical failure by a great distance (23%). Knowing that the incident reports are voluntary reports written mostly by the person who was involved in the incident, this may be the sign that people tend to mostly see the technological failures as the cause of a mishap rather than a human error. Although "*errors*" comes next in the list, all the errors reported in the reviewed reports were errors made by a person other than the reporter and most of them were people out of the circle of the crew, like port operators or an individual in a third company. Only one report contained an error made by a crew member, which was reported by his superior as the cause of the mishap. This may show that despite of the existing oppose discussions for the blame culture (e.g. Russell, 1999, Bond, 2008), this culture is still alive in the mind of mariners that makes them hesitate to either see or report the mistakes made by themselves or their close colleagues.

4.3 *Statistical analysis*

Since the accident and incident reports are reviewed with different approaches, in order to be able to compare the extracted knowledge from them we transferred the results of the accident reports to the categories used for the incident reports (Table 2). Small Spearman rank correlation ($\rho \approx 0.03$) between the rank orders of causes for accident and

Table 2. Frequency of the extracted causes from the incident reports in compare with the translated causes from the accident reports.

General Categories	Incident Reports		Accident Reports	
	Relative Frequency %	Observational Frequency %	Relative Frequency %	Observational Frequency %
Accidental loss of control	9.0	20.3	0.7	4.1
Alarm missing or not clear	0.6	1.4	1.9	11.0
Bad Visibility	0.6	1.4	4.3	24.7
Darkness	0.6	1.4	2.6	15.1
Errors (Skill-based/Judgment/ Decision)	10.2	23.0	10.4	60.3
Fairway	4.2	9.5	5.2	30.1
Hazardous natural environment	2.4	5.4	5.9	34.3
Inappropriate communication & cooperation	0.6	1.4	11.6	67.1
Inappropriate maintenance	2.4	5.4	0.2	1.4
Inappropriate regulations & practices (incl. BRM)	9.0	20.3	6.9	39.7
Inappropriate route planning	0.0	0.0	6.4	37.0
Inappropriate ship/bridge system design or equipment	3.6	8.1	4.5	26.0
Inappropriate training	5.4	12.2	4.5	26.0
Lack of redundancy	7.8	17.6	1.4	8.2
Lack of situational awareness	0.6	1.4	3.1	17.8
Mechanical failure or unexpected behavior	32.9	74.3	3.8	21.9
Organizational factors & support	5.4	12.2	5.9	34.2
Other Personal factors	1.2	2.7	5.0	28.8
Ship moving off course	0.6	1.4	4.0	23.3
Traffic	2.4	5.4	0.5	2.7
Under-manning of necessary stations	0.0	0.0	4.3	24.7
Violation of good seamanship practices	0.6	1.4	6.9	39.7

incident reports shows the difference between the most frequent causes in the accident and incident reports. This difference may be interpreted in two ways. The first interpretation comes from the way that the reports are prepared. Since a systematic approach is followed for the accident reports, they may be considered more valid. Thus, the big difference between the rank orders of the important contributing factors in accident and incidents reports may be a sign that the involved uncertainties in the incident reports are high, which then makes the incident reports almost useless for the purpose of evidence-based modeling. The reports may only act as alerts of the possible threats in the working places. The second interpretation comes from the idea that the incidents are incomplete chains of events towards an actual accident. This means that the more in deep parallel analysis of accident and incident reports may reveal the possible risk control options that were in place to stop the incident to become an accident.

For instance, although *errors* has the second rank in frequency in both types of reports, based on the frequency of *inappropriate communication and cooperation* in the accident and incident reports, we may conclude that "appropriate communication and cooperation" in the incident cases stopped the situation to become serious that it would result in an accident; thus highlighting the importance of a proper interaction between the crew. This conclusion can be confirmed at some level by the statistical results of the study. Inappropriate communication and cooperation is linked to inappropriate route planning ($r = 0.5$, $p < .05$) in the accidents. The importance of appropriate route planning, itself, can be understood by the link that it has with presence of a pilot ($r = 0.5$, $p < .05$) in accident cases, knowing that in 64% of the reviewed accident reports a licensed pilot was present onboard the vessel. It is worth to mentioned that there is a strong link between inappropriate communication and personal factors ($r = 0.7$, $p < .001$) in incident reports, which can show how personality of crew affects the safety through inappropriate communication.

The results also show that the lack of redundancy is an affecting factor in safety as it is reported by 17.6% of the incident cases and shows a strong link with the accidental loss of control ($r = 0.8$, $p < .001$) in the accidents. The results of the accident cases show that the accidental loss of control, itself, can be affected by the inappropriate training ($r = 0.8$, $p < .001$) and the inappropriate maintenance ($r = 0.7$, $p < .05$). Under-manning, which is reported by almost 25% of the accident cases, shows strong connection with inappropriate regulation and practices ($r = 0.6$, $p < .001$) that also includes BRM. This can illustrate the importance of proper policies and training, especially in human resource management, in the maritime safety.

5 DISCUSSION

The results show that the most frequent active failure contributed in the reviewed grounding accidents is the operator errors in decision or judgment, as it comes the second most frequent causes in both accident and incident reports. Combining this knowledge with the high/low frequencies of inappropriate communication and cooperation in accident/incident reports respectively, the importance of proper interaction between the crew members may be highlighted. Most of the operator

errors may be detected and avoided on time through proper monitoring and checking, which is the result of a proper communication and cooperation. Moreover, statistical analysis of the extracted causes in accident and incident reports suggests that inappropriate planning is an important factor affecting safety with regard to the grounding accident. The results show that inappropriate planning can affect maritime safety as it may even cancel out the presence of a licensed local pilot onboard.

Most of the detected contributing factors in the reviewed accident reports belong to the first and second levels of failures in Figure 1, which is mostly related to the operator failure. This may be interpreted in two ways: 1) a more conservative interpretation is that active and latent failures of the frontline operators are the most responsible failures for grounding accidents; which then suggests the need for causality analysis of these failures in order to be able to implement proper control measures; 2) another interpretation, could be that the used frameworks for accident analysis by AIB are not capable of deep analyzing an accident up to the higher levels of failures (level 3 upwards in Fig. 1); which then suggests the use of a more proper and updated framework for the investigations. It is worth mentioning that not only there was no single unique framework used in the investigation of the accidents by AIB, but also in neither of the reviewed reports HFACS has been mentioned as the used framework for investigation. Therefore, since the presented knowledge in each report is affected by the framework that is used for investigating the accident (Lundberg et al., 2009), our study shows that the use of a different framework to review the reports does not have much effect on the knowledge that can be obtained.

The analysis of the reviewed incident reports shows that the current practice of reporting the near-misses cannot contribute much to the evidence-based modeling; because the available evidence only highlight active failures as the contributing factors in the occurred mishap. Besides, incident reports have the tendency to overlook the mishaps related to organizations and operators, and emphasize more on technology failures. This is either because the reports are not prepared based on a holistic investigation and only the observations are reported; or that the blame culture is still highlighted in the minds of the crew that even in an anonymous report they hesitate to report other causes than technology failures. This may be seen as a problem of the voluntary near-miss report systems, as it makes the incident reports to be unreliable with regard to detecting the significant causes of an accident that can be used in evidence-based modeling. Nevertheless, since incidents are broken chain of hazardous events that did not end in an accident, if the current practice of reporting near-misses is changed into a more systematic way of analysis, these reports may be used in evidence-based modeling in combination with accident reports in order to find proper control options. One does not have much to say with regard to the possible controlling options only by knowing about the most frequent causes. Effective control options can be defined and implemented only if the causality has been discovered in the accident, which was not studied in this paper. However, the presented study shows that the statistical analysis on the frequency of the causes may give hints regarding the causal relations between the extracted causes. Causal relations may tell why a mishap, like inappropriate communication, has occurred.

Moreover, the majority of the reviewed near-miss grounding cases were categorized into near-miss groundings because a mechanical problem, like steering or engine malfunction, could have led to the possible loses of maneuverability. Therefore, near-miss grounding cases that are extracted from the ForeSea® database may not be precisely a near-miss accident from our perspective. This again also shows that the incident databases should be used cautiously in evidence-based modeling, as the near-miss definition of an accident may differ with the one that is used in such databases.

Despite the above discussions, the study is bounded with the involved uncertainties. Use of specific databases as AIB and ForeSea® to extract the reports may introduce some level of uncertainty that roots to the way that the databases are formulated. Thus, the study needs to be repeated using reports prepared by other authorities and data providers. The main uncertainty in the result, however, comes from the small used datasets as only 22 accident reports are reviewed. In that respect, increasing the number of reviewed reports can increase the validity of such studies.

6 CONCLUSION

The possibility of using accident reports and voluntary incident reports in evidence-based risk modeling is investigated using accident reports prepared by Finnish Accident Investigation Board and ForeSea® incident database with regard to grounding cases. A version of HFACS framework as HFACS-Ground is introduced to review the grounding accident reports. In conclusion, accident reports are shown as a reliable source of evidence to extract the most significant contributing factors in grounding accidents. Nevertheless, their validity will be better confirmed if their usability for extracting the causal relation between the contributing factors is also tested in future studies.

On the other hand, voluntary incident reports are shown as not very useful in their current form for evidence-based modeling. They may only be useful in the way that they are currently used, as the alerts for possible hazards in the daily operation of shipping. In order to make the incident reports useful for accident modeling, first they need to be prepared in a more systematic way that can address the causality of the mishaps, and second a more consistent definition of near-miss situation needs to be defined to reliably assign occurred mishaps to a specific type of accident.

REFERENCES

Ackoff, R.L. 1989 From Data to Wisdom. *Journal of Applied Systems Analysis,* 16, 3–9.

AIB 2012 Accident Investigation Board of Finland.

Aven, T. 2013 A Conceptual Framework for Linking Risk and the Elements of the Data-Information-Knowledge-Wisdom (DIKW) Hierarchy. *Reliability Engineering and System Safety,* 111, 30–36.

Aven, T. & Zio, E. 2011 Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making. *Reliability Engineering and System Safety,* 96, 64–74.

Bole, A.G., Dineley, W. & Nicholls, C.E. 1987 *The Navigation Control Manual,* London, William Heinemann Ltd.

Bond, J. 2008 The Blame Culture-An obstacle to improving Safety. *Journal of Chemical Health and Safety,* 15, 6–9.

Chauvin, C., Lardjane, S., Morel, G., Clostermann, J.-P. & Langard, B. 2013 Human and Organizational Factors an Maritime Accidents: Analysis of Collisions at Sea Using The HFACS. *Accident Analysis & Prevention,* 59, 26–37.

Chen, S.-T. & Chou, Y.-H. 2012 Examining Human Factors for Marine Casualties Using HFACS—Maritime Accidents (HFACS-Ma). *12th International Conference on ITS Telecommunications.* Taipei, Taiwan.

Chen, S.-T., Wall, A., Davies, P., Yang, Z., Wang, J. & Chou, Y.-H. 2013 A Human and Organisational Factors (HOFs) Analysis Method for Marine Casualties Using HFACS-Maritime Accidents (HFACS-Ma). *Safety Science,* 60, 105–114.

Foresea 2014 About the Database-Purpose http://foresea.net/about_thebank.aspx.

IMO 2002 Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process. Ed. *MSC/Circ. 1023.* London.

IMO (2012) Formal Safety Assessment, Outcome Of MSC 90—*Draft Revised FSA Guidelines and draft HEAP Guidelines.*

Johnson, C.W. 2003 Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting. Glasgow, Scotland, University of Glasgow Press.

Kristiansen, S. 2010 A BBN Approach for Analysis of Maritime Accident Scenarios. In Ale, B.J.M., Papazpglou, I.A. & Zio, E. (Eds.) *ESREL.* Rhodes, Greece, Taylor & Francis Group.

Ladan, M. & Hänninen, M. 2012 Data Sources For Quantitative Marine Traffic Accident Modeling. *Aalto University Publication Series Science + Technology 11/2012.* Espoo, Aalto University.

Lundberg, J., Rollenhagen, C. & Hollnagel, E. 2009 What-You-Look-For-Is-What-You-Find—The Consequences of Underlying Accident Models In Eight Accident Investigation Manuals. *Safety Science,* 47, 1297–1311.

Mazaheri, A., Kotilainen, P., Sormunen, O., Montewka, J. & Kujala, P. 2013a Correlation Between The Ship Grounding Accident And The Ship Traffic—A Case Study Based On The Statistics Of The Gulf Of Finland. *International Journal of Marine Navigation and Safety Of Sea Transportation,* 7, 119–124.

Mazaheri, A., Montewka, J. & Kujala, P. 2013b Modeling The Risk Of Ship Grounding—A Literature Review From A Risk Management Perspective. *WMU Journal of Maritime Affairs*. DOI 10.1007/s13437-013-0056-3.

Mazaheri, A., Sormunen, O.V.E., Hyttinen, N., Montewka, J. & Kujala, P. 2013c Comparison Of The Learning Algorithms For Evidence-Based Bbn Modeling—A Case Study On Ship Grounding Accidents. *Annual European Safety And Reliability Conference (ESREL 2013)*. Amsterdam, The Netherland.

Montewka, J., Goerlandt, F. & Kujala, P. 2014. On a systematic perspective on risk for Formal Safety Assessment (FSA). *Reliability Engineering & System Safety*, 127, 77–85.

Reason, J. 1990 The Contribution Of Latent Human Failures To The Breakdown Complex Systems. *Philosophical Transactions of The Royal Society Of London, Series B, Biological Sciences,* 327, 475–484.

Reinach, S. & Viale, A. 2006 Application of a Human Error Framework to Conduct Train Accident/Incident Investigations. *Accident Analysis & Prevention,* 38, 396–406.

Russell, L. 1999 Incident Investigation: Fix The Problem-Not The Blame. *Journal Of Chemical Health And Safety,* 6, 32–34.

Schröder-Hinrichs, J.U., Baldauf, M. & Ghirxi, K.T. 2011 Accident Investigation Reporting Deficiencies Related To Organizational Factors In Machinery Space Fires And Explosions. *Accident Analysis & Prevention,* 43, 1187–1196.

Shappell, S.A., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A. & Wiegmann, D.A. 2007 Human Error and Commercial Aviation Accidents: An Analysis Using The Human Factors Analysis And Classification System. *Human Factors,* 49, 227–242.

Shappell, S.A. & Wiegmann, D.A. 1997 A Human Error Approach To Accident Investigation: The Taxonomy Of Unsafe Operations. *The International Journal Of Aviation Psychology,* 7, 269–291.

Shappell, S.A. & Wiegmann, D.A. 2000 The Human Factors Analysis and Classification System—HFACS. In Dot/Faa/Am-00/7 (Ed. Washington Dc, Federal Aviation Administration.

Wiegmann, D., Faaborg, T., Boquet, A., Detwiler, C., Holcomb, K. & Shappell, S. 2005 Human Error And General Aviation Accidents: A Comprehensive, Fine-Grained Analysis Using HFACS. Office of Aerospace Medicine.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Winter navigation at the Baltic Sea: An analysis of accidents occurred during winters 2002–2003 & 2009–2013

O.A. Valdez Banda, F. Goerlandt, J. Montewka & P. Kujala
Department of Applied Mechanics, Aalto University, Espoo, Finland

ABSTRACT: The Baltic Sea is the busiest area during winter ice navigation in the northern seas. The winter navigation in the zone commonly presents two main scenarios: navigation when ice is not yet present but it is approaching to the area bringing the first winter storms and extremely poor light conditions, and navigation with sea ice conditions which mainly challenges the capability of the vessels in finding the best route to reach final destination. In this paper, accidents occurred in the zone during winter 2002–2003 and winters 2009 to 2013 are quantitatively and qualitatively analyzed. The aim is to accurate detect the accidents with higher frequencies during winters, the most common vessel operations involved in those accidents, the severity of the accidents, the areas where accidents are occurring, and most important, exactly under which navigational operations and sea conditions accidents are occurring. Based on the findings of this study, collisions and groundings are the most typical accidents occurring during winter time. However, the analyzed data revealed that groundings are more frequent before ice is present, and collisions are the most frequent type of accident under ice sea conditions.

1 INTRODUCTION

Collisions and groundings are the most common accidents in the Baltic Sea, including winter season with or without the presence of ice (Goerlandt, et al., 2012). Even though some specific areas within the Baltic Sea are recognize as relative safe (e.g. the Gulf of Finland), every year approximately 22 to 34 accidents occur in this zone (Kujala, et al., 2009). The collisions and groundings reported are commonly related to human failures which endanger people, environment and the whole transportation system. In the most severe cases these accidents may lead to severe damage (e.g. to the ship structure), compromising ship's integrity, and exposing people and environment to human casualties and cargo spills. In less serious cases, these accidents may result in only small damages to the hull (Kujala, et al., 2007, Kujala, et al., 2009 and Mazaheri, et al., 2013).

In this paper, the description of accidents occurred in the Baltic Sea during the winters 2002–2003 & 2009–2013 are detailed analyzed. The data analysis presented in this paper covers accidents reported on Finnish waters and/or to Finnish vessels registered by the Finnish Transport Safety Agency during the mentioned time periods. The quantitative and qualitative analyses presented in this paper have carefully assessed the accidents occurred under sea ice conditions. Thus, the aim of this study is to present which are the most common accidents occurring in the Baltic Sea during winter time, where and when these accidents are taking place, in which conditions the accidents commonly happen, and the severity of these accidents. Thereby, the outcome of this study can be used to identify when, where and how the risk of an accident is more latent during winter navigation.

2 THE BALTIC SEA DURING WINTER

2.1 *Navigating the Baltic Sea during winter*

The Baltic Sea is composed by 7 zones: Bay of Bothnia, Sea of Bothnia, Gulf of Finland, Gulf of Riga, Central Baltic, South Baltic (coast line), and Western Baltic (Danish waters) (EfficienSea, 2011). All these zones experience different weather and light conditions during winter time. For example, the northern area (Bay of Bothnia) have long periods of darkness, and heavy winter storms which represent the first challenges for the vessels navigating the zone before sea ice is present in the area. In other areas such as central Baltic, Gulf of Finland and South and Western Baltic, the light conditions are not as drastic as in the north, but in these areas, during winter the vessels have to deal with heavy banks of fog constantly (Trafi, 2011). Once the ice is present, the Bay of Bothnia is commonly the first zone which set traffic restrictions during winter. These restrictions specify which are the merchant vessels allowed to navigate the area,

and which ones can receive icebreaker assistance if needed (Trafi, 2013). In order to set limits and designate adequate assistance, the Finnish-Swedish winter navigation system has specific "ice class rules" for the requirements of structural strength and engine output for vessels to be included within a Finnish-Swedish ice class. The system also determines the minimum ice class and deadweight permitted in a certain area for icebreaker assistance (Table 1).

The restrictions begin according to the climate conditions of the zone. For example, on winter 2010–2011 the restrictions started on the 29 of November in the Bay of Bothnia, 4 of December

Table 1. Basis of traffic restrictions (Finnish Maritime Administration).

Ice class	Ice class requirements	Ice thickness
IA super	Ships with such structure, engine output and other properties that they are normally capable of navigating in difficult ice conditions without the assistance of icebreakers.	
IA	Ships with such structure, engine output and other properties that they are capable of navigating in difficult ice conditions, with the assistance of icebreakers when necessary.	Thickness of ice: > 50 cm
IB	Ships with such structure, engine output and other properties that they are capable of navigating in moderate ice conditions, with the assistance of icebreakers when necessary.	Thickness of ice: 30–50 cm
IC	Ships with such structure, engine out and other properties that they are capable of navigating in light ice conditions, with the assistance of icebreakers when necessary.	Thickness of ice: 15–30 cm
II	Ships that have a steel hull and that are structurally fit for navigation in the open sea and that, despite not being strengthened for navigation in ice, are capable of navigating in very light ice conditions with their own propulsion machinery.	Thickness of ice: 10–15 cm
III	Ships that do not belong to the ice classes referred above.	

Table 2. Description of ice types.

Ice type	Description
Fast ice	Is the sea ice that is "fastened" to the coastline, to the sea floor along shoals or to grounded icebergs
Consolidated, compact pack ice	Pack ice in which the concentration is ten-tenths and the floes are frozen together
Close pack ice	Pack ice in which the concentration is seven-tenths to eight-tenths, composed of floes mostly in contact.
Open pack ice	Pack ice in which the ice concentration is four-tenths to six-tenths, with many leads and polynyas, and the floes are generally not in contact with one another.
Very open pack ice	Pack ice in which the concentration is one-tenth to three-tenths and water preponderates over the ice.
New ice	A general term for recently formed ice that includes frazil ice, grease ice, slush, and shuga.
Level ice	Sea ice that is unaffected by deformation.
Ice Crack	Any fracture that has not parted.
Ice boundary	The demarcation at any given time between fast ice and pack ice or between areas of pack ice of different concentrations.
Estimated ice boundary	An estimation of demarcation at any given time between fast ice and pack ice or between areas of pack ice of different concentrations.
Rafted ice	Type of deformed ice formed by one piece of ice overriding another.
Ridge and hummocked ice	Ice piled haphazardly one piece over another in the form of ridges or walls. Usually found in first-year ice. And sea ice piled haphazardly one piece over another to form an uneven surface. When weathered, it has the appearance of smooth hillocks.
Window, brash ice barrier	Accumulations of floating ice made up of fragments not more than 2 m across, the wreckage of other forms of ice.
Ice Lead	Any fracture or passageway through sea ice that is navigable by surface vessels.

in the Gulf of Finland, 12 of December in the Sea of Bothnia, 12 of December in the Gulf of Riga, 1 of January in Central Baltic (EfficienSea, 2011). In this case, the winter 2010–2011 was considered a hard winter which has around 145 000 km² of ice covering the Baltic Sea (FMI, 2011). However, winter 2002–2003 was even harder, the winter restrictions started one month earlier than commonly, and the ice extent experienced was around 232 000 km².

2.2 *Winter ice conditions and their effect on ships*

Ice conditions are the resulted of the climate prevailing during the winter. Although, all winters present different characteristics every year, ice conditions are constantly measured, monitored and shared by the Finnish & Swedish Meteorological Institutes (FMI) (SMHI). Thus, the authorities, shipping companies, and the vessels navigating the Baltic Sea can be constantly informed about the current conditions and the forecast for the zone. A winter navigation map of the Baltic Sea displays information about the characteristics of the ice prevailing in different zones (Table 2), and the ice thickness on those.

One key aspect on knowing the sea ice conditions, is the opportunity to better plan the navigational pattern of a ship. This plan also serves to anticipate the possible effect of ice on ship design and performance, and also to establish in advance the necessary propulsion and the needed characteristics for maneuvering of the ship. (Daley and Riska, 1990). Thus, having monitored and reported the daily sea ice conditions, enable to potentially link those conditions with the coordinates reported in accidents during winter ice navigation.

3 ACCIDENTS AT THE BALTIC SEA (WINTERS 2002–2003 & 2009–2013)

3.1 *Data and methods*

The marine accident statistics produced in this paper, are based on the data from winters: December 2002 to April 2003 and October 2009 to April 2013. The data sources used for this analysis are provided by the Finnish Transport Safety Agency (Trafi), which consist of marine casualties reported on Finnish waters or to vessels registered to Finland. In the particular case of the reports from winters 2009–2013, identification of the accident locations is based on the coordinates of the accidents reported in that time period. And for the purposes of this paper, those coordinates have been allocated within the ice maps reported by SMHI and FMI on those dates. More details such as the kind of vessel involved in the accidents, operations performed when the accidents occurred (only 2009–2013), outcome of the accidents, and the severity of the accidents (only 2009–2013) have resulted from a qualitative data analysis performed to the collected data. The original accident data provided by FMA and Trafi originally provided de following information:

- Number of casualty report
- Date
- Occurrence severity
- Casualty event
- Damage
- Ship(s) type involved in the accident
- Latitude
- Longitude
- Casualty event description

Thus, in order to identify and extract the information relevant for this study, a qualitative method of analysis based on the "5 whys" original method from (Jones and Womack, 1996) was implemented. The adapted method in this study basically applies a questionnaire for the identification of 5 key aspects:

1. Which vessels were involved in the accident?
2. Which type of accident occurred?
3. Which severity category was given to the event?
4. Which operation was performed? (base on the analysis of the event description, an identification of the operation performed was performed)
5. And under Which ice conditions? (base on the link between coordinates reported and the ice map)

3.2 *Analysis of general accidents*

3.2.1 *Number of accidents, vessel type involved and type of accidents*

The total number of casualties in the mentioned periods, covering accidents with and without the presence of sea ice is 119. Figure 1 presents the amount by type of vessels involved on those accidents. And Figure 2 presents the percentages of the type of accidents occurred during the analyzed periods.

3.2.2 *Severity of the accidents*

The severity of the accidents is based on the reported to the Finnish Transport Safety Agency (Trafi). This severity has a three-level categorization: less serious, serious and very serious. The categorization is based on the severity of the outcome of the accident, including damages to the ships, environment and people. A very serious accident is the one that leads to human casualty and/or seriously exposing to it, and/in combination with

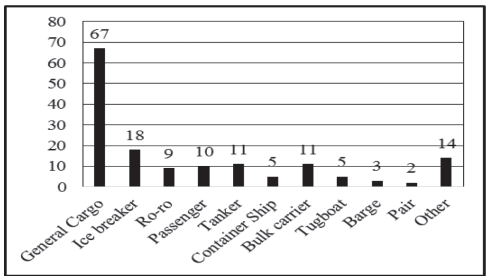


Figure 1. Type of vessels involved in accidents during winters 2009–2012 (FMA, 2003; and Trafi, 2013).

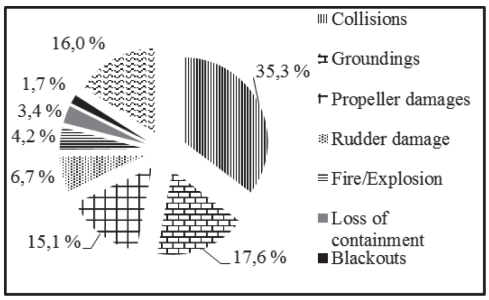


Figure 2. Percentage of the type outcome derived from the accidents (FMA, 2003; Trafi, 2013).

total lost or extremely severe damage to vessels and environment. A serious accident is the one which had severe consequences that could lead to a major impact in human safety, vessel safety and structure, and to the environment. A less serious accident is an accident which had minor repercussion in human safety, minor damage to ship machinery and structure and a no significant impact to the environment. Table 3 presents the type of accidents occurred during winters 2009–2013 and their respective designated severity.

Figure 3 presents the amount of less serious, serious and very serious accidents classified by winter and month of occurrence.

3.3 *Analysis of the accidents under ice conditions*

The accident data collected from winter 2002–2003 are all related to accidents under ice conditions. And from the 68 accidents originally reported during the winters 2009–2013, only 19 were related to operations performed under ice conditions.

3.3.1 *Vessel type, types of accidents and winter*

From the 70 accidents occurred under ice conditions 54% is related to general cargo vessels and 19% to ice breakers. Figure 4 presents the types of

Table 3. Type of accidents and severity (Trafi, 2013).

Accident type	Less serious	Serious	Very serious	Total
Collisions	21	5	1	27
With other ship	13	3	1	17
With other ship not under way	3	1	0	4
With a fixed object	5	1	0	6
Groundings	12	9	0	21
Power	7	8	0	15
Drift	5	1	0	6
Loss of containment	4	0	0	4
Oil spill	4	0	0	4
Fire/ Explosion	4	1	0	5
Fire	3	1	0	4
Explosion	1	0	0	1
Rudder damage	0	2	0	2
Loss of propulsion	1	0	0	1
Blackouts	2	0	0	2
Other accidents	6	0	0	6
Total	50	17	1	68

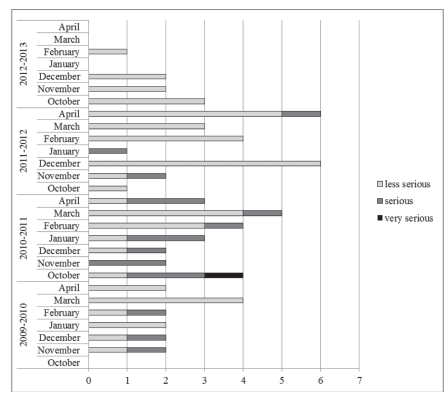


Figure 3. Accident and their severity by winter and month.

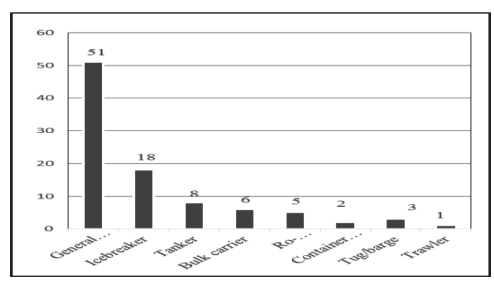


Figure 4. Type of Vessels involved in accidents under ice conditions in winters 2002–03 & 2009–13 (FMA, 2003; Trafi, 2013).

vessels involved in accidents under ice conditions. And Figure 5 presents the types of accidents occurred under ice conditions. The winter 2002–03, and the month of February were the ones with the major number of the accidents occurred.

3.3.2 *Severity of the accidents*

Table 4 presents the type of accidents occurred under ice conditions and their respective designated severity during the periods 2009–2013. Unfortunately, the data base of the winter 2002–2003 had not such classification. Thus, in winters 2009–2013, 3 accidents were designated as serious, and 16 cases were designated as less serious. There were not very serious accidents occurred under ice conditions during the analyzed time periods.

3.3.3 *Icebreaker operations*

In the 31 collisions experienced during the analyzed winters, 18 were related to the assistant operations of icebreakers. Therefore, in this section the descriptions of all icebreakers operations are introduced. There are four identified icebreaker operations (Kujala et al., 2007; Critch 2014, and Ploskonka 2013):

- *Escorting:* an ice breaker is escorting when it breaks an ice channel and the assisted ship follows the icebreaker at a recommended distance.
- *Breaking a ship loose:* an icebreaker is breaking a ship lose when it pass the ship a quite close distance and break the ice beside and in front of an assisted ship, and release the ship from ice pressure.
- *Convoy:* the operation is similar to escorting but in this case there are several ships following the icebreaker from a distance long enough to stop the ship if the ship in front gets stuck.
- *Towing:* is an operation when a ship cannot follow an icebreaker because the ice pressure makes the channel close quickly, or because the channel has too much slush ice, and/or because the assisted ship has not an appropriate performance in ice. An icebreaker may be towing one vessel while simultaneously leading a convoy of one or more other.

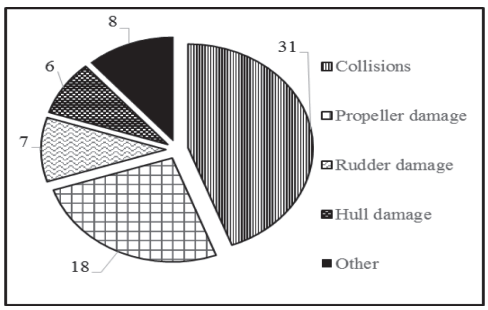


Figure 5. Types accidents under ice conditions during winters 2002–2003 & 2009–2013 (FMA, 2003; Trafi, 2013).

Table 4. Type of accidents under ice conditions and their severity (Trafi, 2013).

Accident type	Less serious	Serious	Very serious	Total
Collisions	14	2	0	16
W/ other ship	13	2	0	15
W/ other ship not under way	0	0	0	0
W/ a fixed object	1	0	0	1
Groundings	1	0	0	1
Power	1	0	0	1
Drift	0	0	0	0
Loss of containment	1	0	0	1
Oil spill	1	0	0	1
Rudder damage	0	2	0	2

3.3.4 *Ice type and ice thickness during the reported accidents*

Figure 6 presents the ice conditions and ice thickness experienced during the 19 analyzed accidents.

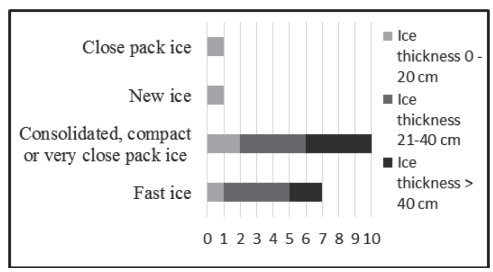


Figure 6. Ice type and ice thickness experienced when the accidents occurred (SMHI, 2013).

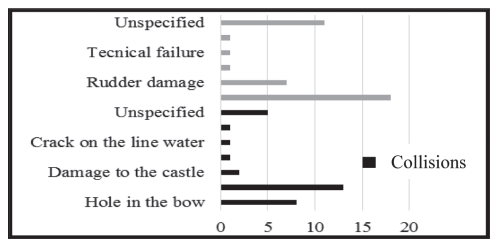


Figure 7. The generated outcome (damages) of the 70 analyzed accidents (FMA, 2003; Trafi, 2013).

3.3.5 *Outcome of the accidents*
Figure 7 presents the resulted outcome of the accidents occurred under sea ice conditions during the 5 analyzed winter periods. These outcome are presented as the common damages and ship affectations derived from the experienced accidents.

4 RESULTS

4.1 *Frequency of the maritime accidents occurred during winter*

4.1.1 *General accidents*
Based on the frequency statistical analysis, the most frequent type of accident was collision with 35% of the total accidents occurred during the analyzed winter periods. The second most frequent accident experience during winter was grounding with 17% of the total data of accidents analyzed. The frequency of collisions during winter months can be observed in Table 5. During the 5 analyzed winters in this study, the month of March has the highest frequency of collisions (2.6), and the total frequency by winter is 7.8 collisions per winter. In the case of groundings (Table 6), the month of December has the highest frequency of groundings (1.5), and the total frequency by winter is 5.25 groundings per winter.

In the case of the other type of accidents, propeller damage had a frequency of 3.6 per winter, loss of containment had a frequency of 1.2 per winter, fire/explosion a frequency of 1.2 per winter, rudder damage a frequency of 1.4 per winter, blackouts with a frequency of 0.4 per winter, and finally loss of propulsion with a frequency 0.2 per winter completes the frequencies of the identified accidents during the winters 2002–2003 & 2009–2013.

4.1.2 *Accidents occurred under sea ice conditions*
The most frequent accidents occurred under ice conditions are collisions. The Table 7 presents the frequency of the 31 collisions occurred under ice sea conditions.

The other accidents reported during sea ice conditions were: propeller damage with a 3.6 frequency per winter, rudder damage 1.4 frequency, ground-

Table 5. The frequency of collisions during winters 2009–2013 (Trafi, 2013).

	Jan	Feb	Mar	Apr	…	Oct	Nov	Dec	Total
2002									
2003	2	6	4						12
…									
2009									0
2010	1	2	3	1		1			8
2011	1	3	3	2		1		2	12
2012	1		2	1				1	5
2013		1	1						2
Total	5	12	13	4		2	0	3	39
Freq. (1/ month.)	1	2.4	2.6	0.8		0.5	0.0	0.6	**7.8**
									(1/winter)

Table 6. The frequency of groundings during winters 2009–2013 (Trafi, 2013).

	Jan	Feb	Mar	Apr	…	Oct	Nov	Dec	Total
2002									
2003									
…									
2009								2	2
2010	1					2	1	1	5
2011	1		1			1	2	2	7
2012		1		1		2	2	1	7
2013									0
Total	2	1	1	1		5	5	6	21
Freq. (1/month.)	0.4	0.2	0.2	0.2		1.25	1.25	1.5	**5.25**
									(1/winter)

Table 7. The frequency of collision under ice conditions during winters 2009–2013 (Trafi, 2013).

	Jan	Feb	Mar	Apr	…	Oct	Nov	Dec	Total
2002									
2003	2	6	4						12
…									
2009									0
2010	1	1	4	2					8
2011		2	3	4					9
2012		1	1						2
2013									0
Total	3	10	12	6					31
Freq. (1/month.)	0.6	2	2.4	1.2		0	0	0	**6.2**
									(1/winter)

ings 0.2 frequency, and loss of containment with a 0.2 frequency completes the frequencies of the accidents occurred during the analyzed periods.

4.2 *Operations, sea area, and sea ice conditions involved in winter accidents*

4.2.1 *Icebreaker operations*

During the analysis of the icebreaker operations in winters 2009–2013 which ended with an accident, "towing" was the operation (Fig. 8) which has reported the major number of accidents, followed by convoy and breaking a ship loose respectively.

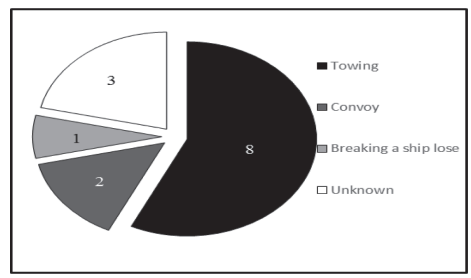


Figure 8. IB operations involved in collisions (Trafi, 2013).

4.2.2 *Sea area and sea ice conditions when accidents occurred*

The number of accidents (Fig. 9) under ice sea conditions during the analyzed winter periods were: the Gulf of Finland 24, Bay of Bothnia 24, Gulf of Riga 7, Central Baltic 5, Sea of Bothnia 2, Saimaa Lake 1, and 7 unknown locations. And about the most common ice conditions reported when collisions occurred in winters 2009–2013 were: consolidate compact or very close pack ice (10 times—63%), fast ice (5 times—31%), and new ice (1 time—6%). In 5 cases when a collision occurred in consolidate compact or very close pack ice, the conditions have also presented ridge and hummocked ice. The ice thickness when collisions occurred were in 5 cases an ice thickness of 1–20 cm, 8 cases 21–40 cm, and 6 cases with more than 40 cm ice thickness.

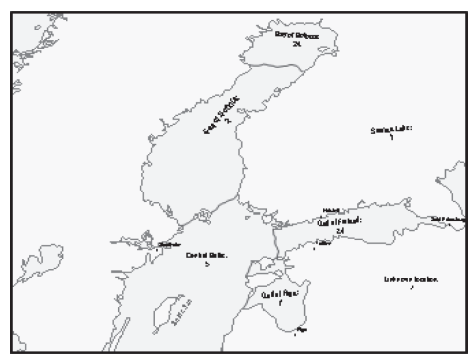


Figure 9. Location of the accidents occurred during the analyzed period (SMHI, 2013).

4.3 *Qualitative data mining to model the exposure to collision during ice breakers assistance*

Having defined the assistance operations of icebreakers and the identified ice conditions during the icebreakers assistance, enable to establish an initial input for modelling the exposure to collision during these operations based on particular ice conditions. The flowchart presented in Figure 10 indicates the ice conditions which are most commonly experienced in the collisions' scenarios during icebreaker assistance. Thus, this particular identification enable creating a structured base to set levels of risks and/or exposure to collisions during ice breaker operations.

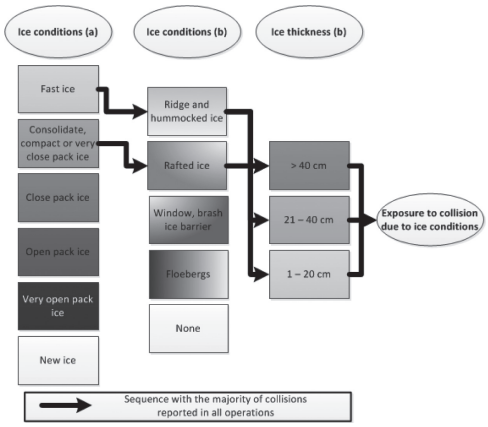


Figure 10. Flow chart with the ice conditions sequence of the collisions reported in all icebreakers operations.

Thus, the applied qualitative data mining to the accident data provided by the Finnish Safety Transport Agency (Trafi) detected that "towing" was the operation with the major number of collisions reported: 4 collisions under consolidated, compact or very close pack ice, combined with rafted ice and an ice thickness over 40 cm, also 4 collisions in fast ice combined with rafted, ridge and hummocked ice and an ice thickness between 1 to 40 cm. For convoy operations: one collision under consolidate, compact and very close pack ice, combined with rafted ice an ice thickness of 1 to 20 cm, and one collision in fast ice with an ice thickness over 40 cm. Finally, for breaking a ship loose: one collision in consolidate, compact or very close pack ice, combined with rafted ice and an ice thickness over 40 cm.

Thereby, based on the analysis of the data: consolidate, compact or very close pack ice and fast ice, combined with ridge, hummocked and rafted ice are the ice conditions whit higher exposure to collision. And the thickest is the ice, the most exposed the icebreaker operation is for ending in a collision.

5 DISCUSSION

The method for accident data analysis followed in this paper, provided a deeper view of the amount and the characteristics of accidents suffered by vessels during winter time in the Baltic Sea. This study has considered two kinds of winters in the Baltic Sea: the winter before the ice sea is present, and the winter under ice sea conditions. This differentiation allowed to accurately identify the types of accidents which are more frequently occurring on those scenarios. Thus, collisions are the most frequent accident occurred during winter time in the Baltic Sea. This statement is aligned to the findings of previous accident analyses performed in the area (e.g. Kujala, et al., 2009). In the mentioned study, groundings are the most frequent accident occurred during 1997–1999, 2001–2003, and 2004–2005. However, the analysis performed in the mentioned research has also detected that; once the Baltic Sea presents ice conditions, the number of groundings significantly decreases, but the amount of collisions significantly increases. Thus, having approximately 3 to 4 months of ice sea conditions in some areas of the Baltic Sea per year, implies an automatic decrease of groundings (the most frequent accident reported each year in the Baltic) which may considerably contributes to decrease the frequency of those reported every year.

Based on the accident data analyzed in this paper, the accident severity in most cases has been reported as less serious. Comparing this finding against previous studies (e.g. Tuominen, et al., 2010), the severity of the accidents occurred under ice conditions has also been considered as less serious in most of the cases. From the total amount of data analyzed in this paper, 75% of 68 accidents reported during the winters 2009–2013 were reported a less serious, 24% as serious, and only 1% as very serious accidents. And about the accidents occurred under ice conditions, 84% were reported as less serious, 16% reported as serious, and there were not accidents reported as very serious. Thus, these indicators may imply that the severity of the accidents may be better estimated and perhaps even controlled by the correct implementation of the current winter navigation system, a correct provision of the different sea ice services, and specially an adequate assistant by ice breakers.

The analysis of the icebreaker operations is a key aspect to consider when analyzing the number of accidents occurred during ice sea conditions. The fact that 19% of the accidents reported under ice conditions are related to the operations of icebreakers, indicates the clear need to improve the efficiency of one key player within the winter navigation system. In the analyzed data, "towing" has been detected as the operation with the major number of accidents with minor severity regarding the accidents outcome. Nevertheless, the operation needs to be analyzed more in deep in order to be improved.

During the analysis of the particular sea ice conditions, "consolidate compact and very close pack ice and fast ice with ridge and rafted ice" have been observed as the most problematic. And in the case of ice thickness, there were similar

numbers of accidents reported under different levels of ice thickness, having a slightly higher representation of thickness over 20 cm. Thus, once the icebreaker operation with the higher frequency of accidents, and the most frequent ice conditions experienced during those accidents were identified, a qualitatively and also quantitatively detection of the sequences of the icebreaker operations (e.g. Fig. 10) with more accidents experienced were extracted. These sequences and their respective numerical indicators must be utilized as an input data to identify and correctly estimate the scenarios which represent the higher risk of an accident when an icebreaker is providing assistance.

The map presented in Figure 9 has identified Gulf of Finland and Bay of Bothnia as the zones where more of the accidents occurred. However, this information is limited to the reports of accidents occurred on Finnish waters or to vessels registered to Finland. Therefore, this paper has remarked the importance of the analysis of the ice conditions experienced during the accidents and the operations of icebreakers which are also being performed in different Baltic Sea zones during winter time.

6 CONCLUSIONS

The winter navigation at the Baltic Sea commonly presents two general conditions challenging the safety performance of the vessels navigating the area: the dark sea with winter storms arriving in open waters, and the sea with harsh ice conditions. These two characteristics influence the kind of accidents typically occurring in the Baltic Sea, while groundings are the most frequent accident reported during winter before sea ice is present, collisions are the most frequent accident under sea ice conditions in the zone.

The severity of the accidents occurred under ice conditions seem to be lower than the reported on open waters during winter time. The accident data analysed in this paper identified general cargo and icebreaker as the type of vessels which are more frequently involved in accidents. In the case of icebreakers, this fact is logically understood due to the assistance operations performed by this kind of vessel. Furthermore, the statistical analysis has identified "towing" as the icebreaker operation with more accidents reported. Consolidate, compact and very close pack ice with ridge and rafted ice is the sea ice condition experienced in more of the reported accidents. Thus, it can be concluded that while there is still the need for more research to complement the analysis for determining the risk of accidents in winter navigation, the analyses performed in this paper, have identified valuable input information which is clearly needed to correctly estimate probabilities of accidents in winter navigation.

ACKNOWLEDGEMENTS

The work of this paper has been carried within Winter Navigation Risks and Oil Contingency Plan (WINOIL) Project, and in association with the Kotka Maritime Research Centre. The authors appreciate the financial contribution of the European Union, the Russian Federation and the Republic of Finland.

REFERENCES

Critch, S., Goerlandt, F., Montewka, J., and Kujala, P. (2011). Towards a risk model for the Northern Baltic maritime winter navigation system. *International Workshop on Next Generation Nautical Traffic Models 2013*, Delf, The Netherlands.

Daley, C. & Riska, K. (1990). *Review of Ship-Ice Interaction Mechanics*. TKK Laivanrakennustekniikka raportti M-102.

EfficienSea (2011). *The Risk Reducing Effect of VTS in Finnish Waters. Efficient, Safe and Sustainable Traffic at Sea*. Public Document part financed by the European Union, Deliverable No. D_WP6_5_01.

Finnish Maritime Administration (FMA). (2003). *Statistics of ships visited Finnish Ports in foreign traffic*, winter 2002–2003. Information service department.

Finnish Meteorological Institute (FMI), (2011). *Ice conditions reported on the Baltic Sea during winter 2010–2011*.

Goerlandt, F., Ståhlberg, K., and Kujala, P. (2012). Influence of impact scenario models on collision risk analysis. *Journal of Ocean* Engineering 47: 74–87.

Jones, D. and Womack, J., (1996). *Lean thinking banish waste and create wealth in your corporation*. New York: Simon & Schuster.

Kujala, P., Mikko, S., and Jalonen R. (2007). *Increasing the Safety of Icebound Shipping.* Final Scientific Report: Volume 1, Helsinki Uviversity of Technology, Ship Laboratory, Espoo, Finland.

Kujala, P., Hänninen, M., Arola, T., and Ylitalo, J. (2009). Analysis of the marine traffic safety in the Gulf of Finland. *Reliability Engineering and System Safety* 94: 1349–1357.

Liikennevirasto (2013). Finnish Transport Agency. *Finland's Winter Navigation*. Vessel Traffic Services on Finnish Waters.

Mazaheri, A., Montewka, J. and Kujala, P. (2013). Modeling the risk ship grounding—a literature review from a risk management perspective. *Journal of the WMU Maritime Affairs*, DOI 10.1007/s13437-013-0056-3.

Ploskonka, H. (2013). *Ice breaker Operations in the Gulf of Finland, Winter 2011.* WINOIL project report, Aalto University, Department of Applied Mechanics, Espoo, Finland, November 2013.

Riska, K. (1999). *Research and development in winter navigation.* Lecture notes at the Ports and Short Sea Shipping—A Baltic Seminar, 14–15 June 1999, Turku, Finland.

The Finnish Transport Safety Agency (Trafi). (2011). *Finland's Winter Navigation. Instructions for winter navigation operations. Winter 2010–2011,* The Winter Navigation Unit.

The Finnish Transport Safety Agency (Trafi). (2013). *Accidents statistics 2009–2013*. Finnish Transport Safety Agency.

The Swedish Meteorological and Hydrological Institute (SMHI). (2013). *Winter Ice Conditions 2009–2013 and maps and ice symbology of the Finnish*—Swedish Winter Navigation System.

Tuominen, R., Rosqvist, T., and Porthin, M. (2010). *Innovative Icebreaking Concepts for Winter Navigation (IceWin)* Report. D5.3 Risk Assessment, WP5. Seventh Framework Programme, Theme 7 Transport 2011.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Structuring contributors to successful operation

Jørn Vatn
Department of Production and Quality Engineering, NTNU, Trondheim, Norway

ABSTRACT: It is often claimed that traditional safety methods and risk analysis in particular are limited by failures and error tabulation in the search for safety improvements. The main objective of this paper is to investigate whether such claims have a sound foundation. To shed light on the problem we start with defining the two terms 'normal operation' and 'successful operation' and discuss duality of these terms in relation to terms like 'failure' and 'error'. Next we introduce a near miss example in railway operation where two trains were almost directed into the same section due to several misunderstandings. The situation is analysed by a STEP (Sequentially Timed Events Plotting) analysis. In the first iteration safety problems are revealed in a standardized manner, whereas we in a second iteration investigate elements of various contributing factors to successful operation. Based on the analysis we suggest ways to improve the STEP methodology such that conditions related to success can have an equal position as conditions leading to failures and errors. Since results from investigation would be important input to risk analysis and subsequent analysis of improvement measures, we discuss how understanding of success and failures can be incorporated into risk analysis frameworks. Although "learning from successful operation" is less emphasized in many investigation and improvement programs, our analysis has not revealed principal differences between "success" and "failure" in the way such terms could be used in investigation, risk analysis, and evaluation of improvement programs.

1 INTRODUCTION

Many investigation methods and risk analysis methods have a focus on failures and what went wrong, or what may go wrong. In recent years it has been recognised that putting more emphasis on success and what goes right could bring complementary understanding and hence improve safety and risk management.

The objective of this paper is to propose ways to structure knowledge and factors related to successful operations. We first introduce a motivating example from railway operation where a disturbance lead to several misunderstanding, and the situation could easily have developed into an accident. However, important operative barriers were in place, and the accident was avoided, and the situation must be categorised as a successful operation. In the first place we use a traditional investigation approach. After introducing the event we introduce and discuss important terms related to normal operations and success. The event is then revisited where we are seeking success, and contributors to success.

2 THE EVENT

We are considering a single track railway without remote control. This means that Local Train Controllers (LTC) are transmitting train announcements to control train operation. A Southbound Train (SBT) is approaching station A while a car driver is observing sparking and smoke from the train, and reports this to station X where he knows the LTC. The LTC at station A receive the SBT unaware of the problems, and transmit necessary train announcements to station B (south of station A). Thereafter the SBT leaves station A towards station B. The LTC at station A now receive the information regarding sparking and smoke, and contact the engine driver at the SBT via train radio. The SBT then stops at position Y south of station A. The Central Train Control (CTC) is then informed about the event. But due to the fact that the train was north of station A at the time of observation (by the car driver), the CTC believes that the train also did stop *north* of station A.

According to the traffic regulation the engine driver at the SBT shall report position in a kilometre measure, but he faulty reports his position (i.e., position Y) by using a local name not familiar to the CTC.

According to the schedule, a crossing between the North Bound Train (NBT), and the SBT shall take place at station B (south of station A). Since the train controller at the CTC believes that the SBT is stopped north of station A, he decides to change the crossing from station B to station A to minimize delay

for the NBT. The new crossing order is transmitted to the LTC at station A and station B. Both LTCs accept the new crossing order. In order to effectuate the crossing order the LTC at station B ask the LTC at station A to cancel the departure announcement of the SBT, so that he can allow the NBT to enter the section between station A and station B (where, the SBT still is residing). The LTC at station A refuses to cancel the departure announcement because he knows that the SBT still is occupying the critical section, and the misunderstanding is resolved. An accident was avoided because the "last barrier" was still functioning, i.e., "make sure that a train cannot be sent into an occupied section".

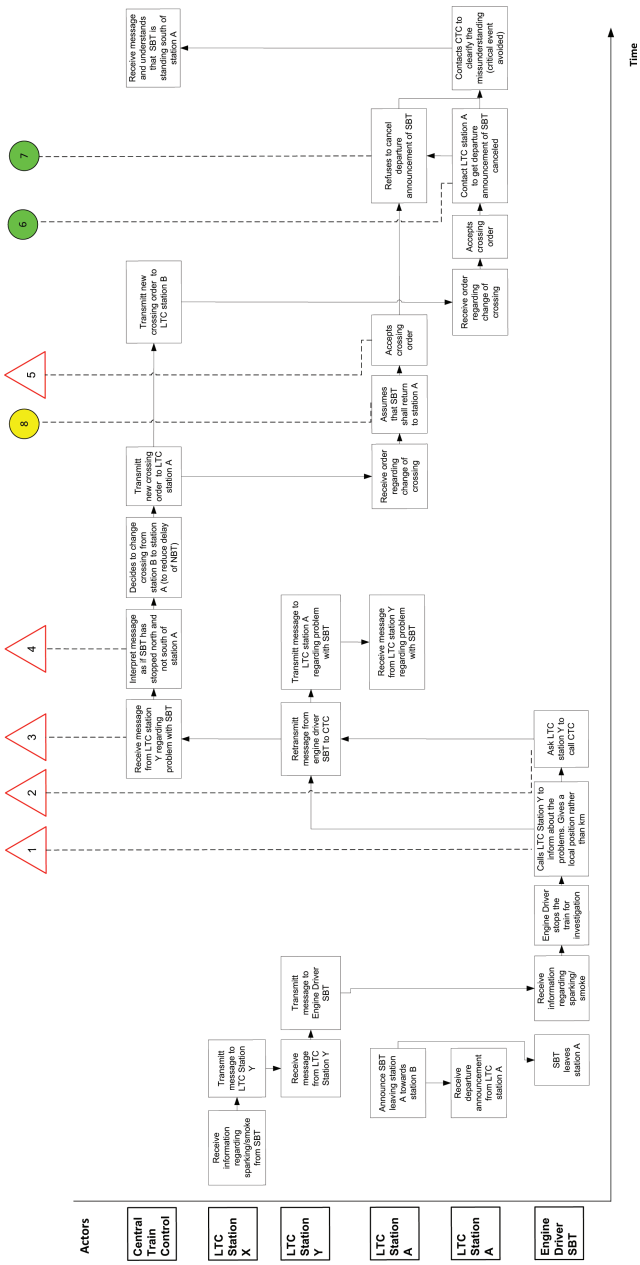


Figure 1. STEP diagram.

The situation was analysed by the STEP investigation method (Sequentially Timed Events Plotting, see Hendrick & Benner, 1987). The STEP diagram is shown in Figure 1.

The following safety problems (triangles in the STEP diagram) were obtained during the analysis:

1. The engine driver on the SBT uses a local name rather than a km specification when informing where he has stopped
2. The engine driver do not contact the CTC directly to inform about his position and his problems, but asks the LTC at station Y to inform CTC
3. Unclear orders and lines of command causes the misunderstanding
4. The operator at the CTC interchanges "south of" and "north of" in his mind since the precise km position of the stopped train was missing
5. LTC at station A accepts the new crossing order (even if he knows that the SBT has left station A)

The "magic event" that "saves the day" is performed by the LTC at station A, who refuses to cancel the departure announcement. This particular event may be seen as a real success making the entire operation that day a successful operation. Before we discuss learning from successful operations, we need some basic theory and terms.

3 THEORY AND BASIC TERMS

The objective of this section is to define the term successful operation. Although concepts like learning from "normal operation" and "successful operations" has been introduced recently to give new momentum to safety research, it is not straight forward to define such terms and contrast them to more traditional concepts like errors and failures.

3.1 *Failure, error and success*

The term 'failure' is easy to define, and the definitions are consistent across standards, textbooks and other presentation. A failure is defined as the point of time when an entity is not able to perform (one of) it's required function(s). The term 'error' is more difficult because it is used both to describe human errors, software errors and also deviations from performance of physical items. In this presentation we will use the term 'error' only related to human errors, and we define human errors as a deviation from an intention in a given context. Note that an "intention in a given context" is slightly less precise than "function" as the "hardware" counterpart since we cannot always describe in detail what is the intention of a human action. See e.g., Reason (1990) and Hollnagel (1993) for further discussions.

In a binary context where it is straight forward to distinguish a failure or an error from the "opposite", we may define the term 'success' as the opposite of a failure or an error. It could be questioned whether such a use of the term 'success' is how we think about success, the fact that an item is not failing will often not be considered as a success. However, to maintain a duality between success and failure we proceed with the proposed definition. For many functions and intention of human actions a clear binary split between success and failure does not exist. For such situations it will be more natural to use multistate formulation of the problem, and neither of the terms failure, error or success are that appropriate.

3.2 *Successful operations and related terms*

Next we will define the terms 'normal operation', 'successful operation' and 'successful recovery'. To give a mental model as a basis for the definitions we borrow the "layer of protection" concept from the process industry. A layer of protection can be seen as safety barriers, and they are often structured in the way they will be activated in an accident scenario. Compared to the presentation given by e.g., Rausand (2014) and CCPS (2007) we simplify and distinguish between:

a. Process design (by using inherently safe design principles).
b. Control, using basic control functions, alarms, and operator responses to keep the system in normal (steady) state.
c. Prevention, using Safety-Instrumented Systems (SISs) and other safety barriers to act upon deviations from normal state and thereby prevent an undesired event from occurring.
d. Mitigation, recovery and emergency response in case of control is lost.

Figure 2 shows the layers of protection.

Having these categories of layers as a basis we now define:

Normal operation corresponds to layer (b). Normal operation may involve adaption to varying conditions as emphasized by resilience engineering. But normal operation does not involve use of extraordinary safety functions representing layer (c). If the primary control is lost and there is a deviation from the normal state, layer (c) is intended to bring the system into a safe state. We define ***successful operation*** as a situation where layer (c) is invoked, and is able to bring the system back to the primary control state. In some situations layer (c) is invoked but without being able to bring the system back to the primary control state.

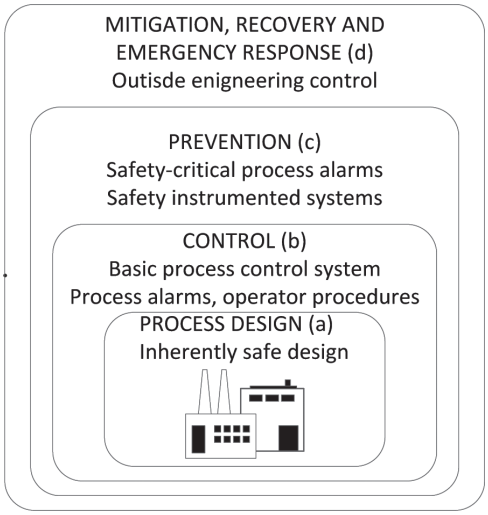


Figure 2. Protection layers (adapted and simplified from CCPS, 2007).

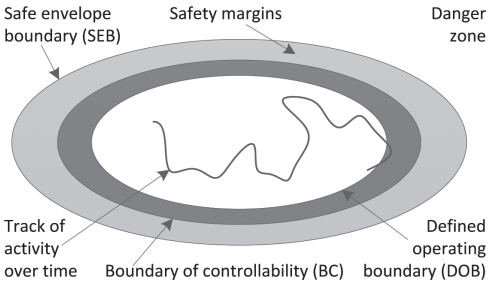


Figure 3. Safe envelope (adapted from Hale et al. 2007).

This is often referred to as a state where the system is outside engineering control. If this is the case, we define ***successful recovery*** as the situation where the system could be brought under control and back to it's normal state (after repairs, clean-up and so forth).

In the literature we also find other mental models for accident avoidance than the protection layers understanding shown in Figure 2. One class of such models is the safety envelope model shown in Figure 3. The inner ellipsis limited by the Defined Operation Boundary (DOB), corresponds broadly to what is controlled by protection layers (a) and (b) the in protection layer model in Figure 2. In some respect we may also treat the elliptical band limited by the Boundary of Controllability (BC) very similar to what is controlled by protection layer (c) in Figure 2. However, there might be differences since the layer of protection concept in Figure 2 is usually based on very explicit identification and design of safety functions, whereas the safety envelope perspective in Figure 3 does not have such an explicit understanding of safety functions. Finally the outer elliptic band limited by the Safe Envelope Boundary (SEB) represents extra safety margins where there is a conceptual link to what is controlled by protection layer (d) in Figure 2, but the similarities are not that evident at this level.

A conceptual advantage of the safe envelope model over the layer of protection model is the visualization of the track of the activity over time. Following our initial definition of success, we would by referring to the safe envelope define successful operation as an operation where defined operating boundaries are exceeded, but where the boundary of controllability is not exceeded (as illustrated in Fig. 3). So far we have not considered a process remaining within defined operating boundaries as a successful operation. However, many will consider an operation to be successful also if we are able to remain in the inner ellipsis of Figure 3. Since we have defined this situation to represent a *normal* operation we will be reluctant to define a normal operation within defined operating boundaries as a success. We will, however consider two special cases (sub sets) of normal operations as successful operation. The first situation is where there are extraordinary conditions making it very difficult to operate within defined operating boundaries. Examples could be a situation where the physical process is hard to control for example due to a situation where the quality of some raw material is low, or it could be related to extreme weather conditions. If we, despite these challenges, are able to operate within the defined boundaries we will define that the particular operation is a successful operation. Another situation we will define as a successful operation is where we are able to control the process "in the middle" of the inner ellipsis of Figure 3. There are at least two reasons why this could be considered as a success. Firstly this will most likely represent a situation where operation runs smoothly and production performance will be high. Next, the fact that the process runs smoothly represents a situation where we use minimal effort to control the operation, and presumptively we are better prepared to handle any process upset that might occur. However, there is an argument in this latter situation that would question how successful such an operation is. The fact that there are no process upsets or situations to act upon, could be passivizing the operations crew in the sharp end limiting their situation awareness (see, e.g., Endsley, 1995, for a thorough discussion on situation awareness). Little effort to control the process could also give little stimuli and training to act upon weak signals.

In the safety envelope model in Figure 3 the boundaries are illustrated as static in time. For many operations the boundaries or safety functions cannot be seen as static. We will in the following distinguish between a situation where (i) operating personnel is aware of this situation, and (ii) operating personnel is *not* aware of the status of a safety function or the limits for safe operation. A very easy example of situation (ii) is car driving where the temperature has decreased below zero degrees Celsius on a wet road without the attention of the driver. Situation (ii) is obvious very critical, and we will also here use the term successful operations in a situation where the operation is following a trajectory towards an accident without the attention of operating personnel for a while, and then operating personnel become aware of the situation, and succeed in bringing the situation under control. This is visualised in Figure 4.

3.3 *Extended definition of successful operation*

Based on the above discussion we propose the following elements to be covered in the term successful operation to be used in (i) accident and incident investigation, and (ii) risk analysis based on insight from such investigations:

1. A situation where we are able to keep the operation within defined operating boundaries and at a particularly desired level where the need of operational control is limited.
2. A situation where operational conditions are particularly challenging due to bad weather, a challenging well with unstable formation pressure etc. But despite these challenges the operation is performed within defined operation boundaries by means of normal control functions.
3. A situation where normal control was lost, and the process escaped the defined operating boundaries in the first place, but controlled was gained by prevention, such as safety critical systems or secondary human control mechanisms.
4. A situation where situation awareness is degraded below a threshold value and the subsequent course of events ultimately will result in loss of control. Then proper situation awareness is regained and the operation is brought under control.

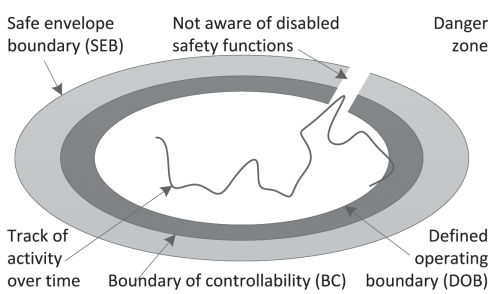


Figure 4. Safe envelope with broken boundaries due to unnoticed deficiencies or problems (based on Hale et al. 2007).

The above mentioned elements relate to the sharp end of the operations. Blunt end factors contributing to the success are not considered as successful operation in this context meaning that we will limit the term successful operation to particular cases. We will also not use the term successful operations in a statistical sense (benchmarking perspective) regarding operations that turn out to have extraordinary low incident and accident frequency. Both blunt end factors, and performance over time will be important as background in an investigation context, but the focus on success should be the particular events under consideration.

As the world is not black and white, there are situations where we have *partial* successful operation and *partial* successful recovery. For example there might be losses and even fatalities, but one may tempt to consider the situation as a successful recovery because the consequences could have been significantly worse.

3.4 *Linking investigation to risk management*

A main reason for proposing four different aspects of successful operation is to help structuring both during the investigation, but also in a learning process where the knowledge gained is to be in cooperated in the risk analysis and continuous safety improvement work. It is anticipated that success influencing factors could be of different nature for the various aspects, and hence a categorization is considered of value.

We will not present a particular accident model for the discussion. However, the conceptual models of layers of protection and safe envelopes will serve as a basis for risk modelling. In risk management and risk control it is fundamental to have a risk model as a reference point when learning from normal operation, successful operation, and successful recovery.

A risk model often comprises a formal logical representation of the system. Fault- and event tree analysis is often building blocks in such a representation. Barriers, safety functions and/or layers of protection are typically represented by basic events. Probabilities are assigned to the outcome of the basic events, i.e., success or failure. A wide range of factors and conditions will influence the outcome of the basic events, and these need to be taken into account when assigning the basic event probabili-

ties. In the literature we find many approaches to link such "soft" factors to the formal logical representation. The literature also presents different names for such factors. In Human Reliability Analysis (HRA) the term Performance Shaping Factors (PSFs) and Error Producing Conditions (EPCs) are used (see e.g., Rausand, 2011). The term contributing Success Factors (SCFs) has also been used in an attempt to establish resilience based early warning indicators (Øien et al. 2010). To avoid different set of factors for positive and negative issues, we will in the following use the term Risk Influencing Factor (RIF) as a general tem, see e.g., Vinnem et al. (2012) for risk modelling of planning and execution of critical tasks.

To define a RIF we first define a QRA parameter as *conditions that affect risk and included as a single parameter in a Quantitative Risk Analysis (QRA) model*. Examples of QRA parameters are failure rates, on demand probabilities for safety systems and ignition probabilities. Primarily we assume that QRA models comprise formal probabilistic techniques like fault- and event trees, and energy related impact techniques, e.g., an ignition model. A RIF is next defined as *a factor or condition that influences the risk*. There are three principal types of RIFs, (i) RIFs that are equal to a QRA parameter, (ii) RIFs where the value of a RIF is assumed to influence a QRA parameter, and where the influence is described in probabilistic terms, and (iii) RIFs that influence a parameter that is not explicitly modelled in the QRA. A working hypothesis is that all RIFs of type (iii) could by proper modelling be of type (i) or (ii). This is to say that all aspects of importance for the risk level could be addressed in the risk modelling. To what extent such structuring and modelling always brings value into risk management is another question.

The main objective of risk modelling is to present a reasonable subset of all accident scenarios we may imagine to reveal threats and hazards, how these threats and hazards may be mitigated, and finally quantify impacts such that there could be a reasonable balance between risk and effort spent to reduce risk. Although threats and hazards are fundamental in risk analysis, the methods and models do not by nature distinguish by failure and success. These lower level terms are ways to structure accident scenarios involving threats and hazards and to what extend one should be failure oriented or success oriented may vary from analysis to analysis.

The objective of investigation by methods like STEP is to shed light on what happened in one particular event or incident in order to learn from what happened. Usually learning is understood as a change in practice and/or an implementation of adequate measures to mitigate what went wrong, and to support and foster what went well. Another important aspect of learning is to improve the generic understanding of accident scenarios by in cooperating the lessons learned as new accident scenarios relevant for similar type of operations and/or to improve existing accident scenarios. The safety problems (triangles) identified in the diagram shown in Figure 1 are then to be considered in existing or new accident scenarios treated in the risk modelling.

4 THE CONCEPT OF SUCCESS IN INVESTIGATION AND STEP ANALYSIS

The traditional STEP diagram lists the course of events in the situation being analysed by separating actions for each actor and relation between activities. Based on the understanding of the course of events the investigator identifies safety problems (triangles in the diagram). The safety problems are linked to events that caused the situation to develop in a negative direction. We now propose to introduce a new symbol in the diagram to represent success, or potential success. A simple disk symbol is used with an identifier, i.e., ⑥, ⑦ and ⑧ in Figure 1. To make the symbols more self-explanatory one could use e.g., smiley face symbols. As for the safety problems where it is important to distinguish safety problems from the course of events, we therefore also propose to "lift" the success symbols to the top of the diagram. The success symbols represent either events in the diagram as such, or a condition or state that was a prerequisite for the events in the diagram to happen.

In the diagram in Figure 1 we have proposed to use two background colours, the green colour for symbols ⑥ and ⑦, and the yellow colour for ⑧. The distinction is related to what actually was a success (⑥ and ⑦) and what could have been a success (⑧). The explanation of the symbols related to Figure 1 is now:

⑥ The Local Train Controller (LTC) at station B is aware of what is going on, and requests a cancelation of the departure announcement of the southbound train.

⑦ The LTC at station A knows that the southbound train has left the station, and not returned to station A (as he mentally was thinking). He therefore refuses to cancel the departure announcement.

⑧ This symbol represent what could have been a success, i.e., that the situation awareness of LTC at station A could have been much better. Such a better situation awareness would most likely have caused e.g., a clarification request from LTC at station A to the Central Train Control

(CTC), and the course of events could have been stopped at an earlier stage.

A remark regarding use of ⑧ versus safety problem 5 needs to be made. Generally the safety problem symbol in the STEP diagram is used to enhance events that should not have taken place (i.e., LTC at station A accepts the crossing order which he should not have done), or a situation where one activity does not take place. For the latter, this means that "negative events" are not drawn in the diagram as an event, but rather as a safety problem, i.e., the fact that a required action is not performed is considered as a safety problem in the analysis. When we look closer to symbol ⑧ representing a not up to date situation awareness, this could have been denoted a safety problem. However, we are a bit reluctant to use the term safety problem in this case because this will emphasise that there is "something wrong", rather than what can be done to "improve" the performance. Therefore seeking for "potential successes" in the course of action could be a better way to learn from the event, and structure into improvement programs and the risk analysis models.

We also observe the different nature of symbols ⑥ and ⑦ pointing to success as dual concepts of a failure, whereas symbol ⑧ does not have such a dual "failure". The duality of symbol ⑥ representing a success, would have been that the LTC at station B did fail to request a cancelation of the departure announcement. For symbol ⑧ representing a potential success, it is not that evident that there exists a corresponding duality, i.e., a failure.

The investigation often terminates by identification of safety problems and conditions leading to success as indicated in the top row in the STEP diagram in Figure 1. In the continuous improvement work as well as for structuring in the risk modelling it is required to see beyond safety problems and success conditions as shown in the STEP. In the following discussion we will emphasize issues related to risk modelling. The STEP diagram could be seen as a way to structure one or more accident scenarios. The events in the diagram correspond more or less to basic events in a fault tree, or barriers and safety functions in an event tree. The identified safety problems and success conditions are not straight forward to include in the fault—and event trees being the basis for the risk model. It will be required to structure both the safety problems and success conditions by means of Risk Influencing Factors (RIFs), where a RIF typically is influencing event probabilities in the fault- and event trees.

For success conditions ⑥ and ⑦ the most evident risk influencing factor would be "compliance to procedures". The investigation of this particular event clearly demonstrates the importance of compliance to achieve success. It might be argued that this lesson contradicts the mantra in resilience engineering advocating adaption and denying compliance to achieve success (EUROCONTROL, 2013). We will not turn into a dispute with the resilience engineering society, but emphasise that for some systems compliance to procedures is extremely important also under so-called varying conditions. Obvious a criterion for that compliance results in success is the situation awareness in the sharp end. Compliance as a principle may fail if a wrong situation awareness exist, and we therefore also emphasise situation awareness as an important risk influencing factor related to success conditions ⑥ and ⑦. Endsley (1995) presents a model for situation awareness in dynamic decision making where the situation awareness could be seen as a first level RIF whereas abilities, experience and training could be seen as second level RIFs in a hierarchical risk influence model as proposed by Vinnem et al. (2012). Situation awareness, or rather lack of such, was considered important related to success condition ⑧. Lack of situation awareness could also be seen as an important element of safety problem 5. This demonstrates that as part of the investigation as well as for the risk modelling, it will be difficult to distinguish clearly between success and failure when we go beyond the explicit safety problems and success conditions. It could therefore be argued that the Safety-I and Safety-II perspectives seen as fundamental different approaches to safety by separating into principles of minimizing failures vs maximizing success respectively (EUROCONTROL, 2013), is not that fruitful for neither investigation nor for risk analysis. We accept that too little attention has been paid to success and conditions influencing success within safety and risk management and have therefore advocated to more explicitly address successful operation as part of investigation and modelling, but we are reluctant to contrast success and failures as proposed by EUROCONTROL (2013).

We end this section by listing some relevant risk influencing factors linked to the various elements of success:

1. Keep operation in the "middle" of the operating boundaries:
   a. Trained operating personnel
   b. Anticipation skills
   c. Understanding the "physics" of the basic operational control functions
2. Safe operations under challenging conditions:
   a. Trained operating personnel
   b. Planning and mindfulness by e.g., Safe Job Analysis
3. Regaining control by prevention mechanisms (e.g., safety critical systems):

a. Compliance
b. Trained to handle deviations

4. Degradation of situation awareness where proper situation awareness is required to regain control:
   a. Situation awareness
   b. Understanding of the "physics" of the problem
   c. Understanding the limitation of basic as well as preventive control functions
   d. Improvisation capabilities (especially in the case of successful recovery)

The purpose of the above list is to indicate that there might be different conditions and factors that are critical depending on the type of success, and should not be used as a categorization list. Further research is to be conducted to shed light on the structure of influencing factors in various types of successful operation. The objective of the project "Learning from successful operations" sponsored by the Norwegian Research Council is to shed light on how we can understand success and learn from it. Hopefully the research also will bring insight into the structuring of success and success factors to obtain a more solid list than indicated above.

5 DISCUSSION

A case study is used to shed light on the term successful operation, but such an approach cannot give general conclusions. Although "flipping the coin" and looking for success rather than failure may not represent a principal different approach, it is considered valuable in the search for more fundamental root causes or risk influencing factors in an investigation context. The case study also demonstrates that compliance could be essential to success in case of varying conditions where a resilience engineering perspective (EUROCONTROL, 2013) "advocates" adaption as a main principle for success. We claim that proper situation awareness is fundamental for "safe" compliance behavior, but we have not really investigated how situation awareness also could play the essential role in "safe adaption" and "safe improvisation". In a successful operation perspective, the four types of successful operation and the concept of successful recovery is believed to be a reasonable starting point for further research on this question.

6 SUMMARY AND CONCLUSIONS

A near miss event has been analysed with a traditional investigation method to reveal safety problems. The STEP method (Hendrick & Benner, 1987) is used as a basis for the investigation. We then propose to extend the investigation by also searching for success. It is proposed to use a dedicated symbol to visualize success issues in the diagram. For proper analysis it is proposed to introduce four different types of successful operations. In the search for underlying success factors a preliminary list of type specific success factors is proposed. The example study shows that searching for success rather than only (safety) problems may reveal other factors such that situation awareness and circumstances for compliance to meet it's intentions. The example also shows that success and failures are intervened in the course of events and should be analysed in parallel. The idea of introducing different safety perspectives (Safety-I and Safety-II) as proposed by e.g., EUROCONTROL (2013) is not seen to give much extra insight. The important message is rather to put equal emphasise both on success and failures in the investigation, with respect to learning, and with respect to improved risk modelling.

REFERENCES

CCPS 2007. *Guidelines for Safe and Reliable Instrumented Protective Systems*. Wiley (Center for Chemical Process Safety of AIChE), Hoboken, NJ.

Endsley, M.R. 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors.* 37(**1**), 32–64.

EUROCONTROL 2013. *From Safety-I to Safety-II: A White Paper*. Brussels: EUROCONTROL. http://www.skybrary.aero/bookshelf/books/2437.pdf (last visited 2013.05.03).

Hale, A.R., B.J.M. Ale, L.H.J. Goossens, T. Heijer, L.J Bellamy, M.L. Mud, A. Roelen, H. Baksteen, J. Post, I.A. Papazoglou, A. Bloemhoff, J.I.H. Oh. 2007. Modelling accidents for prioritizing prevention. *Reliability Engineering & System Safety*, **92**(12), 1701–1715.

Hendrick, K., and Benner, L. 1987. *Investigating accidents with STEP*. Marcel Dekker Inc. MY.

Hollnagel, E. 1993. *Human reliability analysis: Context and control*. Academic Press. NY.

Øien, K., S. Massaiub, R.K. Tinmannsvik and F. Størseth 2010. Development of Early Warning Indicators based on Resilience Engineering. PSAM 10, June 7–11 2010, Seattle, USA.

Rausand, M. 2014. *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley. Hoboken, NJ.

Rausand, M. (2011). *Risk Assessment; Theory, Methods, and Applications*. Wiley, Hoboken, NJ.

Reason, J. 1990. *Human error*. Cambridge University Press. NY.

Vinnem, J.E., Bye, R.J, Gran, B.A., Kongsvik, T, Nyheim, O.M., Okstad, E.H., Seljelid, J. and Vatn, J. 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries*. **25**(2). 274–292.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Country Safety Performance Function and the factors affecting it

Kazimierz Jamroz
Highway Engineering Department, Faculty of Civil and Environmental Engineering, Gdansk University of Technology, Gdansk, Poland

ABSTRACT: This work has been prompted by Poland's poor supply of road safety management tools which are key to developing national road safety policies. They could also be used in other developing countries. Behavioural theories and the results of literature studies have helped to develop the Country Safety Performance Function (CSPF) which describes the relationship between the normal anticipated Road Fatality Rate (RFR) in a country and the variables of its social, economic, road transport and road safety management systems. The CSPF underpins the essence of road safety measured as the national road fatality rate. It can be used to understand the current condition of road safety of a country and the forecasts.

1 INTRODUCTION

Analyses of road safety statistics show that developing Asian and African countries perform much worse than European countries just as Eastern and Central European countries fall behind the countries of Western and Northern Europe. As we know from research (van Beeck et al., 2000; Kopits & Cropper, 2003; Anbarci et al., 2006; Bishai et al., 2006; Koren & Borsos, 2006; Koornstra, 2007/1; Elvik, 2010; Law et al., 2011, Papadimitriou et al., 2013, Yannis et al., 2014) road safety largely depends on the country's social and economic development and the mobility of its population, but there are other equally important factors.

We are at the start of the Global Plan for the Decade of Action for Road Safety following from the UN Declaration and the 4th Road Safety Action Programme adopted by the European Commission for the years 2011–2020. To ensure an effective and efficient road safety policy we need tools to help with strategic decisions. Long-term strategic road safety and road infrastructure programmes and plans rely on road safety forecasts and assessments of the current situation and how it will evolve over extended periods of time (10, 20 or even 30 years).

The experience of OECD countries (1994) shows that road safety can benefit significantly from comprehensive and coordinated policies. Key to their success are well prepared and consistent road safety programmes. The effectiveness of programmes is the strongest if they have clear quantitative targets, well defined safety measures, the right set of dedicated partners and sources of funding. Sweden's Vision ZERO (Tingvall, 1998) is the leading example. This sets the context for the following questions:

- What is the impact of a country's social and economic development on road safety and what are the decisive factors of change?
- Which of the numerous road safety factors should be considered when devising strategic road safety policies?
- Can a country reduce its road deaths almost down to a zero and when can that happen?

One of the most common measures of road safety is road mortality rate, a demographically normalised way of measuring road safety (Hollo et al., 2010). It can be used to build estimation models and forecast road deaths, assess road safety and the effectiveness of treatment. The rate differs significantly from country to country.

The objective of this work is to develop a road fatality rate model to illustrate a country's accident severity at the macro (strategic) level. The paper will specifically address the strategic factors affecting road fatality. It will aim to develop a concept of a simple model looking at the effects of strategic factors on road fatality and subsequently apply the model to identify the degree of change in a country's road safety performance.

The choice of topic is directly related to the lack of road safety management tools which must form part of Poland's national road safety programmes and those that can be used in other developing countries.

This publication draws on research carried out by the author at the Department of Highway Engineering, Gdansk University of Technology between 2008 and 2010 (Jamroz, 2011).

2 THEORY

Despite its advantages, the transport system has an adverse effect on the environment, economy and health. Previous work describing the hazard of road transport has referred to many concepts and theories (Elvik & Vaa, 2004, Jamroz, 2008). Currently, the leading theories are behavioural based on road traffic risk. Societal road traffic risk is usually measured at the strategic level with the number of fatalities, considered as the absolute measure and with the RFR as the relative or normalised measure (Jamroz 2010, 2011, 2012).

Road death rates change at a different pace in developing and developed countries. Unlike the latter, developing countries register more fatalities as the economy improves. When studied over extended periods, the distribution of fatalities in the different countries shows different breakpoints (OECD), (IRTAD). The year of the breakpoint and the maximal number of fatalities mainly depend on the country's population, number of vehicles and gross national product. Breakpoints also occur in the road fatality rate.

The moment of the breakpoint is described by Al-Haji (2007) and Yannis et al. (2010, 2014) who found that for the RFR the breakpoint occurs in relation to the motorization rate in the range of 120 to 350 vehicles per 1000 population. Kopits & Cropper (2003), Anbarci et al. (2006), Bishai et al. (2006), Koren & Borsos (2006), Koornstra (2007/1) have made similar observations and said that the breakpoint can also be found in the road fatality rate and depends on the increase in national income. Koornstra (2007/1) pointed out that the breakpoint of road mortality rate occurs for a GNIPC equal to USD 5000 (US dollars), while Kopits and Cropper (2003) state that depending on the model the breakpoint occurs from ID 5,400 to 8,600 (international dollars). The authors, however, are not specific about the right side of the relationship.

Forty one countries with a RFR breakpoint have been identified. Their breakpoints, however, occur at different periods of the 20th century. For the different parameters of the scale (for X axis) the RFR breakpoints have been identified as follows:

- for time T: in the US in 1937, followed by Australia, Japan, Norway, Sweden in 1970, 1995 in Greece and 2004 in Brazil,
- for the MRMV (vehicles/1000 inhab.): from 91 in Portugal, followed by 225 in the Netherlands to 495 in Cyprus,
- for the HDI: from 0.731 in South Africa, 0.829 in Germany to 0.896 in Spain,
- for the GDPPC (thous. ID/inhab.): from 7.1 in Romania, followed by 9.6 in the US and 16.9 in France to 25.9 in Switzerland.

Based on the literature (Hakkert, 2002, Kopits & Cropper, 2003; Anbarci et al., 2006; Bishai et al., 2006; Koren & Borsos, 2006; Koornstra, 2007/1; Law et al., 2011) and the results of his research (Jamroz 2011) the Author adopted the following concept of how a country's road safety changes if measured with the RFR. According to this concept a country's road safety performance changes non-linearly in relation to changes in social and economic development.

There are different functions which we can use to describe the variability of road accident consequences. A study of available research and publications shows that authors have used different functions to show the relationship of RFR approximating the results cloud: linear functions with breakpoint (van Beeck et al., 2000; Yannis et al., 2010), logarithmic function (Bishai et al., 2006), single peaked function (Koornstra, 2007/1, Paulozzi et al., 2007), Kuznetz function (Kopis & Cropper, 2003; Law et al., 2011) and splines (Kopis & Cropper, 2003).

Of interest (for the purposes of this work) is the approach applied by (Dietze et al., 2008; CDOT, 2009; Kononov et al., 2008; Elvik 2004, Lord & Presaud, 2004) who used the Safety Performance Function (SPF) to forecast road safety on road sections and junctions based on the power and exponential function.

The SPF is a mathematical function which describes the relation between a normal and expected number of road accidents and the factors affecting road safety. Used in road safety management, the function helps to determine the potential for improvement, diagnose road safety problems, identify high risk sites and evaluate the effectiveness of proposed improvement countermeasures (Lord & Presaud, 2004; Kononov et al., 2008).

The Author's proposal is to use the Country Safety Performance Function (CSPF) as a function to describe the relation between a country's normal and expected road fatality rate and the variables of its social and economic, road transport and road safety management systems. The proposal offers a new application of the CSPF concept (Elvik 2004). The features of the function should include simplification, quantification and communications (Wegman & Oppe, 2010).

Considering the results of literature studies and the results of the Author's preliminary research, the following are the assumptions to the CSPF mathematical model:

1. The model should be simple to use for long-term forecasts of safety measures, safety assessments and decision-making.
2. The model should help to study the effects different factors have on road safety measures at

the national (macro) level and take into account area, demographic, economic, motorization, infrastructure and transport (mobility) aspects.

3. The model should meet the following boundary limits:

Condition I:

$$RFR = 0, \quad for \quad \text{GDPPC} = 0 \tag{1}$$

Condition II:

$$RFR = 0, \quad for \quad \lim_{GDPPC \to \infty} = 0 \tag{2}$$

Condition III:

$$RFR = RFR_{\max} \quad for \quad GDPPC = GDPPC_{BP} \tag{3}$$

The variables in formulas 1–3 mean: RFR—road fatality rate, GDPPC—Gross National Product per capita, HDI—Human Development Index.

Condition I is obvious—with no activity of the population there should be no road deaths. Condition II goes back to Vision Zero (Tingvall, 1998) which means no fatalities in road accidents. Condition III takes account of the fact that there is a breakpoint within the series of road fatality rate numbers as a country develops.

3 METHODS AND DATA

Using statistical mathematical models to develop the CSPF, four important scientific problems are identified: selection of data sets, selection of (independent) explanatory variables, selection of scale parameter and selection of the shape and parameters of the approximating function.

Databases (ECMT, Eurostat, FAO, IRF, IRTAD, OECD, TI, UN, WB, WHO) and a number of other sources provided empirical fatality data as well as data from 61 countries. Broken by the different years, they covered geography, demography, economy, social issues, motorisation, roads and transport. For the purposes of the CSPF, the number of countries was narrowed down to 22. The set included countries with solid road deaths statistics and ones that did not record any major changes in the RFR over time. The countries selected (such as Australia, France, Japan, Netherlands and Sweden) have similar RFR. The underlying data come from the period between 1922 and 2010 and cover 983 country-years.

To ensure that the independent variables are significant the interdependence between independent variables (X) and selected safety measures (Y) was analysed. The relationship between variables X and Y was studied using the linear correlation coefficient Pearson's R which measures the power of a straight line relation between two measurable features. Because many relations are non-linear, neural networks were used to determine the power of the relation between the variables. As a result of an in-depth analysis a group of 30 factors was narrowed down to 13 as independent variables.

Based on an analysis of the literature and own work, four parameters of scale were identified: time T, motorisation rate MRMV, human development index HDI and gross domestic product per capita GDPPC.

Eventually, two were selected for further analyses: GDPPC and HDI as parameters of scale for modelling the RFR. GDPPC, however, helps with forecasts (irrespective of time) of the human development index HDI and the motorisation rate MRMV. It can be used to simulate and analyse motorisation rates and road safety at different stages of a country's social and economic development (irrespective of time). The downside of GDPPC is that it reduces the scale as its numerical value decreases (applies mainly to historical data).

The choice of a concrete form of the approximating function depends on how well it can reflect empirical data. The literature includes several cases of RFR modelling, usually adopted as the F/P relation, using exponential models (Koornstra 2007/2) or the Kuznetz model (Kopitz & Corpper, 2003).

Based on analyses the power-exponential function was selected due to its ability of data approximation. The power-exponential function is the product of the power and exponential function. This function is known to have been used for modelling road safety measures (Kononov et al., 2008), (Elvik, 2004). The generalised form of the function is shown in formula (4).

$$Y = \alpha \cdot \prod_{i=1}^{n} X_i^{\beta_i} \cdot \exp\left(\sum_{j=1}^{m} \gamma_j \cdot X_j\right) \tag{4}$$

In this function Y is a dependent variable, X_i—i-th independent variable described with the power function (which is usually a parameter of scale), X_j—j-th independent variable described with the exponential function, m, n—number of independent variables, and α, β, γ—parameters of the equation.

To model the measures of normalised risk, the power-exponential function was used described with general formulas (5 and 6) (Jamroz, 2011):

$$\begin{aligned} RFR.a = {} & \beta_o \cdot GDPPC^{\beta_1} \cdot DP^{\beta_3} \cdot \exp(\beta_4 \cdot GDPPC \\ & + \beta_6 \cdot AVTKPC + \beta_7 \cdot MRMV \\ & + \beta_8 \cdot PMV + \beta_9 \cdot LEI + \beta_{10} \cdot CPI \\ & + \beta_{11} \cdot ACPC + \beta_{12} \cdot PUP + \beta_{13} \cdot PAL \\ & + \beta_{14} \cdot DRP + \beta_{15} \cdot DME) \end{aligned} \tag{5}$$

$$RFR.b = (1 - HDI)^{\beta_2} \cdot DP^{\beta_3} \cdot \exp(\beta_5.(1 - HDI) + \beta_6 \cdot AVTKPC + \beta_7 \cdot MRMV + \beta_8 \cdot PMV + \beta_9 \cdot LEI + \beta_{10}.CPI + \beta_{11} \cdot ACPC + \beta_{12} \cdot PUP + \beta_{13} \cdot PAL + \beta_{14} \cdot DRP + \beta_{15} \cdot DME + \beta_{16}) \quad (6)$$

where: GDPPC—gross domestic product per capita (thous. ID/inhab.), DP—population density (inhab./km^2), PUP—percentage of urban population (%), PAL—percentage of arable land (%), HDI—Human Development Index, LEI—Life Expectancy Index, CPI—Corruption Perception Index, ACPC—alcohol consumption per capita (l/inhab.), MRMV—motorisation rate—motor vehicles (except two and three wheelers) (vehicles/1 thou. inhab.), PMV—percentage of motor vehicles (%),DRP—density of paved roads (km/100 km^2), DME—density of expressways and motorways (km/100 km^2), AVTKPC—average vehicle kilometre travelled per capita per year (km/inhab./year), MRMV—motorisation rate (vehicles/1 thou. inhab.), β_0, β_1, … β_n—equation coefficients.

Some of the components of the model occur interchangeably e.g. GDPPC and HDI and ACPC and MRMV.

4 RESULTS

Two groups of RFR models were elaborated as presented in formulas 5 and 6. The parameters of the equations were calculated using STATISTICA (StatSoft,2008). Table 1 shows the equation parameters for 4 models divided into two groups (group a—GDPPC as the parameter of scale). The models use from one to eleven independent variables representing country characteristics and the relevant transport systems. The variables used in the models are only those with numerical values in the equation parameters.

Table 1 shows the statistics (p, R^2) and test results of the models (Wald test, MSE) for models of group **a**. The variables used have a high degree of significance ($p < 0{,}036$) and meet the Wald test (for a significance level of at least 1%) which shows that the independent variables are significant in the non-linear models. The R^2 coefficient of determination was within 0.46 to 0.80. An analysis of the coefficient shows that models with one variable explain only 46–48% of the variability, models with two variables explain 51–52% of the variability and models with ten or eleven variables explain 77–80% of the variability of the functions.

Table 1. List of parameters of selected RFR models.

Parameters of the model		Group **a** models			
		RFR.a1	RFR.a2	RFR.a3	RFR.a4
β_0		2.106	2.321	72.850	121.93
β_1	GDPPC	2.714	2.708	2.307	2.234
β_2	(1-HDI)				
β_3	DP			–0.072	–0.0895
β_4	GDPPC	–0.184	–0.203	–0.149	–0.127
β_5	(1-HDI)				
β_6	AVTKPC		0.0520	0.0583	
β_7	MRMV				0.00022
β_8	PMV			0.0032	
β_9	LEI			–4.130	–4.322
β_{10}	CPI			–0.016	–0.0213
β_{11}	ACPC			0.0257	0.0248
β_{12}	PUP			–0.0034	–0.0020
β_{13}	PAL			–0.002	–0.0023
β_{14}	DRP			0.0025	0.0022
β_{15}	DME			–0.0595	–0.0377
β_{16}					
N		992	992	859	868
BP—breakpoint		14,75	13.32	15.47	17.54
p		<0,001	<0.001	<0.036	<0.0352
R^2		0,483	0.514	0.798	0.776
Wald test		930,5	544.4	304.2	296.9
MSE (%)		35,4	34.3	22.2	23.6

MSE (22.1–23.6% for models with many variables, models 3 and 4) suggests quite strong differences between the expected and actual value of RFR. Simple models (with one or two variables, models 1 and 2) produce much bigger differences between calculated and actual values.

The available data (for group of 22 countries) do not show the early stages of social and economic development (i.e. HDI < 0.45) or high income per capita (for GDPPC > 50 thou. ID/mk/year). The RFR changes together with the changing levels of the country's social development following the power-exponential function (models marked as 1). In the case of:

– GDPPC as the parameter of scale, in the early stages of socio-economic development the numerical value of RFR increases rapidly until it reaches its maximum (at breakpoint BP which occurs for GDPPC = 13.3–17.5 thou. ID/inhab. depending on the model) and then starts to decline at first quite rapidly to gradually slow down asymptotically to the GDPPC axis,
– HDI as the parameter of scale, in the early stages of socio-economic development the numerical value of RFR increases slowly to reach its maximum (at breakpoint BP which occurs for HDI = 0.82–0.86 depending on the model) and then starts to decrease rapidly down to zero at HDI = 1.

An analysis of Table 1 results suggests that both groups of models give a good description of the expected number of fatalities in relation to the country's changing socio-economic development. Of the two groups of models, the model using GDPPC as the parameter of scale was selected for further work. This is because it gives a better understanding of the effects of road safety policies in a country (the right hand side of the chart is longer) and as such is more practical when elaborating strategic road safety management, forecasting the number of road deaths and assessing road safety.

As mentioned before, by adding a second independent variable to the RFR models (marked 2 and 3), we can significantly improve the quality of the models. Of the other independent variables, transport variables have a significant effect. They are: average vehicle kilometre travelled per capita AVTKPC and motorisation rate relative to motor vehicles MRMV which also represent the mobility of the country's population. The quality of the models can be improved by using AVTKPC. Because this variable may be difficult to estimate for some countries it can be replaced with MRMV.

For further analyses (in this article) the RFR.a3 model was adopted for GDPPC as the parameter of scale and AVTKPC as the measure of mobility. This model was chosen as the Country Safety Performance Function for the country level. With more independent variables the quality of the models is further improved. In the case in question the most significant parameters (significance level of 5%) were those describing the system of the country, transport system, etc. Figure 1 shows the average values of elasticity of the independent variables in the ranges obtained from model RFR.a3.

An analysis of Table 1 results suggests that both groups of models give a good description of the expected number of fatalities in relation to the country's changing socio-economic development. Of the two groups of models, the model using GDPPC as the parameter of scale was selected for further work. This is because it gives a better understanding of the effects of road safety policies in a country (the right hand side of the chart is longer) and as such is more practical when elaborating strategic road safety management, forecasting the number of road deaths and assessing road safety.

As mentioned before, by adding a second independent variable to the RFR models (marked 2 and 3), we can significantly improve the quality of the models. Of the other independent variables, transport variables have a significant effect. They are: average vehicle kilometre travelled per capita AVTKPC and motorisation rate relative to motor vehicles MRMV which also represent the mobility of the country's population. The quality of the models can be improved by using AVTKPC. Because this variable may be difficult to estimate for some countries it can be replaced with MRMV.

For further analyses (in this article) the RFR.a3 model was adopted for GDPPC as the

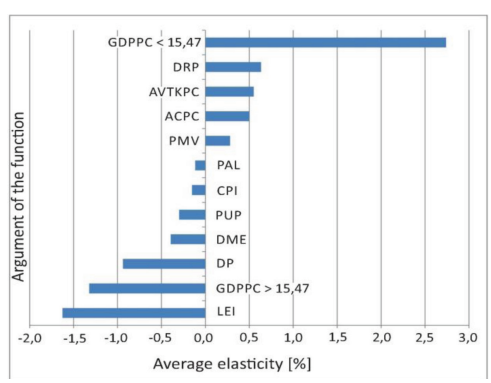


Figure 1. Distribution of Average Elasticity Rates (AER) for the selected model (RFR.a3) of fatality adopted as the RFPF for AVTKPC as parameters of scale.

parameter of scale and AVTKPC as the measure of mobility. This model was chosen as the Country Safety Performance Function for the country level. With more independent variables the quality of the models is further improved. In the case in question the most significant parameters (significance level of 5%) were those describing the system of the country, transport system, etc.

An analysis of Figure 3 shows the most significant factors which change RFR in the countries in question:

– up: GDPPC (in the range < 15.47 thou. ID/mk), DRP, AVTKPC, ACPC and PMV,
– down: LEI, GDPPC (V > 15.47 thou. ID/mk), DP, DME, PUP, CPI and PAL.

When **GDPPC** increases, road fatality RFR increases at first following the power function (AER—2.74%) until it reaches its maximum (at breakpoint BP and GDPPC = 15.47 thou. ID/mk) and after it has hit the breakpoint it decreases following the exponential function (AER—1.32%).

DP tends to increase together with growing population because the area of a country does not usually change. As DP increases, RFR decreases following the power function (AER—0.94%). With high population density, the number and duration of trips goes down and public transport increases its share in total trips.

PUP tends to increase together with the country's economy. As PUP increases, RFR decreases following the exponential function (average elasticity 0.30%). This is due to significantly lower speeds in urban areas as opposed to rural areas.

PAL changes slightly together with economic growth (it increases in some countries and decreases in others depending on the economic policy). When PAL increases, RFR decreases following the exponential function (AER—0.12%). This is due to shorter trips as a result of less fallow land.

LEI changes from 0 to 1 and tends to increase together with the country's economic growth. When LEI increases, RFR decreases following the exponential function (AER—1.63%). This is due to fewer people dying after an accident because the health care system is good.

CPI changes from 1 to 10, when CPI increases, corruption decreases. The higher the social development, the lower the corruption. When CPI increases (i.e. corruption decreases), RFR decreases following the exponential function (AER—0.15%).

ACPC depends primarily on religious and cultural factors. When ACPC increases, RFR increases following the exponential function (AER—0.50%).

PMV rate tends to increase together with the country's economic growth. When PMV increases, RFR increases following the exponential function

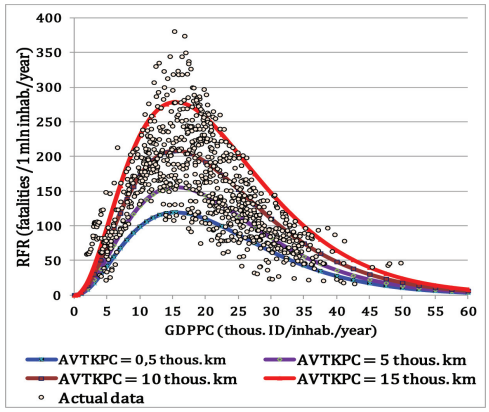


Figure 2. Charts of how the RFR changes in relation to GDPPC and AVTKPC compared to actual data in 22 countries.

(AER—0.28%). This is due to a growing fleet of motor vehicles.

DRP increases together with the country's economic growth (very quickly at first, then slowly asymptotically towards saturation). When DRP increases, RFR increases following the exponential function (AER—0.63%). This is due to higher speeds on improved roads.

DME increases together with the country's socio-economic development when a certain income threshold is exceeded. It grows asymptotically towards saturation. When DME increases, RFR decreases following the exponential function (AER—0.39%). This is due to high volume traffic moving to high quality roads.

AVTKPC increases together with the country's economic growth asymptotically towards saturation which may differ from country to country depending on its transport policy, size and land use. When AVTKPC increases, RFR increases following the exponential function (AER—0.55%). Figure 2 shows the changes in RFR depending on GDPPC and AVTKPC based on average values of the other parameters. This chart confirms that AVTKPC has a significant impact on RFR.

5 DISCUSSION OF RESULTS

The study has confirmed what many authors have postulated which is that a country's RFR depends primarily on its level of social development and a number of independent variables which represent risk exposure, sources of risks and interventions. Of the data analysed gross national product per capita GDPPC (the relation between gross domestic product and the population) was adopted as the

parameter of scale (on X axis). The GDP is on an upward trend (with slight distortions) and is the basic driving force of economic and social development in any country. The number of population changes slowly over time. This is why GDPPC can be used as a normalised measure of gross national income for direct comparisons between countries and for keeping track of the changes. As a result, the relation can be generalized and confirms the assumptions made at the beginning of this article.

If the scale of a country's socio-economic development is divided into ranges representing very low, low, medium, high and very high levels of socio-economic development and CSPF is divided into three areas (increase, breakpoint, decrease), we can say that (Fig. 3):

1. In the range of a very low to low socio-economic development of a country, growing income levels of the population increase mobility, motorisation and paved roads density which also triggers a quick **increase** in CSPF from zero until the maximum.
2. In between a low and medium socio-economic development of a country CSPF reaches its **breakpoint** as a result of a slower pace of motorisation, the launch of a safety system (improved legislation, education, leadership), use of safety management methods (improved enforcement, safety programmes) and a gradual change in road user behaviour (use of seatbelts, no drinking and driving).
3. In the range of a medium socio-economic development of a country CSPF **decreases** quite rapidly and when it reaches the range of a high and very high level of social development it continues asymptotically to zero. This is due to factors such as: levelling off of motorisation, density of paved roads and population mobility, increase in high quality roads i.e. expressways and motorways, development of state and democratic bodies and following from that less corruption, improved health care system, improved safety culture (use of seatbelts, lower alcohol consumption).

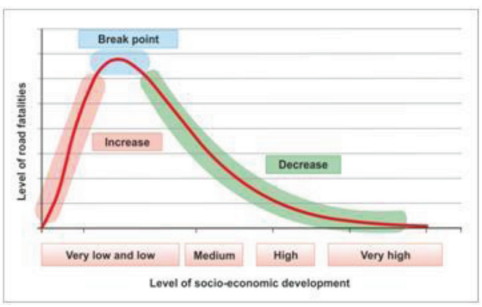


Figure 3. General model of CSPF in relation to the country's socio-economic development.

This general model has been confirmed in this work and its analyses and in earlier work (Kopits & Cropper, 2003; Anbarci et al., 2006; Bishai et al., 2006; Jamroz, 2012; Koren & Borsos, 2006; Koornstra, 2007/1; Yannis et al., 2010, 2014). The proposed model applies to the majority of countries in the world. There are deviations from the model in the group of developing countries (accelerated growth of motorisation which does not match the development of the systems of transport, health care and safety culture) and high income countries with insufficient road safety policies, i.e. significantly below the country's financial and organisational capacity.

If we assume that the resulting CSPF represents the average normalised relation between road fatality rate and the country's level of socio-economic development, the variance between expected and actual values shows:

– the match between estimated data (using the model) and actual data,
– the current level of road safety compared to the expected level in relation to the country's level of socio-economic development,
– the effectiveness of road safety improvements.

The charts above confirm that in general the CSPF has been adequately identified. What may be debatable are the rigorous requirements for the right hand side range of the function towards the target value. However, this approach can be justified by Vision Zero which is confirmed by the actual RFR values for many countries (Australia, Netherlands, Japan, Germany, Portugal). To confirm the claim, we must continue to watch the road fatality rates in these countries.

6 CONCLUSIONS

The Country Safety Performance Function presented in this article gives a good explanation of the essence of road safety measured with the country's RFR. Described with a power and exponential model, the CSPF consists of three distinct parts: increase, breakpoint and decrease. The maximal value of CSPF depends on a number of factors of which the most important ones include mobility of the population, level of health care, the country's organisational system, road network structure, land use and safety culture. This function can be used to explain the current condition of road safety and the forecasts and it shows that it is possible to reduce road deaths in a country down to zero. It is possible when the country has

a very high level of socio-economic development. This is a positive answer to the questions put in the introduction.

The results of the study were used to develop a proposed international classification of road safety and simple didactic methods for estimating the number of road deaths in specific countries. These proposals will be discussed in subsequent publications.

REFERENCES

Al-Haji G (2007).: Road Safety Development Index (RSDI). Theory, Philosophy and Practice. Linkoping University, Institute of Technology, Norrkoping, Sweden.

Anbarci N., Escaleras M., Register CH., (2006): Traffic Fatalities and Public Sector Corruption. Kyklos 59, issue 3, pp. 327–344.

Bishai D. Quresh A., James P., Ghaffar A. (2006): National road casualties and economic development. Health Economics 15, pp. 65–81.

CDOT, (2009): Safety Performance Functions for intersections. Colorado Department of Transportation—Research. Denver, Colorado, Report No. CDOT-2009-10.

Data and databases: ECMT, Eurostat, FAO, IRF, IRTAD, OECD, TI, UN, UNDP, WB, WHO.

Dietze M., Ebersbach D., Lippold CH., et al. (2005): Safety Performance Function. RIPCORD-ISEREST-Delivery 10, 6th FP.

Elvik R. (2004): Traffic Safety. Chapter 16 in Handbook of Transportation Engineering. Editor M. Kutz, McGRAW-HILL.

Elvik R., (2010): The stability of long-term trends in the number of traffic fatalities in a sample of highly motorized countries. Accident Analysis and Prevention 42 pp. 245–260.

Elvik R., Vaa T., (2004): The Handbook of Road Safety Measures. Elsevier.

Hakkert A.S., Braimaister L.,(2002): The uses of exposure and risk in road safety studies. SWOV Institute for Road Safety Research. Report R-2002-12, Leidschendam, 2002, The Netherlands.

Hauer E., (2004): Statistical Road Safety Modelling. Transportation Research Record 1987 pp. 81–97.

Hollo P., (2008): Methods and tools of analyzing road accident data. PIARC International Road Safety Seminar Beijing, China.

Hollo P., Eksler V., Zukowska J., (2010): Road safety performance indicators and their explanatory value: A critical view based on the experience of Central European countries. Safety Science vol. 48, pp 1142–1150.

Jamroz K.,(2008): Review of road safety theories and models. Journal of KONBIN.—Vol. 1, no 1–4, pp. 89–98.

Jamroz K., (2010): Strategic risk measures in road traffic. Journal of KONBiN vol. 1 (13), 2010 pp 197–208.

Jamroz K., (2011): Metoda zarządzania ryzykiem w inżynierii drogowej (in Polish). (Method of risk management in highway engineering). Wydawnictwo Politechniki Gdańskiej. Gdańsk, Poland.

Jamroz K. (2012): The impact of road network structure and mobility on the national traffic fatality rate. EWGT 2012. 15th meeting of the EURO Working Group on Transportation. Procedia—Social and Behavioral Sciences 54 (2012) pp. 1370–1377. www.elsevier.com/locate/procedia.

Kononov J., Bailey B.: Allery B.K., (2008): Exploratory Examination of the Functional Form of Safety Performance Functions of Urban Freeways. TRB Annual Meeting.

Koornstra M.J., (2007/1): Prediction of traffic fatalities and prospects for mobility becoming sustainable-safe. Sadhama vol. 32, part 4, pp. 365–395.

Koornstra M.J., (2007/2): Changing Choices. Psychological Relativity Theory. Leiden University Press.

Kopits E., Cropper M., (2003): Traffic Fatalities and Economic Growth. The World Bank, Policy Research Working Paper.

Koren C., Borsos A., (2009): GDP, vehicle ownership and fatality rate: similarities and differences among countries. 4th IRTAD Conference, Seoul, Korea.

Law T.H., Noland R.B., Evans A.W. (2011): The sources of the Kuznets relationship between road fatalities and economic growth. Journal of Transport Geography 19 pp. 355–365.

Lord D., Persaud B.N., (2004): Estimating the safety performance of urban road transportation networks. Accident Analysis and Prevention 36 pp. 609–620.

OECD Scientific Group, (1994): Targeted Road Safety Programmes. OECD Paris.

Page Y. (2001): A statistical model to compare road mortality in OECD countries. Accident Analysis and Prevention, Vol. 33, pp. 371–385.

Papadimitriou, E., Yannis, G., Bijleveld, F., Cardoso, J.L., 2013. Exposure data and risk indicators for safety performance assessment in Europe. Accident Analysis and Prevention 60, 371–383.

Poulozzi L.J., Ryan G.W., Espitia-Hardeman V.E., Xi Y., (2007): Economic development effect on road transport-related mortality among different types of road users: A cross-sectional international study. Accident Analysis and Prevention 39 pp. 606–617.

StatSoft, (2008): Statistica—guidelines. StatSoft Inc. Kraków, Poland.

Tingvall C., (1998): The Swedish "Vision Zero" and how parliamentary approval was obtained. Road Safety Research. Policing. Educational Conference Wellington, New Zealand.

van Beeck E.F., Borsoboom G.J.J.:, Mackenbach J.P., (2000): Economic development and traffic accident mortality in the industrialized world, 1962–1990. International Journal of Epidemiology; 29; pp. 503–509.

Wegman F., Oppe S., (2010): Benchmarking road safety performances of countries. Safety Science 48 pp. 1203–1211.

Yannis G., Antoniou C., Papadimitriou E., Katsochis D., (2011): When may road fatalities start to decrease? Journal of Safety Research 42 (1), 17–25, 18, 2011.

Yannis G., Papadimitriou E., Folla K. (2014): Effect of GDP changes on road traffic fatalities. Safety Science 63 (2014) pp. 42–49.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Method of dynamic identification of hazardous driver behaviour by traffic parameters detection

M. Sumiła & M. Siergiejczyk
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: This paper outlines a method of detecting in real-time vehicles hazardous for other drivers by employing for that purpose telematics-enabled technology. Further into in the paper discussed are reasons behind defined hazards, technical possibilities feasible thanks to modern telematics-enabled devices used for purposes of Intelligent Transport Systems as well as modelling assumptions. The method and model of selective vehicle detection was presented and discussed in main part of the paper, ended with concise summary and conclusions.

1 INTRODUCTION

Fast-paced and substantial advances in computer and mobile communication technology over the past twenty years meant an equally impressive development of information systems. This is widely experienced through ubiquitous internet access. Already back in the nineties of the last century transport related businesses and institutes saw that potential and consequently spawned a wide range of ICT solutions supporting transport logistics processes as well traffic management. That last-mentioned area of technical solutions is commonly referred to as Intelligent Transport Systems (ITS).

ITS is defined as using advanced software to deliver innovative services with regards to different means of transport and traffic management. They are aimed at different user group of the transport system to provide them with information which not only makes transport safer, more convenient and coordinated, but also makes the entire transport network more "intelligently" and efficiently used.

It is estimated that a wide-scale introduction of ITS solutions to transport could yield tangible benefits in: increasing road capacity by 20–25%, improving road safety (decreasing the number of accidents by 40–80%), bringing down travel times and energy consumption (by 45–70%), reducing environmental footprint of transport (exhaust emissions 30–50% lower), making travel more comfortable and driving conditions more enjoyable for drivers, public transport users and pedestrians, cutting traffic management costs, lowering road servicing, maintenance and renovation costs, increasing economic benefits everywhere they were deployed. (Modelewski 2012).

In its lowest layer, mobile communication is provided by telematics systems, which are responsible for technical solutions facilitating services featured by ITS architecture implemented in given country (Litwin & Modelewski 2013). Convergence of IT and ICT systems resulted in telematics solutions integrated with on-board electronic systems using satellite navigation, emergency warning systems and also electronic toll collection systems.

Many organisations and international commissions are currently developing and integrating ITS some of which are: CEN, ISO, ETSI, IEEE and other.

Among many services offered and developed under ITS, there is strong demand to advance road emergency services known popularly as eCall.

1.1 *eCall*

The method presented in this paper is a vast improvement on the eCall system currently being rolled out across EU which taps into eSafety initiative. It is part of comprehensive European Commission strategy aimed at improving road safety and transport efficiency across Europe, a joint effort of EC and Western European scientific centres. The European Committee for Standardisation CEN/TC 278 as well as organisations the likes of ETSI and 3GPP have already embraced that concept.

The eCall system is envisaged to enable manual and automatic emergency call immediately after a road accident has taken place, involving the vehicle which initiated the call. Manual emergency call may be initiated by pressing a button available to the driver. Calls are started automatically should particular conditions be met concerning seriousness of the accident, based on impact sensor information. Every call is passed to the traffic management centre over cellular network. The operator receiving the call in the Centre, should obtain a Minimum Set of Data (MSD) concerning the accident. MSD contains fundamental information about the

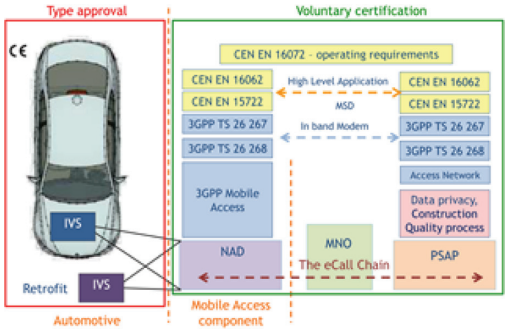


Figure 1. Certification principles (Legend: IVS—In-Vehicle Systems, MSD—Minimum Set of Data, NAD—Network Access Device, MNO—Mobile Network Operator, PSAP—Public Safety Answering Point) (Andy Rooke, iCar Support D4.2—eCall Good Practice. ERTICO, UK 30/11/2012 (http://www.imobilitysupport.eu/imobility-support/its-deployment/ecall/library/reports-13)).

incident. That information includes among other, time, precise geographical location of the vehicle during the accident, vehicle data including its VIN, eCall status including incident priority and information about the operator providing services.

In Authors' opinion eCall lags behind technology of the XXI century. It is quite antiquated and not efficient enough, an opinion which was voiced already 10 years ago (Rychlicki 2006), compared to functionalities offered by ITS. The method presented hereunder enables real-time selective vehicle detection and taking preventative action against vehicles which are identified to breach permitted behaviours and thus pose a threat to driver's life and those in his nearest proximity.

2 CURRENT STATE OF RESEARCH

The most common cause of road accidents is driver error. Typically it involves ignoring road signs, breaching road code of conduct or just plain recklessness. There is, however, a group of incidents, which are related to unforeseen and inadvertent, sudden worsening of driver's psychophysical state. Some the reasons for that deterioration include: exhaustion, influence of medication, driving under the influence of drugs or alcohol, instantaneous mental distress, fainting, cardiac arrest etc. All of the aforementioned lead to unexpected and unusual change in driving direction or speed. Under those circumstances, the vehicle affected becomes hazardous for surrounding vehicles as well as its own driver. Thus far, the only solution to this problem was imposing bans on drunken driving or under influence of drugs, preventing the driver from sitting behind the wheel should psychomotor ability be called into question and installing in-vehicle emergency call system.

The fundamentals of formal driving pattern description were presented in papers (Mac Adam 1981) and (McRuer & Weir 1969). They were expanded upon by descriptions of strategies used by drivers on the road, as presented in (Nechyba & Xu 1997). The paper (Aoude & Desaraju & Stephens & How 2012) suggests as to how to classify driver behaviours on crossroads and verify them based on real-life data provided from road-side equipment and vehicles themselves. Papers concerning modelling driver behaviours (Modjtahedzadeh & Hess 1993) present models of driving patterns used to evaluate vehicle performance, whereas (Okuda & Ikami & Suzuki 2013) puts forward a model using probabilistic "softmax" functions describing motor and decisional driver characteristics. Wide range of methods and models to simulate road safety were presented in paper (Young & Sobhani & Lenn´e & Sarvi 2014). The method presented below, is inclusive of latest advancements in technology, ITS (Intelligent Transportation System) in particular. It provides knowledge on hazardous vehicle detection and further developed, it may also enable safe vehicle management in specific road incidents.

3 HAZARDOUS VEHICLE SELECTIVE DETECTION

The term detection (identification) is defined in literature as an automated process involving operational data collection, extraction of characteristic information, classification and investigation into analysed event (Kozłowski 2010).

3.1 *Detection*

The method described below, is rather complex and thus requires close collaboration between traffic management centre and moving vehicles. To facilitate that, required are technical measures providing architecture for transfer of information between parties involved. There are two groups of detecting devices, being classified as telematics systems. The first are solutions monitoring a selected part of road infrastructure (CCTV cameras, road sensors). The second, more modern group, includes data collection solutions reading data about moving vehicles. Collected data is accessed through V2I or V2V2I solutions combined with dedicated wireless communications standards e.g. DSRC (EN 12253 2004)(EN 12795 2002)(EN 12834 2002) (EN 13372 2004) or WAVE (802.11p) (IEEE 1609 2007)(ETSI ES 202663 2013).

It was concluded that the method could only be used, when available are:

- ITS system, road infrastructure and traffic control centre,
- Devices for traffic stream control on dedicated arteries used for continuous vehicle monitoring.
- In-vehicle V2I devices (Vehicle to Infrastructure) feed information about current speed and position.
- Also on-board, should be installed V2V devices (Vehicle to Vehicle) distributing information about hazards directly between vehicles.
- The vehicle is equipped with MMI devices which facilitate vehicle to driver communication.

3.2 *General assumptions*

Real-time selective vehicle detection may be achieved by identifying parameters in the model defining behaviour of vehicle groups and individual vehicles and then comparing them against parameters obtained from observation of vehicles on roads.

The other assumptions were that observation time was discrete, because of the need to process obtained signals and produce results of analysis. Thus

$$t = t_{syg} + t_{prep} + t_{TX} + t_{net} + t_{proc} \tag{1}$$

where: t_{syg} = time to generate and collect signals from sensors, t_{prep} = time to preliminary process signals and prepare for sending, t_{TX} = message transmission time, t_{net} = message propagation time in by the network, t_{proc} = time to process the message in the centre.

Time t may be also influenced by volume of traffic. It is unrelated, on the other hand, to measuring method described above. For more details on the subject please see (Sumiła 2012). The parameter itself influences accuracy of vehicle trajectory representation, hence the more frequent location checking the higher probability of detecting potentially dangerous vehicles.

It was assumed that road observation area is described by matrix $\mathbb{D}$, size of which resembles the number of lanes in one direction R and length of analysed section W.

$$\mathbb{D}_{R\times W} \tag{2}$$

Observed traffic stream is described by matrix $\mathbb{G}_{R\times M}$, whose size resembles number of lanes R and capacity of each lane M. The maximum number of vehicles in single lane

$$\lim_{x\to M}(x\times l_{vehic} + x\times l_{dist}) = W \tag{3}$$

where: l_{vehic} = assumed vehicle length, l_{dist} = observed section length.

Vehicles can form different groups. Every group is described by matrix C, defined as selected vehicle group occupying road side-to-side (all lanes R), whose length is determined by number H of vehicles on busiest lane. At the same time it was assumed, that the distance between successive vehicles is less or equal to distance determined by either static or dynamic method described hereunder. Hence

$$l_{dist} \le l_{\min col} \tag{4}$$

Thus

$$\mathbb{C}_{R\times H}, where\ H \le M \tag{5}$$

Each of C_{rh} vehicles in the group is described by a vector of parameters

$$c_{rh}(t) = [l_{rhfront}, l_{rhrear}, V_{rh}, d_{rw}] \tag{6}$$

where: $l_{rhfront}$ = the space in front of the vehicle, l_{rhrear} = the space behind the vehicle, V_{rh} = speed of the vehicle, d_{rw} = length of the vehicle.

Those parameters will constitute the matrix of instantaneous speeds of vehicles and their location on the road.

3.3 *Selective group detection*

The first stage of selective vehicle detection is selective group selection from a traffic stream. One of three methods presented below may be used.

Static method involves detecting vehicles with space in front measured by number of average passenger car lengths. This method performs well in case of point observations by e.g. the aforementioned CCTV systems. In this particular solve should be used for observation by the camera placed above the or each lane. The image obtained from this source should be treated in real time, for example by using edge detection methods based on wavelet analysis and further based on the detection of changes in time determine the distance between vehicles.

$$l_{dist}(t) \ge l_{min} = n \times l_{vehic} \tag{7}$$

where: l_{min} = defined minimum spacing of vehicles between groups, n = number of car lengths, l_{vehic} = assumed average car length.

The essence of the method was depicted in Figure 2.

Dynamic method as a solution yields better results in terms of detecting vehicle group out of traffic stream. It involves detecting vehicle spacing within the group and then group spacing based on instantaneous statistic evaluation. Mean spacing of vehicles needs to be computed:

$$l_{śr}(t) = \frac{1}{R \times H} \sum_{r=1}^{R} \sum_{h=1}^{H} \left(\frac{l_{rhfront} + l_{rhrear}}{2} \right) \tag{8}$$

Once population average is known, variance s^2 of distribution is then calculated.

$$s_l^2(t) = \sum_{r=1}^{R} \sum_{h=1}^{H} \frac{(l_{rh}(t) + l_{śr}(t))^2}{R \times H} \tag{9}$$

Should s_1^2 tend to zero it means within observation area it is difficult to detect individual groups, because vehicle spacing is approximately the same.

Variance greater than zero means deciles of vehicle spacing (between observed vehicles) need to be checked. Approximate values of greater amount of deciles indicate homogeneity of population i.e. spacing of vehicles within groups, whilst last deciles indicate spacing of groups.

This method works well for vehicles with front and rear proximity sensors (parking and driving) as well as V2V connectivity.

3.4 *Group characteristics detection*

Once a group is selected from traffic stream, its average speed is determined. In order to do that, individual vehicle average speeds need to be known.

$$V_{śr}(t) = \frac{1}{R \times H} \sum_{r=1}^{R} \sum_{h=1}^{H} V_{rh} \tag{10}$$

By comparing that value with instantaneous speeds provided by speed matrix $\mathbb{V}_{R \times H}$, tendency of vehicle speed change over time t is determined. Also, after comparing current V_{rh} with previous instantaneous speeds, acceleration a_{rh} is determined, represented by matrix $\mathbb{A}_{R \times H}$.

Furthermore, location change of group compared to the entire traffic stream could also be determined, by comparing detected average speed of vehicle group to average speed of traffic stream V_{pot}.

$$V_{pot}(t) = \frac{1}{R \times W} \sum_{r=1}^{R} \sum_{W=1}^{W} V_{rw} \tag{11}$$

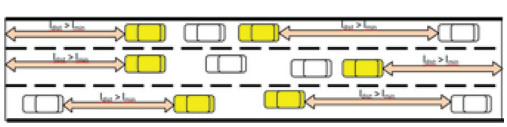


Figure 2. Vehicle group selected by vehicle spacing detection (marginal vehicles denoted in yellow).

Hence if

$V_{śr} < V_{pot}$—group is decelerating and probably will become part of closing up group

$V_{śr} = V_{pot}$—group moves consistently with the stream and maintains formation

$V_{śr} > V_{pot}$—group is accelerating and probably will become part of leading group

That change could be precisely detected based on the grounds of comparing average values for vehicles adjoining directly to analysed group.

3.5 *Detection of permitted behaviours within vehicle group*

Once fundamental group characteristics are identified, behaviours defined as permitted need to be detected whilst the vehicles remains mobile.

Based on knowledge about vehicle location d_{rh} and group average speed and instantaneous speeds of individual vehicles, the following assumptions were taken:

1. vehicles may increase or decrease spacing by accelerating and braking smoothly (meant by smooth is acceleration required by normal driving style),
2. vehicle may abruptly accelerate during overtaking manoeuvre whilst changing lane given there is enough space,
3. vehicle may abruptly brake into a standstill before an obstacle,
4. vehicle decelerates when approaching an obstacle, provided it is within vehicle's braking distance, when approaching crossroads, traffic lights or planned turning.

Above-mentioned assumptions define permitted driver behaviours within a group or in its marginal positions.

Deviation from $V_{avg}(t)$ was also calculated based on standard deviation for population of observed vehicles.

$$\sigma = \sqrt{\frac{\sum_{r=1}^{R} \sum_{h=1}^{H} (V_{rh}(t) = V_{śr}(t))^2}{R \times H}} \tag{12}$$

where: $V_{rh}(t)$ = temporary speed of the vehicle at time t, $V_{śr}(t)$ = the average speed of the column of vehicles at time t.

Given computed standard deviation, an assumption was made that deviation of instantaneous speed in instant t by one or two standard deviations from average speed is acceptable, provided there is enough space between the vehicle and its surrounding.

$$V_{accel} : \mathbb{H} \rightarrow \exists l_{rhfront} V \exists l_{rhrear} \geq n \times l_{vehic} \tag{13}$$

Above assumption does not need to be satisfied for marginal positions in formation, either its utmost front or rear positions. For those marginal cases, vehicles are entitled to accelerate or brake when space in front of them or behind them is greater than $l_{distcol}$.

$$\mathbb{C} = \begin{bmatrix} c_{11} & \dots & c_{R1} \\ c_{1H} & \dots & c_{RH} \end{bmatrix} \tag{14}$$

Hence, it is not advised to include instantaneous speeds of marginal vehicles in determining average speed of vehicle group.

$$V_{śr}(t):\mathbb{C} = \mathbb{V}_{R\times W}(t) - V_{front}(t) - V_{rear}(t)) \tag{15}$$

where

$$V_{front}(t) = [V_{11}(t), \dots V_{R1}(t)] \tag{16}$$

$$V_{rear}(t) = [V_{1W}(t), \dots V_{RW}(t)] \tag{17}$$

Then, cases of lane changing by vehicles moving within the group need to be considered. That manoeuvre is permitted when there is space in the other lane for the vehicle to drive into. When determining instantaneous speeds matrix for moving vehicles, free spaces are represented by elements whose speed V_{rh} is 0 [m/s]. Three possible cases need to be analysed at this stage (two concerning outside lanes and one inside the group). They were depicted in Figure 3.

Speed matrix for vehicles surrounding that space is represented by vector relative to distance matrix $\mathbb{D}_{R\times W}$

$$V_{space}[r,W](t) = [V_{rh}[r,w-1](t), V_{rh}[r-1,w](t), V_{rh}[r,w+1](t), V_{rh}[r+1,w](t)] \tag{18}$$

where: $V_{space}[r, w](t)$ = instantaneous speed vector of vehicles surrounding free space within the group, $V_{rh}(t)$ = next vehicle within the group surrounding the free space.

Note that in marginal cases, vehicle vector is calculated for three elements and will become:

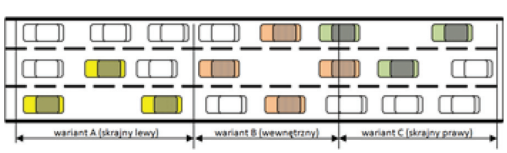


Figure 3. Three cases of spacing within group favourable for lane changing.

– for left marginal case (*option A*)

$$V_{space}[r,w](t) = [V_{rh}[r,w-1](t), V_{rh}[r,w+1](t), V_{rh}[r+1,w](t)] \tag{19}$$

– for right marginal case (*option B*)

$$V_{space}[r,w](t) = [V_{rh}[r,w-1](t), V_{rh}[r-1,\ w](t), V_{rh}[r,w+1](t)] \tag{20}$$

It is obvious that there might be a case where vehicles preceding and succeeding free space could diminish that gap by accelerating or braking. Then the V_{space} element moves in the speed matrix.

3.6 *Detecting vehicles posing potential danger*

The aforementioned selective detection on moving dynamically traffic enables to single out movement dynamics of individual vehicles with single time step precision. Changes in acceleration compared to previous instants and changes in movement trajectory may be detected by selected vehicle matrix $\mathbb{C}_{R\times H}$ and instantaneous speed matrix $\mathbb{V}(t)$ provided assumptions of the model are met. Analysis of changes in speed and trajectory compared to permitted behaviour patterns leads to selecting vehicles moving in an abnormal fashion. The detection process was depicted in Figure 4.

After filtering, based on signals S compared with parameters generated by the model, a new signal S′ may be obtained to select vehicles whose driving patterns in traffic are dubious in terms of safety. The most popular is the Kalman filter which is an algorithm that uses a series of measurements observed over time, containing noise (random variations) and other inaccuracies, and produces estimates of unknown variables. It its extended version, it produces estimates state vectors for non-linear dynamic system described by recursive system of equations. Among other filters the continuous wavelet transform was also considered.

Should results of successive measurements indicate deviation from permitted standard, the traffic management centre should undertake the following measures:

1. attempt to communicate with the driver by in-vehicle telematics-enabled devices and MMI interfaces,

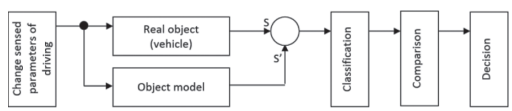


Figure 4. Detection process using output signals.

2. if abnormal activity continues posing constant threat to other road users, surrounding vehicle drivers should be informed about potential danger via available telematics-enabled systems,
3. in case of non-responsive driver, the "Auto Safety Stop" procedure should be deployed, which is subject of author's' upcoming publications,
4. pass information about initiated procedure to surrounding vehicles,
5. deploy the ASS procedure and pilot the vehicle to a safe parking spot.

4 SUMMARY

The paper presented the method of dynamic identification of hazardous driver behaviour by traffic parameters detection. Such identification is possible only when appropriate telematics' solutions are applied both in a road and a vehicle. The mathematical tools used of elements of probability to identify the columns of vehicles and a formal description of acceptable behaviour of drivers on the road led to the possibility to differentiate these vehicles, that movement differs from from the expected behaviour. In this sense proposed approach should be regarded as an innovative and far-emptive currently proposed important in the context of the eCall project.

The method described hereinbefore should be treated as work in progress, which needs further developing. In authors' opinion, the notion of vehicle group (across all lanes) should be reconsidered to concern each lane individually. It seems justified given speed differences between vehicles driving in different lanes.

Further research is expected aimed at carrying out simulations. Should simulation results prove to help increase road safety, implementation of the method may be considered once adequate technology arrives.

REFERENCES

Aoude, G.S. & Desaraju, V.R. & Stephens, L.H. & How, J.P. 2012. *Driver behavior classification at intersections and validation on large naturalistic data set* IEEE Trans. Intell. Transp. Syst., vol. 13, no. 2, 724–736.

CEN/TR 16405:2013 *Intelligent transport systems—ESafety—ECall additional optional data set for heavy goods vehicles eCall.*

EN 15722:2011 *Intelligent transport systems—eSafety—eCall minimum set of data (MSD).*

EN 16072:2011 *Intelligent transport systems—eSafety—Pan-European eCall operating requirements.*

EN 16102:2011 *Intelligent transport systems—eCall—Operating requirements for third party support.*

EN 16062:2011 *Intelligent transport systems—eSafety—eCall high level application requirements (HLAP).*

EN 12253:2004 *Dedicated Short-Range Communication—Physical layer using microwave at 5.8 GHz (review).*

EN 12795:2002 *Dedicated Short-Range Communication (DSRC)—DSRC Data link layer: Medium Access and Logical Link Control (review).*

EN 12834:2002 *Dedicated Short-Range Communication—Application layer (review).*

EN 13372:2004 *Dedicated Short-Range Communication (DSRC)—DSRC profiles for RTTT applications (review).*

ETSI ES 202663 2013. *European Telecommunications Standards Institute.* (Final draft 2009-11).

http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/ITSSG.aspx

http://www.etsi.org/website/technologies/intelligenttransportsystems.aspx

http://sites.ieee.org/itss/

http://www.iso.org/iso/iso_technical_committee?commid=54706

IEEE 1609 2007. *Family of Standards for Wireless Access in Vehicular Environments (WAVE). U.S. Department of Transportation. January 9, 2006.*

Kozłowski, M. 2010. *Badania zerwania przyczepności w ruchu pojazdu szynowego,* WPW, Warszawa.

Litwin, M. & Modelewski K. (2013). *European ITS framework architecture for transportation planning support*, Archives of Transport System Telematics. Vol. 6, Issue 2. Katowice, 51–56.

MacAdam, C. 1981. *Application of an optimal preview control for simulation of closed-loop automobile driving*, IEEE Trans. Syst., Man, Cybern., vol. SMC-11, no. 9, 393–399.

McRuer, D. & Weir, D. 1969 *Theory of manual vehicular control*, Ergonomics, vol. 12, no. 4, 599–633.

Modelewski, K. 2012. *Architektura Inteligentnych Systemów Transportowych*, Prezentacja SKNTL. Politechnika Warszawska, Warszawa.

Modjtahedzadeh & Hess, R. 1993. *A model of driver steering control behavior for use in assessing vehicle handling qualities*, ASME J. Dyn. Syst. Meas. Control, vol. 15, no. 3, 456–464.

Nechyba, M.C. & Xu, Y. 1997. *Human control strategy: Abstraction, verification, and replication*, IEEE Control Syst., vol. 17, no. 5, pp. 48–61.

Okuda, H. & Ikami, N. & Suzuki, T. 2013. *Modeling and Analysis of Driving Behavior Based on a Probability-Weighted ARX Model*, IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, 98–112.

Rosinski, A. 2008. Design of the electronic protection systems with utilization of the method of analysis of reliebility structures. Proc. Nineteenth International Conference On Systems Engineering ICSEng, Paper: 421–426.

Rychlicki, M. 2006. *Zastosowania systemu elektronicznego powiadamiania o wypadkach*, VIII Międzynarodowa Konferencja TST, Ustroń.

Sumiła, M. 2013. *Impact of Telematics-enabled devices on driver behavior*, Archives of Transport System Telematics. Vol. 6, Issue 1, Katowice, 49–52.

Sumiła, M. 2012. *Selected Aspects of Message Transmission Management in ITS Systems*, Telematics in the Transport Environment. Springer Heidenberg 141–147.

Young, W & Sobhani, A. & Lenn, M.G. & Sarvi, M. 2014. *Simulation of safety: A review of the state of the art in road safety simulation modeling*, Accident Analysis and Prevention 66 (2014), 89–103.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The method of risk management of accidental oil spills at sea

K. Łazuga & L. Gucma
Maritime University of Szczecin, Poland

ABSTRACT: The paper presents methodology of risk management of accidental oil spills at sea. The factors affecting the amount of costs incurred removing oil spills and cost and consequences estimating equations are described. The examples of spills costing in the Polish coast. New measures of costs evaluation and optimization have been proposed. These issues sought to be applied to the evaluation criteria of environmental cleanliness and specified cost that is able to bear the society to maintain pollution-free sea coast.

1 INTRODUCTION

The Baltic Sea is one of the most heavily trafficked seas in the world. The main environmental effects of shipping and other activities at sea include air pollution, illegal deliberate and accidental discharges of oil, hazardous substances and other wastes, and the unintentional introduction of invasive alien organisms via ships' ballast water or hulls.

There are around 2,000 ships at the Baltic Sea at any one time. Approximately, 20% of them are tankers, carrying as much as 166 million tons of oil per year (HELCOM, 2010). Each year there are 120–140 shipping accidents in the Baltic Sea area (Fig. 1). The majority of accidents are groundings and collisions (HELCOM, 2010). Around 7% of the shipping accidents in the Baltic Sea results in some kind of pollution, usually containing small amounts of oil (0.1–1 tones). Despite this Baltic Sea is relatively safe comparing to other regions. The largest pollutions accidents are as follows:

– 1990 'Volgoneft', 700–800 t. of waste oil; nearly all oil recovered at sea,
– 2001 'Baltic Carrier', 2,700 t. of oil; around 50% of oil recovered at sea,
– 2003 'Fu Shan Hai', 1,200 t. of fuel oil; around 1,100 tones of oil recovered at sea.

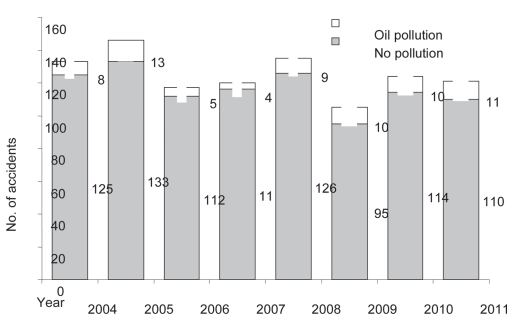


Figure 1. Accidents at the Baltic Sea with and without oil pollution (HELCOM 2011).

2 RISK MANAGEMENT OF MARINE NAVIGATIONAL OIL SPILLS AT THE BALTIC SEA

Risk (R) of accidental oils spills will be defined as:

$$R = \sum P_i C_i \tag{1}$$

where: P_i—frequency of i-tch spill, C_i—consequences of i-tch oil spill.

In further part of this paper the methods of P and C evaluation are presented. Risk management procedure is intentional multistep method consist of risk analysis assessment and control with CBA

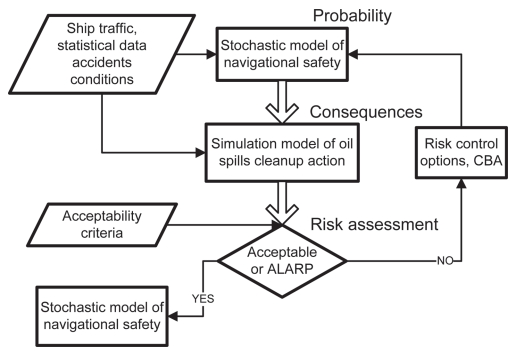


Figure 2. Risk management procedure of accidental oil spills at sea.

optimization. The procedure proposed here utilizes the stochastic model of navigational safety for probability of oil spill assessment and oil spill cleanup simulation model with cost of cleanup action estimation (Fig. 2).

3 FACTORS AFFECTING THE COST OF OIL SPILL

Knowledge of the cost of cleaning the spill provides an important framework for risk assessment and spill response plan. However, there is a very large variation cleaning costs to different incidents, depending on the leakage logistical support in the region of leakage, and the various environmental and sociological factors (Fingas M. edt. 2010).

Number of factors affecting the amount of the costs of removing spills is very large. The most important of them are: the place and time of year in which the event occurred, the type of spilled material and the speed of its spread, the volume of spill, the manner of disposal, weather conditions, the degree of pollution of the coast and others. However, regardless of the nature of the medium they are all interrelated.

As a result of such a large number of factors have been attempts to find relations, which would calculate the estimated cost of disposal of spillages. So far failed to find such a formula, among other things, because no two are the same spill. This makes it harder to take into account all the factors affecting the cost of disposal of spillages. At present, an attempt to predict the cost of the spillage is the study of registered spills, and the resulting database is based on factors that have an impact on costs. This analysis can be used to develop the estimation algorithm presumed cost of marine spills. The final model should take into account various factors simultaneously to create individual methods of forecasting the costs incurred.

4 PROBABILITY OF OIL SPILL ASSESSMENT

The stochastic model of navigational safety and oil modeling presented in (Gucma & Przywarty 2007) could be applied for the first step of risk management procedure. Oil spill accident can occur in arbitrary moment. Scenarios were simulated for risk of oil spill impact evaluation. Meteorological conditions represent average Baltic Sea conditions. On the base of wind and current data probable situations were formed. The data show simulated pollution zones.

The model output is long time spatial distribution of oil spills in given area (Fig. 3). Averaging

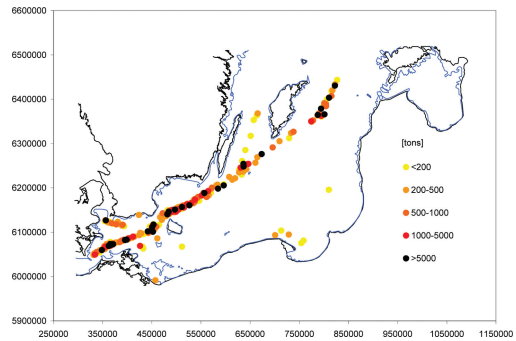


Figure 3. Simulated oil pollutions collision at the southern Baltic Sea (long time simulations results based on (Gucma & Przywarty 2007)).

the results with consideration of simulation times it is possible to find mean probabilities and amount of oil spilled per year.

5 COST OF CLEANUP ACTION BY SIMULATION MODELS

The first approximation of oil spill cost without considering damage to environment could be done by simplified statistical models. One of such model of cleanup cost reveal that unit cost is not dependant of spill size (Fig. 4). The model can be written as (Goryczko & Gucma 2006, Etkin D.S., 2000):

$$C = 255218\, v^{-04184} \tag{2}$$

where: C = cost of oil cleanup in PLN; v = the amount of oil spill (t).

The above formula is too simplify to use it in serious researches therefore the simulation model PISCES II provides the ability to develop, conduct and debrief realistic incident response exercises with reliable cost of oil spill estimation, all in one application. The application's chart and text-based status windows can be directed to large screen displays. This capability lends itself to providing informative command post status displays and is essential for post-exercise debriefing sessions (Fig. 5).

Modelling of the hydrodynamic reaction to the activities of response resources, such as booms, skimmers and chemical dispersants was performed. The simulated processes included: oil spread, evaporation, sinking in the water column, burn-off, and the pollutant's interaction with the coastline. Environmental conditions, including air temperature, wind speed and direction, wave height, current set and drift, could be adjusted dynamically during the simulation. PISCES II enables to calculate

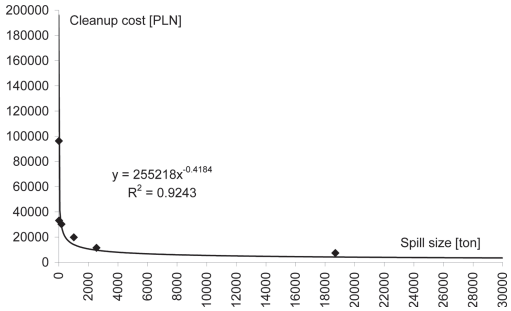


Figure 4. Theoretical model of oil sill up costs (in PLN/ton) by exponential function.

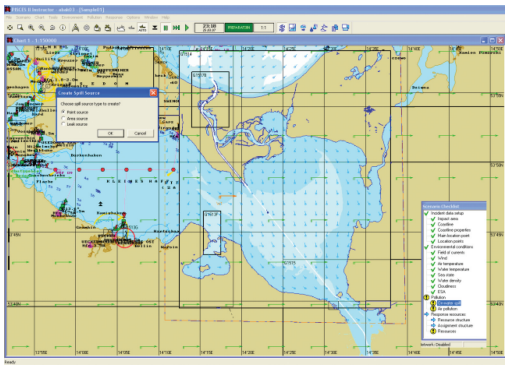


Figure 5. PISCES II graphical interface main window.

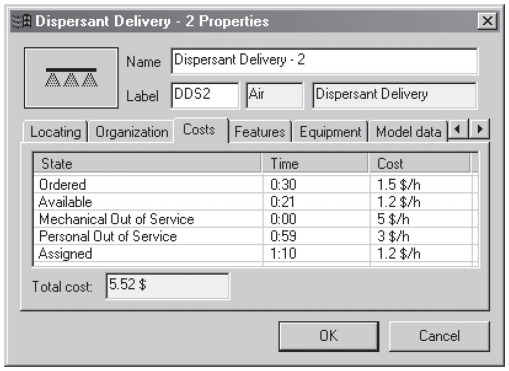


Figure 6. Cost of cleanup action input window.

the cost of applying both the individual resources and the whole operation for the current time. It can be observed the cost of using each resource in the properties window of the object in question by going to the "Total cost" field of the "Costs" tab (Fig. 6).

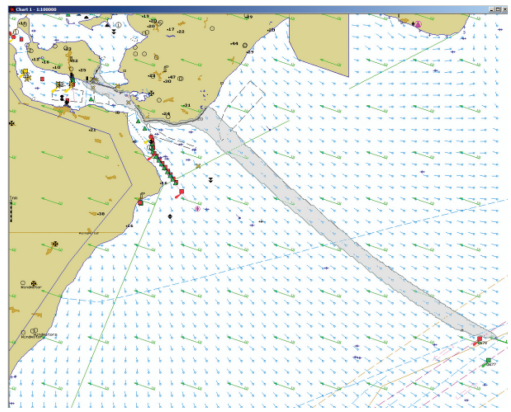


Figure 7. Simulated trajectory of m/t "Baltic Carrier" accident (spill reach Isle of Mon and Bogo).

Calculation of the resource application cost is based on duration of its application, being performed by the program automatically. The track of time is carried out for 5 statuses of the resource: "Ordered", "Available", "Assigned", "Mechanical Out of Service" and "Personal Out of Service". The user has to specify the cost of resource use for different statuses.

Example results of cleanup cost in simulation model of is presented in (Gucma, Lazuga & Perkovic 2013) where validation of m/t "Baltic Carrier" accident have been carried "Baltic Carrier" spill.

6 CRITERIA FOR EVALUATION OF LONG TERM ENVIRONMENTAL DAMAGE DUE TO OIL SPILLS

Quality of Life Index (*LQI*), was developed by the British magazine The Economist, aims to reflect in a more appropriate manner and level of life satisfaction in different countries. The LQI are combined the results of subjective life satisfaction of objective factors of quality of life. Parameters and quality of life measures, which are used to identify parameters include: financial situation, health, political stability and security, family life, community life, climate and geography, job security, political freedom and gender equality. The original definition of *LQI* is as follows (Nathwani et al.):

$$LQI = G^{w} E^{1-w} \tag{3}$$

where: *G*—gross national product per capita, *E*—the average life expectancy, *w*—the ratio of time spent at work by the time outside of work amounting to developed countries from 0.1 to 0.2 (usually a 1/8).

On the basis of the ratio of quality of life it can be possible to carry out risk analyzes and impact of investments on the environment by examining its change after the investment. In further step it could be defined as the optimal cost of protecting a human life *ICAF* (Implied Cost of Averting a Fatality) as:

$$ICAF = |dG|_{\max} dE = ((1-w)/w)GE/4 \quad (4)$$

The estimated value of *ICAF* (2004) for Poland is around 1.8 million PLN for assumptions $G = 18{,}600$ PLN, $a = 0.15$, $E = 70$.

The *NPWI* (Nature Preservation Willingness Index) is similar to *LQI* used to assess the environmental damages. It was introduced originally by (Friis-Hansen 2004) and allows you to calculate how much we are willing to pay for environmental protection. This *NPWI* ratio is calculated as:

$$NPWI = G_q \quad (5)$$

where:
G—gross national product per capita, $q = t/E$—the quality of the environment taking into account the pollution (i.e. the ratio between the time *t* for the period in which the environment remains free of contamination and the average life expectancy *E*). Assuming, as in the case of *LQI* that investment or activity does not impair the quality of the environment it means that you should ensure constancy index from the relationship:

$$dNPWI/NPWI = (G + \Delta G)(q - \Delta q) \geq 0 \quad (6)$$

where: ΔG—change of the gross national product, mostly due to an increase in investment, Δq—change indicator of environmental quality.

Rearranging above equation for the assumed size of the group that uses the values of environmental can find a socially reasonable size amount that society is willing to pay for environmental protection against pollution (μ_p):

$$\mu_p = G\Delta t \left[\left(1 - \frac{\Delta t}{t} \right)^{-1} - 1 \right] N \quad (7)$$

where: *t*—time in which the environment is not polluted, Δt—the average duration of pollution, *N*—the number of person affected by the pollution.

7 OPTIMIZATION OF CLEANUP COSTS (MINIMIZING COST OF RESCUE ACTION)

Created model of optimal allocation refers to the strategic level of response action and is designed to fit the deployment of such a rescue ships in sea rescue bases, in which the time of arrival of ships at the spill site, the cost of the shares and the environmental impact as a result of a failed rescue operation will be as small as possible (Lazuga, Gucma 2014). It is so deploy ships to minimize the sum of the following costs:

- total cost of reaching the spill site,
- the total cost of collecting the spillage by involved vessels,
- cost of contamination on the environment as a result of a failed action,
- the cost of establishing a new port (if needed),
- the cost of buying new ships and their equipment (if none of the proposed arrangements vessels does not provide complete removal of the spill),
- cost of maintaining the ships in the harbour,
- maximize profits from the use of ships for other purposes such as tugs (multi-criteria optimization).

To find minimal cost of response action the following objective function is proposed:

$$Min \quad \sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{k=1}^{K} t_{ijk}c_{ik}x_{ij}y_{ik} + \sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{k=1}^{K} t_{ik}c_{ik}x_{ij}y_{ij} \quad (8)$$

where: *I*—ships, *J*—ports, *K*—pollutions, t_{ijk}—time of reaching *k*-th oil spill form *j*-th port by *i*-th ship, c_{ik}—cost of reaching the spill from given port by ship and cost of given spill cleaning up, *x*—logical variable (0,1) depending of ship allocation in given port, *y*—logical variable (0,1) depending of ship scheduling in given response action.

The created model using evolutionary programming methodology for optimization (minimization) the cost of response action (Lazuga & Gucma 2014). The interface of this model is presetned in Figure 8. It enebles to observe during simulation the advance in cost minimisation throughout generations (left upper panel) of given layout of ports and oil spills (right window).

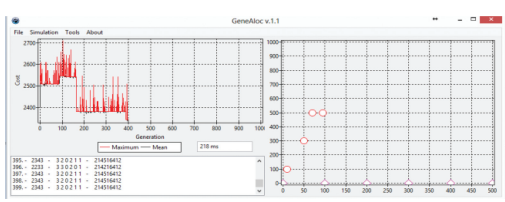


Figure 8. Computer iterface of optimal cost model based on evolutionary programming (Lazuga, Gucma 2014).

8 CONCLUSIONS

Despite much research, and attempt to create a formula for estimation of costs, it should be considered that the costs of removing spills primarily depend on the actual filling factors such as: the number and type of substance. Other factors, of which correlates the amount of costs are: geographical location, local law, or applied method of purifying contaminated sites. The paper also explores a new indicator of the environmental value that it has for society. This ratio refers to the ratio of quality of life. Using indicator of environmental quality, we can quantitatively determine the impact of the investment on the environment and evaluate the risks related to maritime transport of petroleum substances. With after—higher estimates attempted to examine how much we are willing to pay to protect the environment and compares this value with the costs of removal of the spill. For further considerations should be left how the investment made to for more secure against possible spills of petroleum substances will reduce the probability of such a spill. Knowing the value of this probability and presented in the article, the cost of spills can be carried out a full risk analysis of marine traffic engineering systems from the point of view of its impact on the environment. Use of the quality factor of the environment and the potential costs of spills may be helpful in risk analyzes of marine traffic engineering systems.

REFERENCES

Davidson, W.F. & Lee, K. & Cogswell, A. 2008. Oil Spill Response: A Global Perspective. Springer.

Etkin, D.S. 2000. Worldwide analysis of oil spill cleanup cost factors. Proceedings, XXIII Arctic and Marine Oilspill Program (AMOP) Technical Seminar. Environment Canada, Ottawa.

Fingas, M. edt., 2010: Oil spill science and technology. Elsevier.

Friis-Hansen P., 2004. FSA and Risk Analysis. Maritime Safety Research in the Baltic Sea, Malmø.

Gucma, L. & Goryczko, E. 2006. Szacowanie kosztów rozlewów olejowych (Estimation of oil spill cost), NavSup Interenational Conference. Gdynia.

Gucma, L. & Łazuga, K. & Perkovic M., 2013. Validation of an Oil Spill Simulation Model Through the Use of the m/t "Baltic Carrier" Case. European Journal of Navigation. Vol. 11 No 3 December.

Gucma, L. & Przywarty, M. 2007. The Model of Oil Spills Due to Ships Collisions in Southern Baltic Area, Advances in Marine Navigation and safety of sea transportation, Edited by Adam Weintrit, The Nautical Institute, Gdynia.

Harper, J. et al. 1995. Costs associated with the cleanup of marine oil spills. International Oil Spill Conference Proceedings.

HELCOM, 2011. Report on shipping accidents in the Baltic Sea area during 2011. Helsinki Commission.

HELCOM, 2010 Maritime Activities in the Baltic Sea—An integrated thematic assessment on maritime activities and response to pollution at sea in the Baltic Sea Region. Balt. Sea Environ. Proc. No. 123.

Lazuga, K. & Gucma, L. 2014. Model of optimal allocation of response (in print) Proc. of IMSC Conference, Split.

Nathwani, J.S. et al, 1997. Affordable Safety by Choice: The Life Quality Method. Institute for Risk Research, University of Waterloo, Waterloo, Canada.

Ornitz, B.E. & Champ M.A., 2002. Oil Spills First Principles: Prevention and Best Response. Elsevier.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The impact of new technologies on the safety level of air traffic in Poland

K. Krzykowska & M. Siergiejczyk
Warsaw University of Technology, Warsaw, Poland

ABSTRACT: The purpose of this article is to present the impact of implementing new solutions to increase the level of safety in air traffic. The author presents charts and statistics, which are a clear prerequisite to consideration of the need to implement innovative systems in the fastest growing modes of transport—aviation. In addition, illustrated the high demand of Polish economy to new technologies and its "backwardness" compared to other EU countries. For the preparation of this article the authors use available standards and statistics from Civil Aviation Authority.

1 INTRODUCTION

Innovation is a key element in determining the increase in productivity of the company. Understanding the sources and patterns of innovative activity in the economy is the basis for the development of better policy development. As an innovative company in the field of product and process innovations can specify the company, which in the period of time has launched at least one innovation products or process (a new or significantly improved product or a new or significantly improved process). It is worth noting that the contribution of companies in the service sector and industrial companies, which in the years 2007–2009 have introduced innovative products and/or process, in the total number of these companies, was lower than in the years 2006–2008. Decline could happened due to financial crisis attributable to years 2008–2009. Its start is determined by the date of 15 September 2008, which, together with the date of the bankruptcy of Lehman Brothers, immediately resulted in a reduced availability of credits.

2 INNOVATION DEVELOPMENT IN COMPANIES IN POLAND

The least innovative department in the years 2006–2008 was land transport and transport via pipelines, while in the years 2007–2009—air transport. In case of innovation there are particularly important financial outlays that may be incurred for this activity. These include (Proinno-Europe, 2012):

- research—development related to the development of new products and processes;
- acquisition of knowledge from external sources (patents, inventions, designs, patterns);
- purchase of appropriate software;
- purchase and installation of machinery and equipment, purchase of vehicles, buildings;
- training of a personnel;
- marketing of a new product/process;
- other preparations for the introduction of innovations.

Summary of companies that have introduced innovative products and/or process in % of enterprises by size class are shown in Table 1.

The study shall be subject of any expenditure on innovation in products and processes—current and investment incurred in the report of year finished with successful work (ie. implementation of innovation), incomplete (continued) and interrupted or discontinued, regardless of the sources of their funding. Expenditures on innovation can also be considered because of the source of funding.

Table 1. Summary of companies that have introduced innovative products and/or process in % of enterprises by size class.

	Industrial companies		Companies in the service sector	
Number of employed	2006–2008	2007–2009	2006–2008	2007–2009
Total	21,4	18,1	16,1	14,0
10–49	14,5	10,9	13,1	11,6
50–249	33,3	30,1	25,3	20,0
10–249	19,2	15,8	15,2	13,0
More than 249	60,9	59,0	48,2	45,0

We can distinguish the following funding for innovative activities:

– own;
– received from the state budget;
– obtained from abroad (non-refundable);
– from venture capital funds;
– bank loans.

The main source of funding for expenditures on innovation activities in 2009 were own funds of enterprises. They accounted 68.4% in industrial enterprises and 84.2% in the service sector (of all expenditures). In Figure 1 below expenditures for innovative activities to one company conducting innovative activity by province in Poland in 2009 are shown (INNO—Metrics, 2012).

Innovative activity has several basic objectives, including, among others (Proinno-Europe 2012):

– increasing the range of products or services;
– replacement of obsolete products or processes;
– entering new markets;
– increasing market share;
– improving the quality of products or services;
– improving production flexibility;
– increase the production capacity for products or services;
– improving the safety and health at work;
– reduction of personal labor costs per unit of product.

Poland is one of the moderate innovators with a below average performance. The strengths of the country include human resources, finance and support, investment companies and economic effects. Weaknesses are primarily quality of research systems, linkages & entrepreneurship, intellectual value and resource of innovators (INNO—Metrics, 2012).

In the Figure 2 Polish position to the chosen European Union countries in the case of trading companies based on innovation was presented (the graph shows the value in %, where 100% is the total income of the company achieved through innovative products/processes).

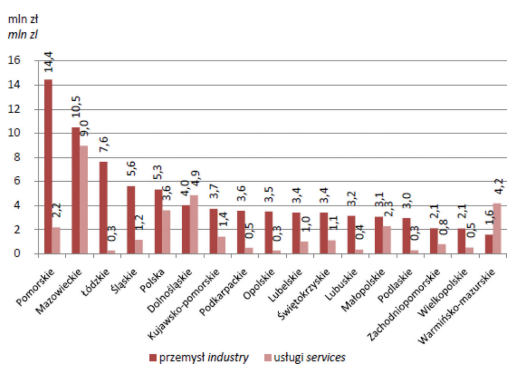


Figure 1. Expenditures for innovative activities to one company conducting innovative activity by province in Poland in 2009.

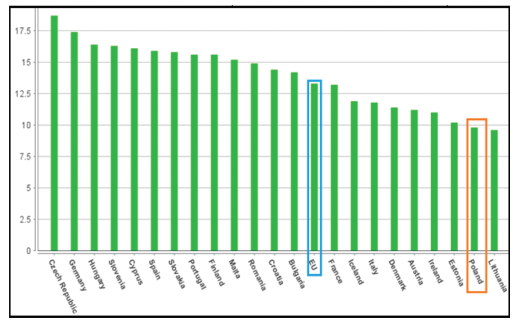


Figure 2. Polish position to the chosen European Union countries in the case of trading companies based on innovation.

3 INFLUENCE OF AIR TRANSPORT DEVELOPMENT ON AIR TRAFFIC SAFETY IN POLAND

Aviation for many years is a dynamically developing branch of the global transport system. Air transport market is dependent on general market trends of the global economy, and thus—market growth rate of air transport affects economy of the world. In Poland, for many years there was no civil aviation infrastructure development program until the adoption of the Development Programme of Network of Airports and Ground Aviation Equipment from 8th of May 2007. The program provided evidence of documents supporting the formulation of applications for funds for the development of the aviation infrastructure in the years 2007–2013 from both the Cohesion Fund and the European Regional Development Fund. Its basic aim, among other things is the development of the network of airports and navigation systems in the country in the direction of economic development, development of airports service, mainly the connection from point to point. In case of the development of navigation systems and due to the limitations of conventional systems—the programme provides for the implementation of new technologies. The aim was to ensure the implementation of European air traffic management programs, including programs for implementing the Single European Sky (SES) and the European Air Traffic Management Strategy (Siergiejczyk M. & Krzykowska K, 2013).

Implementation of new technologies in surveillance systems is considered with a view to maintaining a certain level of safety in air traffic.

Therefore, it is necessary to look at the statistics on number of air events in recent years in Poland. In Figure 3 the number of incidents in civil aviation air in Poland in the years 2006–2011 is shown (European Commision Eurostat, 2014).

Analyzing Figure 3 it should be noted a disturbing steady increase in the number of events in air traffic in commercial aviation in Poland. The number of events in 2010 is more than three times greater than the number of events in 2006. This is undoubtedly related with a constant increase of air traffic in the country. In 2010, a 240,691 of aircraft operations and were done and 20,466,876 passengers were served. The big problem is the increasing number of incursions in Polish airspace controlled. Among them are those that were the result of loss of separation. Statistics are shown in Figure 4.

There is no detailed information on the distinction of aircraft that violated controlled airspace in the years 2009–2010. In Contrast, the Civil Aviation Authority reported that in 2008, out of 47 such events—25 were related to military aircrafts, 11—general aviation, and 4 to commercial aviation. Others are unidentified. The problem of incursions

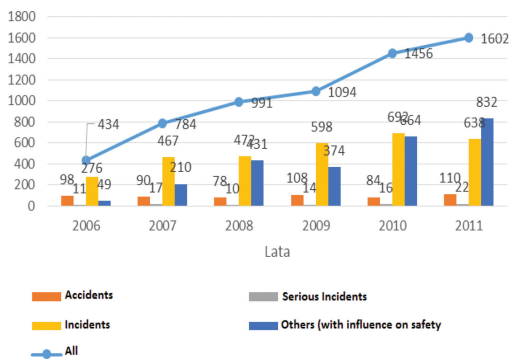


Figure 3. Number of incidents in civil aviation air in Poland in the years 2006–2011.

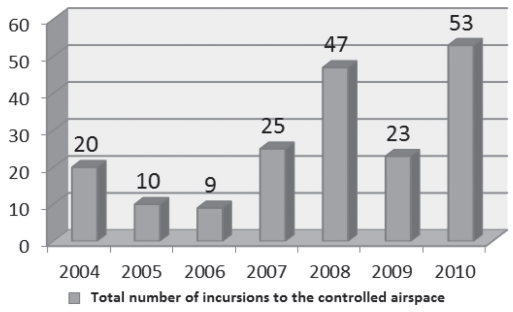


Figure 4. Number of incursions to the controlled airspace in 2004–2010 in Poland.

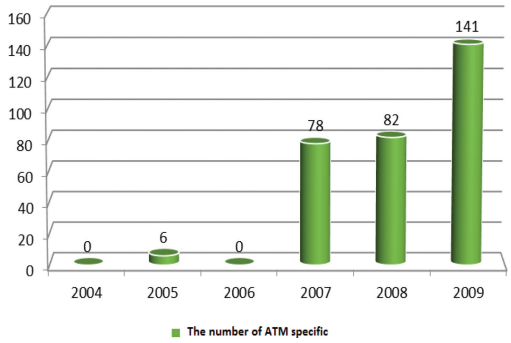


Figure 5. Number of ATM specific in 2004–2009 in Poland.

of controlled airspace could be completely eliminated by the implementation of modern surveillance systems. The basis of their operation is automatic and remote signaling an air traffic controller about the presence of an unidentified object in space.

A significant matter in the analysis of the level of safety in air traffic in Poland has a number of entries so called ATM specific. They mean a crash report of radio—navigation systems. The figure below presents a summary of specific ATM in the years 2004–2009.

In the category of ATM specific recorded events are related to the failure of ground-based radio navigation systems. The increase in the number of these events result from the introduction to the air traffic services new regulations, which are aimed at openness. It also involves the improvement of information flow of events. By 2006, these events have been reported occasionally. Worrying can be fact of the lack of information on such events disturbing comprehensive research results, particularly concerning the failure of CNS services. No precise information does not allow to follow the recommendations of ESARR 2 entitled: Submission of reports and dealing with irregularities in the traffic. Point. A—3.2.2. specifies that "should be developed recommendations for safety improvement actions, or corrective, whose implementation should be monitored. They can take a variety of forms, including the development and implementation of safety requirements, the introduction of standards, development or improving procedures, alteration of system architecture, or correcting ATM training system." (ESARR 2, 2000).

Examples of ATM may be specific events, such as (Civil Aviation Authority, 2014):

– serious incident on the Boeing 737–400, which occurred on 27 April 2006 in FIR Italy; during the flight when descent to FL 260, there was a TCAS message "Traffic Avoidance"; crew made

ATIR; this serious incident was examined by Commission;

serious incident on the Boeing 737-500, which occurred on 28 April 2006 in CTR EDDF; crew during climb after take off in Frankfurt at FL190 received a TCAS RA message "Down"; crew made a request to change the flight level; Minimum vertical separation between two aircraft was 1,000 ft; serious incident was investigated by Commission;

– serious incident on the aircraft Embraer 170, which occurred on 3 May 2006 in TMA EDDF; crew during descent received permission to occupy FL 100; while capturing the mandated level signaling appeared TCAS RA "Climb"; crew made TCAS instructions; after the communication hangman "Clear of conflict" aircraft returned to FL 100; serious incident is under investigation by Commission.

In consequence of the occurrence of such accidents must be considered on the validity of the implementation of additional surveillance systems which would not only detect situations of conflict, but also prevent from occurring such.

4 THE ROLE OF THE SAFETY LEVEL IN AIR TRAFFIC

In 1990 the world airlines consists of more than 15 000 aircraft. They were able to fly over 15 mln km to almost 10 000 airports. Sector of air transport directly employs over 3.3 million people, with more than 1.4 million in the USA. About 12 billion people and 23 mln loads are transferred over the year (Janic M., 2000). Figure 6 shows the number of km of flown routes in years 2011–2012 (Central Statistical Office of Poland, 2014).

Accidents are closely related to the scale of aviation operations. There are many different international institutions, organizations and agencies involved in forecasting future trends, including the International Civil Aviation Organisation (ICAO) and International Air Transport Association (IATA). Manufacturers of air space, such as Airbus,

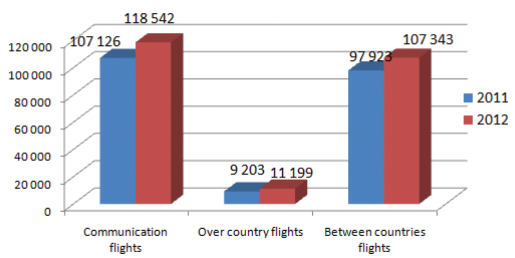


Figure 6. Number of of km of flown routes in years 2011–2012 in Poland.

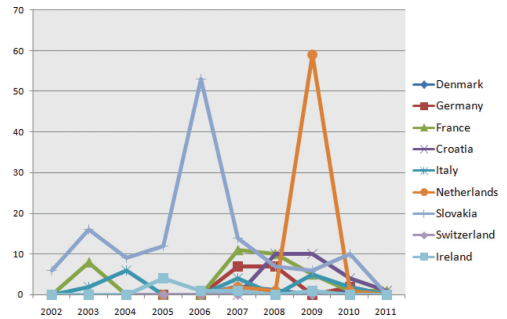


Figure 7. The position of Poland between other chosen European countries with the number of injury accidents.

Boeing and Rolls Royce do the forecast, too. Figure 7 shows the position of Poland between other chosen European countries with the number of injury accidents (Central Statistical Office of Poland, 2010).

It is common that when there is a relatively fast growth of air transport it is also often followed by a series of accidents. The occurrence of such events has stimulated an introduction of technical and operational measures. As a result, overall safety is being improved over time. Some are arguing that the scope for further improvements in safety are becoming exhausted implying that if the accident rate remains the same, while air travel increases, the number of accidents will inevitably rise.

5 CONCLUSIONS

The main problem of air traffic management in the world is to increase airport and airspace capacity and to maintain the required level of safety. Measures aimed at improving the quality of services are based primarily on forecasts of the number of flight operations. Analyzing the statistics it can be concluded that the FIR Warsaw maintains an increase in air traffic volume at the maximum European level. In this phenomenon, however, occurs both benefits and risks. Assuming an average growth of air traffic in Europe—without further delay—the capacity of the airspace required to support this movement should increase by more than 25%. In view of the presented forecasts and actual traffic situations in Poland, the Development Programme of Network of Airports and Ground Aviation Equipment from 8th of May 2007 recommends the rapid changes in the field of optimization and airspace management.

REFERENCES

Air Traffic Bulletin, U.S. Department of Transportation Federal Aviation Administration, Washington, (2005).
Country profiles Poland, www.proinno-europe.eu, (2012).

Central Statistical Office of Poland, Działalność innowacyjna przedsiębiorstw w latach 2006–2009, Warsaw (2010).
Civil Aviation Authority, Informacja o stanie bezpieczeństwa lotów i skoków spadochronowych w lotnictwie cywilnym RP w 2006 roku, Warsaw (2014).
COMMISSION REGULATION (EU) No 691/2010 of 29 July 2010 laying down a performance scheme for air navigation services and network functions and amending Regulation (EC) No 2096/2005 laying down common requirements for the provision of air navigation services.
ESARR 2 Reporting and Assessment of Safety Occurrences in ATM, EUROCONTROL, Warsaw (2000).
EUROCONTROL Medium—Term Forecast: IFR Flight Movements 2011–2017, European Organisation for The Safety of Air Navigation, Brussels, (2011).
European Commision Eurostat, www.epp.eurostat.ec.europa.eu/ (2014).
INNO—Metrics, www.proinno-europe.eu/metrics, (2012).
Janic M., An assessment of risk and safety in civil aviation, Journal of Air Transport Management 6 (2000) 43–50.
Program Rozwoju Sieci Lotnisk i Lotniczych Urządzeń Naziemnych, Ministerstwo Transportu, Warszawa, (2007).
Rozporządzenie Rady (WE) NR 219/2007 z dnia 27 lutego 2007 r. w sprawie utworzenia wspólnego przedsięwzięcia w celu opracowania europejskiego systemu zarządzania ruchem lotniczym nowej generacji (SESAR).
Siergiejczyk M., Krzykowska K., The analysis of implementation needs for automatic dependent surveillance in air traffic in Poland, (w:) A. Weintrit, TransNav—The International Journal on Marine Navigation and Safety of SeaTransportation, Wydawca: CRCPress/Balkema Taylor & Francis Group, London UK (2013), s. 241–245, ISBN: 978-1-138-00107-7.
Siergiejczyk M., Krzykowska K., Wpływ europejskiego programu CASCADE na jakość dozorowania w ruchu lotniczym, (w:) K. Zboiński, Prace Naukowe Politechniki Warszawskiej. Transport. Z. 100. Metody badawcze i badania systemów transportowych oraz ich elementów, Wydawca: Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, (2013).

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Black swan accidents: Predicting and preventing the unpredictable

D.J. Winfield
Deep River, Ontario, Canada

ABSTRACT: Three recent high consequence black swan accidents are used to illustrate the similar root cause safety barrier failures leading to these diverse events. A sampling of some of the major industrial accidents over many decades then demonstrates societal reactive responses of regulation, legislation and subsequent technical advances in process safety management. Despite significant historical advances in these responses, high consequence accidents, seemingly unpredictable and unpreventable, continue across many diverse industrial activities. Conclusions suggest areas where major accident prevention may be improved with more pro-activeness.

1 INTRODUCTION

1.1 *Black swan events*

Black swan events have been defined (Taleb 2007) as having three characteristics:

i. Following the event, explanations and analysis are presented, indicating such events are quite predictable and expected.
ii. The event has a high consequence(s).
iii. Prior to occurrence the event was not predictable or thought to be physically plausible, or assumed to be of very low frequency.

Black swan events can be experienced in a large variety of diverse activities such as finance, scientific discoveries, technological changes and politics. This paper is limited to considering major industrial accidents.

1.2 *Objectives*

The paper considers a small sample of black swan events that caused catastrophic industry related accidents with high consequences for workers and/or public for fatalities and injury, property damage and/or environmental damage. A sample of three recent accidents, 2011–2013, is used, that may all be classified as black swan type, where, to date, comprehensive reports and complete analysis are not yet available. The discussion illustrates that, despite knowledge advances in the industrialized world in all aspects of safety management, severe accidents continue to occur regularly. Failures of particular safety barriers leading to these three diverse events are highlighted.

A short list of seven major historical industrial accidents, spanning many decades, is then used to illustrate a sampling of the ensuing major regulatory and technical responses, both nationally and internationally. Lessons from these accidents are discussed, invariably showing the predominately reactive nature of societal response, rather than proactive anticipation and mitigation.

2 RECENT BLACK SWAN EVENTS

2.1 *Lac-Mégantic 2013*

The July 2013 railway disaster in Lac-Mégantic, Quebec, resulted in 47 fatalities from BLEVE explosions and fires caused by an unattended 74-railcar freight train derailment of multiple railcars containing a total of 8 M liters of petroleum crude oil. The five-locomotive headed train of the Montreal, Maine and Atlantic (MM&A) railway had been left unattended with inadequate braking and rolled uncontrolled down into the town center where it then derailed at high speed, one hour after midnight. Earlier that night a local fire department had been called by a member of the public to a fire in the one locomotive that had been left running with its unattended cab unlocked. The downtown core of businesses and homes was destroyed leaving substantial soil and water pollution requiring a currently-estimated $400M in clean up and unspecified legal costs.

No formal accident investigation report is yet completed, but many relevant facts are known. A cursory risk assessment of the MM&A railway business, requiring few resources and few analytical skills, should have been able to identify the poorly run operational and maintenance state of the company, with a susceptibility to operational incidents, (e.g. a single engineer was required to perform brakeman duties and a very large and hazardous cargo was allowed to be unattended overnight on a

main rail line on an uphill grade above a residential area with one locomotive engine left running).

Evidence of poor locomotive maintenance, inadequate operational staffing and poor track maintenance was subsequently reported. Neither the company nor the national transport regulator had produced even a rudimentary risk assessment for such hazardous material transport operations. No sophisticated quantitative risk analysis would have been needed to identify these basic shortcomings. The Canadian transport regulator had given specific exceptional permission for one-person train operation in 2012, enabling MM&A operational costs to be reduced. With the town left to pay $8M for emergency work in the immediate aftermath, short-term clean up activities were then funded by government financing of $155M. After the accident the railway filed for bankruptcy and was sold for $12M. Lawsuits and longer term clean up costs exceed assets and available insurance by well over an order of magnitude. Lack of a competent regulatory regime and a company risk management system appears, in a relatively short period of time of a year, to have allowed little to no scrutiny of significantly increased numbers of rail shipments of a highly-volatile and potentially explosive material.

For a safety analyst to predict that the Lac-Mégantic derailment would result in the BLEVE that was responsible for most fatalities, injuries and damage at that specific location, though seems unlikely. No analyst, however experienced, would likely have foreseen the extreme volatility and explosive potential of the oil shipment. The highly volatile and explosive nature of the cargo was not publically divulged, after belated testing, until as long as six months after the disaster. For an analyst therefore to probe down to a level discerning that the shipped cargo content had been falsely, and possibly deliberately, labeled as a moderate hazard Class 3 Packing Group III, seems unlikely. The cargo had though, when being shipped en route to the rail-loading facility, been classified as a higher risk PG II product with contradictory MSDS information; PG I and II (respectively very hazardous and hazardous). Additionally, transport risk is not location unique, but will vary significantly along transport corridors. A risk assessment therefore would need to consider the hazardous properties of the goods being transported, by what means and over which transportation corridors. This would have required detailed reviews of routes, towns, population density, train halt procedures, speed limits and most importantly, knowledge of the highly explosive nature of the petroleum crude oil and consideration of the suitability of the rail car design. The vulnerability of the DOT-111 type rail cars used, to failures in collisions and derailings, was though already well known to the rail industry in North America. The apparent absence of any measure of safety culture of the MM&A would additionally seem to have precluded any in-house risk identification and thus, more importantly, precluded any subsequent risk mitigation measures.

The Lac-Mégantic tragedy is the most recent example that could be suitably described with a root cause of conscious incompetence, fitting into the description (Ale 2013) that some businesses view safety costs as uneconomical, so that costs of 'un-safety' are borne by victims, their family and society (taxpayers). Accident prediction and prevention for such a serious event should have been straightforward, particularly in Canada, in view of the 1979 Mississauga, Ontario train derailment accident involving a large mixed cargo of explosive and toxic chemicals. An evacuation of about 220,000 people was required, at that time the largest peacetime evacuation in North American history. Emergency teams acquired the train's accurate manifest from the dispatch center in an adequate time, with a description of the cargo. Emergency procedures with the aid of materials experts from the shipping company then enabled a hugely successful evacuation with no fatalities or injuries.

The most important safety lesson confirmed from the Mississauga accident was the presence of a three-person train crew, including a brakeman who was credited with taking immediate emergency actions, significantly reducing potential accident consequences. Subsequent recommendations for railcar spacing for fire protection were not universally applied. What appear to be root causes of the Lac-Mégantic (self-regulation, poor proactive equipment and track maintenance and a poor safety management system) were accurately predicted precursors (Benedict 2007) anticipating, in general terms, the impending likelihood of such a major rail accident in Canada.

2.2 *West, Texas 2013*

The West, Fertilizer Plant, April 2013 explosion of 270 tons of ammonium nitrate resulted in 15 fatalities, 200 injured, 150 destroyed buildings and the obliteration of the plant. The facility did not register its ammonium nitrate, which would have required a review. A 2011 emergency planning report filing with the Environmental Protection Agency (EPA) stated there was no fire or explosion risk at the facility. The worst possible scenario was said to be a 10-minute release of ammonia gas that would kill or injure no one. Lack of regulatory control and lack of responsibility from the facility appear to be the main organizational root cause failures. As a black swan event, potential consequences though should in this case easily have been predict-

able from a chemical hazard review, knowing the amount of explosives and storage conditions and with the benefit of historical knowledge from many ammonium nitrate explosions. The potential consequences were not at all unprecedented (the largest industrial disaster in US history was a Texas City ammonium nitrate explosion in 1947 resulting in almost 600 fatalities) but the link between possible prediction and implementation of preventive measures was weak to non-existent. It was reported that the last Occupational Safety and Health Administration (OSHA) inspection was 28 years ago and a 1985 state law allowed storage of hazardous materials without liability insurance. After the explosion President Obama issued an executive order requiring federal agencies to review safety rules at chemical facilities. The same root cause description (Ale 2013) used above for Lac-Mégantic seems also quite appropriate.

2.3 *Fukushima 2011*

The tragic March 11 2011 earthquake and tsunami and the ensuing disastrous consequences for the Fukushima power reactors of Tokyo Electric Power Company (TEPCO) are now well documented. Much of the detailed accident progressions and the exact status of the three reactor cores are though still unknown, due to accessibility problems. A 2008 TEPCO in-house study had identified an immediate need to improve facility seawater flooding from possible tsunami-waves up to 10 m, but this was not acted upon. In retrospect it is hard to escape the conclusion that a combination of decisions by TEPCO and the nuclear regulator ultimately resulted in a very realistic tsunami risk being ignored, in the false belief that a severe tsunami accident was impossible. Business production was made a higher priority than safety. By contrast the small town of Fudai on Japan's north east coast had built a protective tsunami wall that was both high and robust enough to withstand the tsunami. This project was promoted and pushed through by the efforts of a non-technical member of the public, which is remarkable. Had TEPCO and the Nuclear and Industrial Safety Agency (NISA) regulator, followed international best practices and standards the Fukushima plant should have withstood the tsunami, if its design had been upgraded in accordance with state-of-the-art tsunami protection.

A number of underlying causes for TEPCO and NISA's failure to follow international best practices and standards can be identified. NISA lacked independence from the government agencies responsible for promoting nuclear power and also from the industry. Regulatory capture has been used describe this issue, where regulators charged with promoting the public interest defer to the agenda of the industry they ostensibly regulate. In the Japanese nuclear industry there was a justifiable historical focus on seismic safety, but to the exclusion of other credible natural risks.

The Fukushima accident underscores the importance of continuing periodic reevaluations of plant safety for external threats, using best international practices. The full consequences of the severe accident core damage sustained by the reactor units would though have been very difficult to predict in advance. Following the accident, the Japanese government adopted a new regulatory regime to oversee nuclear safety.

3 MAJOR HISTORICAL BLACK SWAN EVENTS

Each major and unexpected historical industrial accident, at least in the industrialized world, has prompted subsequent examinations of the existing risk management systems, if any existed, both at the national level and sometimes internationally. Invariably, large accidents have resulted in some major safety and regulatory legislation being enacted nationally. The major responses from the most prominent and well-documented accidents, that could be claimed to be black swan events, are mentioned below. The literature on such accidents, since the industrial revolution began is vast, so only a few major accidents are noted here. A large fraction of events involved releases of some form of high hazard materials. Such events continue to provide impetus for authorities to improve and modify legislation and regulations to eliminate and mitigate their potential occurrence.

3.1 *Pressure vessel explosions 1900–1910*

An average of about 30 boiler explosions were occurring per month in the US in the early 1900's. One of the most significant (Grover 1905) caused 58 fatalities and 150 injured from a fire-tube boiler explosion and resulted in the first ASME Boiler Code Committee being formed in 1911, followed by the first edition of the Boiler and Pressure Vessel Code being published in 1914.

3.2 *First reactor core melt 1952*

The world's first reactor meltdown (NRX 1952) resulted, among many other subsequent recommendations, with the inception of the world's first formal internal nuclear safety review committee, now considered essential for reactors internationally, but still today not necessarily implemented in all reactor facilities.

3.3 *Windscale 1957*

Two years after the 10 October 1957 Windscale military reactor fire and core melt accident formal external regulation of the UK civilian nuclear power industry through the Nuclear Installations Act was enacted in the UK in 1959, under the auspices of the Nuclear Installations Inspectorate. A government press release at the time nevertheless stated that the fire had *"no bearing on the safety of nuclear power stations being built for electricity authorities"*. One substantial later implication of the accident was the establishment of the UK National Radiological Protection Board (NRPB) in 1971.

One particular aspect of the public accident report was that publication was not until 31 years later, in January 1988. A very brief government report summary was produced only 2–3 weeks after the accident blaming the accident on a combination of human error, poor management and faulty instruments. Key technical details and the root technical and organization cause of the accident were not apparent publically until the 1988 report. Some activity release information on Po^{210}, one of the more significant fission products released, also remained classified until the mid 1980s. There is strong evidence in the 1988 report that the organizational root cause of the reactor fire, the first in a nuclear facility, was the relaxation of safety due to nuclear weapon material production pressure, exerted upon the reactor operations staff by the British government.

A review of international accidents on military nuclear facilities, particularly the most recently disclosed details of a potential nuclear weapons disaster (Schlosser 2013), provides a contemporary very cautious reminder that civilian nuclear accidents by no means set an upper limit on manmade disaster consequences, with military secrecy and non-public disclosure being the major barriers against prevention.

3.4 *Flixborough 1974*

The Flixborough 1974 chemical disaster (28 fatalities and 38 serious injuries) resulted in significant tightening of UK regulations of hazardous industrial processes and led directly led to the introduction of the Health and Safety at Work Act 1974, and the formation of the Advisory Committee on Major Hazards (ACMH) under the auspices of the newly formed Health and Safety Executive (HSE) 1975. The history of UK HSE from 1800 to present is instructive reading in this regard providing a more detailed and longer-term perspective to regulatory responses to severe accidents. Flixborough was a watershed event at the time, from which afterwards the term process safety management then emerged.

3.5 *Seveso 1976*

After the Seveso accident (1976) the regulatory response in Europe led to the Seveso II Directive, following the need for consistency throughout Europe. This Directive was largely influenced by the work carried out in the UK by the ACMH. In turn this led in the UK to the formation of the Control of Industrial Major Accident Hazards (CIMAH) Regulations in 1984 subsequently leading to the Control of Major Accident Hazards involving Dangerous Substances (COMAH) Regulations in 1999 and subsequent amendments, which were the enforcing regulations in the UK following the Seveso disaster.

3.6 *Bhopal 1984*

Bhopal in 1984 from the chemical industry is recognized as the worst recorded industrial disaster and led to significant improvements in plant operations in the US, but victims of Bhopal were left with little compensation. In 1986 the US Congress passed the Emergency Planning and Community Right to Know Act. Also in the US the American Institute of Chemical Engineers Centre for Chemical Process Safety was formed in 1985 as a US industry response and also, after the 1989 Phillips accident in the US, Process Safety Management standards were introduced in 1992. In Canada the Major Industrial Accidents Council of Canada (MIACC) was established in 1987 following Bhopal. This was subsequently disbanded in 1999, then leaving no effective oversight for hazardous substances on the national level. In India, the Environment Protection Act (1986), the Air Act (1987), the Manufacture, Storage and Import of Hazardous Chemical Rules (1989) and the Public Liability Insurance Act (1991) were promulgated.

Bhopal and Flixborough perhaps represent the two seminal tragedies in the last 40 years that changed the international approach to process risk management and the intensification of efforts to ensure the safety of high hazard facilities. Process safety management subsequently finally gained widespread recognition as a standard practice. These incidents spurred broad recognition that handling highly hazardous chemicals could lead to incidents that may occur relatively infrequently, but, due to their catastrophic nature, often result in multiple injuries and fatalities.

3.7 *Chernobyl 1986*

Shortly after Chernobyl (1986) the term safety culture was first introduced (INSAG-1 1988) and its development and application was then adopted internationally in the nuclear industry. The errors

and violations of operating procedures, which contributed to the disaster, were evidence of a poor safety culture at Chernobyl and the former Soviet Union nuclear industry in general. After Chernobyl the World Association of Nuclear Operators (WANO) was formed in 1989, linking 130 operators of nuclear power stations in more than 30 countries.

3.8 *Observations from historical accidents*

Observations are presented in three categories covering the process safety management, organizational and regulatory perspectives.

3.8.1 *Process safety management perspective*

Process safety management (encompassing all types of analysis techniques and safety management system techniques) has made great advances over the last 50 years. With increasing globalization, industrial development becomes more complex and change is continuous. Vigilance in maintaining updated safety knowledge and corporate memory is thus constantly relevant for high-risk industrial systems. An integrated safety management system is needed to encompass risk identification, safety analysis and risk mitigation implementation. From a risk identification and safety analytical perspective there is no shortage, amongst the myriad of application-specific safety analysis techniques, the established of which are well developed and mature. Recognition is though needed that constant updating and new areas will continue to evolve. Safety assessment should be considered a continuous process, not a one-off exercise that does not need to be revisited. Different industries tend to utilize different techniques but there may be a tendency, particularly for large organizations, to become complacent in use of their traditional methods and be reluctant to utilize different and perhaps more appropriate assessment techniques for their own industrial environment.

The lesson should be that, regardless of the industry, a suite of diverse analytic techniques should always be considered. The nuclear industry for example has for instance put much effort and resources into Probabilistic Safety Assessment (PSA), with an emphasis on the core melt frequency metric. PSA is a particularly expensive, complex and usually a very lengthy technique requiring significant training and is quite difficult to review. PSA would not though have predicted the specific accident sequences and management system failures of any of the three major power reactor accidents; Three Mile Island, Chernobyl and Fukushima. PRA quantitative absolute global frequency predictions of low-probability catastrophic accidents are particularly suspect because of fundamental limitations of the modeling technique (Raju 2014 and Cochran 2011). Regardless of the nature of any type of analysis technique no single method would be able to predict the entire realm of possible failures. Care should therefore be taken that safety analysis resources, which are always limited, are not dominated by one method at the expensive of others.

Some accidents arise from engineering errors or omissions that are epistemologically unforeseeable. Epistemic accidents then occur because a technical assumption proves to be erroneous. The Davis Besse reactor pressure vessel head massive external corrosion event in 2002 is such an event that had not been predicted. No PSA or other type of study had identified and alerted to the possibility of such an event, that in retrospect looked like a simple failure mode to predict, in view of the corrosive nature of boron in solution from reactor coolant leaks. Discovery, very belatedly, was by physical inspection. This failure mode then overcame the long held leak-before-break theory postulated for reactor pressure vessels. A similarly long held leak-before-break mantra was claimed for pressure tube reactors until a large longitudinal rupture, due to an unanticipated failure mode, occurred in 1984 in a CANDU reactor pressure tube. Events such as these, firmly established in conventional wisdom, continue to challenge engineering knowledge and the false assumption that engineering facts are always objectively known. One of the main reasons for failures of foresight lies in a misplaced, but institutionally deep-rooted confidence that such failures will not happen. Misguided believe in the infallibility of model results for example, having faith, for example in a core melt frequency metric, can leave a company ill-prepared for scenarios such as Fukushima and Chernobyl. Unpredictable hazards are such that we should always be aware of the fundamental limitations and associated uncertainties of specific modeling techniques.

Utilizing the whole range of numerous methodologies that comprise the comprehensive framework of the OSHA Process Safety Management elements should, if applied, provide excellent coverage. External peer periodic safety reviews also can often bring in fresh perspectives. Risk identification and safety analysis are predominantly objective and technical and, other than the hopefully very small residual hidden black swan design and operational flaws, most large organizations are capable of good performance. Scenarios envisioned by analysts where recommendations are implemented may then be prevented but subsequent failures still periodically seem to arise from unforeseen black swan scenarios. More problematic is then moving from analysis predictions

into risk mitigation recommendations and from there to achieving implementation. The later process includes a variety of organizational review and decision making activities that are people orientated. These are much more subjective than technical analysis.

3.8.2 *Organizational perspective*

Detailed reviews of the accidents mentioned in this paper show that organizational errors dominate the root causes. A large amount of evidence from comprehensive studies of accidents and disasters across a wide variety of industries (Reason 1998) also promotes this conclusion. Financial factors in high hazard facilities such as cost cutting, maintenance activity reductions, production pressures and staff downsizing typically result in accident-causing situations, not unexpectedly, with counterproductive effects then increasing costs and decreasing revenues. Organizational and managerial factors in the form of high level policy and decisions often set the stage for human error at the operational level and for equipment precursor failures that finally can result in a disaster. Invariably large modern organizations have in place the important pro-active features of PSM methods such as operational safety support, maintenance, inspection and audit, as part of their integrated safety management program. Organizational decisions though can negate the impact of any or all of the PSM methods if the findings are ignored.

Organizational structures can fundamentally undermine the capability of the organization to deal correctly with process safety issues if the organizational structure disempowers safety support staff experts. Failings also often result from complacency and lack of memory at the corporate level. Senior leadership may discourage bad news and may have little or no understanding of the importance of process safety. This can stem from a simple lack of technical awareness of safety culture or moral responsibility, that maybe clouded by financial incentives not structured to draw management attention to process safety hazards. Metrics such as lost time accidents may be misinterpreted as reflecting process safety. Rasmussen 2000 notes that most major accidents including Bhopal, Flixborough and Chernobyl all demonstrated that they were not caused by simple independent failures or human errors but rather by '*a systematic migration of organizational behavior under the influences* of *pressure toward cost effectiveness in an aggressive competitive environment'* and, as a result facilities were operated outside their design basis. Lac-Mégantic would also appear to demonstrate these same organizational flaws.

As sections 2.1 and 2.2 demonstrate, not only large well-financed companies operate high hazard operations. Small companies are unlikely to have full time safety staff in the operation and so external consultants would be required, the hiring of which may not be a priority for company directors and managers. For small companies in particular, safety standards and internal implementation and/or enforcement are thus more likely to be weak. Reviews, inspections and enforcement, only available through external inspection by appropriate regulators, then may or may not be effective. Regardless of the technology hazard differences, resources will always practically limit the application of any risk assessment program. Such limitations would not usually be unnecessarily restrictive for large industries but would more likely influence small companies. Small size may generally be representative of small technical complexity, but the examples of sections 2.1 and 2.2 show that severe accident consequences do not necessarily go hand in hand with lack of complexity. Duffey, 2008 notes that *'All responsible industries strive to provide safe conditions'* and that *'Management generally wants to do what is right'* but does not discuss the ensuing problems when these conditions are not met. In such cases stricter and more effective regulatory standards for facility inspections, the possibility of public access to safety information and public participation in decision-making, such as contained in the recent Seveso III Directive for Europe would seem to be very appropriate.

3.8.3 *Regulatory perspective*

As noted in section 3, in the industrialized world if major disasters are catastrophic enough for the public, the society response is usually the formation of various types of regulatory bodies, mainly government operated. Despite progress over many decades with regulation, associated legislation the occurrence of major accidents in strongly-regulated industries continues. The impact of regulation in helping to prevent and mitigating major accidents cannot very easily be quantified but it is clear from the three large nuclear accidents mentioned in this paper that the regulatory barriers failed (US, Russia, Japan). The very existence of some form of external regulatory government oversight, regardless of effectiveness, may by itself be beneficial but, as with safety improvements, trying to quantify regulatory effectiveness would likely be illusory.

A regulatory system is of course predicated on the existence of an adequately-funded and competent regulator who places the safety goal of public protection before the economic concerns of the regulated facilities. Much is made, particularly in the nuclear industry of an independent regulator.

Fukushima focused recent attention in Japan on this issue. Full regulatory independence itself is though not so easy to assure due to the many undue influences that can compromise the function of a regulatory body; changing political circumstances; funding cuts (which may or may be politically motivated); uncertainties and competing interests and influences from other government departments or other organizations. The goal should be to ensure that a nominally independent safety regulator stays independent and is not captured by the commercial industry that it regulates, but remains publicly accountable. Highly competent personnel for instance may be restricted from regulatory organization employment because they have formally worked for the regulated industry. On the other hand revolving-door staff employment between the regulator and industry has also disadvantages. More useful perhaps than just independence would be to focus on measures to assure regulatory competency and integrity. Independence by itself guarantees neither of these much more essential requirements.

One high level recommendation from the Three Mile Island accident (1979) which was, perhaps wisely, not implemented, was to establish a new independent safety group to oversee both industry and the regulator, thus potentially creating yet another layer of checks. In reality, for all types of regulation, complete independence can never be absolutely independent in all respects from the rest of government. Sources of regulatory funding, independent of state funding, are feasible but other funding sources would then be unlikely to have the public safety interest paramount and the regulatory powers would still in any case have to be enacted by government.

4 CONCLUSIONS

The historical pattern of response following major accidents has been invariably reactive to introduce institutionalized regulatory control. Within the same industries continued accidents over long periods of time has resulted in modifying and expanding existing external regulatory controls. Three recent major accident examples have indicated weak external or weak self-regulation failed to provide adequate accident barriers. While there is no evidence to claim the very existence of an external regulator reduces major accident frequency the converse, self-regulation, does indicate the likelihood of increased accidents.

The achievement of regulatory independence is not simple, because of conflicting pressures from government and industry as well as financial considerations. It is suggested that effort placed into achieving high regulatory competence, effectiveness and integrity should be as important, if not more important, than independence. Unless the public is served by effective regulatory agencies acting in the public interest there is little prospect that future severe industrial accidents will be avoided.

Safety assessment techniques, organizational safety management systems and operating and maintenance practices are all essential tools in a suite of risk management activities, but it is important to be aware of the limitations, imperfections and assumptions inherent in all these various tools and not necessarily allow over confidence from one aspect. Conventional established technical wisdom might well be challengeable. Safety assessments in particular should always be viewed as work in progress, even for old facilities, as history shows new technical insights and improved safety practices invariably arise. Design safety review can be a continuous and protracted process, but it is not a one-off exercise that does not need to be revisited. Companies perhaps rarely question the need to meet annual insurance coverage premiums. It is suggested the need for ongoing periodic safety reviews should be viewed the same way.

The long history of severe accidents indicates that black swan industrial accidents of significant impact are unlikely to be significantly reduced in the absence of a very foresighted proactive approach to process safety management. Challenges in creating and maintaining organizational memory and corporate culture at the highest management level are important reasons why incidents continue to occur. Management decisions based on ignorance of technical realities, incorrect assumptions and unrealistic production pressure can lead to ineffective risk management practices or a false sense of security. No matter how sophisticated and analytical models become it is likely they will never encompass the entire realm of what is possible.

REFERENCES

Ale, B.J.M. 2013. Better science does not make decisions easier. In: Proceedings of the European safety and reliability conference, ESREL 2013, Amsterdam, The Netherlands, 29 September–2 October 2013. Safety Reliability and Risk Analysis: Beyond the Horizon; 3–9.

Benedict, E.W. 2007. Canada's Railway Safety Regulatory Regime: Past Present and Future, Transportation Law Journal 34(2): 147–165.

Cochran, T.B. & McKinzie, M.G. Global Implications of the Fukushima Disaster for Nuclear Power. In: World Federation of Scientists International Seminar on Planetary Emergencies, August, 2011. http://docs.nrdc.org/nuclear/files/nuc_11102801a.pdf.

Duffey. R.B & Saull, J.W. 2008, Managing Risk: The Human Element, Wiley.
Grover Shoe Factory Disaster, Brockton, Massachusetts, March 20, 1905.
INSAG-l. 1986. International Nuclear Safety Advisory Group, Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident, Safety Series No.75-INSAG-l, IAEA, Vienna (1986).
NRX Reactor Accident, Chalk River, Ontario, December 12 1952.
Raju, S. 2014. Estimating the risks of nuclear accidents. http://arxiv.org/pdf/1405.6658v1.pdf.
Rasmussen, J. & Svedung, I. 2000. Proactive Risk Management in a Dynamic Society. Swedish Rescue Services Agency, Karlstad.
Reason, J. 1998. Managing the Risks of Organizational Accidents, Ashgate Publishing Ltd, Aldershot.
Schlosser, E. 2013. Command and Control, Penquin Random House.
Taleb, N.N. 2007. The Black Swan: The Impact of the Highly Improbable. Random House, New York.

Analytical methods in system safety and reliability

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Studies of the jet engine control quality based on its response to the disturbance inflicted on the object, designated from its response to the set point inflicted to the controller

K. Golak
Faculty of Mechanical Engineering, Bialystok University of Technology, Bialystok, Poland

P. Lindstedt
Air Force Institute of Technology, Warsaw, Poland

R. Grądzki
Faculty of Mechanical Engineering, Bialystok University of Technology, Bialystok, Poland

ABSTRACT: Aircraft engines and other technical systems are controlled on the basis of responses from the set-point to the controller, while the quality control process is influenced by the response from disturbances acting on the object. However, it turns out that the airplane engine, which is tested during ground tests by inflicting setpoint to the controller is used in flight where random noises acting on the engine. Therefore the emergency operation of the object, which has the decisive influence on its safe and effective use are not tested. The article proved that it is possible to assess the state of regulation of complex technical systems and assess their response to unpredictable disturbances (including variable environmental conditions) acting on the controlled object, based on tests conducted under standard conditions (without disturbance or disturbance with a low force).

1 INTRODUCTION

Comprehensive examination of the complex technical systems operating state should include simultaneous assessment of its state of regulation the technical condition (wear parameters, service life) and the state of the reliability. Operating practice shows that special attention is given to control problems, because it gives the knowledge about technical state of the system (because each adjustment made during maintenance indicates a change in the technical condition) and binds his change of its reliability state.

Only properly adjusted technical system could wear in the optimal way. Every change of the technical state (wear) requires immediate appropriate new regulation and proper update and hence the decision about the further method of use. [4]

Air turbine jet engines are tested during periodic maintenance inspections, and after repairs carried out during the standard ground tests. It proceeds according to a strictly defined tests program. This tests are based on set signal of the turbojet engine rotational speed (its value, the rate of change and duration of the changes) delivered by the engine control lever. Disturbances during this tests are small and haven't any impact on the working engine. Input function is delivered to controller. [3]

However, during its operational use (during the flight) disturbance from signals from both the weather conditions (wind, pressure variation) and resulting from the airplanes operation (tight turns, firing rockets, the acquisition of air stream from other aircraft in group fly) become high power, and thus the importance of the quality of the engine. Disturbances during the flight are the input signal for the object (engine). During the ground tests carried out on the engine disturbance signals have low power and therefore have little effect on engine performance. [1, 7, 9, 10]

So there is a situation that the turbojet engine adjusted correctly during ground tests may be inappropriately prepared to work during the flight (in a variable environment and the difficult to predict disturbances) which may have a significant impact on the quality of engine operation and thus the safety of the flight. Hence the need for new methods to assess control quality of air turbine jet engine based on tests ground in such a way as to provide a high quality of control during flight.

2 TURBINE JET ENGINE SIMULATION MODEL

For tests of the assessment of the control quality of the turbine jet engine the simplified model of rotational speed control was built. It operates from both the input value to the controller delivered by the engine control lever ("*w*") and input from disturbance "*z*" to the object (engine). It has been shown in Figure 1 [2, 9]

The model is considered in two parts: as the model (with the transfer function $G_W(s)$) from the set value "*w*" acting on the controller ($G_R(s)$) and as a model from the disturbance "*z*" acting on the object ($G_O(s)$) with the transfer function $G_Z(s)$. [2, 5, 6]

$$G_W(s) = \frac{G_R(s) \cdot G_O(s)}{1 + G_R(s) \cdot G_O(s)} \tag{1}$$

$$G_Z(s) = \frac{G_O(s)}{1 + G_R(s) \cdot G_O(s)} \tag{2}$$

The analysis of the transfer functions (1) and (2) show that the transfer function describing the operation of the engine from the disturbance $G_Z(s)$ may be obtained by multiplying the transfer function $G_W(s)$ by the inverse of the controller transfer function $G_R(s)$.

$$G_Z(s) = G_W(s) \cdot 1/G_R(s) \tag{3}$$

Thus, it is possible to control quality evaluation of the turbine jet engine in flight (operating from disturbance "*z*") using its tests ground (from the setpoint "*w*").

3 BASIS OF THE METHOD FOR ASSESSING OF THE QUALITY OF CONTROL OF THE TURBINE JET ENGINE

3.1 *Describe using the transfer function*

Transfer functions describing simplified model of the turbine jet engine rotational speed control system from Figure 1 in form of dependences (1) and (2) are presented underneath as formulas (4) from input signal "*w*" delivered by the engine control lever acting on the controller and (5) from input signal "*z*" as random disturbances acting on the object (engine).

$$G_W(s) = \frac{15.67s^2 + 46.86s + 6}{3.916s^3 + 18.47s^2 + 46.86s + 6} \tag{4}$$

$$G_Z(s) = \frac{1.305s^2}{3.916s^3 + 18.47s^2 + 46.86s + 6} \tag{5}$$

Impulse responses of the transfer functions (4) and (5) for the impulse input signal with limited amplitude $A = 100$ and duration $t = 0.01$ s are presented on the Figures 2 and 3.

Transfer functions $G_w(s)$, $G_z(s)$ and their response functions from the setpoint input "*w*" and disturbance input "*z*" are clearly different.

Transfer function of the controller is presented as formula (6).

$$G_R(s) = \frac{31.33s^2 + 93.72s + 12}{2.611s^2} \tag{6}$$

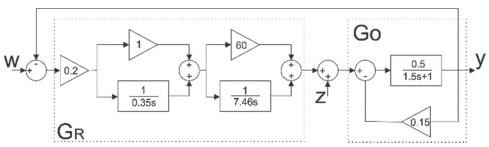


Figure 1. Simplified model of the turbine jet engine rotational speed control. [2, 5, 6, 8, 10].

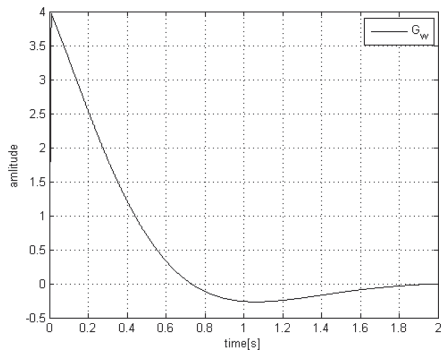


Figure 2. Impulse response of the transfer functions $G_w(s)$.

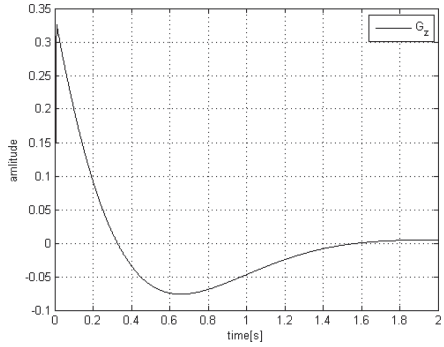


Figure 3. Impulse response of the transfer functions $G_z(s)$.



Figure 4. Impulse response of the transfer functions $G_W(s)$ and $G_Z(s)$.

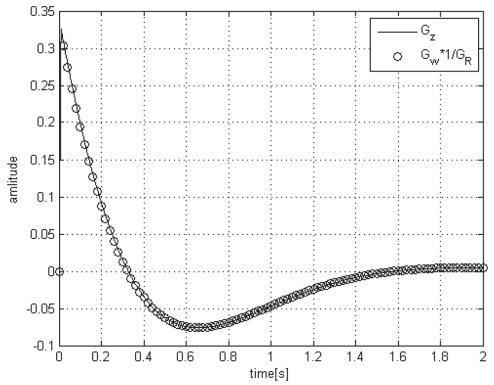


Figure 5. Impulse response of the transfer functions $G_Z(s)$ from disturbance "z" and the same transfer function obtained only from "w" as $G_W(s)$*1/$G_R(s)$.

As a result of multiplication of the transfer function $G_w(s)$ describing model from the set value "w" by the inverse of the controller transfer function $1/G_R(s)$ (being part of the transfer function $G_W(s)$) is possible to obtain the $G_Z(s)$ transfer function and thereby response from disturbance "z". Described above operation shows scheme in Figure 4. [3, 7]

As a result of multiplication of the transfer function $G_W(s)$ from the setpoint "w" describing engine during ground tests by the inverse of the controller transfer function $G_R(s)$ (from the same tests) it is possible to obtain transfer function $G_Z(s)$ from disturbance "z" describing engine during flight. This gives us a basis to assess the quality of regulation of the turbine jet engine in flight, on the basis of the standard of attempts to ground (from "w") without performing dangerous and therefore prohibited operation tests from the disturbance signal "z".

Results showing the accuracy of the operation from the Figure 3 in the form of obtained impulse responses shows Figure 4.

3.2 *Describe using the transfer function estimated from power spectral density of input and output signals*

Transfer functions $G_W(s)$ and $G_Z(s)$ describing simplified model of the turbine jet engine rotational speed control (Fig. 1) could be written as the quotient of the cross power spectral density (from input and output) and the power spectral density (of input). Transfer functions of the controller and object could be shown as formulas (7) and (8). [3]:

$$H_R(\omega) = \frac{S_{ue}}{S_{ee}} \tag{7}$$

$$H_O(\omega) = \frac{S_{y_w u}}{S_{uu}} \tag{8}$$

where "S" is the cross power spectral density.

From (7) and (8) based on (1) and (2) we can obtain:

$$H_W(\omega) = \frac{\frac{S_{ue}}{S_{ee}} \cdot \frac{S_{y_w u}}{S_{uu}}}{1 + \frac{S_{ue}}{S_{ee}} \cdot \frac{S_{y_w u}}{S_{uu}}} \tag{9}$$

$$H_Z(\omega) = \frac{\frac{S_{y_w u}}{S_{uu}}}{1 + \frac{S_{ue}}{S_{ee}} \cdot \frac{S_{y_w u}}{S_{uu}}} \tag{10}$$

From formulas (9) and (10) Figure 6 and Figure 7 were obtained. Them shows normalized impulse response of the $H_W(\omega)$ and $H_Z(\omega)$ corresponding to the absolute and normalized transfer functions $G_W(\omega)$ and $G_Z(\omega)$ (formulas 4 and 5), which shows high accuracy of the transformation.

When we multiply the power transfer function $H_W(\omega)$ by the inverse of the controller power transfer function $H_R(\omega)$ we can obtain the $H_Z(\omega)$ transfer function.

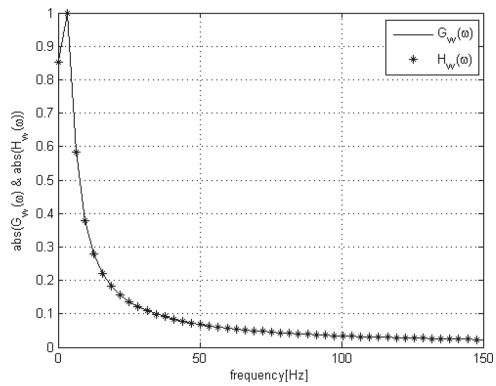


Figure 6. Normalized impulse response of the transfer functions $H_W(\omega)$ and normalized absolute transfer function $G_W(\omega)$.

$$H_W(\omega)\cdot\frac{1}{H_R(\omega)}=\frac{\dfrac{\cancel{S_{ue}}}{\cancel{S_{ee}}}\cdot\dfrac{S_{y_w u}}{S_{uu}}}{1+\dfrac{S_{ue}}{S_{ee}}\cdot\dfrac{S_{y_w u}}{S_{uu}}}\cdot\frac{\cancel{S_{ze}}}{\cancel{S_{ue}}}=H_Z(\omega) \tag{11}$$

When we multiply the power transfer function $H_W(\omega)$ by the inverse of the controller power transfer function $H_R(\omega)$ we can obtain the $H_Z(\omega)$ transfer function.

$$H_W(\omega)\cdot\frac{1}{H_R(\omega)}=\frac{\dfrac{\cancel{S_{ue}}}{\cancel{S_{ee}}}\cdot\dfrac{S_{y_w u}}{S_{uu}}}{1+\dfrac{S_{ue}}{S_{ee}}\cdot\dfrac{S_{y_w u}}{S_{uu}}}\cdot\frac{\cancel{S_{ze}}}{\cancel{S_{ue}}}=H_Z(\omega) \tag{12}$$

The results of operation shown on formula (12) compared to the results from Figure 7 was shown on Figure 8.

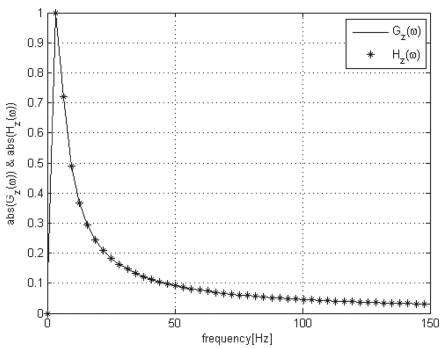


Figure 7. Normalized impulse response of the transfer functions $H_Z(\omega)$ and normalized absolute transfer function $G_Z(\omega)$.

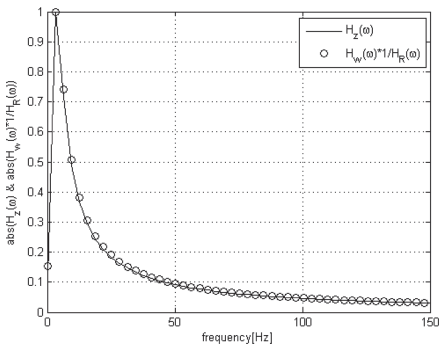


Figure 8. Differences between the normalized impulse response of the power transfer functions $H_Z(\omega)$ and $H_W(\omega)$*1/$H_R(\omega)$ in the frequency domain.

Responses obtained from normalized impulse response from the formulas (10) and (11) corresponding to power transfer function from disturbances $H_Z(\omega)$ in the frequency domain are similar.

4 SUMMARY

The article proved that it is not necessary to carry out research from disturbances "*z*" delivered to the object (for example, by partially covering of the engine nozzle what is dangerous and therefore prohibited) during turbine jet engine ground tests to evaluate its control quality during flight. It could be easily done based on the signals from the standard ground tests of the engine carried out from the input signal "*w*" delivered to the controlled by the engine control lever.

ACKNOWLEDGEMENT

Karol Golak was supported by the Bialystok University of Technology under the research project No. W/WM/7/2013.

Rafał Grądzki was supported by the Bialystok University of Technology under the research project No. W/WM/9/2013.

REFERENCES

Balicki W., Szczeciński S. 2001. *Diagnosing of the air turbine engines.* (Diagnozowanie lotniczych silników turbinowych.), Biblioteka Naukowa Instytutu Lotnictwa, Warsaw.

Bodner W.A. 1958. *Automatic control of the aircraft engines (Automatyka silników lotniczych)*. Wyd. MON, Warsaw.

Golak K. 2013. *Validity check of the assessment of a jet turbine engine regulation in flight using a computer simulation*. Solid State Phenomena, Zurich.

Lindstedt P. 2010. *A comprehensive method for predicting functional properties of the turbine engine in flight, on the basis of ground tests (Kompleksowa metoda predykcji własności użytkowych silnika turbinowego w locie na podstawie badań naziemnych)*. Wyd. ITWL, Warsaw.

Lindstedt P., Golak K. 2011. Basis of method for the evaluation of engine regulation condition in variable environment. *Journal of KONBIN* 1.

Lindstedt P., Golak K., Borowczyk H. 2012. A comprehensive method for predicting functional properties of the turbine engine in flight, on the basis of ground tests (Kompleksowa metoda predykcji własności użytkowych silnika turbinowego w locie na podstawie badań naziemnych). In: *Problemy Badań i Eksploatacji Techniki Lotniczej*, red. Lewitowicz J., Cwojdziński L., Kowalski M., Szczepanik R., Warsaw.

Sheviakov AA. 1970. Automation of aircraft and rocket propulsion systems, Mechanical Engineering, Moscow.

Szczeciński S. 1995. *Engine of the I-22 IRYDA aircraft (Napęd samolotu I-22 IRYDA)*. WPTiL nr 3/1995, Warsaw.

Szopliński Z. 1975. *Research and design of control systems (Badanie i projektowanie układów regulacji)*. WNT, Warsaw.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The mathematical formula of safety of aircrafts

J. Lewitowicz, S. Rutkowski, R. Tomaska & A. Żyluk
Air Force Institute of Technology, Poland

ABSTRACT: The flight of on aircraft has been realized in an operational subsystem. The operation of on aircraft and its safeability are determined for aircraft fleet the so-called flight safety. Aircraft operation and its safeability determine the flight safety of aircraft fleet. The flight safety can be modelled, condition diagnosed, put the procedures of genesis and prognosis. As the results of these activities the prevention treatments can be worked out. A aircraft safety, air system safety or air safety can be considered. Within the flight safety science.

1 INTRODUCTION

The flight safety science uses such concepts as the SP safety, aircraft system safety, and aviation (air) safety. The aircraft safety determines an aircraft capability under complex operation conditions to stay within a risk range nor exceeding a criterion value.

The aircraft system safety is a set of properties of a system comprising aircrafts, ground control measures and aviation control measures, aircraft crews, ground personnel and ground maintenance personnel taking care of aircraft proper technical condition and preventing the arising of emergency situations, protecting passengers and offering rescue measures in case of equipment breakdowns, crew errors or ground personnel errors as well as in the cases of unwanted external impacts.

2 THE MATHEMATICAL FORMULA

The aircraft safety manifests itself by dangerous situations resulting in various effects occurred in aircraft accidents due to occurrence of unwanted events. The science of aviation safety and in particular the science of flight safety concerning the system C(P)-SP-O: man (pilot, crew)-aircraft-environment researches all these phenomena, concepts and properties.

The problem of flight safety and aviation—air—safety is studied within a set of aircraft flight safety (BLSL) and a single aircraft flight safety (BLSP). The SP safety depends also on its design. It can be called a technical safety. The flight safety is dependent both on the design safety and on the design of other parts of a system, i.e. on the human (people) and environment.

The aviation—air—safety is understood as a system of knowledge the main purpose of which is to discover laws and regularities and working out rules and ways of action in order to ensure safe performance of flights by aircrafts when taking into account adverse impacts from the environment.

The safety level for systems of operating aircraft fleets is analysed in a continuous manner. The safety level and its trends are expressed with the aid of various measures: e.g. risk, factors, event probability using for it analytical methods, e.g. theory of probability, geometric methods, neural networks. According to relevant current requirements the most usual measure of the flight safety is defined by different coefficients and by the accident rate function FW.

One of the main flight safety coefficients is the coefficient of grave accidents WWc defined as a ratio: number of accidents Wc to the flying time N (in flight hours or as a standard time of 100 000 flight time in air forces or to the number of passengers L for civil aviation (standard number of 1 million of passengers).

The accident rate function (FW) is a real function $W(t)$ which for every real value of t determines the probability P of an aviation system (defined by the number of aircrafts) capable of operation expressed by a selected property (number of aircrafts capable of flying) at the t_o time, where after a $\Delta\tau$ time this capability will be decreased by a value proportional to the change of the accident rate function ΔW.

The $W(t)$ function depends on the properties of operation of the system under discussion characterized by features (k), on its operation conditions and requirements (s), which in order for the system to be accepted as fit must be met. If the accident rate is measured with the accident factor, e.g. heavy accidents WWc, when aircrafts are lost and this WWc is multiplied by a factor (average losses) of the weight p and by the planned flying

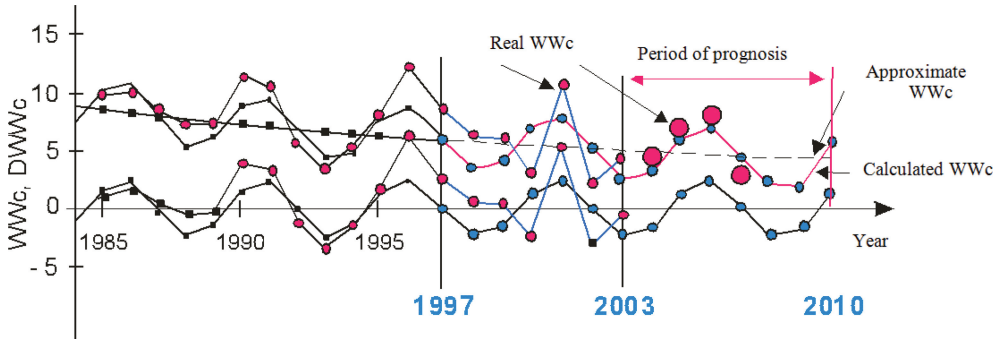


Figure 1. *WWc* and *DWWc* changing over 1984–2010.

time *Np.* (standard: 10^5 flight hours) this function can be expressed as:

$$W(t) = \mathrm{P}\{p, Np, WWc(\tau; k, s); 0 < \tau \leq t, WWc(o; k, s)\} \quad (1)$$

where: τ—prediction time interval; *WWc*—function of the heavy accident factor; *Np*—number of planned flying time over τ time; *p*—coefficient of average losses of aircrafts or crews; *k*—aviation system characterics; *s*—conditions for operating an aviation system and requirements for it.

The accident rate function in its $W(t)$ form and short-term changes *DWWc* make it possible to prognosticate changes of the *WWc* coefficient and losses of aircrafts and crews. The applied calculation method provided the basis to predict a certain growth (local maximum) of the *WWc* factor over 2005–2007 and 2005–2006 and further predicts this coefficient to rise after 2010 for Polish Air Forces (Fig. 1). As the *WWc* over 2003–2007 fairly well agrees with the theoretical predictions it demonstrates that the number and character of factors causing unwanted events did not change substantially.

3 CONCLUSIONS

The analysis of flight safety coefficients and the function of accident rate are used to work out adequate prophylactic recommendations (Lewitowicz 2006, Lewitowicz et al. 2008, Kersterson 2000).

REFERENCES

Kersterson, B. 2000. Human factors and human reliability. Proc. *Maintenance, Reliability and Cost Analysis Seminar*, Long Beach (USA).

Lewitowicz, J. 2006. *The fundamentals of aircraft operations*, vol. 3. The operation systems of aircrafts (in Polish). Warsaw: ITWL.

Lewitowicz J., Gołębiowski W. & Kustroń K. 2008. Safety of operation and maintenance systems of aircraft fleet. *Journal of KONBIN*, No 4(7), 2008.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The reliability analysis of the satellite's driving system based on the IABCBLT method

Wensheng Peng, Jianguo Zhang & Linjie Kan
Science and Technology on Reliability and Environmental Engineering Laboratory, Beijing, China
School of Reliability and Systems Engineering, Beihang University, Beijing, China

ABSTRACT: In the design and analysis process of the aeronautical & astronautic systems, some difficulties emerged: on one hand, there is not enough information that can be used directly; on the other hand, a lot empirical data can't be used well. And at the same time, the aeronautical & astronautic systems themselves are too complex, which bring difficulties in analyzing their stochastic behaviors. In order to utilize the uncertain information fully and accurately in the analysis of the aeronautical & astronautic systems, this paper proposes an system stochastic behavior analysis method named the Improved Artificial Bee Colony optimization Based Lambda-Tau (IABCBLT), and applies in the Satellite Antenna's Driving System (SADS). This method firstly models the SADS with petri net, then analyzes its failure rate λ and repair time τ based on the traditional Lambda-Tau method, the fuzzy vague theory and the improved artificial bee colony optimization algorithm. The improved ABC algorithm uses the genetic hybrid genes and the chaotic-search strategy based on the traditional ABC algorithm, and makes the optima process converge quickly and avoid getting trapped in the local optima easily. The IABCBLT method can solve the problem that the fuzzy membership function will wide spread with the increase of the complexity of the system, and it can analyze the system's behavior more accurately with the uncertainty information. At last, this paper analyzes an engineering example of the SADS to verify the availability of this method.

Keywords: the improved artificial bee colony, fuzzy logical math, Lambda-Tau methodology, satellite antenna's driving system

1 INTRODUCTION

Modern mechanical products such as aeronautical & astronautic systems show the features as follows: complex structure, nonlinear performance, limited samples, less information and strict demand of reliability and maintainability. All these features make the reliability and maintainability analysis is a huge challenge in precise and efficiency. Introducing the system engineer methodology into the mechanical products' reliability analysis is an important and practical way. The traditional system reliability analysis methods such as FTA, reliability block diagram, Markovian approach and Petri nets are on the basis of history data. These methods can't work well and even could be inadequate in system analysis because of the complexity of structure and nonlinearity of their behaviors. For example, the space satellite is a system with complex structure. Its samples are very limited because of expensive cost, and its work environment is very complicate and uncertain.

Because of these obstacles, researchers paid attention to the industrial systems' behavior analysis. For example, Gupta et al. (2005) used numerical method for behavior analysis of a dairy plant. Aksu et al. (2006) proposed a methodology based on FTA and Markovian approach for the reliability and availability assessment of a pod propulsion system. Yuzgec (2010) had optimized the feeding profile of an industrial scalefed-batch baker's yeast fermentation process using four different differential evolution algorithms. Wu et al. (2011) proposed an improved particle swarm optimization algorithm for solving the reliability problems. Additionally, there are some other types of reliability problems developed by the researchers such as process control reliability (Estevez 2000), distribution system reliability (Hosseini, 2009), reliability of dynamic systems (Fales R, 2010) and so on. Knezevic and Odoom (2001) highlighted these ideas and analyzed the behavior of a general repairable system by introducing the concept of fuzzy Lambda-Tau technique coupled with PN in terms of various reliability indices utilizing quantified data. Komal et al (2009) used this approach for behavior analysis of press unit using FTA instead of PN in a paper mill while the authors (Sharma SP, 2011, Komal, 2007, Garg H, 2012, Garg H,

2011) have analyzed the behavior of some complex repairable industrial system by using PN and fuzzy approach. But there are few researches and works in the analysis of the complex mechanical systems.

The main object of this paper is to analyze the reliability of the complex mechanical system on the base of the Lambda-Tau (L-T) methodology and fuzzy math. In order to quantify the uncertain of the system reliability more close, this paper utilizes the improved artificial bee colony algorithm to optimize the L-T methodology. The obstacle of the complex structure will be conquered with the help of the petri nets approach. An example of a satellite antenna' drive system is taken account to demonstrate this method. The system reliability model of the drive system is built by the petri net and the reliability behavior is analyzed with the IABCBLT proposed in this paper. At last, the results obtained from GABLT, PSOBLT and traditional ABCBLT are compared and it can be conducted that that the method proposed by this paper could get more precise results in uncertain mathematic.

2 FUZZY CUT-SET AND PETRI NET THEORY

In fuzzy set theory, the elements are not determined to belong to a set or not, instead, the degree presents elements belong to set is proposed. The degree of membership is described by $\mu_{\tilde{A}}(x)$ between in [0,1]. The fuzzy set is uncertain, and it has no certain range itself, so the mathematic is useful if only the fuzzy sets were transferred into the crisp sets. The cut set level technique plays an important role in the transfer procession.

Defining a fuzzy set A in the a discourse domain, for any $\alpha \in [0,10]$, the set $A_\alpha = \{u \mid \mu_{\tilde{A}} \geq \alpha, u \in U\}$ is the cut level α of A. For example, for a triangle membership function $\mu_{\tilde{A}}$:

$$\mu_{\tilde{A}}(x) = \begin{cases} \dfrac{x-a}{b-a} & a < x < b \\ 1 & x = b \\ \dfrac{c-x}{c-b} & b < x < c \end{cases} \quad (1)$$

Then the α cut set of the fuzzy set is $[a^{(\alpha)}, c^{(\alpha)}]$, as in Figure 1.

For the large complex system, when calculating the minimal cut sets in FTA, the computation is very large, even results in the NP problem. Petri net is a special directed net, which contains the static performance as well as the dynamic performance. The petri net can describe the status changing and the events developing, so the petri net is considered as the reliability modeling method instead of the FTA. The static performance of the petri net

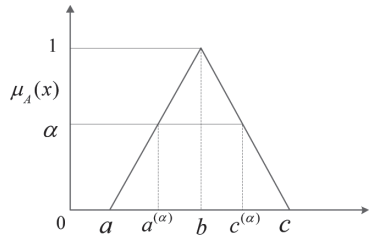


Figure 1. The cut-level of the triangle membership function.

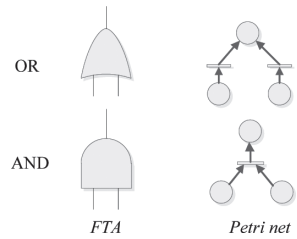


Figure 2. The expression of the logical gate in petri net.

includes three primitives: place, transition and arcs. And the dynamic performance includes the tokens and the rules firing. The systems' status change and the relationship of the changes are reflected through the flow of the tokens in the petri net. At the present, many research about the petri net and its application in improving the FTA, in the reliability qualitative analysis, quantitative calculating and the prognostic and management of the failures.

This paper utilizes the petri net to build the reliability model of the mechanical systems, the disjoint nodes of the system are the place and the transition, and the arcs present the spread relationship of the failures in the system. In case of the complex mechanical system, this paper modeling the system on the base of the static hierarchical petri net.

The expressions of the FTA logical gates in petri net are shown in Figure 2.

3 LAMBDA-TAU THEORY

The Lambda-Tau is a traditional methodology for system reliability analysis, and this method is suitable for the FTA model. The failure rate of every component required to obey exponential distribution function and the failure rate λ and the repair time τ of the system obtained by the logical gates of the system's FTA.

On the base of the traditional L-T methodology, Knezevic and Odoom analyzed the stochastic behaviors of an repairable system with the petri net

Table 1. The basic expression of Lambda-Tau methodology.

Gate	λ_{AND}	τ_{AND}	λ_{OR}	τ_{OR}
Expression	$\prod_{j=1}^{n}\lambda_j\left[\sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}\tau_j\right]$	$\frac{\prod_{i=1}^{n}\tau_i}{\sum_{i=1}^{n}\left[\prod_{\substack{j=1\\ j\neq i}}^{n}\tau_j\right]}$	$\sum_{i=1}^{n}\lambda_i$	$\frac{\sum_{i=1}^{n}\lambda_i\tau_i}{\sum_{i=1}^{n}\lambda_i}$

and the fuzzy mathematic. In this theory, the fuzzy membership function combined with the Lambda-Tau methodology are utilized to analyze the fuzzy performance of the system's reliability. This is suitable for the system because of the shortage of the information and the human/environment factors. But this method has a detect that the fuzzy uncertainty of the system will be larger and larger when the system become more and more complex. In case of this situation, Harish Garg (2012) combined the fuzzy Lambda-Tau method and the particle swarm optimization algorithm, in detail, the membership of the systems reliability indices is optimized by the PSO. Thereby, the uncertain degree of the membership is dropping. The author also has verified this method with the illustration example of the feeding unit of a paper mill. However, for the large complex system, especially for the mechanical systems, the PSOBLT also has disadvantages in accuracy and the efficiency. In the intelligent optimization algorithms, the artificial bee colony algorithm is an advanced algorithm in both the accuracy and the efficiency. Inspired by the artificial bee colony algorithm and the GA algorithm, this paper improves the traditional ABC algorithm, the genetic cross factor in GA algorithm is introduced into the ABC algorithm, and then the IABC algorithm is used to optimize the fuzzy membership function of the fuzzy Lambda-Tau method. The accuracy and the calculation efficiency are improved in this paper.

4 IABCBLT METHODOLOGY

4.1 *The IABCBLT method*

IABCBLT method is the combination of two techniques: the improved artificial bee colony algorithm and the Lambda-tau method. The key point of IABCBLT is using the numerical calculation and the optimization algorithm instead of the fuzzy arithmetic, this can improve the accuracy of the reliability indices of the systems efficiently. In the fuzzy L-T methodology, the failure rate and the repair time of the top level of the system is an interval $[a^{(\alpha)}, c^{(\alpha)}]$ at the cut level α. At a determined membership function, if the range of the interval is smaller, then the reliability indices is more accuracy.

The upper boundary of the interval at the cut level α is:

$$\begin{aligned}&\text{Maximize} && \widetilde{F}(\lambda_1,\lambda_1,\ldots,\lambda_n,\tau_1,\tau_2,\ldots\tau_m) \text{ or}\\ &&& \widetilde{F}(t/\lambda_1,\lambda_1,\ldots,\lambda_n,\tau_1,\tau_2,\ldots\tau_m)\\ &\text{Subject to} && \mu_{\lambda_i}(x)\geq\alpha\\ &&& \mu_{\tau_j}(x)\geq\alpha\\ &&& 0\leq\alpha\leq 1 \quad i=1,2,\ldots n;\ j=1,2,\ldots m\end{aligned}$$

The lower boundary of the interval at the cut level α is

$$\begin{aligned}&\text{Minimize} && \widetilde{F}(\lambda_1,\lambda_1,\ldots,\lambda_n,\tau_1,\tau_2,\ldots\tau_m) \text{ or}\\ &&& \widetilde{F}(t/\lambda_1,\lambda_1,\ldots,\lambda_n,\tau_1,\tau_2,\ldots\tau_m)\\ &\text{Subject to} && \mu_{\lambda_i}(x)\geq\alpha\\ &&& \mu_{\tau_j}(x)\geq\alpha\\ &&& 0\leq\alpha\leq 1 \quad i=1,2,\ldots n;\ j=1,2,\ldots m\end{aligned}$$

The advantages of the IABC algorithm are:

(1) Avoid the traditional fuzzy arithmetic, the form of the fuzzy membership function will not widely spread due to the arithmetic, especially for the complex systems; (2) the artificial bee colony algorithm has a higher efficiency in the optimization process, so it could reduce the time cost; (3) the ABC algorithm has improved compared to the traditional ABC, it increase the ability of the global sought, so the results will more precise.

The conditions for applying the IABCBLT:

Through the literatures, the conditions for applying the IABCBLT method are:

i. component failures and repair rates are statistically independent, very small
ii. component failures and repair rates obey exponential distribution function;
iii. the failure rate λ << the repair time τ
iv. after repairs, the repaired component is considered as good as new.

The basic steps of the IABCBLT method are:

1. The FMECA and structure analysis of the mechanical system;
2. Collecting the data of the mechanical system, and identifying the failure rate and the repair time of the components;

3. Building the reliability model of the mechanical system with the petri net;
4. The obtained crisp data of failure rate and the repair time are converted into fuzzy numbers, and then putting them into the petri net;
5. Optimizing the fuzzy membership function with the improved artificial bee colony algorithm;
6. Finally the fuzzy failure rate and the fuzzy repair time of the system is obtained.

Next, the improved artificial bee colony algorithm is proposed.

4.2 *The improved Artificial Bee Colony algorithm*

Artificial Bee Colony (ABC) algorithm was proposed by Karaboga (2007, 2008) for optimizing numerical problems. In ABC algorithm, the position of a food source represents a possible solution to the optimization problem and the nectar amount of a food source corresponds to the quality (fitness) of the associated solution. The number of the employed bees or the onlooker bees is equal to the number of solutions in the population. At the first step, the ABC generates a randomly distributed initial population P ($G = 0$) of SN solutions (food source positions), where SN denotes the size of the population. Each solution $x_i (i = 1, 2, \ldots SN)$ is a D-dimensional vector. Here, D is the number of optimization parameters. After initialization, the population of the positions (solutions) is subjected to repeated cycles, $C = 1, 2, \ldots$, MCN, of the search processes of the employed bees, the onlooker bees and scout bees. An employed bee produces a modification on the position (solution) in her memory depending on the local information (visual information) and tests the nectar amount (fitness value) of the new source (new solution). Providing the nectar amount of the new one is higher than that of the previous one, the bee memorizes the new position and forgets the old one. Otherwise, she keeps the position of the previous one in her memory.

An artificial onlooker bee chooses a food source depending on the probability value associated with that food source, P_i, calculated by the following expression (1):

$$P_i = (fit_i) / \sum_{n=1}^{\mathrm{SN}} fit_n \tag{2}$$

where fit_i is the fitness value of the solution i which is proportional to the nectar amount of the food source in the position i, and SN is the number of food sources which is equal to the number of employed bees. In order to produce a candidate food position from the old one in memory, the ABC uses the following expression (3):

$$x_j = x_{ij} + \phi_{ij}(x_{ij} - x_{kj}) \tag{3}$$

where $k \in \{1, 2, \ldots, \mathrm{SN}\}$ and $j \in \{1,2, \ldots, D\}$ are randomly chosen indices. Although k is determined randomly, it has to be different from i. φ_{ij} is a random number between [0, 1]. It controls the production of neighbor food sources around x_{ij} and represents the visual comparison of two food positions by a bee.

In the ABC algorithm, in order to avoid trapped into the local optima, paper learn from the cross-portfolio and the variation in the genetic, the strongest individual fitness bee in the employed bee s is the queen bee, and its fitness is $g_i(x)$, and the onlooker bee is the drone bee. After the mating of the drone and the queen bee, it will generate a employed bee and a new drone. The stronger offspring bee will replace the parents bee, the drone colony and the employed bee colony get updated by the advantage selective. The update of the drone makes the solution convergence faster in global optimization process; and the updating of the employed bees makes the colony variable, and avoids premature convergence at the same time.

The drone colony, employed bee colony and the queen bee all have their fitness themselves. The drone colony are selected by the roulette, the individual has strong fitness would be selected in large probability, and it will mate with queen bee, transforming its genetic information to the next generation. The probability of the individual be selected is:

$$p_i = g_{m_i}(x) \Big/ \sum_{i=1}^{n} g_{m_i}(x) \tag{4}$$

where p_i is the probability, $g_{mi}(x)$ denotes the fitness of the no. i drone.

According to the fitness mating probability P and the mating times c, the drone mating with the queen bee, the fitness mating probability is:

$$P_i = p_i \left(\sum_{i=1}^{n} g_{m_i}(x) \right) \Big/ \sum_{i=1}^{n} g_{m_i}(x) + r_0 \tag{5}$$

where r_0 is the minimum probability, the function of mating times is

$$c_i = L(1 - P_i) + a_0 \tag{6}$$

where L is the length of the chromosome, a_0 is the minimum cross times.

The process of the IABC is:

1: Initialize the population of solutions x_i, $i = 1 \ldots$ SN
2: Evaluate the population
3: cycle = 1
4: repeat

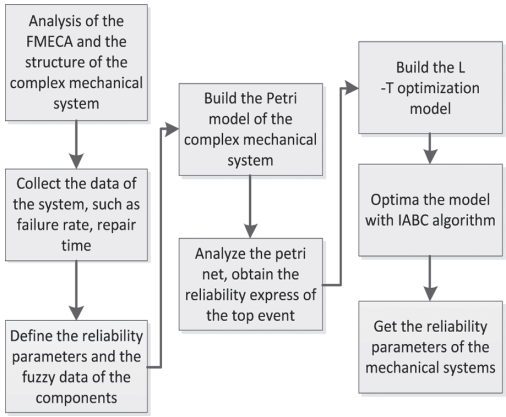


Figure 3. The flow chart of the IABCBLT technique.

5: Produce new solutions v_i for the employed bees by using (3) and evaluate them
6: Apply the greedy selection process
7: Calculate the probability values P_i for the solutions x_i by (5)
8: Produce the new solutions v_i for the onlookers from the solutions x_i selected depending on P_i and evaluate them
9: Apply the greedy selection process
10: Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution x_i by (3)
11: Memorize the best solution achieved so far
12: cycle = cycle + 1
13: until cycle = MCN.

The flow chart of the IABCBLT technique is as show as Figure 3.

5 THE EXAMPLE OF THE DRIVE MECHANICAL SYSTEM OF THE SATELLITE ANTENNA

5.1 *The description of the biaxial drive mechanical system*

The biaxial drive mechanism is the key component of the biaxial motion mechanism of the SAD system. The biaxial drive system contains of two drive components and these two drive components are the same in structure: a stepper motor, a harmonic reducer and an angle sensor. The angle sensor includes a photoelectric encoder and a micro switch. The harmonic reducer includes a steel gear, a flexible gear and a cam. The reliability analysis of the drive mechanical system is the critical point for guaranteeing the satellite antenna's reliability work in the orbit. The CAD model of the biaxial drive system is showed in Figure 4.

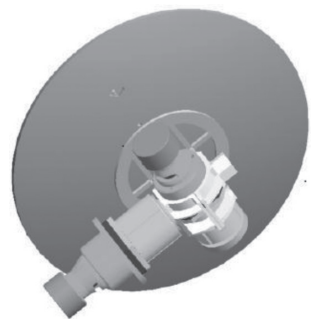


Figure 4. The CAD model of the a biaxial drive mechanical system.

5.2 *Building the FFA and Petri net of the SAD system*

Now a failure event of the drive mechanism can not move is chosen for building the FTA and the petri net. The FTA and the Petri net are in Figure 5 and Figure 6.

5.3 *Defining the reliability parameters of components*

Through the references of the simulation, the history data and the expert's estimation, we assume that the reliability parameters of components in bottom level of the system as in Table 2.

The fuzzy membership function of the failure rate and the repair time is:

$$\mu_{(x)} = \begin{cases} \dfrac{x-0.85}{0.15} & 0.85 < x < 1 \\ 1 & x = 1 \\ \dfrac{1.15-x}{0.15} & 1 < x < 1.15 \end{cases} \tag{7}$$

It means that the membership function of the λ_i and τ_i are:

$$\mu_{\lambda_i} = \mu_{(x)} \cdot \lambda_i \quad i = 1, 2, 3 \ldots, n \tag{8}$$

$$\mu_{\tau_i} = \mu_{(x)} \cdot \tau_i \quad i = 1, 2, 3 \ldots, m \tag{9}$$

5.4 *The reliability behavior analysis of the biaxial drive system with the IABCBLT methodology*

Firstly, the minimal cut sets of the petri net are obtained:

$\{P_1\},\{P_2\},\{P_3\},\{P_4\},\{P_5, P_6\},\{P_7\},\{P_8\},\{P_9\},$
$\{P_{10}\},\{P_{11}, P_{12}\},\{P_{13}, P_{14}\}, \{P_{15}\},\{P_{16}\}$

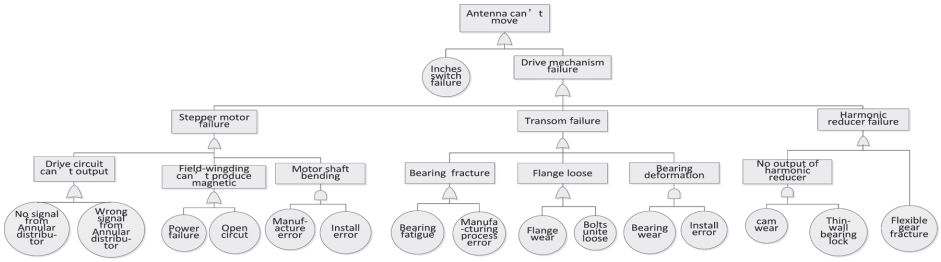


Figure 5. The fault tree of the antenna can not move.

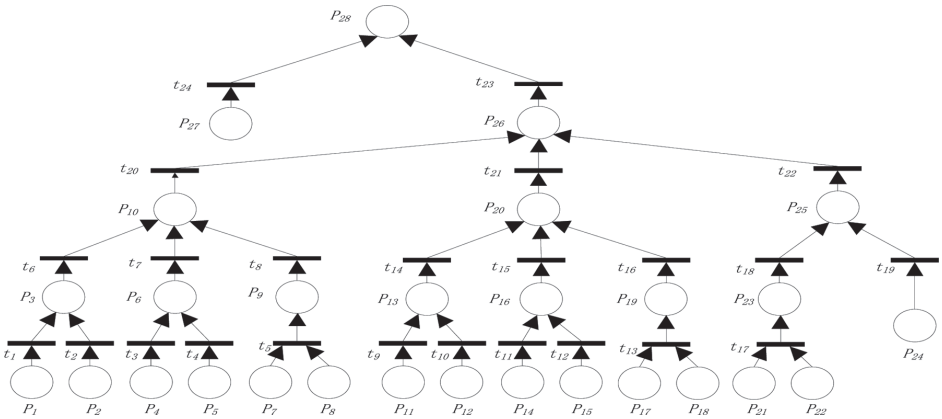


Figure 6. The petri net model of the antenna can not move.

Through the logical expression, the failure rate and the repair time of the top level in petri net are:

$$\lambda_s = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 \cdot \lambda_6 \cdot (\tau_5 + \tau_6) + \lambda_7 + \lambda_8 + \lambda_9 + \lambda_{10} + \lambda_{11} \cdot \lambda_{12} \cdot (\tau_{11} + \tau_{12}) + \lambda_{13} \cdot \lambda_{14} \cdot (\tau_{13} + \tau_{14}) + \lambda_{15} + \lambda_{16}$$

$$\tau_s = \frac{\lambda_1 \cdot \tau_1 + \lambda_2 \cdot \tau_2 + \lambda_3 \cdot \tau_3 + \lambda_4 \cdot \tau_4 + \lambda_5 \cdot \tau_5 \cdot \lambda_6 \cdot \tau_6 + \lambda_7 \cdot \tau_7}{\lambda_s} + \frac{+\lambda_8 \cdot \tau_8 + \lambda_9 \cdot \tau_9 \lambda_{10} \cdot \tau_{10} + \lambda_{11} \cdot \lambda_{12} \cdot \tau_{11} \cdot \tau_{12}}{\lambda_s} + \frac{\lambda_{13} \cdot \lambda_{14} \cdot \tau_{13} \cdot \tau_{14} + \lambda_{15} \cdot \tau_{15} + \lambda_{16} \cdot \tau_{16}}{\lambda_s}$$

Building the optimization model of the failure rate and the repair time, the failure event is that the drive mechanism can't move:

$$\begin{aligned} &\text{Maximize} \quad \widetilde{F}(\lambda_s, \tau_s) \\ &\text{Subject to} \quad \mu_{\lambda_i}(x) \geq \alpha; \qquad \mu_{\tau_i}(x) \geq \alpha \\ &\qquad 0 \leq \alpha \leq 1 \quad i = 1, 2, \ldots 15; j = 1, 2, \ldots 15 \end{aligned}$$

$$\begin{aligned} &\text{Minimize} \quad \widetilde{F}(\lambda_s, \tau_s) \\ &\text{Subject to} \quad \mu_{\lambda_i}(x) \geq \alpha; \qquad \mu_{\tau_i}(x) \geq \alpha \\ &\qquad 0 \leq \alpha \leq 1 \quad i = 1, 2, \ldots 15; j = 1, 2, \ldots 15 \end{aligned}$$

Optimizing the model with the IABC algorithm, choosing the α-cut at 0,0.2,0.4,0.6,0.8,1.0, the optima iteration process of the variable λs' upper boundary is as shown in the Figure 7.

The optimization results of the model can be seen in Figure 8 and Figure 9, in order to verify the efficiency and accuracy of the IABCBLT, this paper also optimize the model with the methods of GA, PSO, the traditional ABC algorithm.

6 RESULTS AND DISCUSSION

The optimization results are showed in Table 3. Comparing the variable's iteration process in IABC optimization and the ABC optimization, it can be known that the IABC has a higher efficiency in the process. For example, Figure 6 and Figure 7 show the iteration process of the variable λ_s's upper boundary, in traditional ABC algorithm, the optimization process needs 800 times to obtain the best result, while in the IABC algorithm, the iteration times are 500.This experiment shows that the convergence of the IABC is obviously better than the ABC. The reason result in this situation is that in the IABC algorithm, the search strategy is

Table 2. The failure rate and the repair time of the components.

Components	P_1 ($i=1$)	P_2 ($i=2$)	P_4 ($i=3$)	P_5 ($i=4$)	P_7 ($i=5$)	P_8 ($i=6$)	P_{11} ($i=7$)	P_{12} ($i=8$)	P_{14} ($i=9$)	P_{15} ($i=10$)	P_{17} ($i=11$)	P_{18} ($i=12$)	P_{21} ($i=13$)	P_{22} ($i=14$)	P_{24} ($i=15$)	P_{27} ($i=16$)
Failure rate λ_i (10^{-4})	1.5	8	40	0.2	1	10	6	1	15	10	70	5	40	1	2	30
Repair time τ_i (h)	10	10	1	2	3	3	3	3	3	1	2	2	3	3	5	2

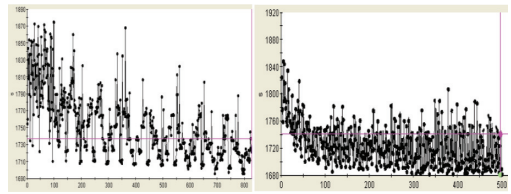


Figure 7. The iteration process of the λ_s in the level of $\alpha = 0.4$ utilize the ABC (left) and IABC (right).

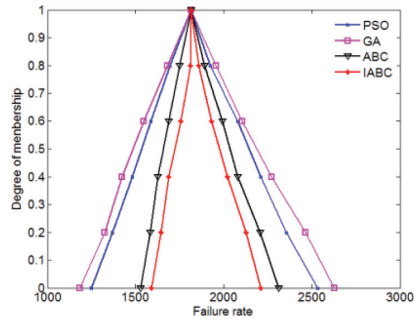


Figure 8. The degree of membership of λ in different algorithms.

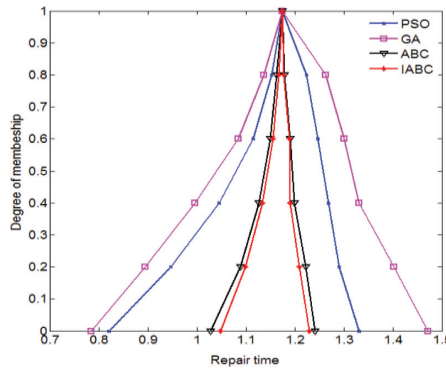


Figure 9. The degree of membership of τ in different algorithms.

chaotic serious search. The chaotic serious search is more efficient than the random search strategy. In the nonlinear, multivariable, complex mechanical system, this is very important.

At last, the paper also optimizes the model with the algorithm GA, PSO, ABC. The range of the failure rate and the repair time' cut set interval at α-cut level are used to measure the accuracy of the different algorithms. For example, when the $\alpha = 0$, the interval of the membership function is: [1249.412, 2534.1345](GA), [1183.571, 2626.8656]

Table 3. The optimization results of the IABC.

α	0	0.2	0.4	0.6	0.8	1
λ_{max}	2212.28	2126.01	2021.17	1931.23	1859.74	1813.7
λ_{max}	1588.65	1643.03	1687.37	1757.22	1809.70	1813.7
τ_{max}	1.2292	1.20851	1.18991	1.1879	1.1768	1.1746
τ_{min}	1.0482	1.09787	1.1327	1.1558	1.1661	1.1746

(PSO); [1528.65, 2312.28] (ABC); [1588.49, 2213.198] (IABC); as showed in Figure 8, the ABC algorithm is much better than the GA, PSO algorithm in accuracy. The IABC algorithm is almost the same with the ABC algorithm in the accuracy of the optimization result, but the results show that the IABC algorithm is still better than the ABC.

7 CONCLUSION

The IABCBLT methodology proposed in this paper combines the IABC optimization algorithm, the fuzzy Lambda-Tau theory and the petri net. And a satellite antenna' driving system is used for the engineering case to verify this methodology. Firstly, the petri net is used to build the reliability model. And then, the fuzzy set theory and the artificial intelligent optimization algorithm is utilized on the basis of the L-T methodology to analyze the failure rate and the repair time of the system. This method can solve the difficulties brought by the complexity of the system's structure. Also, it can solve the problem such as limited history data and available information in aeronautical & astronautic mechanical. The fuzzy theory can utilize the information fully and avoid the waste of the information in the engineering. The widely spread of the fuzzy uncertain cause by the complexity of the structure is also solved by the IABC algorithm, this can improve the accuracy the reliability indices of the system.

REFERENCES

Aksu S, Turan O. 2006. Reliability and availability of pod propulsion system. Journal of Quality and Reliability International 2006;22:41–58.

Estevez–ReyesL. 2000. Process control reliability; the key to investing in your infrastructure. ISA Transactions 2000; (Author 1989a, b, Author & Author 1987) *instead of* (Author, 1989a,b; Author and Author, 1987) 39(1):115–21.

Fales R. 2010. Uncertainty modeling and predicting the probability of stability and performance in the manufacture of dynamic systems. ISA Transactions 2010;49:528–34.

Garg H, Sharma SP. 2012. Behavior analysis of synthesis unit in fertilizer plant. International Journal of Quality and Reliability Management 2012;29(2):217–32.

Garg H, Sharma SP. 2011.Behavior and system performance optimization for an industrial system by using particle swarm optimization. In: 2011 IEEE international conference on intelligent computing and intelligent systems (ICIS 2011), Guangzhou, China; 2011.p.237–41.

Gupta P, Lal AK, Sharma RK, Singh J. 2005. Numerical analysis of reliability and availability of the serial processes in butter-oil processing plant. International Journal of Quality and Reliability Management 2005; 22(3):303–16.

Harish Garg, S.P. Sharma. 2012. Stochastic behavior analysis of complex repairable industrial systems utilizing uncertain data. ISA Transactions 51(2012)752–762.

Hosseini M, Shayanfar HA, Fotuhi–Firuzabad M. 2009. Reliability improvement of distribution systems using SSVR. ISA Transactions 2009;48(1):98–106.

Karaboga D., B. Basturk. 2007. A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm, J. Global Optim.39 (2007) 459–471.

Karaboga D., B. Basturk. 2008. On the performance of artificial bee colony (ABC) algorithm, Appl. Soft Comput. 8 (2008) 687–697.

Knezevic J, Odoom ER. 2001. Reliability modeling of repairable systems using Petri nets and Fuzzy Lambda-Tau Methodology. Reliability Engineering and System Safety 2001;73(1):1–17.

Komal, Sharma SP, Kumar D. 2007. Reliability analysis of the feeding system in a paper industry using Lambda-Tau technique. In:3rd international conference on reliability and safety engineering (INCRESE), IIT Kharagpur, India; 2007.p. 531–7.

Komal, Sharma SP, Kumar D. 2009. RAM analysis of the press unit in a paper plant using genetical gorithm and lambda-tau methodology. In: Proceeding of 13th online international conference WSC-2008. Applications of soft computing (Springer book series), vol. 58; 2009. p. 127–37.

Sharma SP, Garg H. 2011. Behavioral analysis of a urea decomposition system in a fertilizer plant. International Journal of Industrial and System Engineering 2011;8(3):271–97.

Wu P, Gao L, Zou D, Li S. 2011. An improved particle swarm optimization algorithm for reliability problems. ISA Transactions 2011;50:71–81.

Yuzgec U. 2010. Performance comparison of differential evolution techniques on optimization of feeding profile for an industrial scale bakers yeast fermentation process. ISA Transactions 2010;49(1):167–76.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The effectiveness of the FMEA technology in the process of the aerospace product development

J. Shuyuan, L. Fuqiu, W. Jinjing & L. Meinan
China Aerospace Standards Institute, China

ABSTRACT: In the process of the aerospace product development and production, the technology of FMEA has been very common to recognize and analyze the failure mode. However, there are still many misunderstandings in the application of FMEA technology. In this paper, the research concerns the following aspects: the FMEA concept, the FMEA essence, various correspondences of FMEA analysis process, FMEA work form, the relationship between FMEA and other reliability work items. By analyzing the FMEA problem of the aerospace product development and production, we analyze and summarize the solutions against the FMEA work errors to enhance the effectiveness of FMEA technology.

Keywords: FMEA; effectiveness; failure; failure mode; failure cause; failure effect

1 OVERVIEW

Aerospace products have features such as exploration, advancement, high risk, small samples, high reliability, and high quality, which challenges the reliability assurance in the process of the aerospace product development. Thus, scientific and effective work of reliability must be adopted to enhance the effectiveness of reliability technology, in order to reduce launch risk and satisfy aerospace products requirements of high longevity and reliability.

In the process of the aerospace product development, Failure Mode and Effects Analysis (FMEA) can be adopted to discover product defects of design and process. Then we can locate weak point and put forward prevent and correct measures against it. Although this method does some work in many cases, the application effectiveness of FMEA technology needs to be further improved. This paper have thoroughly discussed how to improve effectiveness of FMEA technology in the process of the aerospace product development.

2 EXISTING PROBLEMS IN FMEA WORK

The essence of FMEA method is to start with unit functions, and discover failure impacts or consequences to adopt corresponding prevent and correct measures through identifying and arranging all possible failure modes and seeking the causes. It can reduce risk in the process of the aerospace product development. Nevertheless, there exists following problems in FMEA work.

2.1 *A lack of teamwork, existing situation that one designer accomplishes FMEA independently*

FMEA is a teamwork, many departments must cooperate and work together to implement the task. It is a group action instead of that by designer individual. As for aerospace products which usually have high complexity, different designers are inconsistent with the understanding of failure mode, failure cause and failure effect during FMEA development, and they easily neglect the interface problems, that leads to a lack of content coherence. The weak point discovered by it could be far from the real condition of product.

2.2 *Establishing not along with the process of product development, the lack of closed loop management*

For ensure the effectiveness of FMEA, it should be established along with the product development phase. It is common that FMEA is accomplished afterward for reparation, although some instances are not like this, there exists that FMEA development does not begin at the reasonable time. That means FMEA is not synchronous with product design. In a sense, it misses the opportunity to timely discover the weak points and improve the design in the phase of product design. Therefore, that FMEA is developed along with the product design cannot be satisfied, effectiveness of FMEA decreases enormously.

FMEA work is a repeated and dynamically iterative process along with product development. Due to

the different focus during every development stage, function FMEA should be launched in scheme stage, and iteratively carried on and modified along with product development process. In addition, failure prevention and correct measures should be practicable in relevant design tasks and technology documents, achieving the closed loop management.

2.3 *Hard to collect data, a lack of failure mode accumulation, completely analyzing failure mode by experience*

FMEA process needs mass history data information. Owing to a lack of necessary failure mode information accumulation, difficulty of collection and extensive work load, it is common that failure mode analysis mainly relies on experience and failure modes are incomplete. Consequently, how to collect failure data information becomes very significant. Due to a lack of public database of aerospace system and equipment failure, such as entire carrier rocket, control system and engine failure modes, we need accumulate these information combining with system development process. Failure information collection requirement and collection table can be established for developer to gather the finite failure information, which can effectively and entirely support FMEA work.

2.4 *Disaccord of term understanding, informal expressions*

2.4.1 *Informal and indefinite expression of failure modes*

Failure mode means manifestation of failure. Failure mode analysis in FMEA usually appears expressions like "……failure", "……fault". Describing failure modes this way which is inaccurate cannot clarify the real manifestation of failure. For example, one failure mode of some communication product is described as "communication failure", and this expression cannot demonstrate the specific form of failure. We should present that communication signals cannot be received, sent, or intermittent, from the perspective of specific function realization.

2.4.2 *Inaccurate statement of "failure impact"*

Failure effect is generally divided into three layers: local effect, higher layer effect and ultimate effect, each one respectively corresponding to lowest agreement layer, agreement layer and the initial agreement layer. When the initial agreement layer is an entire satellite or rocket while minimum agreement layer of FMEA is its components, it is difficult to describe clearly from the component layer. So FMEA designer is recommended to communicate comprehensively with system designer. Moreover, filling out all three layer failure effects with "no effect" is unreasonable, there will always be certain effect on some product layer as long as it is a failure. For some products with redundant design, even if the loss of redundancy cannot affect the final function (mission), loss of redundancy will directly cause the redundancy failure, and effectiveness of redundancy needs to be analyzed.

2.4.3 *Filling in "The failure criticality" arbitrarily*

The criticality is a qualitative description of the consequence of failure mode. Criticality level criteria should be given in advance. It is usually determined by ultimate effect, criticality level should be high corresponding to huge ultimate effect. For example, failure mode of some product can cause ultimate effect "loss of system function", while the criticality is set for "level III" which is not appropriate. For loss of product/system function, it should be at least "level II"criticality due to the severity. Moreover, many designers opine that relevant design measures have been adopted, the criticality should decrease, and that may also cause problems. The level of criticality should be in the condition that the preventive and corrective measures have not been done. If relevant preventive and corrective measures have been taken, the level of criticality in FMEA could decline next round.

2.4.4 *Poor operability of "preventive and corrective measures" and "compensatory measures"*

Preventive and corrective measures are measures that change design and process respects after discovering the failure causes, and compensatory measures means remedial actions after failure happening. Preventive and corrective measures provide design and process changing, while compensatory measures are in operation, maintenance, support even degradation ways. Generally, there could be no preventive and corrective measures, while compensatory measures is needed, corresponding plans against failure should established in serious situation.

2.5 *Informal FMEA worksheet*

FMEA work is an analytical process, while its manifestation is FMEA worksheet. The normalization of FMEA worksheet directly influence the effect of FMEA technology. The following issues should be noticed when filling in FMEA worksheet.

2.5.1 *Incomplete recognition and omission of failure modes*

Incomplete recognition of failure modes usually appears in FMEA work. Except the limited failure information, recognizing design weak points did not follow the unit functions which comprises a product,

recognizing failure modes did not follow different operation modes, and a lack of interface consideration become the main reasons for incomplete recognition of failure modes. In addition, FMEA technology is in a mono factor manner, when analyzing the failure reasons, failure modes that result of multiple reasons are likely to be missing.

For instance, there are two failure modes "cannot open" and "cannot close" of typical valve in carrier rocket. In valve design, "cannot open" is the main concern, so valves in parallel are adopted to solve the problem. However, due to the lack of the consideration to failure mode "cannot close", this failure frequently occurs in practical application. The parallel valves design increases the risk of failure "cannot close", and reduces product reliability.

2.5.2 *Inaccurate statement of "failure cause"*

In FMEA process, inaccurate and indefinite statement of failure cause frequently occurs. For example, failure cause corresponding to failure mode "dynamo conflict" is described as "reducer failure", however, "reducer failure" does not explain what the actual reason of dynamo conflict is. The reason should illustrate how the reducer fails, such as a reducer control software problem, a reducer hardware problem or an environment problem. Such relevant preventive measures can suit the remedy to the case. If it is an operating environment problem, improving environment or environment adaptability should be adopted; if it is a control software problem, work related to enhancing software reliability should be done. FMEA work is an activity that goes into the whys and wherefores, if the failure cause cannot be properly distinguished, we could not put forward appropriate technology improvement measures, so effectiveness of FMEA is doubtful. For this reason, the failure cause should be analyzed carefully instead of superficial and simple failure appearance.

2.5.3 *Insufficient criterion of failure possibility, arbitrary judgment by experience*

Failure possibility is significant composition of qualitative FMEA, which can be divided into A, B, C, D and E five levels. However, this classification is qualitative and not specific enough existing certain arbitrariness, and operability is poor as well. Failure possibility involves information sources, so it is very difficult to determine the possibility, which will influence effectiveness of qualitative FMEA.

2.5.4 *Poor pertinence and operability of measures*

"Preventive and corrective measures" and "failure cause" in some FMEA is not corresponding and a lack of pertinence. "Compensatory measures" and "failure effect" have the problems neither. Some control measures are in a slogan way, such as "enhancing analysis", "strict production procedure control", "strict product acceptance checks" and "enhancing coordinating management", which does no help with design improvement.

3 FMEA EFFECTIVENESS ASSURANCE MEASURES

3.1 *Starting lowest agreement layer with the components, raw material, software and so on*

For improving the effectiveness of FMEA and discovering the weak points of aerospace product development, the lowest agreement layer should begin with fundamental units like components, raw material and software. Because almost every product failure can be located at some specific component, raw material and some software, and the above fundamental units are also a starting point of systematical design related to reliability. Thus, these fundamental units need to be classified and defined together and relevant database should be established. For example, failure modes of electronic components include open circuit, short circuit, appearance damage, loss of function, parameter drifts, structural damage, defective insulation, poor contact and so on.

3.2 *Standardizing FMEA worksheet, straighten corresponding relationships between each section in FMEA*

In order to guarantee the effectiveness of FMEA, we need to master the core technology, and understand corresponding relationships between each FMEA section. Figure 1 shows the correspondence between the various sections. As Figure 1 shown here, the failure mode is closely related to the task and function realization, while failure cause, failure effect and failure detection correspond to the failure mode. Preventive and corrective measures correspond to failure cause and compensatory measures corresponds to failure effect. Local effect, higher layer effect and ultimate effect, each one respectively corresponds to lowest agreement layer, agreement layer and the initial agreement layer. The above correspondences will directly determine the normalization of a FMEA worksheet.

3.3 *Judging the possibility making full use of information to ensure accuracy*

In the early design phase of aerospace products, we usually only consider criticality of the severe failure effects to minimize the risk. If failures are not eliminated in early design phase, preventive and compensatory measures should be determined considering

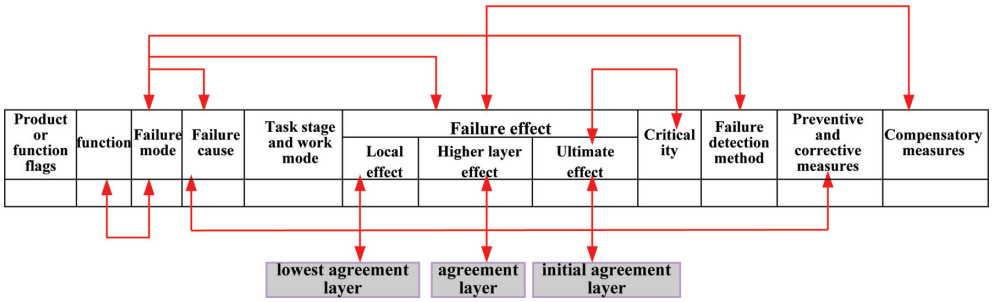


Figure 1. Corresponding relationships between each FMEA section.

the possibility and criticality of failure. Setting possibility level of failure needs to comprehensively consider information from design program itself. The following aspects are usually considered: technology (product) maturity, engineering analysis results (safety factor, degradation), design (product) producibility and testability, history experience of similar design (product), operation condition of adopted technology (product), environmental change and so on, in order to avoid arbitrary judgment.

3.4 *Identifying failure mode and failure cause comprehensively and precisely*

FMEA work should analyze functions according to product consisting of its units, and analyze functions, interfaces and characteristics according to diverse task modes and task stages, in order to conclude failure modes completely. FTA method can also assist in failure cause analysis to ensure comprehensiveness, failure causes can draw from different aspects like "personnel, equipment, material, principle, environment, measurement" as well.

3.5 *Making preventive and corrective measures and compensatory measures operational and effective*

FEMA designers should distinguish the differences between "preventive and corrective measures" and "compensatory measures" to ensure effectiveness. "Preventive and corrective measures" is proposed for recommendation from the design point of view according to design state at present. "Compensatory measures" are required to correspond to failures one by one. If one catastrophic or fatal failure mode is not able to eliminated, designers should explain the reasons to accept the failure modes, including design features, the completed testing, inspection or history information of similar design. Moreover, "preventive and corrective measures" should be highly operable, specific and quantitative to avoid "lie, boast and empty verbiage". "Strict control on productive process" and "strengthen the acceptance checks" are principles, not specific measures.

3.6 *Extending means to acquire failure data, establishing failure information database*

For effectiveness of FMEA, we need a mass of failure data. Through quality problem elimination work and continuously collecting following data, failure information provides FMEA raw material, which reflects unknown weak points of product design, process and testing, etc. Taking one equipment for example, reliability data can reflect functioning condition and performance of the product, once it failed, we can locate the failure quickly through data analysis. Therefore, the foundation of data accumulation is to adequately discover the key features including design, craft and process, and quantifying them with data, then gather certain amount of data by units.

For the problem of incomplete reliability information collection, developers should establish effective ways for reliability data collection, storage and analysis, specify content and management of reliability information data, and solve the problem of a serious shortage of basic reliability data. Data collection related to reliability and safety includes: product development requirements, reliability design analysis, reliability evaluation, safety evaluation, similar product quality problems, and failure elimination.

4 CONCLUSION

This paper studied the concepts and terms of FMEA, FMEA working essence, correspondence between the sections of FMEA, precautions in filling in the worksheet and so on. In addition, we thoroughly analyzed the FMEA work problems in aerospace product development process, and summarized responses and solutions to improve the effectiveness of FMEA. This paper can provide some reference and guidance to effectively carry out FMEA work in aerospace product development.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability modeling method of space mechanism considering dynamical cascading effects

C.L. Tan
Institute of Spacecraft System Engineering, CAST, Beijing, China

J.G. Zhang, P. Wang & L.J. Kan
Science and Technology on Reliability and Environment Engineering Laboratory, Beihang University, Beijing, China

ABSTRACT: As science and technology developed so fast, space mechanisms have become complex electromechanical system. With prominent characters of multi-factor, multi-level and high-dynamic, dynamical cascading reliability problems of space mechanisms have been increasingly complex and cannot match the assumptions of static state, independence and large samples of traditional reliability theory. Based on Discrete Bayesian Networks, this paper establishes dynamical cascading reliability model of space mechanisms with the introduction of dynamic response and clearance. By using hierarchies theory and uncertainty propagation directed graph thought and according to product components of system and its hierarchical relationship, this paper describes dynamical cascading reliability issues of space mechanisms in detail and works the problems that traditional reliability modeling methods cannot accurately describe and estimate results easily. In the last, the proposed reliability modeling method is verified by a two-axis-position mechanism.

1 INTRODUCTION

The assessment and prediction of reliability of space mechanisms are very critical challenges, due to multi-factor, multi-level and high-dynamic (J.Q. Hua, 2011). The reliability problem of space mechanisms have become increasingly complex, dynamical, cascading characters of and cannot match the assumptions of static state, independence and large samples in reliability theory (Joseph Homer Saleh, 2011). Traditionally, the reliability of space mechanisms has been evaluated by testing individual systems and verifying their performance is within some acceptable limits. In order to collect sufficient data, sometimes some limited testing have to be implemented for components or subsystems when full scale testing is not feasible for system under actual work environment. Simulation modeling methods are often available for whole system while the full scale testing for the environment is not feasible. The data of component level is easier and cheaper to obtain compared with the system data, so it is beneficial if establishing individual component and/or subsystem level models and incorporating them into a system level model is possible. Therefore the uncertainty in the system model is relate with the component and/or subsystem level data (Angel Urbina, 2009). Moreover because testing cannot reflect the capability of system under the whole environments, the model must extrapolate beyond the data which was developed from. To improve the confidence of an extrapolated model prediction, sources of uncertainty must be identified, quantified and propagated to the response quantity of interest at the system model (Angel Urbina, 2009).

Currently, many researches focus on developing components and/or subsystems level models using first principles. First building a model based on a sample exploratory experiment, then validating it within a different set of experiment, finally using it in a more complex model (Oberkampf, W.L. 2000) (Sindir, M.M. 1996). For example, in this work, one could reach the component of a two-axis-position mechanical by sample experiments. First a model is established which affects some phenomenon of interest, then its performance is validated under a different use environment, finally it is used as part of a larger system. The method above is defined as a hierarchical approach to building a system level model. It investigates a complex system by developing the models of its components and/or subsystems and couples them together into a full system model (Rebba, R. 2005). Several researches of this hierarchical modeling approach have been done. To improve the precision of the model, multiple tests

of these components must be taken to obtain an estimate of the variability for quantify the uncertainty of the model. But the interactions of these components were never tested. No information on the coupling of components could be available. It may add an extra uncertainty. In addition, the interactions of components could have been tested at excitation levels that arenot comparable to those of the full system. In Ref. (Urbina, A. 2006), the information available at the different levels was not used to augment the knowledge about the model of a component in a different configuration. This data was merely used to assess the model's predictive capability for the intended work environment (U.S. Department of Energy, 2000, AIAA, 1998) (i.e. model validation). By using Bayesian updating techniques and Bayesian networks, it is possible to incorporate the available data, updating the model parameters and the model predictions consequently, to reflect the new information that was previously not available for any individual level of complexity. This methodology has been explored in Ref. (Rebba, R. 2005,) for a system where one is the application domain of interest and for one component. Our paper extends that work to dynamic coupling and cascading of complexity and to a multicomponent problem and it adds the additional complications of working with actual experimental data and complex dynamics simulation models.

In this work, the aim is to quantify and propagate uncertainty to eventually use it to evaluate the confidence in the extrapolated dynamic coupling response of a prediction of a full system model. To demonstrate the reliability methodologies developed in this work, a problem developed at a two axis position mechanical is used. The following section gives a brief description of a Bayesian Network (DBN) to uncertainty quantification and its implementation to the selected problem.

2 BAYESIAN NETWORKS

A Bayesian Network (BN) (E. Zio 2009) as a probability-based knowledge representation method is appropriate for the modeling of causal processes with uncertainty. The BN is composed of nodes (variables) and arcs linking the nodes. It is a Directed Acyclic Graph (DAG) whose nodes represent random variables and links define probabilistic dependencies between variables. When the node obtain the available data (or evidence), the instantiation of that node occurs. Note that the amount or quality of the data is not required. That means the available data in this research is assumed as representative of the phenomenon observed and what is being modeled. By the Ref (Jensen, Finn V., 2001), the heart of Bayesian network is building the relationship between each variable involved in the model. These relationships are quantified by associating a conditional probability table with each node, given any possible configuration of values for its parents.

In this paper, a BN (Jensen, Finn V, 2001) is employed to represent the system structure of space mechanisms. A general BN consists of nodes, and directed arcs between some nodes (Li J, Wilson AG, 2007). Each node X_i is a response with random variable. If there is a directed arc from X_i to X_j, X_i is called a "parent" of X_j. There may be no or more than one parents for each node. An arc characterizes the probabilistic dependency of a node on its parent nodes. That is, depending on the values a node's parents take on, the conditional probability distribution of the node may be different. In this paper, a BN is employed to represent the cause-and-effect failure relationship among elements of space mechanisms, in which nodes are components responses of the space mechanisms. Since components are at different levels, a slightly different notation is adopted for nodes.

Furthermore, arcs in the BN representation of space mechanisms have some new interpretations. Specifically, arcs between nodes at the same level represent intra-level cascading failures; arcs between nodes at different levels represent inter-level failure relationship, e.g., how the failure of sub-systems affect the failure of the system (Mingyang Li, 2014).

We assume that a typical BN graph where nodes X represent the responses of different components in each subsystem (Mingyang Li, 2014). The BN model is a way to model probability distribution function on the sequence of N discrete responses $X = \{X_0, X_1, \ldots, X_n\}$ and the sequence of discrete observables $Y = \{Y_1, Y_2, \ldots, Y_N\}$ that has the following factorization, which satisfies the requirements for BNs that:

$$P(X_i) = \prod_{i=1}^{N} P(X_i | Pa(X_i)) \tag{1}$$

where, X_i is the ith node and $Pa(X_i)$ are the parents of X_i in the graph with same levels and different levels. $P(X_i|Pa(X_i))$ is the response probability density function (pdf). The network also facilitates the inclusion of new nodes that represent the observed data and thus the updated densities can be obtained for all the nodes. The joint probability density function for the network of the BN with the observation pdf $P(Y_i|X_i)$ can be updated using Bayes theorem when data is available. The expression for Bayes theorem is

$$f_\theta(\theta|Y) = \frac{f_\theta(\theta) f_\theta(Y|X(\theta))}{\int f_\theta(\theta) f_\theta(Y|X(\theta)) d\theta} \tag{2}$$

Several inference methods for a discrete-state and time BN can be used. The integration in the denominator of Equation 2 can be conveniently done using Markov Chain Monte Carlo techniques (Gilks, G.R., Richardson, S,1996). The marginal pdf of any node in the BN can be obtained by the integration of the joint pdf over all the values of the remaining variables. Thus the Bayes network approach offers a rational and effective methodology to extrapolate inferences from component level information to the system level. With this background now we look at the specific implementation of the Discrete BN (DBN) to the example problem (two-axis-position mechanism).

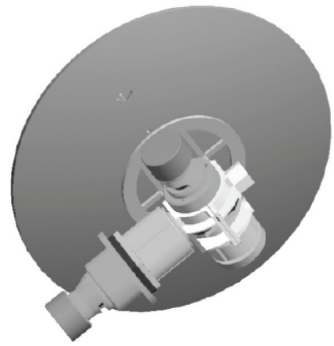


Figure 1. Two-axis-position mechanism.

3 MARKOV CHAIN MONTE CARLO (MCMC) SIMULATION

Even if the expression of posterior distribution is available as a product of likelihood and prior, the shape of distribution can only be estimated by calculating its values at different points (Dawn An., 2011). A traditional way is to compute the values of PDF at nodes after identifying the effective range and to calculate the value of the posterior distribution at each node. This method, however, has several drawbacks, such as the difficulty in selecting the location, spacing, and scale of the points (Dawn An., 2011). In addition, it becomes computationally expensive when the number of updating parameters increases. MCMC simulation is a computationally effective choice which generates a chain of samples to plot the PDF (C. Andrieu., 2003). The Metropolis–Hastings (M–H) algorithm is a common choice for MCMC simulation; Since the MCMC method is a sampling-based one, it has to include enough samples so that the statistical characteristics of the distribution can be well captured. There are some methods available to determine the convergence condition, such as El Adlouniet al. (S. El Adlouni., 2006) and Plummer et al. (M. Plummer 2006).

4 SPACE MECHANISMS RELIABILITY PROBLEM

4.1 *Problem state*

A two-axis-position mechanism of satellite antenna (shown as Fig. 1) is a typical spatial mechanism as a key component that performs two degrees of freedom movement to realize the accurate positioning, posture alignment and tracking of the satellite antenna. The reliability of this mechanism correlates with mission success (Huibo Zhang 2012). It mainly consists of rack, longitudinal shaft and cross shaft. The longitudinal shaft and the cross shaft use the same driving assembly and structure both composed by stepping motor, harmonic reducer and angular transducer. The stepping motor has a redundancy backup. The angular transducer adopts photoelectric encoder and micro-switch. The rack assembly consists of support to assemble components, support between shafts and support to assemble antenna.

It mainly consists of longitudinal shaft and cross shaft. The longitudinal shaft and the cross shaft use the same driving assembly and structure both composed by stepping motor, harmonic reducer and angular transducer. The stepping motor has a redundancy backup. The angular transducer adopts photoelectric encoder and micro-switch. The rack assembly consists of support to assemble components, support between shafts and support to assemble antenna. The constitutional diagram of system structure is shown as Figure 2.

The clearance leads to impact and contact and affected the dynamic characteristic and pointing accuracy of the two-axis-position mechanism. With the enlargement of clearance, the error of velocity and acceleration increased and it leads to descent of reliability. The problem has the following features:

1. It is a multi-component problem where one branch of the problem involves a longitudinal shaft and the other is a type of e cross shaft. Both have clearance wear.
2. It is a multi-level problem where the phenomena observed at the lowest level is assumed to be present at subsequent levels.
3. It is a dynamic problem where the response is changing all the time and the clearance becomes larger because of wear.
4. The individual component branches converge to a system level mechanism where the two couple together. The interaction of the two physics is a potential source of uncertainty since this had not been tested previously.

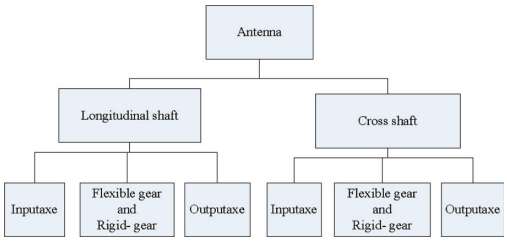


Figure 2. The constitutional diagram of system structure.

5. Experimental data consists of repeated tests on several, nominally identical mechanisms. These are intended to quantify the variability inherent in a physical system. Virtual prototype models (see Fig. 3) are built and calibrated to simulate a particular behavior of the mechanism. The model parameters have been calibrated from simple, discovery experiments aimed at isolating the particular physical phenomenon that the model is trying to represent.
6. In general, there are some correspondences between the subsystem and system that was tested at the various levels.

This paper proposed a dynamic reliability modeling method of DBN, in order to find out the solutions of comprehensive system reliability modeling issues such as the above problems with discrete responses. Using this method to build reliability models of complex mechanical systems can reduce complexity.

4.2 *Data descriptions*

1. Material Parameter Characterization

Elastic Modulus: The first step in the process is to characterize the material model that describes the behavior of axes, flexible gear and rigid gear and also to quantify the variability in the material. Through physical measurements, tension/compression and torsional experiments, the material density, elastic and shear moduli were obtained calibrating to represent the dynamic behavior of them at room temperature. Using the data obtained from these samples and from these tests, a probabilistic description of the randomness of them was obtained and subsequently used in more complex system. More specifically, for these components, the elastic modulus is treated as random variable.

Clearance: With the enlargement of clearance, the error of velocity and acceleration increased and it leads to descent of reliability. Through physical measurements, the clearances of four components (input & output axes, flexible gear & rigid—gear) were obtained at room temperature. Using the data

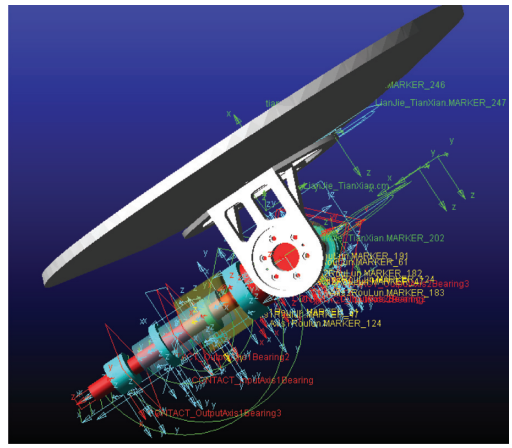


Figure 3. Virtual prototype model of two-axes-position mechanism.

obtained from these samples and from these tests, a probabilistic description of the randomness of was obtained and subsequently used in two-axes-position mechanism. More specifically, for these components, the clearance is treated as random variable.

2. Component Level/Subsystem Level

20 test samples were constructed and modal tests were conducted at component level (input & output axis, flexible gear & rigid gear). (A modal test is one in which the preferred rotating speed and torque are estimated.)

Test samples were constructed and modal testing was performed at subsystem level (longitudinal shaft & cross shaft). Material density was measured and clearance, contact forces and modulus of elasticity was calculated for each test case at both levels.

Modal frequencies of the deformation were obtained for each experiment at each level.

3. System Level

The final step in the process merges the two parallel paths (longitudinal shaft and cross shaft) into a single system. For this project, the physical system of interest simulates a two-axes-position mechanism. Each of the systems was assembled, disassembled and re-assembled and tested ten times so that a hundred tests were performed. With these test, unit to unit and test to test variability was quantified. Base rotating speed was controlled; components rotating speed and torques responses were measured at many locations.

4.3 *Discrete Bayes network*

To begin, let's construct the Bayes Network (BN) for the dynamic cascading reliability problem of two-axes-position mechanism. Considering the

discrete dynamic responses, the BN is shown in Figure 4.

The definition of the nodes in the Bayes network shown in Figure 4 is given below:

$\theta_{1\&2}{}^{f} = [E, H]$—Flexible gear parameters. The elastic modulus and gear depth.

$\theta_{1\&2}{}^{r} = [K, d]$—Rigid gear parameters, stiffness coefficient and gear diameter.

$\theta_{1\&2}{}^{w} = [F]$—Input-axe parameters, the rotating speed.

$X_{M1\&2}^{f\&r} = g\left(\theta_{1\&2}{}^{f\&r}\right)$—Function evaluation: modal rotating speed and torque from (1) component and (2) subsystem level model simulations. This takes the form of $g(\theta_{1\&2}{}^{f\&r})$ which is either a finite element model or dynamics simulation representation relating the modal of rotating speed and torque.

$X_{v1\&2}^{w} = g(\theta_{1\&2}{}^{w})$—Function evaluation: modal rotating speed and torque from input-axe. This takes the form of $g(\theta_{1\&2}{}^{f\&r})$ which is either a finite element model or dynamics simulation representation relating the modal of rotating speed and torque.

$X_{s1\&2}$—Function evaluation: modal rotating speed and torque from output-axe.

X_A—Function evaluation: modal rotating speed and torque from an antenna.

$Y_{M1\&2}^{f\&r}$—Experimental data: from (1) component and (2) subsystem level experiments.

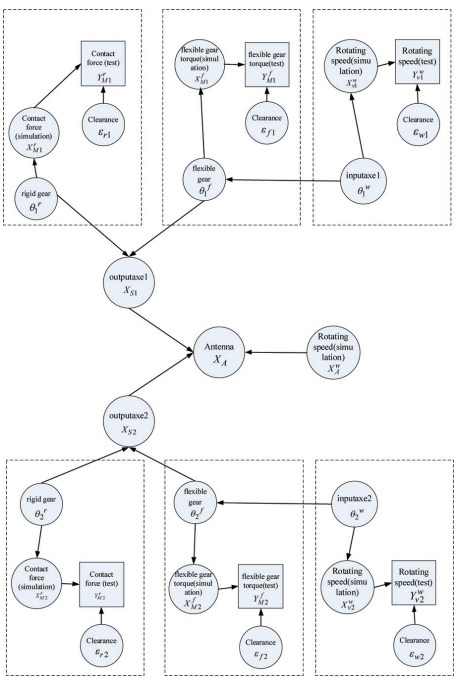


Figure 4. The BN of two-axis-position mechanism.

Y_v^w—Experimental data: from (1) component and (2) subsystem level experiments.

$\varepsilon^f, \varepsilon^r, \varepsilon^w$—The clearances of different components which are calculated by contact forces and experiments.

4.4 *Analysis result*

For the components used at each of the levels, a detailed finite element model and dynamics model were build (see Fig. 3) and it is used as the basis for training individual GP (Gaussian process) models. There is a significant amount of computation needed when performing a Bayesian updating so a fast function evaluation is highly desirable. Some selected results of the BN implementation are shown below. For the estimation of probability density functions, 10,000 samples were used. These were in addition to 20,000 samples used as burn-in samples to allow the Markov chain to become stationary.

The resulting pdf sets of parameters (partial) are shown as following (Figs. 5–7).

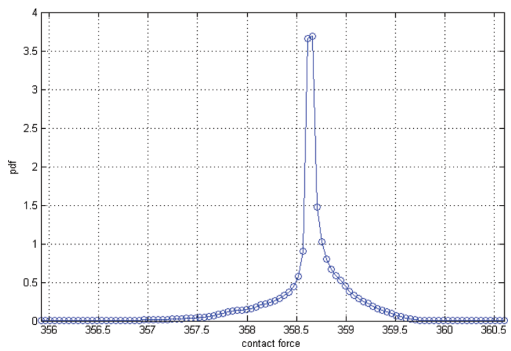


Figure 5. Rigid gear contact force.

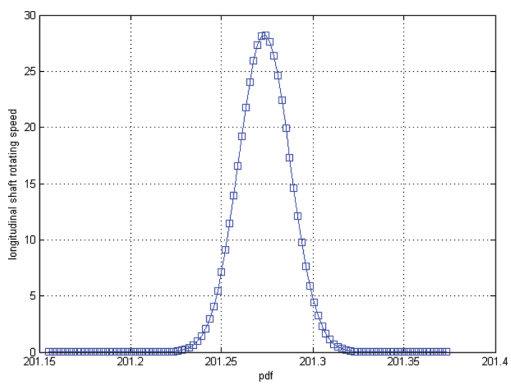


Figure 6. Longitudinal shaft rotating speed.

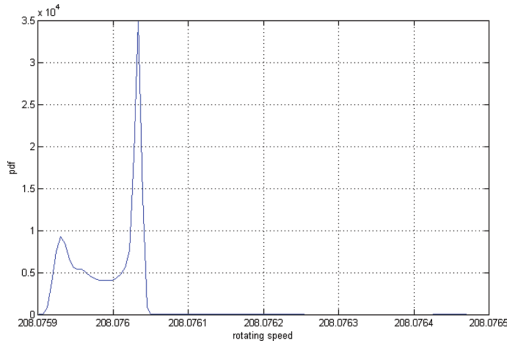


Figure 7. Antenna rotating speed ($0.01°/s$).

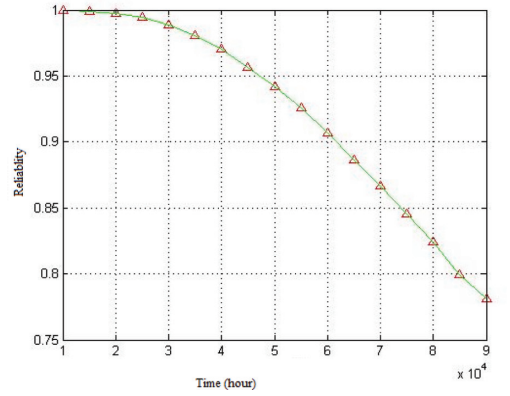


Figure 8. Time-dynamic reliability curve.

In this context the calculation of the probability of failure (or the probability of exceeding a given threshold $2.09^0/s$) needs to be performed using the results obtained from the Bayes network which results from the inclusion of uncertainty as shown in the previous section. We can obtain that the reliability of the two-axes-position mechanism is 0.9963 by MC (Monte Carlo) method at the primary clearance.

Considering the clearances in the different components become larger by the contact forces when the system is working, the reliability will decline by time changing. At last, we discrete the clearances by unit time and use the discrete Bayes network to calculate the reliability at each time with MATLAB programming. The reliability of the two-axes-position mechanism is varying as shown in Figure 8.

5 CONCLUSION

Based on Discrete Bayesian Networks, this paper establishes the dynamical cascading reliability model of space mechanisms with the introduction of dynamic response and clearance.

Using this method to build reliability models of complex mechanical systems can reduce complexity and solve the limit samples problem. It can also effectively reflect the dynamic characteristic of reliability, the feature of multiple failure modes and reliability logical relationships between different system levels of complex mechanical systems, which provides a good foundation for the future reliability design and analysis.

By using hierarchies theory and uncertainty propagation directed graph thought and according to product components of system and its hierarchical relation, this paper describes dynamical cascading reliability issues of space mechanisms in detail and works the problems that traditional reliability modeling methods cannot accurately describe and estimate these issues easily.

This work is supported by Space Mechanisms Reliability and its Dynamics and System Control, National Basic Research Program of China (2013CB733000).

REFERENCES

AIAA, 1998. Guide for the Verification and Validation of Computational Fluid Dynamic Simulations, American Institute of Aeronautics and Astronautics, AIAA-G-077-1998, Reston, VA.

Ang AH-S, Tang WH., 1975. Probability concepts in engineering planning and design, vol. I-basic principles. NewYork, NY: JohnWiley and Sons.

Angel Urbina, Sankaran Mahadevan, Thomas L. Paez., 2011. Quantification of margins and uncertainties of complex systems in the presence of aleatoric and epistemic uncertainty [J]. Reliability Engineering and System Safety 1114–1125.

Angel Urbina, Sankaran Mahadevan., 2009. Uncertainty Quantification in Hierarchical Development of Computational Models. 50th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 17th 4–7 May, Palm Springs, California.

C. Andrieu, N. de Freitas, A. Doucet, M. Jordan, 2003. An introduction to MCMC for machine learning, *Machine Learning*, 50, 5–43.

Dawn An, Joo-Ho Choi, Tony L. Schmitz, Nam H. Kim, 2011. In situ monitoring and prediction of progressive joint wear using Bayesian statistics. Wear 270: 828–838.

E. Zio., 2009. Reliability engineering: Old problems and new challenges [J]. Reliability Engineering and System Safety, 125–141.

Gilks, G.R., Richardson, S., Spiegelhalter, D.J., 1996. Markov Chain Monte Carlo in Practice, Interdisciplinary Statistics, Chapman & Hall/CRC, London.

Huibo Zhang, Jun Chen, Dong Pan, Xinggui Wang, Chunlin Tan., 2012. Research on Dynamic Characteristic of Two-Axes-Position Mechanism for Satellite Antenna with Joint Clearance, *Journal of Astronautics*, (Jan.).Vol. 33, No. 1, pp. 33–39.

Jensen, Finn V., 2001. Bayesian Networks and decision graphs, Springer-Verlag, New York.

Jinqiu Hu, Laibin Zhang, Lin Ma, Wei Liang., 2011. An integrated safety prognosis model for complex system based on dynamic Bayesian network and ant colony algorithm Expert Systems with Applications, 1431–1446.

Landes, R.D., Loutzenhiser, P.G. and Vardeman, S.B., 2006. Hierarchical Bayesian Statistical Analysis for a Calibration Experiment, IEEE Transactions on Instrumentation and Measurement, Vol. 55, No. 6, pp. 2165–2171.

Li J, Shi J., 2007. Knowledge discovery from observational data for process control using causal Bayesian networks. IIE Trans, 39(6):681–690.

M. Plummer, N. Best, K. Cowles, K. Vines, 2006. CODA: convergence diagnosis and output analysis for MCMC, R News, 6 (1): 7–11.

Mingyang Li, Jian Liu, Jing Li, Byoung Uk Kim., 2014. Bayesian modeling of multi-state hierarchical systems with multi-level information aggregation Reliability Engineering and System Safety, 158–164.

Oberkampf, W.L. and Trucano, T.G., 2000. Validation Methodology in Computational Fluid Dynamics, SAND 2000-1656C, Sandia National Laboratories, Albuquerque, NM.

Rebba, R., 2005. Model Validation And Design Under Uncertainty, Vanderbilt University, Nashville, TN.

S. El Adlouni, A.C. Favre, B. Bobe, 2006. Comparison of methodologies to assess the convergence of Markov Chain Monte Carlo methods, Computational Statistics & Data Analysis 50(10): 2685–2701.

Saleh J.H., Castet J-F., 2011. Spacecraft reliability and multi-state failures [M], Georgia Institute of Technology USA.

Sindir, M.M., Barson, S.L., Chan, D.C., Lin, W.H., 1996. On the Development and Demonstration of a Code Validation Process for Industrial Applications. American Institute of Aeronautics and Astronautics, AIAA Paper No. 96-2032, 27th AIAA Fluid Dynamics Conf., New Orleans, LA.

U.S. Department of Energy, 2000. Advanced Simulation and Computing (ASCI) Program Plan. 01-ASCI-Prog-01, Sandia National Laboratories, Albuquerque, New Mexico.

Urbina, A., Paez, T.L., Gregory, D., Resor, B., Hinnerichs, T.D. and O'Gorman, C.C., 2006. Validation of a Combined Non-Linear Joint and Viscoelastic Encapsulating Foam. Proceedings of the 2006 Society for Experimental Mechanics, St. Louis, MO.

Urbina, A., Paez, T.L., Gregory, D., Resor, B., Hinnerichs, T.D. O'Gorman, C.C., 2006. Validation of a Combined Non-Linear Joint and Viscoelastic Encapsulating Foam. Proceedings of the 2006 Society for Experimental Mechanics, St. Louis, MO.

Wilson AG., Huzurbazar AV., 2007. Bayesian networks for multi level system reliability. *Reliab Eng Syst Saf*, 92(10): 1413–420.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparative analysis of calculation methods of pressure drops for two-phase flow through pipelines

G. Boccardi & R. Trinchieri
Laboratory of Thermal Fluid-Dynamics Applied to Energy Systems, ENEA, Rome, Italy

R. Bubbico & B. Mazzarotta
Department of Chemical Engineering, Materials and Environment, "Sapienza" University, Rome, Italy

ABSTRACT: Despite the importance of an adequate and correct sizing of emergency relief systems, a high level of uncertainty is still present when two-phase liquid-vapor flow can establish. In such a case, no single correlation is presently generally applicable to calculate the pressure drop through a relief pipeline in a wide range of relief conditions. In the present paper a large number of new experimental data have been produced and compared with two of the most widely known and adopted calculation methods: the Friedel model and the classical Lockhart-Martinelli model. They belong to either of the two main groups of prediction models, the homogeneous and non-homogeneous models. The results provide useful insights in their accuracy and range of applicability, and are expected to be of help in the correct sizing of these fundamental safety systems.

1 INTRODUCTION

Proper sizing of relief systems is of the utmost importance both in the protection of process equipment and in the prevention of serious accidents possibly involving people and structures within or outside the plant. Reliable equations are available for single-phase flow through relief devices (safety valves, rupture disks, etc.), headers and other discharge system elements. However, when two-phase flow is possible, no single and reliable calculation method is available, but a number of procedures have been proposed in the literature over the years (see for example CCPS 1998, Fauske 1999, Fisher et al. 1992, Kim & O'Neal 1995, Leung 1996). This is because of the complex phenomena occurring between the two phases during release and of the interactions among the many parameters involved, which are difficult to be mathematically represented. With specific reference to relief devices (mainly safety valves) many analyses have been presented in the recent years with the aim of identifying the most proper models to be applied, at least for a given range of variability of the parameters (Boccardi et al. 2005, 2008, 2010, Darby 2004, Diener & Schmidt 2004, Leung 2004). As a result of this effort, despite the high level of uncertainty still present, the number of models applicable to safety valves is relatively low, and some flexible and enough reliable methodologies have been finally published (ISO, 2008). Along with the particular relief devices adopted, relief headers and pipelines also represent fundamental items of the whole relief system, and, differently from the case of valves, here the situation is even worse: in fact, depending on the particular operating conditions, different flow patterns can establish which can significantly affect the flow characteristics and, in particular, the connected pressure losses. At the same time, an accurate evaluation of the pressure drop along the discharge system is important also for a proper selection and sizing of the relief device itself.

The total pressure difference between two sections along a given pipeline, is given by three different terms:

$$\Delta P_{tot} = \Delta P_{acc} + \Delta P_h + \Delta P_{fr} \tag{1}$$

where ΔP_{acc} is the acceleration term, associated with a velocity variation, ΔP_h is linked to a height variation, and ΔP_{fr} represents the friction losses.

The acceleration term can be written as

$$\Delta P_{acc} = G_s^2 \left(v_{out} - v_{in} \right) \tag{2}$$

where G_s = specific mass flow rate, v_{out} and v_{in} the outlet and inlet specific volumes, respectively.

For horizontal pipes, the elevation term is zero. The calculation method for the friction term preliminarily depends on the type of flow elements, whether straight lengths of pipes, fittings (valves,

elbows, joints, etc.), or cross-section variations (restrictions, pipe entrances and exits and so on). Furthermore, in the case of two-phase flow, some models assume that the friction losses also depend on the specific flow pattern established.

Based on Equation 1, for horizontal pipes, the total pressure drop can be calculated by quantifying ΔP_{acc} and ΔP_{fr}. However, as can be seen from Equation (2), ΔP_{acc} depends on the pressure profile established along the flow, through v_{out} and therefore an iterative procedure is required. Furthermore, the evaluation of ΔP_{fr} is affected by a high level of uncertainty, and this makes the total pressure loss prediction quite complex.

In the present paper, an experimental rig has been adopted to measure the pressure profile along a relief header, including both straight pipe lengths and fittings. The acceleration term has thus been directly calculated from Equation 2, and the resulting friction term, derived from Equation 1, has been compared with some of the most common calculation methods.

2 CALCULATION OF PRESSURE DROP ALONG PIPELINES

Due to the complexities in the mathematical representation of the flow of a two-phase liquid-vapor mixture, different simplifying hypotheses are often introduced, giving rise to a number of different models. A preliminary distinction can be made between models assuming or neglecting the slip between the two phases. This is an important issue because, depending on the assumption adopted, the specific volume of the mixture has to be calculated with different expressions, i.e.:

$$v_m = x^2 \frac{v_g}{\varepsilon} + (1-x)^2 \frac{v_l}{(1-\varepsilon)} \tag{3}$$

$$v_h = x \cdot v_g + (1-x) \cdot v_l \tag{4}$$

respectively with or without slip, where g and l are the subscripts for vapor and liquid, x is the vapor quality of the mixture, ε the vapor hold-up, v_h the homogeneous specific volume and v_m the momentum specific volume in the presence of slip.

In the present paper, the experimental data will be compared with two models, one for each of the above categories, i.e.: the Lockhart & Martinelli (1949) model (with slip) and the Friedel (1979) model (homogeneous).

2.1 *The Lockhart and Martinelli model (1949)*

The model by Lockhart and Martinelli is widely known since long and therefore it will be recalled very briefly here.

Since it takes into account the slip between the two phases, the average specific volume has to be calculated by Equation 3.

By this simple model, the two-phase pressure drops are calculated as a function of the pressure drops generated by one of the single phases, assumed as flowing alone,

$$(dP/dL)_{fr} = \frac{2 \cdot f \cdot G_s^2}{\rho \cdot d} \tag{5}$$

corrected by a proper multiplier

$$\left[(dP/dL)_{fr}\right]_{2p} = \phi_l^2 \cdot \left[(dP/dL)_{fr}\right]_l = \phi_g^2 \cdot \left[(dP/dL)_{fr}\right]_g \tag{6}$$

In the above equations f = friction factor, G_s = specific mass flow rate, ρ = density, d = pipe diameter.

The multiplier ϕ to be introduced in Equation 6 depends on the specific single phase adopted and can be derived from graphs and correlations as a function of the Martinelli parameter X^2, defined as

$$X^2 = \frac{\left[(dP/dL)_{fr}\right]_l}{\left[(dP/dL)_{fr}\right]_g} \tag{7}$$

2.2 *Friedel model (1979)*

The equation proposed by Friedel has been derived by correlating about 25000 data obtained on a number of two-phase systems (water-steam, water-air, oil-air, and so on):

$$\frac{\left[(dP/dL)_{fr}\right]_l}{\left[(dP/dL)_{fr}\right]_g} = (1-x)^2 + x^2 \cdot \left(\frac{\rho_l \cdot \zeta_g}{\rho_g \cdot \zeta_l}\right) + 3.21 \cdot x^{0.78} \cdot (1-x)^{0.224} \cdot \left(\frac{\rho_l}{\rho_g}\right)^{0.91} \cdot \left(\frac{\mu_g}{\mu_l}\right)^{0.19} \cdot \left(1 - \frac{\mu_g}{\mu_l}\right)^{0.7} \cdot Fr_{tf}^{-0.0454} \cdot We_{tf}^{-0.035} \tag{8}$$

with

$$\left[(dP/dL)_{fr}\right]_l = \frac{\zeta_l \cdot G_s^2}{2 \cdot d \cdot \rho_l} \tag{9}$$

where

$$\zeta_j = 64/\mathrm{Re}_j \tag{10}$$

for Re < 1055

$$\zeta_j = \left[0.86859 \cdot \ln\left(\frac{\mathrm{Re}_j}{1.964 \cdot \ln(\mathrm{Re}_j) - 3.8215}\right)\right]^{-2} \tag{11}$$

for Re > 1055
and the non-dimensional numbers are, as usual,

$$\mathrm{Re}_j = \frac{G_s \cdot d}{\mu_j} \tag{12}$$

$$Fr_{tf} = \frac{G_s^2}{g \cdot d \cdot \rho_h^2} \tag{13}$$

$$We_{tf} = \frac{G_s^2 \cdot d}{\sigma \cdot \rho_h} \tag{14}$$

Since this model assumes a homogeneous flow for the two phases, the homogeneous two-phase density, ρ_h, is calculated from Equation 4.

3 PRESSURE DROPS THROUGH FITTINGS

The additional elements possibly present along a given pipeline can be widely variable: bends (elbows) and other directional variations, connections like tees and others, cross-sectional area variations (restrictions, enlargements), joints (welds, flanges, others), orifices, nozzles, sensors for instrumentation, all different kinds of valves, and many others. All these elements introduce a pressure loss to the flowing fluid, which is not easy to predict because of both the extreme variability of those elements, and the difficulties in the mathematical representation of the flow characteristics through them.

As a consequence, different approaches have been proposed in the literature over the years. One of the most widely adopted methodologies, makes use of the so-called "pipe length equivalent", which is characteristic for each specific pipe element. This parameter represents the length of a straight section of pipe (with the same characteristics of the fitting, in terms of diameter, roughness, etc.) giving rise to a pressure loss *equivalent* to that introduced by the fitting itself. This length, which can be usually derived from a number of data bases and references (Perry et al. 1997, Crane Co. 1969), is typically obtained for single-phase flow, and no specific information is available for two-phase flow. In order to check the applicability and accuracy of this methodology, the equivalent length of the first elbow of the experimentation circuit has been determined by running various tests under different operating conditions (pressure and flow-rate) with all-liquid flow: a 0.55 cm equivalent length has been thus calculated. Subsequently, the length of straight sections of pipe giving rise, under two-phase flow, to the same pressure drops measured across the elbow under the same conditions, have been derived, with varying operating conditions. The resulting two-phase equivalent lengths, as a function of the Reynolds number, are reported in Figure 1.

The Reynolds number has been calculated as

$$\mathrm{Re} = \rho_{tp} U D / \mu_{tp} \tag{15}$$

where the two-phase density ρ_{tp} and viscosity μ_{tp} have been calculated as weighted averages of the corresponding single phase values by means of the vapor quality. The inlet velocity has been calculated as:

$$U = \left[G_l\left(\frac{1}{\rho_l}\right) + G_v\left(\frac{1}{\rho_v}\right)\right] \Big/ A \tag{16}$$

where A is the cross-sectional area of the pipe (of diameter D), and $G_{l/v}$ the specific flow-rate of the liquid and vapor, respectively.

It can be seen that for Re > 10^6 the average value of the equivalent length corresponds fairly well to the value obtained for only-liquid flow. However, for Re < 10^6, a marked deviation if found. Furthermore, as reported in Figure 1, all the runs corresponding to vapor qualities higher than 8% fall in the area Re > 10^6 somehow suggesting that, under these conditions, the behavior of the mixture is close to a homogeneous flow,

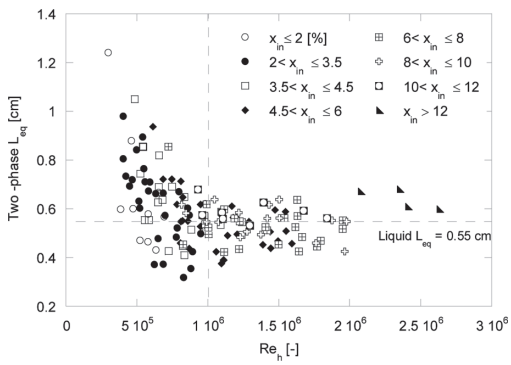


Figure 1. The equivalent length as a function of the Reynolds number, obtained from two-phase flow experiments.

as already reported in previous analyses (Fisher et al. 1992).

In the present investigation, this methodology has been applied to check the accuracy of the Lockhart-Martinelli and Friedel models also used for the straight sections. The acceleration terms have been calculated as explained in the previous section.

4 THE EXPERIMENTAL SETUP

A general view of the experimental rig adopted in the present investigation is reported in Figure 2.

The main components of the facility were:

- a volumetric pump;
- a recovery heat exchanger;
- an electric boiler;
- a control valve;
- a heat exchanger connected to an external cooling system;
- a pressurizing system.

The volumetric pump provided a fixed flow-rate independent of other test conditions, while the inlet pressure could be varied and controlled by means of the pressurizing system and the control valve downstream of the test section.

This latter consisted of a horizontal straight pipe, 2.3 m long and with 10 mm internal diameter, including one 90° elbow at each end (see Fig. 3); along that section the pressure was recorded in a number of locations (manometers from PS 3 to PS 10).

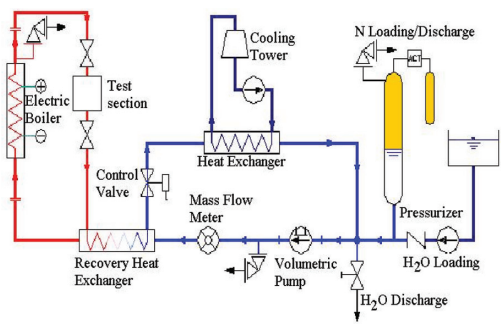


Figure 2. The experimental rig.

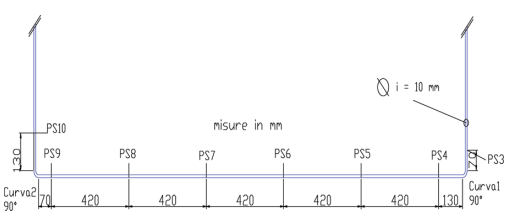


Figure 3. The test section.

Table 1. Parameters variability range.

	Straight line	Elbows
Parameter	Range	Range
Inlet pressure (bar)	3.4–17.6	4.0–17.7
Vapor quality (%)	0.1–15.4	0.1–13.3
Flow rate (kg/s)	0.083–0.35	0.083–0.35

The inlet vapour quality was controlled by varying the power input provided at the electric boiler. Since the pump did not withstand temperatures higher than 50°C, an external cooling system was required, but, in order to reduce the power consumption at the electric boiler ahead of the test section, an internal heat-recovery system has also been used, consisting of two plate-and-frame heat exchangers.

The closed loop of the facility allowed the test conditions to be maintained without time restrictions, making the measurements more stable.

By independently varying mass flow rate, inlet pressure and vapour quality, a total of 3285 effective measurements were obtained (those comparable with the instruments error were disregarded). The resulting ranges of variability of the main operating parameters, both for the straight line and for the elbows are reported in the following Table 1.

5 RESULTS AND DISCUSSION

In order to assess the level of accuracy of the models investigated and to allow their direct and immediate comparison, besides the raw data reported in the following figures, some synthetic statistical parameters have also been adopted and calculated.

The first parameter of interest is the Root Mean Square (RMS) of the relative (percentage) differences (sometimes also called *residuals*) between the calculated and the measured pressure drops with respect to the measured value (Δ_i):

$$\mathrm{RMS} = \sqrt{\frac{\sum (\Delta_i)^2}{N-1}} \tag{17}$$

where N is the total number of measurements. This parameter directly provides the magnitude of the average absolute error and therefore represents a measure of the level of accuracy of the model.

A further parameter is the standard deviation of the relative error with respect to the mean error (Δ_{av}):

$$\sigma = \sqrt{\frac{\sum \left(\Delta_i - \Delta_{av}\right)^2}{N-1}} \tag{18}$$

This parameter represents the spread of the errors with respect to the average error. It can be observed that when the average error tends to zero, RMS and σ tend to be identical. Therefore, the better the model, the lower and the closer the values of RMS and σ; conversely, high and quite different values of RMS and σ denote an inaccurate model with wide spread of the predictions.

5.1 *Models comparison for straight pipes*

In the case of the homogeneous (no slip) Friedel model, the acceleration term of the total pressure variation between two pipe cross-sections can be directly calculated from Equation 2, with the homogeneous specific volume estimated from Equation 4. This allows the direct calculation of the friction loss by Equation 1.

In Figure 4, the pressure drop per unit length (bar/m) due to friction losses calculated with the Friedel model is reported against the experimental values relative to the same pipe sections. In order to check the possible influence of some other parameters involved in the flow, the vapor quality at the entrance of each section has been classified in a discrete number of intervals, and the measurements belonging to each class have been reported with different marks in the figure (see attached key). It can be seen that no significant effect is associated with the vapor quality.

As far as the statistical parameters are taken into consideration, their values (RMS = 16.6% and σ = 16.5%) denote a quite good capability of the model in predicting the friction losses.

Despite the Friedel model is considered a general one, independent of the flow pattern, in order to assess its possible influence, the flow pattern has been characterized for all the runs. The flow pattern map proposed by Moreno-Quiben & Thome (2007) has been adopted, and it was found that, based on that classification, the flow pattern in all the runs could be associated with either the *intermittent* or *dispersed bubble* regimes. In Figure 5, the ratio between the calculated and experimental data is reported, as a function of the vapor quality, with the flow pattern as a parameter.

The pressure drops reported in Figure 5 refer to the whole straight portion of the pipeline (i.e. between manometers P4 and P9 in Fig. 3).

It can be seen that, in comparison with the dispersed bubble flow regime, the intermittent pattern is characterized by a larger deviation from the optimum condition ($\Delta p_c/\Delta p_{exp}$ = 1), as well as by a larger dispersion of the data. And, for both regimes, this is particularly true for lower values of the vapor quality. Furthermore, as already found from Figure 4, a decrease of the ratio is observed at increasing values of x, with a tendency toward underestimation.

In Figure 6, the pressure drop calculated by means of the Lockhart-Martinelli model is reported against the experimental measures. Again, a classification of the data, based on the inlet vapor quality x is also reported.

Based on the synthetic information provided by the statistical parameters, it can be observed that this model is less accurate than the Friedel one in the representation of the pressure drop by friction (RMS 25 and 16.6%, respectively). A larger

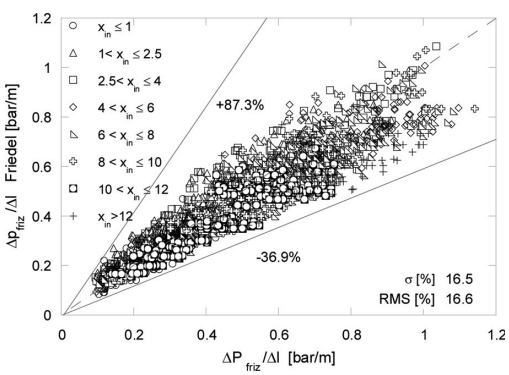


Figure 4. Pressure drop in straight pipes. Comparison between Friedel model's predictions and experimental data.

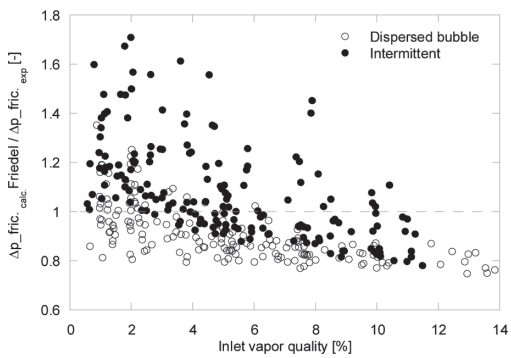


Figure 5. Friedel: $\Delta p_c/\Delta p_{exp}$ as a function of the vapor quality and for the different flow patterns.

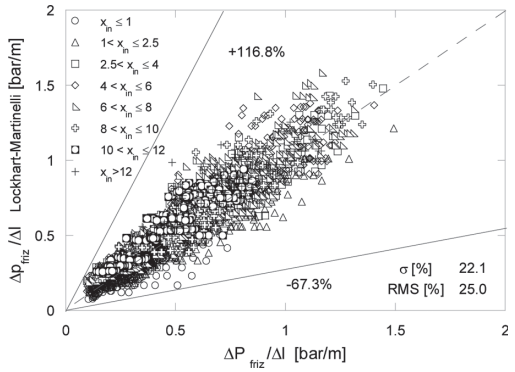


Figure 6. Pressure drop in straight pipes. Comparison between the Lockhart-Martinelli model's predictions and experimental data.

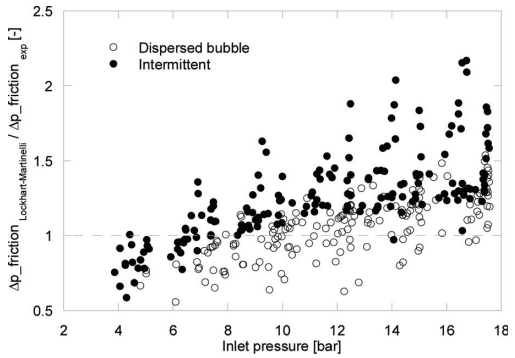


Figure 7. Lockhart-Martinelli: $\Delta p_c/\Delta p_{exp}$ as a function of the inlet pressure and for the different flow patterns.

deviation from the experimental values, as well as a higher dispersion of the data, is also found (maximum errors +116.8% and –67.3% *vs* +87% and –37%, respectively).

As already done for the Friedel model, the possible influence of the specific flow pattern has been checked also for the Lockhart-Martinelli model. However, since the influence of the vapor quality has been already found negligible from the previous results, the ratio of the predicted pressure drop over the experimental one, has been plotted as a function of the inlet pressure (Fig. 7). It can be seen that, apart from the expected marked dispersion of the data (based on the RMS value already reported in Fig. 6), a general increase of the ratio is observed at increasing inlet pressures. Again, an apparent dependency of the predictions with the flow pattern is found, with the intermittent flow regime always characterized by larger ratios of the pressure drop, compared with the dispersed bubble.

5.2 *Models comparison for fittings*

In the present section, the pressure drops calculated by means of the Friedel and the Lockhart–Martinelli models, for the first of the two elbows of the experimental rig, are compared with the measured values.

In Figure 8 the experimental pressure drops and those calculated with the Friedel model are reported for all the runs, along with the corresponding statistical indicators. The indicators present slightly higher values than in the case of straight pipelines, but the average error is still quite low.

In order to check the possible influence of the flow conditions, in the following Figures 9 and 10, the same comparison has been presented separately for the runs with $Re < 10^6$ and $Re > 10^6$, respectively, also reporting the calculated values both with the all-liquid and the two-phase equivalent lengths.

In the case of Figure 9, the statistical parameters indicate that the predictions of the model for

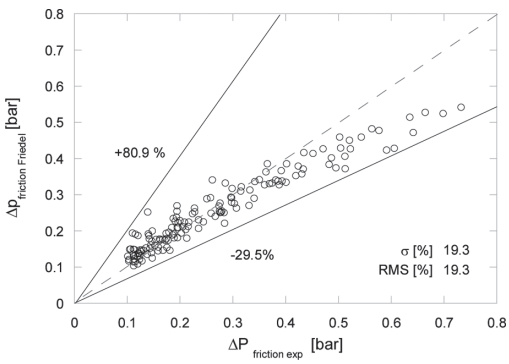


Figure 8. Δp_c calculated with Friedel correlation using the liquid equivalent length as a function of experimental Δp_{exp}.

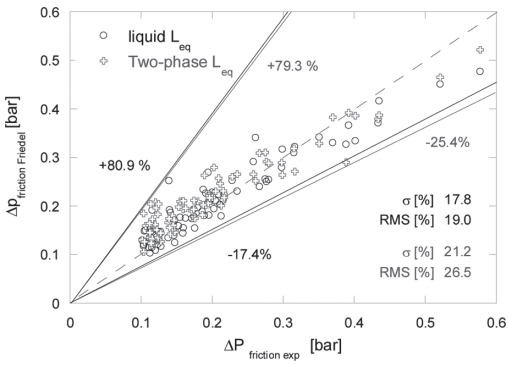


Figure 9. Δp_c calculated with Friedel correlation using the all-liquid and the two-phase equivalent lengths as a function of experimental Δp_{exp}. Tests with $Re < 10^6$.

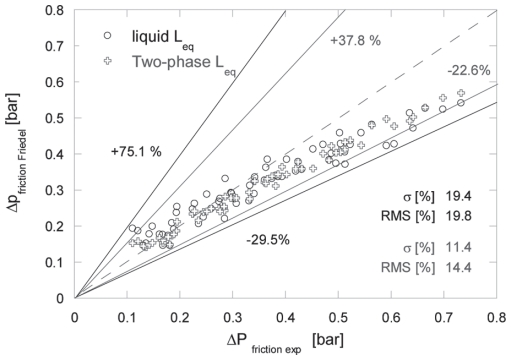


Figure 10. Δp_c calculated with Friedel correlation using the all-liquid and the two-phase equivalent lengths as a function of experimental Δp_{exp}. Tests with Re > 10^6.

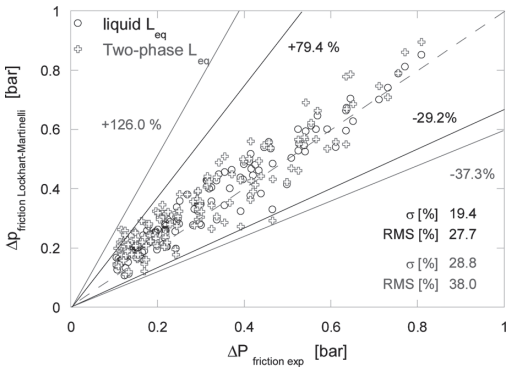


Figure 11. Friction pressure drop calculated with the Lockhart-Martinelli correlation using both liquid and two-phase equivalent length as a function of experimental friction pressure drop.

Re < 10^6 are rather good, especially when using the equivalent length calculated for the all-liquid flow, and they are comparable with the results obtained for straight pipes. Conversely, in the case of Re > 10^6 (Fig. 10), the best predictions are obtained using the two-phase equivalent length. They are definitely better than in the case of straight pipes, with RMS and σ equal to 14.4% and 11.4%, respectively, denoting a not negligible average error, but a very limited spread of the data around it. Since the Friedel model does not take into consideration any slip between the two phases, this result might be explained assuming that at higher flow rates (high Re numbers) the flowing system more likely behaves as a homogeneous mixture.

In Figure 11, the predictions obtained with the Lockhart-Martinelli model, using both the all-liquid equivalent length and that derived from two-phase flow measurements, are compared with the experimental values. As can be seen by comparing the statistical parameters there reported with those relative to the Friedel model, the accuracy is worse for the Lockhart-Martinelli model: σ is similar in both cases (around 19%), but RMS is 28 *vs* 19%, respectively. Furthermore, the accuracy becomes even much worse when the two-phase equivalent length is adopted (RMS = 38% and σ = 28.8%).

If the data corresponding to Re < 10^6 only are taken into consideration (see Fig. 12), the above results are more apparent, with the statistical parameters worse than those obtained for the Friedel model, when the single phase equivalent length is adopted, and definitely the worst in absolute when adopting the measured two-phase equivalent length (σ 34.2% and RMS 46.4%).

Finally, when the data for Re > 10^6 are considered (Fig. 13), as already found in the case of Friedel's

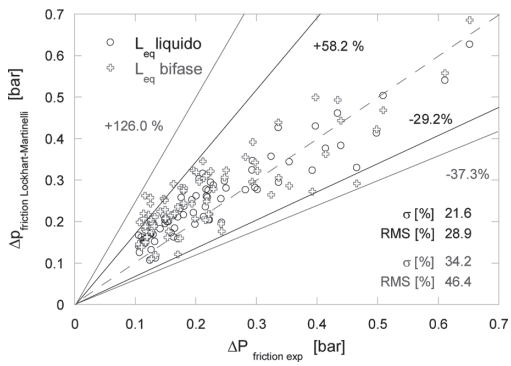


Figure 12. Friction pressure drop calculated with the Lockhart-Martinelli correlation using both liquid and two-phase equivalent length as a function of experimental friction pressure drop. Tests with Re < 10^6.

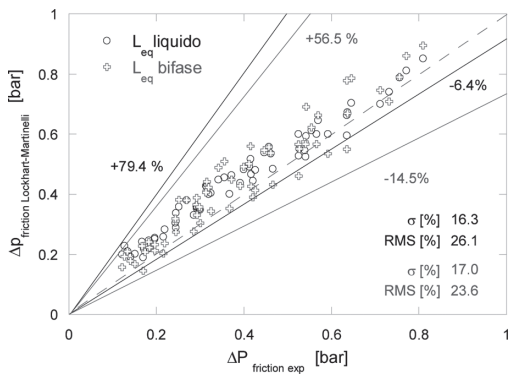


Figure 13. Friction pressure drop calculated with the Lockhart-Martinelli correlation using both liquid and two-phase equivalent length as a function of experimental friction pressure drop. Tests with Re > 10^6.

model, a remarkable improvement of all the statistical indicators is found, and in this case, the adoption of the two-phase flow equivalent length, further improves the results: quite close values of σ(16.3 and 17% respectively), but a noticeable reduction of RMS (26.1 *vs* 23.6% for the two-phase equivalent length).

6 CONCLUSIONS

Based on the presented results, different conclusions can be drawn with reference to the straight sections of pipeline and the connected elbows.

In the case of the straight sections, the Friedel model has proved to provide better predictions of the friction losses for a two-phase steam-water system, at least within the tested ranges of variability of the involved parameters. Despite a rather limited spread of the theoretical predictions, the average error is extremely low. No significant influence of the vapor quality has been detected, whereas the specific flow pattern assumed by the flowing system seems to affect the prediction accuracy: a small error is found for dispersed bubble flow, while a much larger deviation of the results is observed for the intermittent flow pattern. A similar effect has been observed also for the Lockhart-Martinelli model, thus suggesting that general models are more suited for homogeneous flow conditions. This latter model proved to be less accurate overall.

As far as the friction losses generated by the elbows are concerned, more complex considerations can be derived. Generally speaking, the prediction capability of both models is worse, compared with the results obtained for straight pipes. The Friedel model still proves to be much more accurate than the Lockhart-Martinelli, especially in terms of average error, but other parameters can play a significant role here. In particular, both models behave differently at different Reynolds numbers, with better results at high Re and worse predictions at low Re. Furthermore, this discontinuity is also dependent on the particular equivalent pipe length calculation method adopted: the experimentally determined two-phase equivalent pipe length markedly emphasizes the different behavior with the Reynolds number, but while the average Friedel model's behavior does not change so much with respect to the straight pipe sections, the Lockhart-Martinelli model's calculations become much more inaccurate.

In conclusion, based on the present experimentation, the Friedel model resulted to be characterized by a higher level of accuracy in the calculation of the friction losses for two-phase vapor-liquid flows. However, further work is needed for the characterization of the pressure losses connected with fittings, where the particular method adopted for the calculation of the equivalent pipe length can play a significant role.

REFERENCES

Boccardi, G., Bubbico, R., Celata, G.P., Mazzarotta, B., 2005. Two-phase flow through pressure safety valves. Experimental investigation and model prediction. *Chemical Engineering Science*. 60(19): 5284–5293.

Boccardi, G., Bubbico, R., Celata, G.P., Di Tosto, F., 2008. Geometry Influence on Two-Phase Flow in Safety Valves. *Journal of Loss Prevention in the Process Industries.* 21: 66–73.

Boccardi, G., Bubbico, R., Celata, G.P., Di Tosto, F., Trinchieri, R., 2010. Comparison among Three Prediction Methods for Safety Valves Design in Two-Phase Flow in the case of a Small Valve. *Chemical Engineering Transactions,* 19: 175–182.

CCPS, Center for Chemical Process Safety, 1998. *Guidelines for pressure relief and effluent handling systems*. New York. AIChE.

Crane Co., 1969. *Flow of fluids through valves, fittings and pipes.* Tech. Paper 410.

Darby, R., 2004. On two-phase frozen and flashing flows in safety relief valves. Recommended calculation method and the proper use of the discharge coefficient. *Journal of Loss Prevention in the Process Industries*. 17: 255–259.

Diener, R., Schmidt, J., 2004. Sizing of Throttling Device for Gas/Liquid Two-Phase Flow Part 1: Safety Valves. *Process Safety Progress*. 23(4): 335–344.

Fauske, H.K., 1999. Determine two phase flows during releases. *Chemical Engineering Progress*. 95(2): 55–58.

Fisher, H.G., Forrest, H.S., Grossel, S.S., Huff, J.E., Muller, A.R., Noronha, J.A., Shaw, D.A., Tilley, B.J. 1992. *Emergency Relief System Design Using DIERS Technology, The DIERS Project Manual*. New York. AIChE.

Friedel, L., 1979. Improved friction drop correlations for horizontal and vertical two-phase pipe flow. *Proceedings of the European Two-phase Flow Group Meeting,* paper E2, Ispra, Italy.

ISO/DIS4126-10, 2008. Safety devices for protection against excessive pressure—Part 10: Sizing of safety valves for gas/liquid two-phase flow.

Kim Y., O'Neal D.L., 1995. A comparison of critical flow models for estimating two-phase flow of HCFC22 and HFC134a through short tube orifices. *International Journal of Refrigeration*, 18(7): 447–455.

Leung, J.C., 1996. Easily size relief devices and piping for two-phase flow. *Chemical Engineering Progress*. 92 (12): 28–50.

Leung, J.C., 2004. A theory on the discharge coefficient for safety relief valve. *Journal of Loss Prevention in the Process Industries*. 17: 301–313.

Lockhart, R.W. & Martinelli, R.C., 1949. Proposed correlation of data for isothermal two-phase, two-component flow in pipes. *Chem. Eng. Progress*, 45(1): 39–48.

Moreno Quiben, J., & Thome, J.R., 2007. Flow pattern based two-phase frictional pressure drop model for horizontal tubes, Part II: New phenomenological model. *International Journal of Heat and Fluid Flow*. 28: 1060–1072.

Perry, R.H., Green, D.W. Maloney, J.O. (eds)., 1997. *Perry's Chemical Engineers' Handbook,* 7th ed. New York. McGraw-Hill.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Empirical Bayes inference with nonlinear homogenizations and correlated intensity functions: Use in asset degradation modelling

G. Blair
Scottish Water, Dunfermline, Scotland, UK

J. Quigley & L. Walls
University of Strathclyde, Glasgow, Scotland, UK

ABSTRACT: We develop and evaluate a method to estimate the frequency of an asset failure when experience event data are available for multiple assets of a given type. Typically such data contains information on assets of mixed ages, operating in different environments and in many cases the number of recorded events might be few or even zero. Assets are known to have slow age-related degradation and we have access to engineering experts who are able to provide judgment about the degradation rates. An empirical Bayes method is developed to allow us to estimate the failure rates for an asset on a particular site by using the available observational data pool together with structured engineering judgment of the degradation rate for the asset type. Our method aims to address the challenges of asset pool heterogeneity and environmental conditions across sites. We describe our practical motivation which is informed by a real problem facing a water utility. We explain the principles and mathematics underpinning the new methods, before describing a simulation based evaluation of their accuracy. We show that the empirical Bayes methods provide accurate estimates of the failure intensities for a range of parameters considered in this controlled study and that empirical Bayes estimators can compensate for bias in initial judgmental assessments of degradation rates. We discuss how the method can be applied in the industry context.

1 INTRODUCTION

Scottish Water is a statutory organisation that provides water and sewerage services to the people of Scotland. It is accountable to the public through the Scottish Government. Scottish Water is the sole provider of water and waste water services to an area of over 77,000 square kilometres (km), a third of the area of Britain. The organisation operates and manages over 48,000 km of water mains, approximately 50,000 km of sewers, and over 6000 above ground assets, which consist of treatment works, pumping stations and storage facilities.

The Asset Management directorate, within Scottish Water, is responsible for 'long-term planning at lowest cost' to ensure customers pay the lowest water bills while assets are being managed and operated in an optimal way. Scottish Water use data and modelling to inform and shape its policy, decisions and business plans. For example, analytical methods are used to predict economic levels of leakage, hydraulic modelling is used to predict security of supply.

Some models require predictions of the frequency of events affecting individual assets in some future time interval. This can be challenging because Scottish Water manages many types of assets with complex histories and incomplete historical data records. Indeed there are many assets which have very few or no failures in their recorded history.

To address this challenge we develop a new method of estimation drawing upon the principles of empirical Bayes inference (Carlin and Louis, 2000; Efron, 2005; Quigley and Walls, 2011). Our proposed method is distinctive because we need to develop an appropriate means of homogenising the pooled asset experience data to support better estimation when the underlying failure intensity function is dynamic. We also need to capture the relationships that may exist between the asset degradation rates due to the environmental conditions to which they are exposed.

We develop a new method for the general data structures present in the Scottish Water context. Our method aims to combine the relevant empirical data on historical assets failure events with engineering judgement for the following reasons. The historical event data provides useful information about the underlying level of the asset failure intensity, while structured engineering judgment can provide information about the underlying rate of asset degradation in given environmental conditions. We focus upon expressing the mathematical estimators assuming a time-dependent Non-Homogeneous

Poisson Process for the event process and presenting an evaluation of performance of the estimation methods. We conduct a controlled simulation experiment to examine the accuracy of the estimation methods under two situations: first when expert judgement is perfectly calibrated and unbiased; second when the judged rate of asset degradation is subject to positive or negative bias. We examine the simulation results in relation to some theoretical properties of the proposed estimators. We conclude by discussing how the method might be implemented in the industrial context.

Section 2 describes the empirical data characteristics in more depth. Section 3 presents the mathematical estimation methods including a discussion of assumptions made and some consideration of theoretical properties of the proposed estimators. Section 4 outlines the design of the simulation experiment, while Section 5 presents and discusses selected results. Section 6 suggests ways of expanding this work both methodologically and in application.

2 INDUSTRY MOTIVATION AND DATA

Scottish Water, like many organisations, maintains inventory and event databases. The inventory database contains information about asset characteristics, such as type, location, date installed. The event data base contains information about where and when an asset failed. Table 1 shows typical failure event data while Table 2 describes some of the asset characteristics. See Rausand and Hoyland (2004) for a general discussion of such field data.

It is relatively inexpensive to collect asset characteristics as shown in Table 1, but it can be costly to collect data on all the characteristics that potentially affect asset reliability. This is why we believe an empirical Bayes method which combines the available empirical data with expert judgment on the degradation is an efficient approach for estimating the failure intensity and supporting prediction of future failure frequencies. By forming an empirical data pool by selecting related assets, for example, of the same type, then we can use failure event data for similar assets to estimate the typical level of the failure intensity. Practically this reduces the need to model each asset characteristic individually, which might not only be inefficient but also ineffective since we might have poor statistical estimates for sparse event data sets. By using expert judgment to understand the degradation rate in different environments we are effectively using a proxy for the distinguishing characteristics of an individual asset.

Table 1. Example asset event data structures.

Asset identifier	Asset type	Location	Date installed	Number of failures in year 1	2	…	Y
X1	Pump	East	01/06/2001	0	1	…	0
X2	Pump	West	10/01/2010	0	0	…	1
X3	Pump	North	27/03/2003	1	0	…	3

Table 2. Description of asset characteristics.

Asset characteristics	Description
Asset identifier	Unique reference code to distinguish one asset from another and to provide link between failure and inventory data.
Asset type	Grouping classification for an asset, may be high or low level information. e.g. High level: Pump, Filter, etc. e.g. Low level: Submersible pump, Screw pump, etc.
Location	High level or low level information e.g. High level: North, South, East, West. e.g. Low level: Address of the site where the asset is held.
Date installed	Date at which the asset was installed and can be used to estimate asset age.
Date failure reported	Date at which the asset was reported to have failed.

Given the heterogeneity in the environment for Scottish Water assets, but yet information about the relationships between assets of the same type across these environments, a method for estimating failure intensity grounded in empirical Bayes provides a potentially effective and efficient approach. The method logic is to pool failure events across assets by essentially averaging over differing operating environments but then adjust the pooled event frequency using the empirical data and the judgmental assessments of degradation for a particular asset on a given site. Therefore the failure frequency estimate is a weighted average of the pool of historical experience and information relating to the past and future of a particular asset. Thus we develop a method that uses the data available and, if we can establish the performance of the estimation method, then we can also reduce the burden of collecting costly data in future.

3 EMPIRICAL BAYES INFERENCE METHOD

3.1 *Modelling assumptions & asset heterogeneity*

We assume a Non Homogeneous Poisson Process (NHPP) to describe the stochastic behavior of the

failure of assets subject to age-related degradation. Specifically, we assume a Power Law intensity function for each asset, as given in Equation (1), to model the number of events $N_i(t)$ realized over operating time (0, t) for asset i.

$$P\left[N_i(t)=n_i\middle|\alpha_i,\beta_i\right]=\frac{\left(\alpha_i t^{\beta_i}\right)^{n_i}e^{-\alpha_i t^{\beta_i}}}{n_i!} \tag{1}$$

Such an approach to modeling allows each asset to have its own scale parameter, α_i and degradation parameter β_i, thus acknowledging the heterogeneity within the asset pool due to variation in asset type and operational environment.

3.2 *Approach to inference*

When historical data indicates that failures are too infrequent to empirically estimate the model in Equation (1) for each asset, pooling the data available to obtain estimates is feasible but questionable when the assets represented by the model form a heterogeneous pool. Therefore we propose to use expert judgment to estimate the degradation rate for each asset, β_i, and use empirical Bayes methods to estimate the scale parameter by first pooling the empirical data to estimate the scale parameter across the pool and then adjust the estimate for each asset in-line with its experience.

Mathematically this is accomplished by assuming the scale parameter for each asset is realized from a common Gamma distribution with shape parameter a and rate parameter b, given by the following probability density function,

$$f(\alpha;a,b)=\frac{b^a\alpha^{a-1}e^{-b\alpha}}{\Gamma(a)}. \tag{2}$$

This results in a predictive distribution for the number of failure events, which is in the form of a Negative Binomial distribution as shown in Equation (3). This is akin to assuming that a prior distribution has been provided for the scale parameter in the form of a Gamma distribution.

$$\begin{aligned}P\left[N_i(t)=n_i\middle|\beta_i\right]&=\int_0^\infty\frac{\left(\alpha_i t^{\beta_i}\right)^{n_i}e^{-\alpha_i t^{\beta_i}}}{n_i!}\frac{b^a\alpha_i^{a-1}e^{-b\alpha_i}}{\Gamma(a)}d\alpha_i\\&=\frac{\Gamma(n_i+a)b^a t^{n_i\beta_i}}{\Gamma(a)n_i!\left(b+t^{\beta_i}\right)^{n_i+a}}\\&=\frac{\Gamma(n_i+a)}{\Gamma(a)n_i!}\left(\frac{b}{b+t^{\beta_i}}\right)^a\left(\frac{t^{\beta_i}}{b+t^{\beta_i}}\right)^{n_i}\end{aligned} \tag{3}$$

This model is expressed in terms of the parameters (a,b) which are common to the pool and so the pooled empirical data can be used to obtain estimates of these parameters using either maximum likelihood estimation or moment matching methods. Once the pool parameters have been estimated, Bayes Theorem can be used to update the prior for each asset to obtain its posterior based on the individual asset experience. The resulting posterior distribution for the failure frequencies over a given time horizon for a particular asset is a Poisson distribution with a mean that is a weighted average of the pooled mean and the individual asset experience.

3.3 *Moment matching estimates of* (a,b)

Moment matching for parameter estimation ensures that the first and second moment of the model for the pool experience equals the observed first and second moment in the data. The moment estimates for the pool parameters are given by

$$\hat{a}=\frac{U^2}{W-U^2}\quad\text{and}\quad\hat{b}=\frac{U}{W-U^2} \tag{4}$$

where

$$U=\frac{\sum_{i=1}^m n_i}{\sum_{i=1}^m t^{\beta_i}}\quad\text{and}\quad W=\frac{\sum_{i=1}^m n_i^2-\sum_{i=1}^m n_i}{\sum_{i=1}^m t^{2\beta_i}}. \tag{5}$$

We can show that these are consistent estimators of the pool parameters under the modeling assumptions. As pool size, m, increases the estimates converge to the true values of the distribution. Since

$$\begin{aligned}E[U]&=\frac{a}{b}\frac{\sum_{i=1}^m t^{\beta_i}}{\sum_{i=1}^m t^{\beta_i}}=\frac{a}{b}\\E[W]&=\frac{\sum_{i=1}^m E\left(\alpha_i t^{\beta_i}+\alpha_i^2 t^{2\beta_i}\right)-\frac{a}{b}\sum_{i=1}^m t^{\beta_i}}{\sum_{i=1}^m t^{2\beta_i}}=\frac{a(a+1)}{b^2}\end{aligned} \tag{6}$$

then

$$\begin{aligned}\lim_{m\to\infty}\frac{U^2}{W-U^2}&=\frac{\left(\frac{a}{b}\right)^2}{\frac{a(a+1)}{b^2}-\left(\frac{a}{b}\right)^2}=a\\\lim_{m\to\infty}\hat{b}&=b.\end{aligned} \tag{7}$$

3.4 *Effect of biased judgment on estimates*

Consider the effects on inference of bias in the engineering judgment assessment of the degradation rate. Assume a true underlying rate of degradation for asset i is denoted by β_i. Further assume that at the time of analysis, t, an engineering expert has provided an estimate of the form $S_i t^{\beta_i}$, where a value of $S_i = 1$ indicates an unbiased estimate. Using moment matching we obtain the following

$$U = \frac{\sum_{i=1}^{m} n_i}{\sum_{i=1}^{m} S_i t^{\beta_i}} \quad \text{and} \quad W = \frac{\sum_{i=1}^{m} n_i^2 - \sum_{i=1}^{m} n_i}{\sum_{i=1}^{m} S_i^2 t^{2\beta_i}}. \tag{8}$$

Assume also that the degree of bias changes from one asset to another but all S_i have a common distribution with mean and standard deviation

$$E[S_i] = \theta \quad \text{and} \quad Var[S_i] = \sigma^2.$$

Then we obtain the following limit as the number of assets in the pool, m, tends to infinity

$$\lim_{m\to\infty} U = \frac{\frac{a}{b}\sum_{i=1}^{m} t^{\beta_i}}{\sum_{i=1}^{m} \theta t^{\beta_i}} \underset{m\to\infty}{\underset{m\to\infty}{=}} \frac{a}{b\theta}$$

$$\lim_{m\to\infty} W = \frac{\sum_{i=1}^{m} E\left(\alpha_i t^{\beta_i} + \alpha_i^2 t^{2\beta_i}\right) - \frac{a}{b}\sum_{i=1}^{m} t^{\beta_i}}{\sum_{i=1}^{m} \left(\sigma^2 + \theta^2\right) t^{2\beta_i}} \underset{m\to\infty}{\underset{m\to\infty}{=}}$$

$$= \frac{a(a+1)}{b^2\left(\sigma^2 + \theta^2\right)} \tag{9}$$

This implies the following

$$\lim_{m\to\infty} \frac{U^2}{W - U^2} = \frac{a}{\frac{1}{\gamma^2+1} - a\frac{\gamma^2}{\gamma^2+1}} \tag{10}$$

$$\lim_{m\to\infty} \frac{U}{W - U^2} = \frac{b\theta}{\frac{1}{\gamma^2+1} - a\frac{\gamma^2}{\gamma^2+1}} \tag{11}$$

where $\gamma = \sigma/\theta$.

Therefore,

$$\lim_{m\to\infty} \hat{a} = \frac{a}{\frac{1}{\gamma^2+1} - a\frac{\gamma^2}{\gamma^2+1}}$$

and

$$\lim_{m\to\infty} \hat{b} = \frac{b\theta}{\frac{1}{\gamma^2+1} - a\frac{\gamma^2}{\gamma^2+1}} \tag{12}$$

The empirical Bayes estimator for a given asset of the expected number of failure events at time $(t+x)$ given the observations for that asset up to time t, is the mean of the posterior distribution of the scale parameter for the asset estimated using all observations for all assets up to time t multiplied by $(t+x)^{\beta}$, which reflects the non-linear degradation rate. Let $\underline{n}(t)$ denote the vector representing the event history up to time t, where the ith element is the history of the ith asset denoted by $n_i(t_i)$, then the empirical Bayes estimate is given by

$$E\left[N(t_i + x)\middle|\underline{n}(t)\right] = E\left[\lambda_i (t_i + x)^{\beta_i}\middle| n_i\right] = \frac{\hat{a} + n_i}{\hat{b} + t^{\beta_i + \varepsilon_i}} (t+x)^{\beta_i + \varepsilon_i} \tag{13}$$

where $\varepsilon_i = \ln(S_i)/\ln(t)$.

As pool size increases the estimates of the parameters of the prior distribution approach those given in Equation (12). Hence for large pools we can obtain the expectation for the accumulated number of events x time units beyond the time t as follows

$$\lim_{m\to\infty} E\left[N_i(t+x)\middle|\underset{\sim}{n(t)}\right] = \frac{a + n_i(t)}{b\theta + t^{\beta_i + \varepsilon_i}} (t+x)^{\beta_i + \varepsilon_i}. \tag{14}$$

The form of Equation (14) indicates that the error in expert judgment, ε_i, affects future predictions of the expected accumulated number of failures by either decreasing (increasing) the scale estimate or increasing (decreasing) the degradation rate. By examining the percentage change in the predicted expected number of failures as a function of this error, we find that the net effect is an increase in error as the predicted time horizon lengthens, as follows

$$\frac{d\ln\left(\lim_{m\to\infty} E\left[N_i(t+x)\middle|\underline{n}(t)\right]\right)}{d\varepsilon_i} = \ln(t+x) - \frac{t^{\beta_i+\varepsilon_i}}{b\theta + t^{\beta_i+\varepsilon_i}} \ln(t) > 0 \tag{15}$$

If engineering experts are consistently biased in their judgments, such that $\sigma = 0$, then the ratio between the predicted mean and the actual mean has the following simple expression for large pool size.

$$\lim_{m\to\infty} \frac{E\left[N_i(t+x)\middle|\underline{n}(t)\right]}{\frac{a+n_i(t)}{b+t^{\beta_i}}(t+x)^{\beta_i}} = \frac{\frac{a+n_i(t)}{a+n_i(t)}}{\frac{b\theta+t^{\beta_i+\varepsilon}}{b+t^{\beta_i}}}(t+x)^{\varepsilon} = \left(1+\frac{x}{t}\right)^{\varepsilon} \quad (16)$$

Equation (16) allows the impact of the error assessment of the degradation parameter to be established. Since $\varepsilon = 0$ for an unbiased expert judgment, the ratio between the expected mean and the true mean is 1. However, an expert who under (over) estimates degradation would have a negative (positive) ε.

3.5 *Maximum likelihood estimates of* (a,b)

We also show the derivation of the Maximum Likelihood Estimates (MLE) of the model parameters as an alternative inference approach to the moment method. While MLE's provide more accurate estimates for this model there is not a closed form expression, so numerical methods are required to obtain a solution.

The log-likelihood function for the model obtained from Equation (2) is expressed as follows,

$$l(a,b) \propto \sum_{i=1}^{m}\left[\ln(\Gamma(n_i+a)) - a\ln(b+t^{\beta_i}) - n_i\ln(b+t^{\beta_i})\right] - m\ln(\Gamma(a)) + ma\ln(b)$$

The resulting score functions are then given by

$$S_a(a,b) \propto \sum_{i=1}^{m}\left[\sum_{k=0}^{n_i-1}\frac{1}{k+a} + \ln(b) - \ln\left(b+t^{\beta_i}\right)\right]$$

and

$$S_b(a,b) \propto \sum_{i=1}^{m}\left[\frac{a}{b} - \frac{a+n_i}{b+t^{\beta_i}}\right]. \quad (17)$$

Setting both functions in Equation (17) to 0 and solving provides the MLE of the parameters (a,b). Note that the form of $S_b(a,b)$ implies that the prior mean scale parameter equals the posterior for the pool. The solution to these expressions can be simplified slightly. We can isolate a in $S_b(a,b)$ to obtain the following

$$\hat{a} = \frac{\sum_{i=1}^{m}\frac{n_i}{\hat{b}+t^{\beta_i}}}{\sum_{i=1}^{m}\left(\frac{1}{\hat{b}} - \frac{1}{\hat{b}+t^{\beta_i}}\right)}. \quad (18)$$

In turn this can be substituted into $S_a(a,b)$ to reduce it to a one parameter function, allowing us to solve,

$$\sum_{i=1}^{m}\left[\sum_{k=0}^{n_i-1}\frac{1}{k+\frac{\sum_{i=1}^{m}n_i\hat{p}_i}{\sum_{i=1}^{m}\left(1-\hat{p}_i\right)}} + \ln\left(\hat{p}_i\right)\right] = 0 \quad (19)$$

where $\hat{p}_i = \frac{\hat{b}}{\hat{b}+t^{\beta_i}}$.

4 SIMULATION EVALUATION DESIGN

The purpose of the simulation is to further evaluate the performance of the proposed estimation methods to better understand the accuracy and the impact on estimation error of any bias in expert judgement prior to application to real data. The design of the simulation is informed by the typical characteristics of the data context of Scottish Water in terms of the typical number of assets per class, the relative size of failure intensities and the relative time horizons for the historical data records as well as for future predictions. Our simulation study is not exhaustive since it is constrained to a set of possible situations as summarised in Figure 1.

4.1 *Set-up to assess estimation accuracy*

Here we consider the cases of pool sizes of 20 and 40 assets to examine the effect of amount of empirical data being used. For each pool size we consider the same sets of parameter values for the prior distributions for each asset as given in Equation (3). That is, combinations of the shape parameter, a, which is set to 0.1, 0.5, 0.9, 1, and 2, and the scale parameter, b, which is set to values of 1, 10, and 100. The α_i are simulated from a $\Gamma(a,b)$ distribution with parameters (a,b). We set the true value of β to be 2, which represents an increasing intensity function for the Power Law process and hence represents asset degradation. The numbers of failure in the time interval (t_j, t_{j+1}) are then simulated from a Poisson distribution with mean $\alpha_i(t_{j+1}^{\beta_i} - t_j^{\beta_i})$.

Through simulation we effectively create a sample data set of the form shown for the Scottish

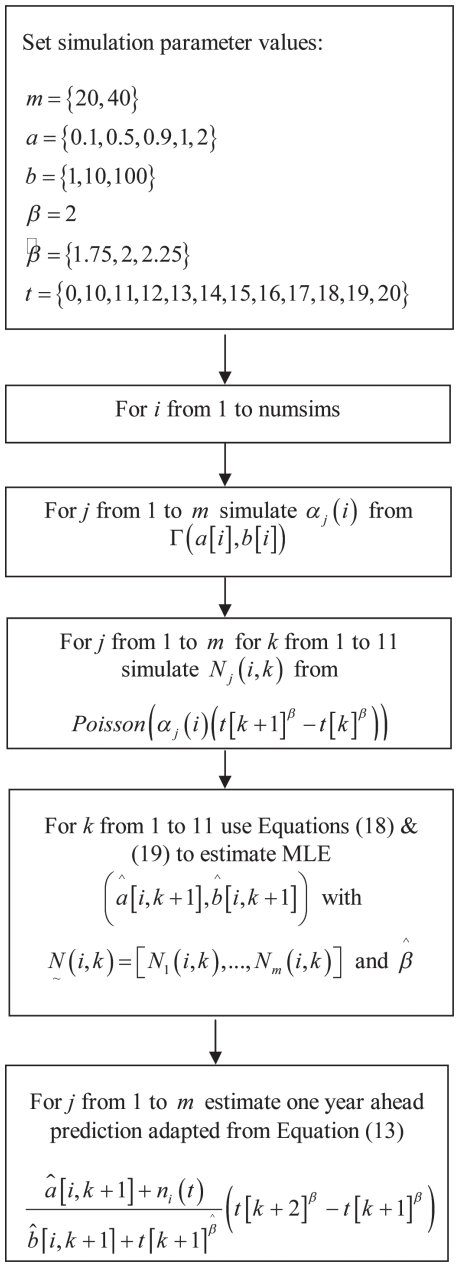


Figure 1. Simplified simulation logic diagram.

Water data in Table 1, but where we have a record of the annual number of failures over a 10 year period. Note that unlike the real data, we are making a simplifying assumption in this initial simulation by treating all simulated assets as new at the start of observation. That is, we create simulated data records over the period (0,10) years for each asset in the first instance. We use k as a counter for the years in our simulation of the empirical data history. Our goal is then to use the proposed inference method to estimate the number of failures in the next year. Since we are simulating reality we can also extend our simulated sample paths for each asset for years 11–20 thereby giving us an ability not only to make dynamic one year ahead predictions but also to compare our predicted estimate for each of years 11–20 with our simulated observations.

4.2 *Design to assess bias in engineering judgment*

To examine the effect of possible bias in the engineering judgement of the true degradation rate, β, we examine three scenarios by setting the judged value, $\hat{\beta}_i$ to be set to 1.75, 2, and 2.25 which corresponds to an underestimation, perfect estimation and overestimation of the degradation rate respectively.

5 SIMULATION EVALUATION FINDINGS

Table 3 shows a summary of means and standard deviations for the simulated scale parameter of the Power Law process, α_i, for each size of asset group. Since α_i were generated for each asset from a gamma distribution, $\Gamma(a,b)$, the mean and standard deviation, respectively, should be

$$\mu \approx a/b \quad \text{and} \quad \sigma \approx \sqrt{a/b^2}.$$

Table 3. Mean and standard deviation of power law scale parameter for simulated asset groups.

		Number of assets in the group			
		20		40	
a	b	Mean	Standard deviation	Mean	Standard deviation
0.1	1	0.0314	0.0841	0.0624	0.1709
0.1	10	0.0056	0.0116	0.0079	0.0211
0.1	100	0.0008	0.0021	0.0008	0.0019
0.5	1	0.3767	0.4665	0.4372	0.6232
0.5	10	0.0323	0.0411	0.0465	0.0579
0.5	100	0.0094	0.0132	0.0044	0.0073
0.9	1	0.7439	0.6526	0.9232	0.8204
0.9	10	0.0966	0.0820	0.1075	0.0985
0.9	100	0.0094	0.0109	0.0086	0.0075
1	1	0.8716	0.8564	1.1704	1.0053
1	10	0.1146	0.1211	0.0798	0.0745
1	100	0.0068	0.0061	0.0117	0.0099
2	1	1.9745	1.3172	2.1822	1.7062
2	10	0.2133	0.1589	0.1894	0.1497
2	100	0.0205	0.0155	0.0201	0.0141

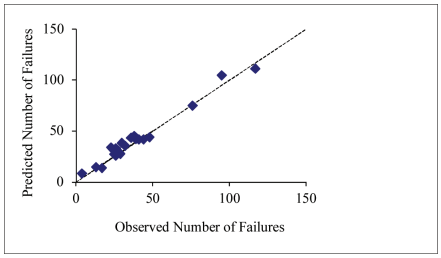
We find that the scale of the simulated mean failure intensity functions range from just over 0 failures per annum (i.e. 0.0008) at a = 0.1 and b = 100 to around 2 failures per annum at $a = 2$ and $b = 1$.

5.1 *Estimation accuracy*

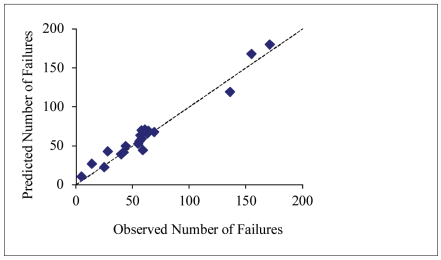
Generally our preliminary results indicate that prediction accuracy is good. We present only a selection of results to illustrate our indicative findings for changing α_i, when β is fixed at a value of 2.

Figure 2 shows plots of the predicted against observed number of failures in years 11 and 17 for single simulations of each of the two cases where there are 20 and 40 assets in the pool when the level of the intensity is around 2 failures per annum (i.e. $a = 2$ and $b = 1$). The patterns in these selected diagrams are indicative of those found in all simulations for this case. It appears that our method produces accurate estimates, on average, since the predicted against observed accumulated number of failure profiles vary randomly around the 45° line. The densities of points also typify the forms of the underlying Poisson models. The degree of accuracy seems to increase through time, as we might expect as more empirical observations are used in estimation.

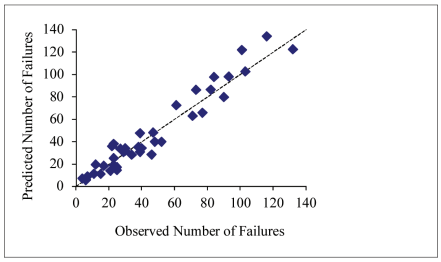
For the situation where we have the lowest level of the intensity at 0.0008 failures per annum, then we inevitably simulate many asset sample data sets with zero observed failures in a given year. For example, in some years we find that none of the assets experienced a failure event, but in other years only a single asset experienced a failure. Due to the properties of empirical Bayes estimation we find that in such circumstances an average weighted towards the pooled mean is allocated for zero event assets. In years when there is a failure event, even if only for one out of say the 20 assets in the pool, then this tends to increase the pool mean and hence the year ahead predicted number of failures. Equally in years where there are no observed failure events then the pooled mean decreases due to the additional exposure accumulated. It is also clear that the predicted number of failures for those particular assets which experience events are increased above the pool mean to account for their local history.



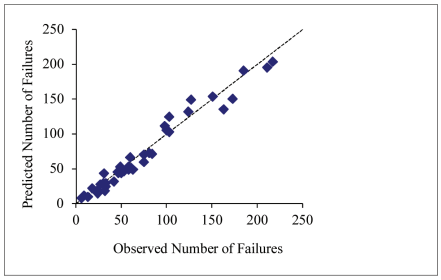
m=20, t=11, a=2, b=1



m=20, t=17, a=2, b=1



m=40, t=11, a=2, b=1



m=40, t=17, a=2, b=1

Figure 2. Predicted against the observed number of failures for selected scenarios of *m, t, a* and *b* when $\beta = 2$ and mean α_i is simulated to be approximately 2.

5.2 *Estimation accuracy in presence of judgmental bias in degradation rate*

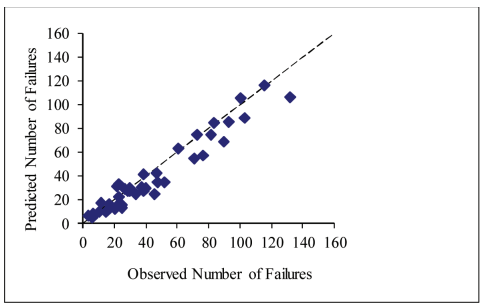
Now let us examine the effects on estimation accuracy when we control the degree of bias in the judgemental assessment of the degradation rate. We investigate this accuracy by simulating the number of failures under the true degradation state when $\beta = 2$, but compute the expected number of failures using the assumed subjective judgement values of $\hat{\beta}_i = 1.75$, 2 and 2.25. Since we have established that there is no discernable difference between size of the asset pool we only present selected results for the case of 40 assets.

Equally for comparison with the unbiased scenario shown in Figure 2 we only present results for the case of $a = 2$, $b = 1$.

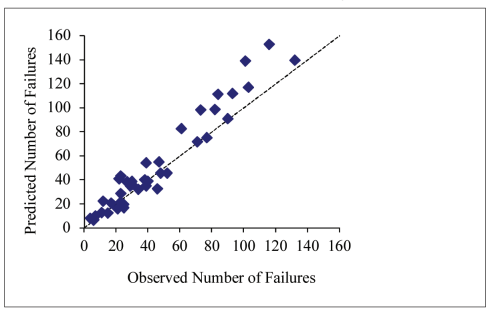
Figure 3 shows plots of the predicted number of failures against the true observed number of failures at year 11 for the scenarios mentioned above, while Figure 4 shows the equivalent plots for the predicted failure frequencies for year 17 based on updated estimate using empirical data available up to year 16.

We find that when the degradation rate is judged to be 1.75, and so less than the true rate, that the predicted number of failures tends to underestimate those observed under the true model, but the degree of underestimation visually appears to reduce as more experience is accumulated. Likewise, if the degradation rate is assumed to be judged by an expert to be 2.25, and so higher than its true value, then the predicted number of failures is slightly greater than observed under the true model.

For the case of unbiased assessment of the degradation rate, the judged and true values of β are 2. We find the predicted number of failures is an accurate estimate of the observed under the true model as we have shown earlier in, for example, Figure 2.

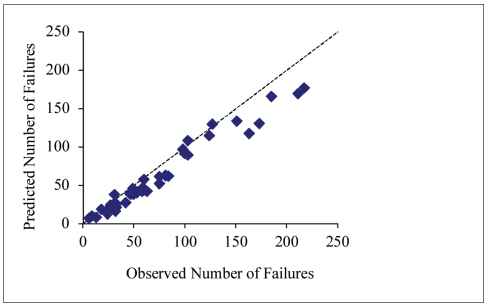


m=40, t=11, a=2, b=1, β_i=1.75

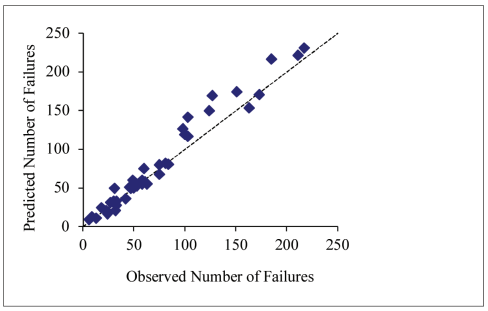


m=40, t=11, a=2, b=1, β_i=2.25

Figure 3. Predicted against the observed number of failures for 40 assets at t = 11 for true degradation of β = 2.



m=40, t=17, a=2, b=1, β_i=1.75



m=40, t=17, a=2, b=1, β_i=2.25

Figure 4. Predicted against the observed number of failures for 40 assets at t = 17 for true degradation of β = 2.

6 CONCLUSIONS AND FURTHER WORK

A method, based on the principles of empirical Bayes, is developed to support prediction of failure rates for a particular asset by using the available observational data for a pool of like assets together with engineering judgment for the asset degradation rate. We have conducted a preliminary theoretical and simulation evaluation of the performance characteristics of our proposed estimation method.

From our simulation study we find that we can obtain accurate estimates especially when the judgmental assessment of the degradation rate is unbiased. Even when there is bias in the expert judgment, then we can quantify its effect as a function of the prediction time horizon and the model parameters. For example, as we might anticipate accuracy will be better for shorter prediction time horizons and for larger asset pool sizes where empirical data has been accumulated over longer observation periods. Our preliminary simulation results suggest that the empirical Bayes method appears to allow the observational data to compensate for any initial bias in the engineering judgment of the degradation rate as the estimates

are updated dynamically as operational experience increases.

Our simulation study is limited to a selected set of parameter values and only a limited number of simulation runs. We need to investigate a more rich experimental space and to increase the number of simulation repetitions to more fully investigate the degree of any learning in the failure intensity predictions under an empirical Bayes approach for situations such as that motivated by Scottish Water.

Our motivation for this study was a need to estimate future number of failure of control and monitoring assets which, in the broadest terms, are pieces of electrical equipment. To apply the proposed empirical Bayes approach we require Scottish Water analysts to form sound engineering classes of control and monitoring asset types so that the data from these assets will then form the empirical pool of data to be used in estimation. Scottish Water also require subject matter experts who are well qualified to assess changes in failure patterns throughout the asset lifetime based in an understanding of the degradation process under the operating environment at particular sites.

From our evaluation it is evident that bias in such expert judgment of the assessed degradation rate will impact the accuracy of any estimates, especially in the initial stage of making predictions using past records. Therefore in terms of practically applying our method to Scottish Water assets, we require to ensure that a structured expert judgment elicitation is conducted according to one of the recognized scientific processes (Cooke, 1991). Preliminary expert judgment studies have been conducted with engineers and scientists working with assets, such as control and monitoring equipment and rapid gravity filters, hence the principle of combing judgmental with empirical data for better predictive accuracy has been established as practically feasible.

REFERENCES

Carlin, B.P. and Louis, T.A., 2000. Bayes and Empirical Bayes Methods for Data Analysis. Chapman and Hall.

Cooke, R., 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press.

Efron B., 2005. Bayesians, frequentists and scientists. *Journal of American Statistical Association*, 99:96–104.

Quigley, J. and Walls L., 2011. Mixing Bayes and empirical Bayes inference to anticipate the realization of engineering concerns about variant system designs. *Reliability Engineering and System Safety*, 96: 933–941.

Rausand M. and Hoyland, A., 2004. *System Reliability Theory*, Wiley.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dependence of the gas supply system criticality indicator(s) on the system elements' reliability

B. Jokšas & I. Žutautaitė
Lithuanian Energy Institute, Kaunas, Lithuania

J. Augutis & T. Rekašius
Vytautas Magnus University, Kaunas, Lithuania

ABSTRACT: The country's energy systems are closely related with other systems. The prosperity of country depends on the well-run operation of each of the systems. The disruption in the energy systems can affect the activities of all systems. System criticality level is one of the most important indicators of reliable power supply. The criticality of the system depends on the relations with other parts of energy system. In energy sector, natural gas supply system is one of the most related systems to other systems. Elements of gas supply system have high value of criticality indicator within energy sector. Natural gas is the most commonly used by the heat and electricity generation technologies over the world. The natural-gas supply system was selected as a case study involving analyses of the operability and availability. The pilot numerical calculation was performed to demonstrate how this model is useful to assess the impact of gas supply system to heat and power systems criticality. The natural gas system simulation was performed by optimization method. The probability distribution of criticality indicator is obtained as a result of this study using a Monte Carlo method. The results of this analysis may also be used in the development of energy infrastructure criticality analysis.

1 INTRODUCTION

In this paper we made assumption, and we analyzed just single country critical infrastructure. The failure of critical infrastructures may adversely affect the functioning of the country. Disruptions in one type of infrastructure often transverse to other dependent infrastructures and possibly even back to the infrastructure, where the failure emerged.

Some energy infrastructure interferences which occurred in the last decay are the following:

- 2013 December (Blackout) in Venezuela, affected 15 states of Venezuela (70% of the country);
- 2012 October (Gas dispute), in Turkey (disrupted by Iran), disruption of gas supply;
- 2012 July (Blackout) in India, affected over 620 million people;
- 2011 August (Blackout) in the East Coast and Puerto Rico, affected more than 9.3 million customers;
- 2011 September (Gas disruption) in the USA (The Gulf of Mexico), the shut-in a peak of 2.2 Bcf/d of gas production;
- 2011 February (Gas disruption) in the Texas, the shut-in of 600 (MMcf/d) The grid lost 7000 megawatts of capacity, 50 power plants stopped working;
- 2011 September (Blackout) in the area around San Diego, California, USA, affected 2.7 million customers;
- 2009 (Gas dispute) in the European Union, Balkan region, affected 18 countries in European Union and Balkan region;
- 2006 in Lithuania, Telšiai, an accident at –26.5 °C in the district heating system led to the loss of heat supply for thousands of people for almost a week.
- 2003 (Blackout) In north USA and Canada, affected approximately 10 million people in Ontario and 45 million people in eight U.S. States;
- Some authors analyzed critical local cities of critical infrastructures. For example, Gdnask city [Kulawiak et al, 2013]. Authors usually used GIS system to visualize the infrastructure [Kulawiak et al, 2013; Jenelius et al, in press 2014; Rodríguez-Núñez et al, 2014].

The other authors propose to analyze separate infrastructures, such as power grid, road network, etc. [Zonouz et al, 2013; Jenelius et al, in press 2014; Roelich et al, 2014], authors [Zonouz et al, 2013] propose the algorithm for power control networks, that combines information from different sources.

The security level of states individual system are assessed by authors.

Authors usually estimated the risk level of infrastructure [Salling, 2013] or performed the vulnerability analysis [Jenelius et al, in press 2014].

Often authors analyze in detail the separate objects of infrastructure. They used the criticality assessment methods, such as Failure Modes their Effects and Criticality Analysis [Hammoum et al, 2013].

Some authors analyze interdependencies of infrastructure and analyze theoretical (or expert evaluation) assessment among the infrastructure layers [Huang et al, 2014], or used topological network analysis of infrastructure [Shuang et al, 2014], this analysis are the most commonly used with one type of infrastructure.

The criticality measurement could be related with consumers demand and with satisfaction percent of demands [Rodríguez-Núñez et al, 2014].

The criticality assessment method was used in the paper [Augutis et al, in press 2014]. The infrastructure system is supplemented by new objects. The criticality of elements of gas supply system was evaluated according to the presented method and performed important measurement (Fussell-Vesely and Birnbaum) of those elements. Also the logistic regression analysis was used for the first time to assess the components' influence on system criticality value.

2 PROPOSED CRITICALITY ASSESSMENT METHOD

In this paper we analyze infrastructure of heat, power and gas supply systems. These systems are very important for each country to ensure the economic prosperity and national energy security, especially in cold period (extreme weather conditions). To ensure the social prosperity, it is necessary to ensure uninterrupted heat and power supply for the consumers. Our model analyzes energy infrastructure composed of different type of energy generation technologies, such as Boiler Houses (BH), combined heat and power plants with back-pressure units (CHP), combined heat and power plants with extraction units (PP); renewable energy resources: hydro power plants (HP), wind villages (WP), biomass boiler houses and CHP (BIOchp). The generation technologies, such as CHP, BH and PP use natural gas as main fuel. Oil is used as alternative fuel in the CHP and PP. Each generation technology is defined as a functional unit with characteristic parameters and algorithms of operation. The system of heat, power and gas supply has internal functional relations. The function of the one subsystem depends on operating of other subsystems. The structural scheme of system is presented in the Figure 1. The disturbance occurred in any part of the system affects all subsystems (directly and indirectly).

The generation technologies used in our model are defined in more detail (functionality expression) in the paper (Augutis et al, in press 2014).

Each system element is described by functional expression:

$$Tch_i = (P_i,\ Q_i,\ \eta_{el},\ \eta_h), \tag{1}$$

where P_i—the installed electric capacity in to ith technology (MW); Q_i—the installed thermal capacity in to ith technology (MW); η_{el}—the efficiency of primary energy conversion for electricity using main fuel; η_h—the efficiency of primary energy conversion for heat using main fuel.

All generation technologies are simulated by input-output method. The demands of heat and electricity are allocated for generation technologies by the Simplex optimization method. The optimization is performed to maximize energy generation in each analyzed city. The mathematical model of this problem could be written:

$$\max_x \mathbf{b}^T \cdot \mathbf{x},\ when \begin{cases} \mathbf{T}_H \cdot \mathbf{x} \le \mathbf{C}_T, \\ \mathbf{T}_A \cdot \mathbf{x} = \mathbf{D}_{HL}, \\ \mathbf{L}_{capacity} \le \mathbf{x}, \end{cases} \tag{2}$$

where $\mathbf{b}$—the objective coefficients vector (in our case it could be economic coefficients of generation technologies), $\mathbf{T}_A$—coefficients matrix of equations constraints; $\mathbf{T}_H$—coefficients matrix of linear inequality constraints; $\mathbf{C}_T$—the vector of the generation technologies capacity; $\mathbf{D}_{HL}$—the vector of the local heat demands quantities; $\mathbf{L}_{capacity}$—the low boundary vector of minimal capacity load of technologies.

This mathematical model allows to distribute local heat demand for local generation technologies with regard to economic aspect. The elements of

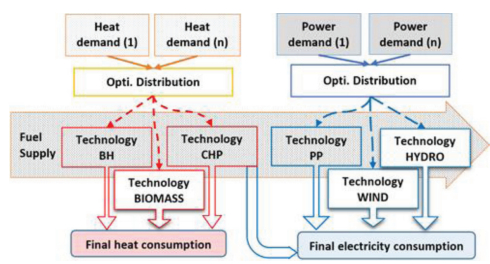


Figure 1. Structural scheme of system criticality assessment method.

matrix of equations constraints $\mathbf{T}_A$ are composed of coefficients of generation technologies, which could be used in generation process. The elements of matrix of linear inequality constraints $\mathbf{T}_H$ are identification of local generation technologies.

The demand of electricity is distributed for generation technologies by the same optimization model as heat demand. Preference is given to technologies using renewable energy sources (hydro power plants, wind power plants, etc.).

Gas supply system is defined by graph of 89 main pipelines. The natural gas is supplied to the system from two sources: the debit of import from neighbor country is 31.2 Mm^3/day and the other source is terminal of liquid natural gas, the debit is 11 Mm^3/day. The mathematical optimization model (optimization of maximum flow with goal programing) is used to simulate gas supply system.

Gas supply network is represented as graph:

$$G = (V, E),\ V = V_{FN} \cup V_{CN},\ \text{there } V_{FN} \cap V_{CN} = \varnothing \tag{3}$$

where V_{FN}—set of the final pipeline nodes of graph; V_{CN}—set of the pipeline connection nodes of graph; E—set of the edges (edge represents physical pipelines), which connect nodes V.

One of the model aims is to maximize the satisfaction of consumer demands. The maximum flow optimization method was used to achieve this goal. Simplex method of linear programing was used to find the maximum flow in the pipeline network. The mathematical model of this problem could be written as:

$$\max_x \mathbf{f}^T \cdot \mathbf{x},\ \text{when } \begin{cases} \mathbf{C}_M \cdot \mathbf{x} = 0, \\ \mathbf{C}_{FN} \cdot \mathbf{x} \le \mathbf{D}_{FN}, \\ \mathbf{L}_{flow} \le \mathbf{x} \le \mathbf{M}_{flow}, \end{cases} \tag{4}$$

where $\mathbf{f}$—is the objective coefficients vector (in our case the edges of incoming flow into final nodes), $\mathbf{C}_M$—coefficients matrix of equations constraints; $\mathbf{C}_{FN}$—coefficients matrix of linear inequality constraints; $\mathbf{D}_{FN}$—the vector of the demands quantities of final nodes; $\mathbf{L}_{flow}$—the low flow boundary vector of pipeline edges; $\mathbf{M}_{flow}$—the maximum flow boundary vector of pipeline edges; $\mathbf{x}$—the vector of pipeline edges.

This mathematical model allows to evaluate the quantities of supplied gas to the final nodes (consumers). The constraints of the matrix elements $\mathbf{C}_M$ are coefficients of directed graph (it means that in connection nodes should be balance). The coefficients values of incoming edges into the node V_{CN} are equal to –1, and the coefficients values of outgoing edges from the node are equal to 1. The balance of incoming and outgoing flow must be on each pipeline connection node of graph.

The elements of matrix of linear inequality constraints $\mathbf{C}_{FN}$ are composed by coefficients of incoming edges to final nodes V_{FN}. And the coefficients' values of matrix of linear inequality constraints are equal to 4. The elements of low flow boundary vector of pipeline edges are composed of 0. The values of elements of maximum flow boundary vector are dependent on pipeline diameter, pipeline length, the pressure in the system, specific gravity of the gas and other coefficients.

All these optimization models enable the implementation of directives (economical, ecological, etc.) and emergency management plans. Monte Carlo method (MC) was used to obtain simulated data of the operation of the system. Operation statement of system element was generated in each iteration to simulate the real system work. The estimates of failure probability of system elements were used from reports and journals: Security of supply of electricity market Lithuania monitoring report, 2012; Energy in Lithuania 2012, 2013; Gas pipeline incidents, 2011; Lurie, 2008.

The criticality of the kth element may be estimated using the reliability indicators of final consumers obtained in case when kth element is out of order

$$C^{(k)}(t) = 1 - \sum_{i=1}^{M} cf_i^{(k)}(t) \cdot \beta_r,\ k = 1, 2, \ldots, N, \tag{5}$$

where N—number of the elements in the energy system; $cf_i^{(k)}(t)$—the reliability indicator that shows how much the energy demand is satisfied for the ith element; β_r—the weighted coefficient of the rth final consumer within system (for instance, weighted coefficients are estimated with regards to the energy demand of consumer, and they satisfy equality $\beta_1 + \cdots + \beta_M = 1$; M—number of the final consumers in the energy system).

The system element criticality value is from interval [0; 1]. For example, $C^{(k)}(t) = 1$ means that disruption of the kth element work stops the operation of all energy infrastructure at time moment t. The criticality rage could be described as shown in Figure 2.

The importance measures were estimated to compare the impact of gas supply system elements with the baseline scenario (all system elements availability are random). Fussell-Vesely (FV) and Birnbaum Importance (BI) measures of gas supply system elements were estimated in this work. The purpose of this analysis was to identify components with high value of FV and BI. When both importance measurements are high, the criticality can be

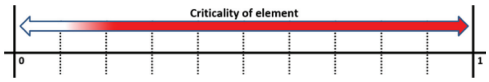


Figure 2. The element criticality value range.

reduced by decreasing the components unavailability or by improving the defense in depth against a failure of the component (Borst et al, 2001; Kim et al, 2009; Espiritu et al, 2007; Baroud et al, 2014). The selection of system components whose criticality needs to be reduced are performed by *FV*.

$$I_k^{FV} = \frac{C(base) - C(x_k = 0)}{C(base)}, \tag{6}$$

where $C(base)$ is the average of criticality, when all system elements availability is random; $C(x_k = 0)$ is average criticality, when kth element is working (with probability equals to 1) and other elements availability is random.

The *BI* is completely dependent on the structure of the system model and is independent on the current probability of the basic event.

$$I_k^{BI} = C(x_k = 1) - C(x_k = 0), \tag{7}$$

where $C(x_k = 1)$ is kth element is 100% unreliable and availability of other elements is random.

The logistic regression model was designed to examine how functionality of the gas supply system elements affect energy system criticality value by using probability scores as the predicted values of the dependent variable of gas supply system. The purpose of this statistical analysis is to determine which elements of gas supply system influence high value of system criticality (statistical classification model) (Ozdemir, 2011; Flahaut, 2004; Fang et al, 2012).

Categorical variable Y is defined

$$Y = \begin{cases} 0, & C^{(0)} \notin I, \\ 1, & C^{(0)} \in I, \end{cases} \tag{8}$$

where $C^{(0)}$—criticality of system when operating statement of all elements are random with regard to its failure probabilities; I—analyzed interval of criticality.

The mathematical model is expressed as

$$p_i = \frac{e^{z(x_i)}}{1 + e^{z(x_i)}}, \quad z(x_i) = b_0 + \sum_{j=1}^{N} b_j x_{ji}, \tag{9}$$

where $i = 1, \ldots, n$, $j = 1, .., N$, p_i—probability that criticality value is from analyzed interval I $p_i = P(Y = 1)$, i—iteration; N—number of explanatory; x_i—the realization of system elements availability; b_j—coefficients of logistic regression.

Simulation data of system functionality: availabilities elements, criticality value of system with regard to availabilities elements. The effect of jth element unavailability to system criticality is estimated by the odds ratio of system element.

3 THE CRITICALITY ANALYSIS AND MEASUREMENT OF ENERGY SYSTEM

The pilot numerical calculations were performed to demonstrate our criticality the applicability of assessment method for any system. The assumptions of the system: closed energy system; the demands of heat and power were selected from statistical sources (Energy in Lithuania 2012, 2013). The system was composed of 151 elements. The parameters of generation technologies are presented in Table 1 and Table 2.

The energy system scheme is presented in Figure 3.

The criticality assessment was performed when analyzed kth element is out of order, operating statement of other elements is obtained using random number generator with respect to its failure probability: scenario of elements availability is generated (generation process is repeated 100000 times). The experiment is repeated when kth element operates with probability equal to 1, operating statement of other elements is obtained using random number generator with respect to its failure probability.

The estimate of system criticality is calculated in each case. Obtained conditional probability distributions of elements criticality of power system, when kth element is out of order and operating statements of other elements are random, are presented in Figure 4.

This graph shows the relative frequency of each element (of gas supply system) criticality of the power system. According to relative frequency, the range of criticality value can be divided into intervals: 1st interval [0, 0.05)—the vicinity of zero, the

Table 1. The list of electricity generation technology of model.

	Installed power capacity (MW)	Installed heat capacity (MW)
Hydro power plant	100.8	0
Small hydro power plant	25.7	0
Power plant 2 unit	1955	1752
Wind farm 2 unit	201.7	0

Table 2. The list of summed heat generation technology of model.

	The quantity of CHP	The quantity of BH	The quantity of biofuel boiler houses	Sum installed power capacity (MW)	Sum installed heat capacity (MW)
City A	1	7	3	170	1068.5
City B	1	4	1	30.8	1062
City C	1	2	5	186	732
City D	1	8	7	35	741
City E	1	5	1	14	612
City F	2	4	2	384	2955

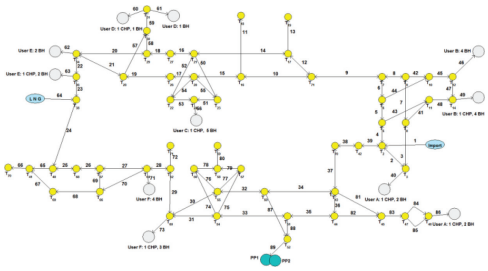


Figure 3. The scheme of analyzed energy system.

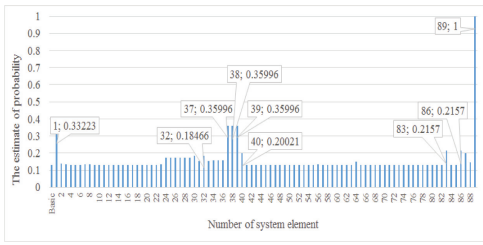


Figure 5. The estimate of probability of non-null criticality of power system in case of analyzed kth element is out of order.

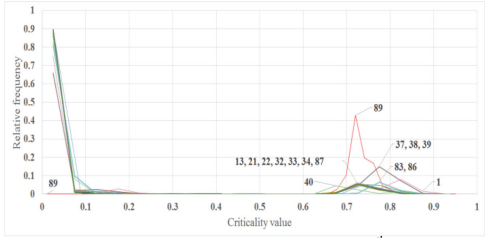


Figure 4. The relative frequency distribution of kth element criticality of the power system $k = 1, \ldots, 89$th.

completely functionality state is the most common state of the system; 2nd interval [0.05, 0.25); 3rd interval [0.25, 0.6); 4th interval [0.6, 1]. The criticality is described by mixture distribution according to the graphs of relative frequencies, see Figure 4.

The 89th element of gas supply system is the most critical element for the power system: in most cases, its criticality value is from the interval [0.56, 0.947]; mode is 0.72, median is 0.727 and mean is 0.733, and the estimate of probabilities of non-null criticality is 1, as shown in Figure 5. The other critical elements are: 1th, 37th, 38th, 39th, 86th. The group of element (37th, 38th, 39th) has important transmission elements in the gas network and connect major customers. The relative frequencies of the 1st and the 2nd intervals are high, but the criticality values are low, detailed analysis is not essential for these intervals. The power system criticality interval $I = [0.6, 1]$ is analyzed in more detail only (in the next step).

The obtained conditional probability density functions (Fig. 4) are used to calculate characteristics of element criticality: the estimate of probability of non-null criticality $P(X > 0 \mid e_k)$, e_k—kth element is out of order, $k = 1, \ldots, 89$th is presented in Figure 5.

Obtained conditional probability distributions of elements criticality of heat system, when kth element is out of order and the operation statements of other elements are random, are presented in Figure 6.

The situation of criticality of heat system is much better than the power system, as shown in Figure 6.

Generation capacity is much larger than customers demand, and there are more generation technologies with different types of fuel (gas, oil, biofuel, etc.). The most critical element is the 1th element (main gas import pipeline), see in Figure 7. There are several critical elements in both systems (power and heat): 37th, 38th, 39th, see Figure 5 and Figure 7. The critical element of heat system depends on the location, its mean, element that connects large customers with main pipeline networks. The estimates of probability of non-null criticality (of heat system) of gas supplies system elements is shown in Figure 7.

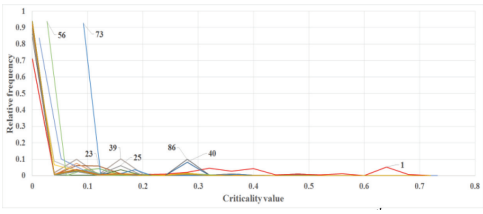


Figure 6. The relative frequency distribution of kth element criticality of the heat system $k = 1, \ldots, 89$th.

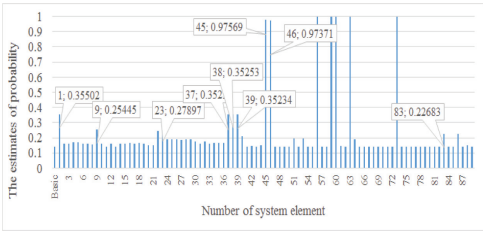


Figure 7. The estimates of probability of non-null criticality of heat system in case of analyzed kth element is out of order.

The other elements to be noticed are 56th, 59th, 60th, 73th elements. As shown in Figure 7, the estimate of probability value of non-null criticality is 1. The 9th and the 23th elements are connections between the main pipeline and the consumers. The estimate of probability of non-null criticality are 0.25 (9th) and 0.27 (23th), they are higher than average probability (0.14) of other system elements.

To identify the most important elements of the energy system we used the importance measurement of Fussell-Vesely and Birnbaum importance. The importance measurement of Fussell-Vesely and Birnbaum importance of all gas supply system elements were calculated to determine the most critical elements of the system.

The result (only with not null importance measurements) for the criticality of power system and heat system are presented in Figure 8 and Figure 9.

There is one important element of gas supply system for the power system, as shown in Figure 8. This element is 89th: $FV = 0.82$ and $BI = 0.72$ (the values of FV and BI are high). The other elements of the gas supply system are not so important neither for power system, neither for heat system. The results of importance measurement of heat system showed that other elements of gas supply system have no significant impact on the heat system.

The criticality assessment results show that the gas supply system has more influence on the power system than the heat system.

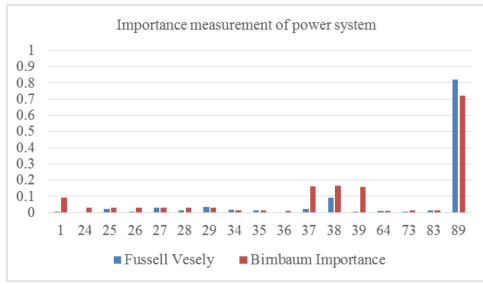


Figure 8. Importance measurements of power system.

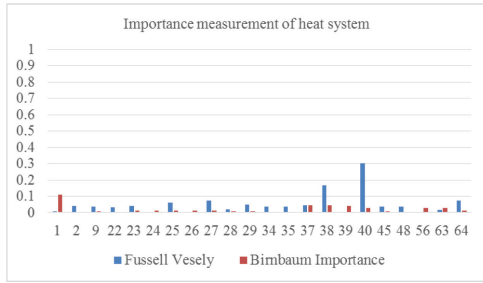


Figure 9. Importance measurements of heat system.

It is important to determine which combination of gas supply system elements more affects power system.

The logistic regression result is the list of gas supply system that have the greatest impact on the system criticality value.

The simulation data for logistic regression analysis was composed of basic scenario (the operating statements of all elements are random). Data was obtained by Monte Carlo method (with 100000 repeats). The categorical variable Y is estimated by the equation (7), the interval of power system criticality which is analyzed in the logistic regression analysis is $I = [0.6, 1]$.

The statistically significant ($\alpha = 0.05$) odds ratios of gas supply system elements are presented in Figure 10.

The gas supply system elements that have the greatest impact on power system criticality value: 89th, 32th, 33th, 34th (from the results presented in Figs. 4, 5, 7 and 8).

When element 89th is out of order, the power system criticality value belongs to considered interval. 89th element is excluded from the analysis because of quazi separation problem.

When element 33th is out of order, it increases the chance (4.7 time) that criticality value of power system will be from the interval [0.6, 1]. The 32th and 34th elements increase the chance 3.8

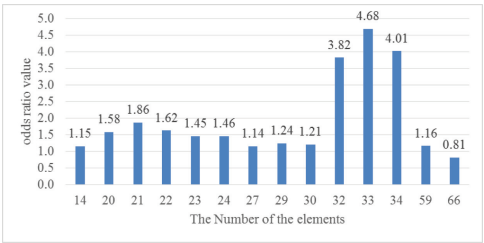


Figure 10. Odds ratio of gas supply system elements.

and 4 times the criticality value will be from the interval [0.6, 1].

4 CONCLUSIONS AND RESULTS

The criticality assessment method supplemented by importance measurements and elements classification method (by logistic regression) was presented in this paper.

The criticality assessment pilot calculation of hypothetical system was performed to demonstrate the practical application of the method: gas supply system reliability influence on power and heat systems and to identify most critical elements.

Criticality characteristics of gas supply system (the estimate of probability of non-null criticality, mean value of criticality, the importance measurements and odds ratio for each element) were estimated. The estimates of probability of non-null criticality (of power system) are from interval [0.13, 1], the mean values of criticality (power system) are from interval [0.065, 0.733]. The estimates of probability of non-null criticality (heat system) are from interval [0.163, 1], the mean values of criticality (heat system) are from interval [0.009, 0.118].

The identification of the most critical components (or their groups) of gas supply system and assessment of their impact on power and heat system could be performed by the proposed method.

The more detailed analysis of power system allowed to determine the group of elements, which failures increase the odds to achieve the high value of criticality (i.e. value greater than 0.6) by logistic regression model.

The estimation of importance measurements (*FV* and *BI*) allows to determine system elements which criticality could be reduced by decreasing unavailability of these element. In the numerical example the 89th element was determined.

The list of elements obtained by logistic regression correlates with the list of elements determined by criticality assessment method.

The implementation of this assessment method could be performed for real country energy system, ensuring privacy of results for security.

ACKNOWLEDGEMENTS

This research was funded by a grant (No. ATE-04/2012) from the Research Council of Lithuania.

REFERENCES

Augutis, J., Jokšas, B., Krikštolaitis, R., Žutautaitė, I., 2014 Criticality assessment of energy infrastructure. *Technological and economic development of economy*, (In press).

Baroud, H., Barker, K., Ramirez-Marquez, J.E., Rocco S., C.M., 2014. Importance measures for inland waterway network resilience, *Transportation Research Part E: Logistics and Transportation Review*, Volume 62, Pages 55–67, ISSN 1366-5545.

Borst, M., Schoonakker, H., 2001 An overview of PSA importance measures, *Reliability Engineering & System Safety*, Volume 72, Issue 3, Pages 241–245, ISSN 0951-8320.

Espiritu, J.F., Coit, D.V., Prakash, U., 2007. Component criticality importance measures for the power industry, *Electric Power Systems Research*, Volume 77, Issues 5–6, Pages 407–420, ISSN 0378-7796.

Fang, W.T., Huang, Y.W., 2012. Modelling Geographic Information System with Logistic Regression in Irrigation Ponds, Taoyuan Tableland, *Procedia Environmental Sciences*, Volume 12, Part A, Pages 505–513, ISSN 1878-0296.

Flahaut, B., 2004. Impact of infrastructure and local environment on road unsafety: Logistic modeling with spatial autocorrelation, *Accident Analysis & Prevention*, Volume 36, Issue 6, November 2004, Pages 1055–1066, ISSN 0001-4575.

Gas pipeline incidents, 2011. 8th EGIG report, December 2011, Doc. Nr. 11.R.0402 v2.

Hammoum, H., Bouzelha, K., Aider, H.A.,2013. Naceur Eddine Hannachi, Tanks criticality assessment by the dependability method. Case study, *Engineering Failure Analysis*, Available online 31 July 2013, ISSN 1350-6307.

Huang, C.N., Liou, J.J.H., Chuang, Y.C., 2014. A method for exploring the interdependencies and importance of critical infrastructures, *Knowledge-Based Systems*, Volume 55, Pages 66–74, ISSN 0950-7051.

Jenelius, E., Mattsson, L.G., 2014. Road network vulnerability analysis: Conceptualization, implementation and application, Computers, *Environment and Urban Systems*, Available online 1 March 2014, ISSN 0198-9715.

Kim, K., Han, S., 2009. A study on importance measures and a quantification algorithm in a fire PRA model, *Reliability Engineering & System Safety*, Volume 94, Issue 5, Pages 969–972, ISSN 0951-8320.

Kulawiak, M., Lubniewski, Z., 2013. SafeCity—A GIS-based tool profiled for supporting decision making in urban development and infrastructure protection, *Technological Forecasting and Social Change*, Available online 5 October 2013, ISSN 0040-1625.

Lietuvos energetika 2012. Energy in Lithuania 2012 // Kaunas: *Lietuvos energetikos institutas*, 2013. 17 p. ISSN 1822-5268.

Lurie, V.M., 2008. Modeling of Oil Product and Gas Pipeline Transportation, *Wiley-VCH*, pp. 1–214., ISBN: 978-3-527-40833-7.

Ozdemir, A., 2011. Using a binary logistic regression method and GIS for evaluating and mapping the groundwater spring potential in the Sultan Mountains (Aksehir, Turkey), *Journal of Hydrology*, Volume 405, Issues 1–2, 21.

Roelich, K., Dawson, D.A., Purnell, P., Knoeri, C., Revell, R., Busch, J., Steinberger, J.K., 2014. Assessing the dynamic material criticality of infrastructure transitions: A case of low carbon electricity, *Applied Energy*, Available online 17 February 2014, ISSN 0306-2619.

Rodríguez-Núñez, E., García-Palomares, J.C., 2014. Measuring the vulnerability of public transport networks, *Journal of Transport Geography*, Volume 35, Pages 50–63, ISSN 0966-6923.

Rodríguez-Núñez, E., Carlos, J., 2014. García-Palomares, Measuring the vulnerability of public transport networks, *Journal of Transport Geography*, Volume 35, Pages 50–63, ISSN 0966-6923.

Salling, K.B., 2013. A New Approach to Feasibility Risk Assessment within Transport Infrastructure Appraisal, *Procedia—Social and Behavioral Sciences*, Volume 74, Pages 468–477, ISSN 1877-0428.

Security of supply of electricity market Lithuania monitoring report, 2012. Referred on the 10th of February in 2014 Link to the internet http://www.enmin.lt/lt/activity/veiklos_kryptys/elektra_ir_siluma/MONITORINGAS.pdf.

Shuang, Q., Zhang, M., Yuan, Y., 2014. Node vulnerability of water distribution networks under cascading failures, *Reliability Engineering & System Safety*, Volume 124, Pages 132–141, ISSN 0951-8320.

Zonouz, S., Haghani, P., 2013. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior, Computers & Security, Volume 39, Part B, Pages 190–200, ISSN 0167-4048.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparing societal consequence measures of outages in electrical distribution systems

F. Landegren, J. Johansson & O. Samuelsson
Department of Industrial Electrical Engineering and Automation, Lund University, Sweden
Lund University Centre for Risk Assessment and Management, Sweden

ABSTRACT: Quality of supply regulations are today in use in a large number of countries. While these regulations are likely to decrease the direct economical consequences from power outages it is less clear to what extent they take into account the societal criticality of consumers. In order to advance knowledge in this area, two different ways of estimating consequences of power outages are here contrasted. In recent years a system, named Styrel, has been introduced in Sweden, intended to enable prioritization of critical power customers from a societal perspective during times of power shortage. The Styrel prioritizations are here used as a proxy for the societal consequences of power outages. The second way of measuring consequences that arise makes use of the Swedish power outage regulation concerning outage compensations to customers. A case study is carried out for a real-life distribution system in Sweden, where failures of different sizes are simulated and the two consequence measures are calculated for each failure scenario. The overall result is that the present power outage regulation poorly mirrors the societal consequences as estimated by the Styrel prioritizations, leading to the conclusion that present day power outage regulation in Sweden is not satisfactorily taking some aspects of societal criticality into account.

1 INTRODUCTION

Society is today highly dependent on a number of critical infrastructures. Among these, arguably, few are as vital as the electrical power system, considering that many other critical infrastructures are to some extent dependent on a reliable supply of electricity. Not only is the power system of vital importance for society, its importance is also increasing, something which is reflected in steeply increasing customer costs from power outages. A Norwegian study showed that within the short time span of 10 years, from 1991 to 2001, costs for a 1 h interruption grew by a factor of 4 within the commercial sector and with as much as a factor of 12 in the agricultural sector. Cost also nearly doubled among residential customers and in the industrial sector, with inflation taken into account (Kjolle et al. 2008). Besides the direct costs that outages give rise to, power outages might also give rise to indirect consequences. As discussed by Rao et al. (2010), while interruptions in a small residential area will normally only cause direct damage, such as food spoilage or inconvenient building temperatures, more widespread interruptions with a longer duration might cause indirect damage such as civil disobedience, breakdown of logistic chains, etc. There has for a long time existed an awareness that the power system should be managed in a way that takes into account the economic costs that an outage will entail for different consumer groups (Sanghvi 1982). In order to achieve this power quality regulations have been introduced in a number of countries. (For a review of regulations in European countries see Tahvanainen et al. (2004), for a review of regulations in American states see Sappington et al. (2001)). However, these regulations, although beneficial for individual customers, might not lead to a result that is favorable when the well-being of society is taken into account. This difficulty is high-lighted by Linares and Rey (2012). They suggest that the consequences of electricity outages can be classified into three categories: direct economic impacts, indirect economic impacts and social impacts and they claim that an optimal analysis should capture all three impact categories. The regulations in place today in Europe and America are likely to take account of the first of these categories. It is however an open question to what extent the second and third categories are taken into account.

Linares & Rey point out that a major obstacle to attaining an optimal analysis is lack of data. It is hard to find credible data concerning the indirect and the overall societal consequences from power outages. To overcome this obstacle assessments that have been done as part of a Swedish power regulation, Styrel, are here used as a proxy for the societal criticality of power customers.

The purpose of the paper is to provide insights concerning how well a present day quality of supply regulation in Sweden reflect societal consequences as measured through the Styrel prioritizations system. The quality of supply regulation, which is one of the two power quality regulations in use in Sweden today, has been chosen because it has a major impact on the revenue of power companies and can therefore be assumed to have a large influence on how power companies invest in as well as restore their networks.

1.1 *Background*

A large number of studies assess the economic costs incurred by power outages. Woo and Pupp (1992) review 16 such studies and identify four principal methods that are used for making these economic assessments, they are briefly presented below:

Customer surveys: This method, which is the one used most frequently, consists in asking consumers questions concerning perceived consequences of a power outage of certain duration. The question can be either direct or indirect. In the former case the customer is asked to assess the cost of the outage. In the latter case the customer will instead be asked questions concerning what they would pay to avoid the outage, known as the Willingness To Pay (WTP), or how much the customer would demand in return for accepting to suffer the outage, known as the Willingness To Accept (WTA).

Case studies: In this method a past power outage is analysed in order to determine the consequences that resulted from it. Widely studied power outage are the New York outage in 1977 and the blackout of Northeast US in 2003.

Market based methods: This is also known as revealed preference, as opposed to the stated preference obtained through surveys. When using this method the consequences of an outage are assessed based on the customers' behavior on the market. Expenditures on backup facilities and the use of interruptible contracts can, for instance, provide information on how households or industries value interruptions of the power supply.

The production function approach: This method estimates the consequences of outages through lost production (for firms) or lost leisure time (for households). The cost is calculated as the ratio of an economic measure (e.g., gross output, gross domestic product GDP) and a measure of electricity consumption. The main benefit of the approach is that it makes use of readily obtainable data. The draw-back is that it makes unrealistic assumptions. For instance it says that if x% of the yearly power supply of a company is lost its yearly productivity will decrease by x%. However this could lead to overestimations in case some form of production can go on also without power supply and it can lead to underestimations if power outages cause reduction in productivity not only during the time of the outage but afterwards as well due to long term damages. (De Nooij 2007: Balducci et al. 2002; Linares & Rey 2012; Samdal 2003; Kjolle 2008).

Once data has been gathered concerning outage consequences, they can be used to create a cost model. Three main kinds of cost models are used by power system planners. Customer Damage Function (CDF) models represent the costs as a function of the interruption duration. Cost of Energy Not Supplied (CENS) models represent the costs as a function of the unsupplied energy. Finally, Combined Cost Models (CCM) represent interruption costs as a sum of two components: one is a function of the interruption load demand ILD, another is a function of the expected energy not served EENS. (Raesaar et al. 2006, Bozic 2000).

Among the categories defined by Linares & Rey, referred to above, present methods for assessing consequences from power outages are likely to take direct economic impacts into account in a satisfactory way. However, it is less likely that indirect economical or societal consequences are taken into account satisfactorily. Customer surveys measure only the economic consequences for the informant not for those actors depending on the informant or the interests of society in general. The market based approach reflects only the interests of the consumer, which is likely to be mostly concerned with how outages will affect their own revenue or household economy. Therefore it will mainly assess the size of primary economic consequences. The product function approach by its very nature will focus on the direct economic consequences. The case study is clearly advantageous for assessing societal consequences since in hindsight the relevant data is obtainable, although perhaps not easily so. Its weakness though is that it is far from clear what inferences that can be justifiably drawn from past accidents with respect to future ones. When, for instance, studies based on evidence from the 1977 New York black-out are used as guides to understanding the consequences from present day outages it should be borne in mind what remarkable changes society and technology have undergone in the meantime. Conclusions should therefore be based primarily on the relatively few events that have occurred in recent time.

In the following a Swedish quality of supply regulation is described and the Styrel system is also introduced. The Styrel system is here used as a new means of estimating societal consequences from power outages.

1.2 *Outage compensation*

The present regulatory system for outage compensation was initiated by the Swedish government in 2005. In this regulation the compensation increases with the outage time (see Table 1.) and hence the regulation acts as an incentive to make the power companies improve the reliability of their systems so that long power outages will be less likely.

Table 1. Disruption compensations for different power outage lengths.

Outage time (days)	Compensation (% of yearly fee)	Minimum compensation (SEK)
>0.5	12.5	900
>1	37.5	1,800
>2	62.5	3,600
>3	87.5	4,500
>4	112.5	5,400
>5	137.5	6,300
>6	162.5	7,200
>7	187.5	8,100
>8	212.5	9,000
>9	237.5	9,900
>10	262.5	10,800
>11	287.5	11,700
>12	300	12,600

Table 2. Consumer categories as defined in Styrel (The number of points given to customers is in most, but not all cases, in accordance with below).

Priority class	Point	Power customer
0	8	Critical facilities belonging to the power company
1	8	Consumers that in a short time span (hours) have a large impact on life and health
2	7	Consumers that in a short time span (hours) have a large impact on the functioning of society
3	6	Consumers that in a longer time span (days) have a large impact on life and health
4	5	Consumers that in a longer time span (days) have a large impact on the functioning of society
5	4	Consumers that represents large economic values
6	3	Consumers that have a major importance for the environment
7	2	Consumers that have importance for societal and cultural values
8	1	Other consumers

1.3 *Styrel*

The Swedish Energy agency has in cooperation with the Swedish Civil Contingencies Agency and Swedish national grid developed Styrel (MSB 2010). It is meant to be used during times of power shortage to prioritize consumers based on their importance to society. Consumers are grouped into nine predefined priority classes and each consumer is also given a number of points (see Table 2). Governmental, county and municipal levels are all involved in the process of deciding which power customers to prioritize. The prioritizations of customers to supply in case of power shortages are made according to the following rules:

1. The overall number of non-supplied customers with priority 0 or 1 should be minimized
2. The sum of points for all non-supplied customers with priority 2 or less should be minimized
3. Rule 1) has precedence over rule 2).

2 METHODOLOGY

As explained in the previous section, the purpose of this paper is to contrast present Swedish outage regulation against societal consequences that arise as estimated through Styrel.

To do this a case study of a distribution system of a midsize city in Sweden (see Fig. 1) is carried out. The system has also been studied in (Jönsson et al. 2008). The distribution system is an 11 kV system consisting of altogether 1203 components, 539 nodes (representing network stations, transformers, bus bars and feeder station breakers) and 664 edges (representing underground cables). The network is supplied from 10 in-feed transformers from higher voltage levels and serves roughly 40,000 customers. Only topology is considered in the model of the network using a graph model where the graph $G(V, E)$ is defined by two sets, V consisting of

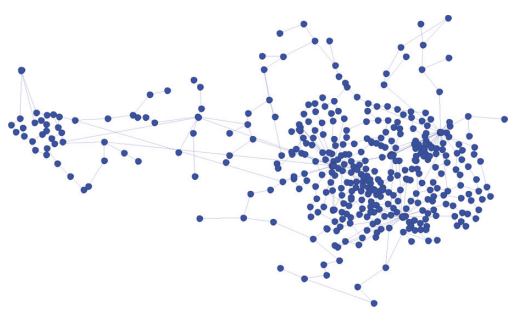


Figure 1. The power distribution network.

the N nodes and E consisting of the M edges (or links), defined as (Johansson 2010):

$$V = n_1 \quad n_2 \quad \dots \quad n_N$$

$$E = e_1 \quad e_2 \quad \dots \quad e_M$$

The complete set of components in the network C is constituted by the sets V and E, i.e.:

$$\begin{aligned} C &= n_1\, n_2 \quad \dots \quad n_N \quad e_1 \quad e_2 \quad \dots \quad e_M \\ &= c_1 \quad c_2 \quad \dots \quad c_{N+M} \end{aligned}$$

An adjacency matrix A is used to represent the connections in the network:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix}$$

where a_{ij} is 1 if n_i is connected to n_j by means of an edge and 0 if no connection exists. A failure of node n_i is simulated by setting all elements in row i and column i of the adjacency matrix A to 0. A failure of edge e_i connecting n_j and n_k is simulated by setting a_{kj} and a_{jk} to 0.

Capacity is not considered in the network model, e.g. there is no limit concerning the amount of power that can pass through nodes or edges. A customer is therefore considered to be supplied with power if there is at least one unbroken path leading from the network station supplying the customer to at least one of the ten in-feed transformers.

A customer is considered to be supplied with power if there is at least one unbroken path leading from at least one of the ten in-feed transformers to the network station supplying the customer. A breadth-first search strategy is used to find all nodes that can be reached from at least one transformer. The possible drawbacks of only considering topology are discussed in 4.1.

The effect of outages are simulated using the network model, altogether 6 different strain sizes are studied: N-1, N-2, N-3, N-6, N-9 and N-12. (N-x denotes a failure of x components among the total number of components, N, in the system.) For N-1 and N-2 all possible failure scenarios are analyzed. The strain vectors for the N-1 and N-2 strain sizes ($SV_{N\text{-}1}$ and $[\![SV]\!]_{\downarrow}(N-2)$) are defined:

$$SV_{N-1} = \begin{matrix} C_1 \\ C_2 \\ \vdots \\ C_{N-1} \\ C_N \end{matrix}$$

$$SV_{N-2} = \begin{matrix} C_1 & C_2 \\ C_1 & C_3 \\ \vdots & \vdots \\ C_{N-2} & C_N \\ C_{N-1} & C_N \end{matrix}$$

For higher strain sizes sampled scenarios are used due to the excessive simulation times that would result if a complete scenario set was used. One failure scenario takes about 15 ms to calculate (using a DELL laptop with 5 core processor, 8 GB RAM and 64-bite OS) therefore a complete N-3 analysis, encompassing about 578 million scenarios, would require roughly 7 weeks of simulation time. The strain vectors containing sampled scenarios have the following form:

$$SV_{N-x} = \begin{matrix} c_{r1} & \cdots & c_{rx} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rx} \end{matrix}$$

where C_{ri} denotes the i:th component randomly chosen among the set of still functioning components. One million randomly generated failure scenarios are used for the N-3, N-6, N-9 and N-12 strain sizes.

For each failure scenario, outage compensation and Styrel consequence is calculated. The overall Outage Compensation (OC) for a certain scenario is calculated in the following way:

$$OC = \sum_{i=1}^{N_1} Fee_i * NormComp(t) + MinComp(t) * N_2$$

$N_1 + N_2$ is the number of customers without power. N_1 is the number of customers that are receiving more than the minimum compensation (see Table 1) and Fee_i is the yearly fee for customer i. *NormComp* and *MinComp* are functions of the outage time of the particular distribution stations (see Table 1). In this paper the outage time for all customers is assumed to be 12 h meaning that *NormComp* is 12.5% and *MinComp* is SEK 900. As is seen in Figure 2 the number of customers (87% of customers) that will get the minimum compensation after a 12 h outage is relatively high since all customers with a yearly fee of SEK 7,200 or less will get this. This means that small customers will carry more weight, relatively, than if a longer outage time was chosen.

By ranking the OC consequence values for all simulated scenarios (see Table 4) the outage compensation Normalised Rank (ONR) can be obtained using the following formula:

ONR = (N-*Rank*)/(N-1)

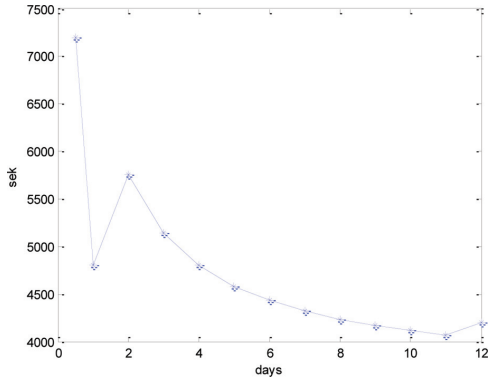


Figure 2. Highest yearly fee that will give minimum compensation as function of days of outage.

Scenarios are ranked in descending order and scenarios with the same consequence are given the same rank, N is the number of different rank levels.

The Styrel Normalized Rank (SNR) is determined by using the Styrel prioritization rules (see 1.3). A scenario A has higher rank than a scenario B if the number of non-supplied customers with priority 0 or 1 is larger in A than in B or, if the number of non-supplied customers with priority 0 or 1 is the same in A and B, the sum of points for all non-supplied customers with priority 2 or less is higher in A than in B. When the scenarios for a certain strain level have been ranked according to this ranking procedure the Styrel Normalized Rank (SNR) of each scenario is described as follows:

$$\text{SNR} = (N\text{-}Rank)/(N\text{-}1)$$

As before, scenarios with the same consequence will get the same rank and N is the number of different rank levels.

The following simple example illustrates how ONR and SNR is calculated: a scenario ranked nr 577 (concerning outage compensation or Styrel) among a total number of 1000 rank levels will be given the ONR/SNR (1000–577)/1000 = 0.423. The ONR and SNR will always vary within the interval [0,1]. For the subset of scenarios without affected top priority customers (priority 0 or 1) the correlation between the two ranking methods are analysed. In order to do this we use Spearmans rank correlation coefficient.

In order to test how well the result converges, for this number of scenarios, the coefficient of variation, α, is applied to the outage compensation results.

$$v_i = [x_1, x_2, \ldots, x_i]$$

$$\alpha_i = \frac{std(v_i)}{mean(v_i)}$$

Std denotes standard deviation and v_i is a vector containing the first i simulation results. We use simulation results concerning outage compensation, then $\alpha_{1,000,000}$ is 1.48 for N-3, 1.06 for N-6, 0.88 for N-9 and 0.76 for N-12 and it quickly converges to these final values meaning that one million samples should be sufficient.

3 RESULTS

Using the ranking methodology described in the previous section we have ordered outage scenarios in accordance with how a DSO would prioritize them based on the two schemes. This is done for 6 different scenario runs, N-1, N-2, N-3, N-6, N-9 and N-12. On the x-axis is shown the ONR, i.e. how the scenarios would be ranked based on the outage compensation scheme, on the y-axis is shown the SNR, i.e. the scenarios as ranked based on the Styrel scheme. By arranging the plots in this way the decision making perspective of the DSO is captured and it can easily be seen if the two ways of reaching a decision concerning investments in the network are consistent or not. If there is indeed a close agreement between the two measures the scenario points will form a more or less straight line, and the correlation between ONR and SNR will be close to 1. On the other hand, any major aberration from this straight line, or a correlation significantly lower than 1, indicates that the ONR is not reflecting the societal consequences shown by the SNR.

The results from the simulations of N-1, N-2 and N-3 are given in Figure 2 to 4. As can be seen in Figure 2, for N-1, there is a high correlation between the results given by the two ranking schemes, but several scenarios get high SNR

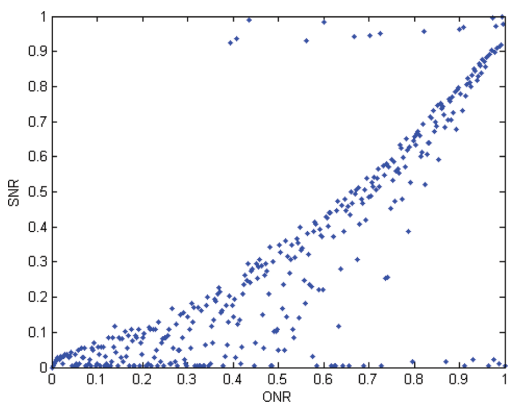


Figure 3. All N-1 scenarios.

and low ONR and vice versa. In *N*-2 (Fig. 4) and *N*-3 (Fig. 5) patterns emerge that are not evident for N-1. The scenarios are divided into several segments, i.e. groups of scenarios that are separated in space from other groups of scenarios. It can be seen that they are separated along the y-dimension, based on the SNR values of the scenarios (distribution of the segments is indicated in Fig. 5). Investigation has shown that each such segment contains scenarios in which a certain number of top priority customers (priority 0 or 1) are affected. The lowest segment contains scenarios with no affected top priority customers, the next higher segment contains scenarios in which one top priority customer is affected, the following segment contains scenarios with two affected top priority customers, and so forth. The total number of these segments increases with the magnitude of the strain since the likelihood of several top priority customers being out at once increases with increasing strain size. It can be seen also that within each segment there is a clear correlation

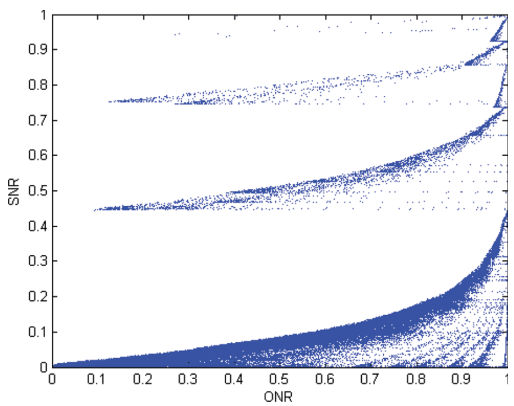


Figure 4. All *N*-2 scenarios.

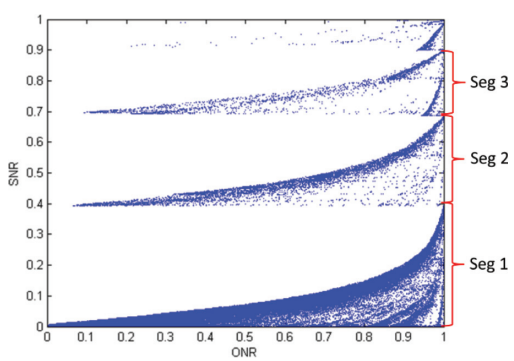


Figure 5. *N*-3, segments 1-3 marked out, 1M iterations.

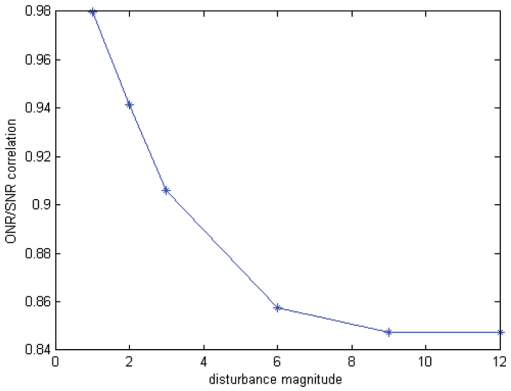


Figure 6. Correlation between ONR and SNR as a function of size of strain, only scenarios with lower priority customers considered.

between SNR and ONR and that the scenarios are distributed in a lower triangle shape. The latter means that no scenarios get higher SNR, within the segment, than ONR, while the opposite may be the case. The graphs for the higher strain levels repeat the pattern seen in the *N*-2 and *N*-3 graphs, and they are therefore left out. As can be seen in the graphs there is a poor correlation between the ranking results for strain sizes >1.

As it is apparent that ONR and SNR correlates poorly for top priority customers in Figures 4 and 5, Spearman rank correlation is instead calculated only for those scenarios that does not contain any top priority customers for the different simulated strain sizes (see Fig. 6). Here the focus is to evaluate the correlation between ONR and SNR for customers with lower prioritization values. The result reveal that the correlation decreases with increasing strain size, although the correlation is relatively high for all strain sizes. This suggests that although there is a poor correlation between ONR and SNR when all scenarios are included, there is a higher degree of correlation for lower priortized customers. As discussed further in the next section, this implies that high prioritized customers need to be treated separately and are not sufficiently considered in the outage compensation scheme.

4 DISCUSSION

Outage compensation is one of two existing power quality regulations in Sweden, and it has major impact on the revenue for Swedish DSOs. It can therefore be assumed that investments in the network as well as the way in which outages are

handled, both being performed by the DSO, will be decided to a large extent by the outage compensation regulation (this is a valid assumption only to the extent that DSOs strive to reduce their costs and increase their profit). Since the ONR is based solely on the customers' yearly fee, it is reasonable to ask if it takes aspects such as the societal criticality of the customer into account in a satisfactory way. In this paper the customer prioritizations made within the Styrel project were aggregated and used as a proxy for the societal criticality of customers supplied by a power distribution system. The results revealed that there is a clear correlation between SNR and ONR for the *N*-1 strain size while for larger sizes of strain the scenarios are divided into several distinct segments and the correlation between SNR and ONR is consequently low. Within each segment the scenarios form lower triangles, meaning that no scenario receives higher SNR than ONR. In other words, within each segment ONR reflect SNR in the sense that a high SNR implies a high ONR although the reverse is not the case. Since the scenarios are divided into segments based on the number of affected top priority customers (customers with priority 0 or 1) it is the existence of such customers that is responsible for the big overall disagreements between the SNR and ONR. This implies that customers given top priority in the Styrel system need to be treated separately and are not sufficiently considered in the outage compensation scheme.

Strandén et al. (2010) discuss the outage compensation scheme used in Finland, which is similar to the Swedish one, and point out that with present day regulations "small even if very critical customers, […], are more or less ignored", and this as well as the inverse situation, when large although socially non-critical customers are given a high priority, is the main reasons behind the discrepancies found between the rankings in this paper. A possible way to improve this situation is to take SNR, or other indicators of the societal criticality of power customers, into account when calculating the compensation that DSOs should pay to customers that have suffered outages. It is especially important that top priority customers are given more weight in the outage compensation regulation. If such changes were made it would be likely to steer the investments in the power grid so that the overall societal consequences from power outages are reduced.

4.1 *Validity*

The validity of the presented results depends on several factors. One factor is that only topology, but not capacity, is taken into account in the network model. This might lead to underestimations when the largest strain sizes are simulated. For instance, when capacity is not considered, the entire system could be supplied from one single infeed-point. Another issue is how well the Styrel priority values reflect the actual societal criticality of the power customers. The Styrel priorities are decided in cooperation between all political levels in Swedish society, which means that detailed knowledge as well as overview of the customers criticality for society should be reflected in the prioritizations. However, it could be questioned if the points given to customers can indeed, as is the practice of the DSO, be used as weights. This implies that 4 normal households, which have 1 point each, carry as much weight as a large industrial facility and that 7 households have equal weight as one customer that has large impact on the functioning of society in the short time span. This apparent weakness should be considered when judging the results. Another concern is, as mentioned in part 2, that the outage duration was assumed to be 12 hours for all affected customers. For a 12 hour outage all customers with a yearly fee of SEK 7,200 or less will get the minimum compensation (see Fig. 2), meaning that they are raised above what they would get if the compensation in percentage (12.5%) is used. As the outage time increases the number of customers that are raised to the minimum amount will decrease and they will thereby become relatively less important. Overall small customers will, due to this, carry less weight in determining outage compensation as the outage time increases.

5 CONCLUSIONS

It has been found that outage compensation, reflecting the economic cost of outage scenarios for a DSO, have a poor correlation with results given by Styrel priorities, reflecting the societal consequence of outages. The two correlate well for single component failures, but worse as the magnitude of strain increases. It is found that the low correlation is due to the influence of top priority customers, and this implies that this small group of customers is not sufficiently considered in the outage compensation scheme. It can be concluded, from observing the low correlation, that the investments in the system, motivated by cost-cutting efforts, will not reflect the priorities that society has with regard to protecting critical power customers. A compensation scheme that weighted outage compensation according to the criticality of the customer (using Styrel priority or some other criticality measure) would be likely to steer investments in the network as well as repair

work so that overall societal consequences from power outages are reduced.

ACKNOWLEDGEMENT

The DSO that supplied the data on which this paper is based and the Swedish Civil Contingencies Agency (the PRIVAD-project) which funded the research are both greatly acknowledged.

REFERENCES

Balducci, P.J., Roop, J.M., Schienbein, L.A., DeSteese, J.G., & Weimar, M.R. 2002. Electrical power interruption cost estimates for individual industries, sectors and US economy. Pacific Northwest National Laboratory.

Billinton, R., & Sankarakrishnan, A. 1995. May. A comparison of Monte Carlo simulation techniques for composite power system reliability assessment. InWESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE (Vol. 1, pp. 145–150). IEEE.

Bozic, Z. 2000. Customer interruption cost calculation for reliability economics: practical considerations. In Power System Technology, 2000. Proceedings. PowerCon 2000. International Conference on (Vol. 2, pp. 1095–1100). IEEE.

De Nooij, M., Koopmans, C., & Bijvoet, C. 2007. The value of supply security: The costs of power interruptions: Economic input for damage reduction and investment in networks. Energy Economics, 29(2), 277–295.

Johansson, J. 2010. Risk and vulnerability analysis of interdependent technical infrastructures. PhD thesis, Lund Universitety.

Jönsson, H., Johansson, J., & Johansson, H. 2008. Identifying critical components in technical infrastructure networks. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 222(2), 235–243.

Kjolle, G.H., Samdal, K., Singh, B., & Kvitastein, O.A. 2008. Customer costs related to interruptions and voltage problems: Methodology and results. Power Systems, IEEE Transactions on, 23(3), 1030–1038.

Linares, P., & Rey, L. 2012. The costs of electricity interruptions in Spain. Are we sending the right signals? (No. fa05-2012).

MSB 2010 Inriktningsdokumnet, Diarienr: 2009–3054.

Raesaar, E.P., Tiigimägi, E., & Valtin, J. 2006. Assessment of electricity supply interruption costs under the restricted time and information resources. InProceeding of International Conference on Energy & Environment Systems (IASME/WSEAS 2006) (pp. 409–415).

Rao, J.M., Prasad, P.V.N., & Das, G.T.R. 2010. Customer outage cost evaluation in electric power systems. ARPN Journal of Engineering and Applied Sciences, 5(8), 88–96.

Samdal, K., Kjølle, G., Singh, B., & Kvitastein, O. 2003. Customers Interruption Costs–What's The Problem?. In CIRED 17th International Conference and Exhibition, Barcelona, Spain.

Sanghvi, A.P. 1982. Economic costs of electricity supply interruptions: US and foreign experience. Energy Economics, 4(3), 180–198.

Sappington, D.E., Pfeifenberger, J.P., Hanser, P., & Basheda, G.N. 2001. The state of performance-based regulation in the US electric utility industry. The Electricity Journal, 14(8), 71–79.

Strandén, J., Krohns, H., Verho, P., & Sarsama, J. 2010. Modeling the interruption criticality of customers of distribution networks. In The 9th Nordic Electricity Distribution and Asset Management Conference 2010, NORDAC 2010, 6–7 September 2010, Aalborg, Denmark.

Tahvanainen, K., Viljainen, S., Honkapuro, S., Lassila, J., Partanen, J., Järventausta, P., & Mäkinen, A. 2004. Quality regulation in electricity distribution business. In Nordic distribution and asset management conference (pp. 23–24).

Woo, C.K., & Pupp, R.L. 1992. Costs of service disruptions to electricity consumers. Energy, 17(2), 109–126.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On the resilience analysis of interconnected systems by a set-theoretic approach

X. Liu & I. Prodan
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy, Electricité de France, École Centrale Paris—Supélec, France

E. Zio
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy, Electricité de France, École Centrale Paris—Supélec, France
Department of Energy, Politecnico di Milano, Italy

ABSTRACT: The paper deals with the resilience analysis of critical infrastructure systems. An infrastructure system is a network of subsystems, which interoperate through dependencies of various types. The interaction and dependency among the subsystems make the entire infrastructure system more complex and possibly vulnerable. We interpret resilience as a system property related to the prevention of, robustness to and recovery from undesired disturbances and events. Such resilience property of interconnected systems depends also on their structure and design parameters. In this paper, we abstract the structure of the system by a directed graph. A state dynamics is associated to each of the subsystems, with interdependent terms that can represent different types of interdependencies. The system response to undesired disturbances and events could, then, be analyzed using notions from set theory, to identify regions of operation and recoverable or non-recoverable conditions. Moreover, a characterization of the system resilience as a function of the design parameters can be provided, which is useful for resilient design and operation purposes. The benefits of the proposed approach are highlighted through an illustrative, numerical application.

1 INTRODUCTION

In recent years, the protection of critical infrastructure systems (e.g., electric power grids, telecommunication systems, transportation systems and so on) has become an important topic. The notion itself of "critical infrastructure" implies that these interconnected systems are important. They serve our everyday life, e.g. they provide the water and electricity in our homes, for our physical and financial welfare, and support the development of modern societies.

As all systems, these critical infrastructures are exposed to hazardous natural and artificial events, such as earthquake, hurricanes, random failures and sabotages etc., which make them vulnerable (Wolfgang & Zio 2011) Given their importance, the critical infrastructures need very high-levels of reliability and protection (Carlyle et al. 2006, O'Rourke 2007, Murray & Grubesic 2007).

A critical infrastructure is composed of subsystems whose operation is interdependent in different ways and to different degrees (Rinaldi et al. 2001, Rinaldi 2004). The interdependencies and the interactions among the subsystems are the force and the weakness of the critical infrastructures. With respect to the latter, the major risk is that of an initiating failure which propagates from one subsystem to another rendering the global system dysfunctional and unstable. The modeling of this dynamics is quite a challenging task (Buldyrev et al. 2010, Dobson 2008, Pederson et al. 2006).

Several properties make up the capability of a system to provide its function and continue to do so or recover it, in the presence of failures of some of its subsystems. The system must have built-in capacity to resist to the disturbances and be capable to adapt to changing environments. The resilience of a system includes all these properties, specifically, the prevention of and robustness to disturbances, and the capability of recovery from failure.

The analysis and characterization of the resilience of critical infrastructures is receiving a lot of attention from the scientific and technical community. For example, (Nozick et al. 2005) uses a supply-demand graph to represent the interdependency between infrastructures, and Markov and semi-Markov processes for describing the state transitions dynamics. Furthermore, the system performance is measured and analyzed using a probabilistic distribution. Reference (Faraji &

Kiyono 2012) proposes a weighted stochastic Petri Net modeling approach for the analysis of critical infrastructures to describe the cascading failure impacts and assess the reliability of the infrastructure. The work in (Bloomfield et al. 2010) builds a stochastic model for the interconnected critical infrastructures, whereby each component is modeled as a random process with a probability to switch between two states, operational and failed. The metric to measure system performance is given in terms of the cascade size resulting from the failure process. A System Dynamics (SD) infrastructure vulnerability assessment framework is proposed in (Tonmoy & El-Zein 2014) to simulate the dependent behaviors of the infrastructure subsystems, and a measure of system performance is provided. An extensible graph-theoretical model is provided in (Svendsen & Wolthusen 2007) for investigating the interdependencies among critical infrastructures. The interactions between their components are modeled through a set of response functions on the graph edges and resources on the nodes. Reference (Reed et al. 2009) introduces a linear input-output model for describing the interdependencies among infrastructures. Methods based on fragility measures and quality functions are proposed to evaluate the system restoration from natural hazards.

Furthermore, (Filippini & Zio 2013, Angelo & Filippini 2013) represent the infrastructure systems in a directed graph and a state dynamics is associated to each subsystem for describing the failure and recovery processes and their interdependent effects. A first attempt of resilience analysis is proposed based on invariance concepts and asymptotic stability. However, a thorough characterization of the resilience and a metric of the system resilience are not provided.

In the present paper, we embrace a similar approach as in (Angelo & Filippini 2013). We consider a topological model of the infrastructure systems described by a directed graph, with nodes and edges representing the subsystems and the functional dependencies between the subsystems, respectively. Next, we proceed with the modeling of the dynamics of each subsystem and the related interdependencies. For this, we use a state space model with specific dynamics governed by parameters characteristic of the failure and recovery processes. The analysis of the interconnected systems dynamics is performed with the objective of identifying the resilience region for which the system state converges to the operation mode, no matter the disturbances affecting the system. Invariance concepts are used to find the resilience region and to provide conditions on the design parameters, which ensure the successful operation of the interconnected systems. Some interesting behaviors of the system are highlighted, e.g. a chattering behavior.

The rest of the paper is organized as follows. Section 2 introduces the topological description of the interdependent systems, and their associated dynamic model. Section 3 presents the conditions on the design parameters, which ensure the existence of a resilience region. Discussions based on simulation results are presented in Section 4. Finally, Section 5 draws the conclusions and presents the future work.

2 PRELIMINARIES AND PREREQUISITE

This section provides a detailed description of the system modeling and also introduces set invariance notions, which will be instrumental for the resilience analysis of infrastructure systems.

2.1 *System modeling*

The entire interconnected system can be represented by a directed graph, with nodes and directed edges describing the network structural characteristics. Figure 1 shows such an interconnected system as a directed graph, where each node represents a subsystem and the direction of the edge connecting two nodes indicates the dependency relationship between two subsystems (i.e., the head node is dependent on the tail node).

Within one interdependent infrastructure system, its subsystems depend on each other by different types of interdependencies. These have different causes and modes of manifestations (Buldyrev et al. 2010, Dobson 2008); formally, these can be described in terms of dynamic models and input/output constraints.

In this paper, we refer in particular to physical interdependencies, cyber interdependencies and also logical interdependencies. In other words, we describe the situation for which one subsystem needs the resources such as power, control signal, water and so on, from another subsystem to keep its functionality. Logical interdependencies can also

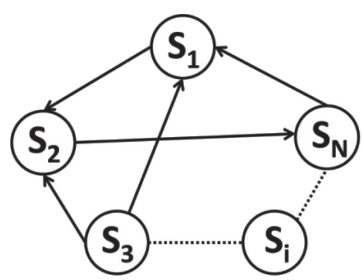


Figure 1. Interconnected system.

be taken into account by adding coupling factors to adjust the states of the subsystems depending on their logic configuration. When all the resources needed are provided, the subsystem works in its nominal operation mode; otherwise, it switches into the out-of-operation mode. This is a dynamic behavior common to many interdependent systems and it is well captured by the switching model considered here.

In a switching dynamic model, as the functionality of a subsystem relies on the production or the service provided by other subsystems, the conditions of the switching of this subsystem depend on its input subsystems. From a system-level point of view, a subsystem may continue operating even when the inputs of certain resources are partially unavailable; in this sense, the buffering and restoration processes are both taken into account as two different dynamic modes.

The dynamic model for any subsystem S_i is given by the switching dynamical equations below:

$$\dot{x}_i(t) = \begin{cases} -\mu_i(x_i(t) \\ \quad -\sum_{j\in I_i} \alpha_{ji} x_j(t)) + d_i, & \text{for } x_j \le \sigma_j,\ \forall j \in I_i \\ \lambda_i(1 - x_i(t)), & \text{for } x_j \ge \sigma_j,\ \exists j \in I_i \end{cases} \tag{1}$$

where, I_i is the set of input subsystems of S_i.

Equation (1) represents a switched dynamics in the sense that the value of $\dot{x}_i$ alternates between an operation and a failure mode, depending on the value taken by the current state x_i and the state x_j of all of its input subsystems S_j. Subsystem S_i is in a nominal operation state if all the states of its input subsystems are within their corresponding thresholds σ_j, as described by the first equation in (1). Conversely, if one of its input subsystems fails, the subsystem is in an off-operation state and its dynamical behavior is described by the second equation as a failure process.

Note that for N subsystems we have a total of 2^N modes of functioning for the interconnected system, depending where each of the states x_i resides.

Taking into account the dynamics of the entire system, we can use a switched Linear Time-Invariant (LTI) dynamic equation to describe system behavior:

$$\dot{x}(t) = A_m x(t) + b_m, \tag{2}$$

where, $x(t) = [x_1^T(t), \ldots, x_N^T(t)]^T$ represents the state vector of the interconnected system, and matrices $A_m \in \mathrm{R}^{N\times N}$ and $b_m \in R^{N\times 1}$ are constructed accordingly, where $m = 1, \ldots, 2^N$.

To describe the interdependencies and the related dynamics of the interconnected infrastructure system, we introduce the following variables and parameters in the system model:

$x_i(t) \in [0, 1]$ represents the percentage of the loss of service or the production unrealized by subsystem S_i at time t.

For the subsystem S_i, $x_i(t) = 0$ means that S_i can provide full service, or enough products to meet the requirement, or other resource support, to the other subsystems connected to it as expected/demanded. When the subsystem S_i cannot do so, the value of its state variable augments, $x_i(t) > 0$.

Under the assumption that the actual amount of power produced cannot exceed the intended/demanded service, the value of the state variable is $x_i(t) \in [0, 1]$.

The following parameters are introduced to describe the state dynamics:

$\sigma_i \in [0, 1]$ indicates the threshold for state variable $x_i(t)$, which allows evaluating if the subsystem S_i can provide the output required for the functioning of its connected subsystems; in other words, it represents the tolerance of system S_i for the percentage of loss of service: if $x_i(t) > \sigma_i$, then the output is insufficient.

$d_i(t) \in [0, 1]$ represents both external and internal perturbations, which affect the behavior of the system in nominal operation. It can be instantaneous and more or less strong (e.g. caused by natural disasters, such as earthquake, hurricane or a random fault) or continuous and relatively mild (such as sustained wind, electromagnetic interference, degradation etc.).

In some situations, instantaneous and continuous perturbations can co-exist.

$\lambda_i \in [0, 1]$ represents the failure rate for the *ith* subsystem S_i. The time for the state x_i of S_i to reach the threshold is the time to failure TTF_i, introduced in the following equation:

$$\int_0^{TTF_i} \lambda_i e^{-\lambda_i t} = \sigma_i. \tag{3}$$

From equation (3), we obtain:

$$\lambda_i = \frac{log(1-\sigma_i)}{TTF_i}. \tag{4}$$

Figure 2 illustrates the variation of the time to failure with the threshold, for a given value of the failure rate. As illustrated, the time to failure increases with the threshold and for larger failure rate values the curve gets closer to the horizontal axis, which means that the subsystem fails earlier at a lower threshold, as reasonable.

$\mu_i \in [0, 1]$ represents the recovery rate for subsystem S_i. The Time to Recovery (TTR_i) is the time that subsystem S_i takes to recover from the failed state to the threshold:

$$\int_0^{TTR_i} \mu_i e^{-\mu_i t} = 1 - \sigma_i. \tag{5}$$

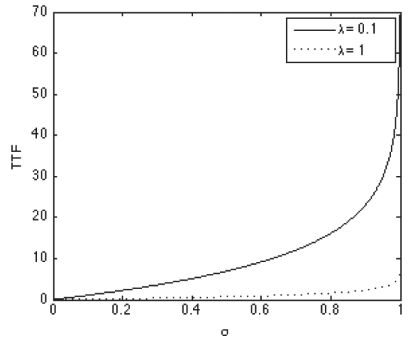


Figure 2. Variation of the Time to Failure (TTF) as a function of the threshold σ.

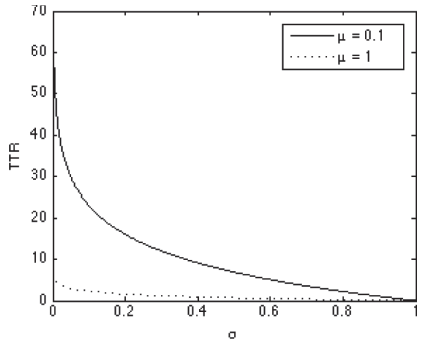


Figure 3. Variation of the Time to Recovery (TTR) as a function of the threshold σ.

From equation (5), the recovery rate is obtained as:

$$\mu_i = -\frac{log(\sigma_i)}{TTR_i}. \quad (6)$$

The recovery process describes a resilience feature of the system. The time to recovery is a critical characteristic of the resilience of infrastructure systems. In Figure 3, we can see that the time to recovery decreases with the value of the threshold and for large recovery rates the time to recovery is small, as logical.

The parameter $\alpha_{ij} \in [0, 1]$ is the coupling factor representing the dependency of the subsystem S_i on the subsystem S_j. The term associated to it in the equation (1) represents the rate of the loss of service that the *jth* subsystem contributes to the *ith* subsystem due to the logical dependencies between them.

The dependency relationships among the subsystems represent the logics between producer and user, supplier and consumer, controller and controlled, etc. In these functional relationships, physical quantities and information are produced, consumed or/and transmitted among the subsystems to ensure their functionality. The threshold for one subsystem state is set with respect to all its downstream or output subsystems controlled by it. The value of the threshold indicates the level of tolerance for the downstream subsystems with respect to the acceptable percentage of lost input from the controlling subsystem.

The proposed model not only captures the functional relationship between the subsystems (e.g. due to physical and cyber dependencies) but also takes into account the logical dependency among the subsystems. These are originated from human decisions and actions. The coupling factor allows considering the degree of logical interdependencies in the dynamic process of system evolution.

2.2 *Invariance notions*

In this sub-section, few basic concepts related to the set-theoretic approach are introduced as necessary.

Definition 1 (Equilibrium point). *The point $x_f \in R^n$ is an equilibrium point (or fixed point) for the differential equation,*

$$\dot{x}(t) = f(x(t)).$$

If $f(x_f) = 0$.

Definition 2 (Positive invariance). *(Blanchini, 1999) A set $P \subset R^n$ is said to be positively invariant for a system of the form*

$$\dot{x}(t) = f(x(t)).$$

If every solution of the equation with initial condition $x(0) \in P$ verifies $x(t) \in P$ for $t > 0$.

Definition 3 (Robust positive invariance, RPI). *(Blanchini, 1999) A set $P \subset R^n$ is said to be robustly positively invariant for a system of the form*

$$\dot{x}(t) = f(x(t), w(t)),$$

where $w(t) \in W$ is an exogenous input. If for all $x(0) \in P$ and $w(t) \in W$, the condition $x(t) \in P$ holds for all $t \geq 0$.

3 DETERMINATION OF THE RESILIENCE REGION

This section presents the necessary conditions on the design parameters for the existence of a resilience region. The region is identified using the invariance concepts introduced in Section 2.2 above.

Proposition 1. *Let there be a convex and compact set $O \in R^n$ and consider the dynamics from (2). Whenever equilibrium point x_f associated with these dynamics lies into O, we have that there exists a subset of O which is an invariant set.*

Proof. If x_f is an equilibrium point for one mode of the switched system

$$\dot{x}(t) = A_m \cdot x(t) + bm,$$

where $m = 1, \ldots, 2^N$.

In any functioning mode of the system, the dynamic equation of each subsystem is an affine equation. Moreover, the eigenvalues λ_A of matrix A satisfy $|\lambda_A| \leq 1$, according to the setting of the parameters. Hence, the system given by (2) is asymptotically stable.

Therefore, $O \in R^n$ is a domain of attraction and we can say that all initial states entering in set O will remain within the set at all future instances, thus O is an invariant set.

We assume that x_f is an equilibrium point in a certain dynamic mode of the system, so for the differential equation that describes the system dynamics, the equilibrium point satisfies:

$$0 = A_m \cdot x_f + b_m. \tag{7}$$

In our case, we can compute the equilibrium point for each operation mode:

$$x_f = (I - A_m)^{-1} \cdot b_m. \tag{8}$$

For a system with N subsystems, there are 2^N dynamic modes and the system switches from one to another depending on the states of each subsystem. The state space of the entire system is a hyper-cube $[0, 1]^N$, a set divided into 3 main parts: operation region, failure-recovery region and out-of-operation region. In the operation region, all the trajectories of the systems lie in the set $O := [0, \sigma_1] \times [0, \sigma_2] \times \ldots \times [0, \underline{\sigma}_N]$. The out-of-operation region is the opposite, $\overline{O} := [\sigma_1, 1] \times [\sigma_2, 1] \times \ldots \times [\sigma_N, 1]$, whereby all the states of all subsystems are of failure and the trajectories converge to an equilibrium point inside this failure region. In the proposed model, the equilibrium points may exist in the operation and out-of-operation regions.

For the operation mode, all the subsystems take the first differential equation:

$$\begin{cases} \dot{x}_1 = -\mu_1 \left(x_1 - \sum_{j \in I_1} \alpha_{j1} x_j \right) + d_1 \\ \quad \vdots \\ \dot{x}_i = -\mu_i \left(x_i - \sum_{j \in I_i} \alpha_{ji} x_j \right) + d_i \\ \quad \vdots \\ \dot{x}_N = -\mu_N \left(x_N - \sum_{j \in I_N} \alpha_{jN} x_j \right) + d_N \end{cases}, \tag{9}$$

So the equilibrium point of the operation mode is

$$x_0 = (I - A_o)^{-1} \cdot b_o, \tag{10}$$

where, A_O and b_O are matrices with appropriate dimensions.

If the equilibrium point is situated inside the operation region we can say that it is invariant: $x_O \in O$. Thus, one of the conditions on the design parameters for the existence of a resilience region is:

$$[0, \ldots, 0]^T \leq x_O \leq [\sigma_1, \ldots, \sigma_N]^T. \tag{11}$$

For all the initial states in the operation region, the trajectories of system dynamics remain inside the operation region and converge to x_O.

Similarly, the out-of-operation region has the dynamics:

$$\begin{cases} \dot{x}_1 = \lambda_1 (1 - x_1) \\ \quad \vdots \\ \dot{x}_i = \lambda_i (1 - x_i) \\ \quad \vdots \\ \dot{x}_N = \lambda_N (1 - x_N) \end{cases}. \tag{12}$$

If there is an equilibrium point,

$$x_{\overline{o}} = (I - A\overline{o})^{-1} \cdot b_{\overline{o}}, \tag{13}$$

it satisfies $x_{\overline{O}} \in \overline{O}$:

$$[\sigma_1, \ldots, \sigma_N]^T \leq x_{\overline{o}} \leq [1, \ldots, 1]^T. \tag{14}$$

Once the state of the system enters the out-of-operation mode, the system cannot recover to the operation region. The next Proposition demonstrates the existence of a resilience region.

Proposition 2. *Let there be a set R_m, which is RPI under the mth functioning mode of dynamics (2). Hence, the resilience region of the interconnected system given in (2) is described by:*

$$R = \bigcup_{m=1}^{2^N} R_m.$$

Proof. In the following, we propose a sketch of the proof. Consider a set R_{ms}, which represents the collection of all the sets where the system initial states reside to O through the corresponding dynamic equation of the *mth* functioning mode, after s time steps. Therefore, the RPI set under the *mth* functioning mode can be written as $R_m = \bigcup_{s=1}^{s_{max}} R_{ms}$, where s_{max} is the number of time steps for which the initial states in R_m converge to O. From Proposition 1, we have that O is invariant. This implies that the resilience region of the interconnected system (2) is given by:

$$R = \bigcup_{\substack{m=1 \\ s=1}}^{\substack{m=2^N \\ s=s_{max}}} R_{ms} = \bigcup_{m=1}^{2^N} R_m.$$

We denote the region outside the operation and out-of-operation regions as the failure-recovery

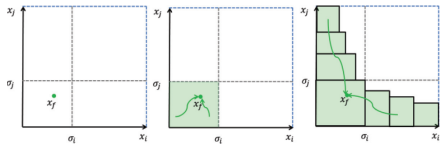


Figure 4. Steps for describing the resilience.

region. For initial states inside this region, they may converge either to the operation region or to the out-of-operation region in a finite time. We denote by reachable regions all those regions composed by the system initial states, which converge to the operation region in a finite time. Consequently, the overall resilience region is represented by the union of the operation region and the reachable regions. In other words, the resilience region is defined as the set of all initial states of the system that eventually will reside into the operation region in finite time (i.e. it is composed by the operation region itself plus the reachable regions situated within the failure-recovery region).

Figure 4 illustrates the steps for describing the resilience region.

Up to this point we can describe the resilience regions as they appear from the interdependencies relationships and the subsystems' characteristics. Indeed, the maximization of the system resilience region is the final design, operation and maintenance goal. We exemplify this by analyzing the response of the system as a function of its parameters, adding an element of control in the dynamics such that a supervisor can actively counteract failure modes and steer the overall system towards the operational functioning region.

4 EXAMPLE AND SIMULATION RESULTS

In this section, we consider a simple example of an interconnected system composed by two subsystems as in Figure 4. Given the methodological flavor of the work, the structure of the system is purposely chosen as simple as possible, in order to not add complexity to the study of the interdependencies among the subsystems and their dynamical behavior, aimed at characterizing the system resilience as a function of the design parameters. The interconnected system in Figure 4 could, for example, represent a system composed by a power supply system and a telecommunication system, whereby the components of the telecommunication system depend on the power supplied by the power supply system which, in turn, for its functioning makes use of the control and monitoring signals provided by the telecommunication system. A theoretical analysis of system resilience is performed and the results are collected into a Table which reports the parameters values of different scenarios of system evolution.

Consider each subsystem in Figure 5 described by the dynamic equation given in (2). There are four operation modes for the interconnected system, in which the dynamics is represented by the following equations:

Operation mode, where $x(t) \in O := [0, \sigma_1] \times [0, \sigma_2]$:

$$\begin{cases} \dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) + d_1 \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t)) + d_2 \end{cases}; \tag{15}$$

Failure-recovery mode 1, where $x(t) \in R_1 := [0, \sigma_1] \times [\sigma_{2,1}]$:

$$\begin{cases} \dot{x}_1(t) = \lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t)) \end{cases}; \tag{16}$$

Failure-recovery mode 2, where $x(t) \in R_2 := [\sigma_{1,1}] \times [0, \sigma_2]$:

$$\begin{cases} \dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t)) \end{cases}; \tag{17}$$

Out-of-operation mode, where $x(t) \in \bar{O} := [\sigma_{1,1}] \times [\sigma_2, 1]$:

$$\begin{cases} \dot{x}_1(t) = \lambda_1(1 - x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t)) \end{cases}. \tag{18}$$

Following the procedure described in Section III, the equilibrium states for the operation mode and the out-of-operation mode are identified:

$$x_o = \left[\frac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2} \; \frac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2} \right]^T$$

and $x_{\bar{O}} = [1\,1]^T$.

According to Proposition 1, if x_O is inside the operation region, there exists an invariant set and the equilibrium point locus is the location where all the states in the invariant set will converge. In this case, the invariant set is the operation region itself.

A similar result is found for the out-of operation region, which is also an invariant set with the

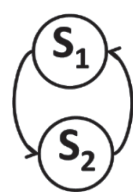


Figure 5. Interconnected system composed by two subsystems.

equilibrium point (1,1) being the attractor in this region.

The conditions for the equilibrium point to be inside the operation region are the following:

$$\begin{cases} 0 \le \dfrac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_1 \\ 0 \le \dfrac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1-\alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_2 \end{cases}. \tag{19}$$

In order to analyze the intrinsic characteristics of the equilibrium point, we simplify by neglecting the logical interdependencies between the subsystems, i.e., $\alpha_{12} = \alpha_{21} = 0$. In this case, the above conditions become:

$$\begin{cases} 0 \le \dfrac{d_1}{\mu_1} \le \sigma_1 \\ 0 \le \dfrac{d_2}{\mu_2} \le \sigma_2 \end{cases}. \tag{20}$$

Replacing relation (7) in the above equations, we obtain:

$$\begin{cases} TTR_1 \le -\dfrac{\log(\sigma_1)}{d_1}\sigma_1 \\ TTR_2 \le -\dfrac{\log(\sigma_2)}{d_2}\sigma_2 \end{cases}. \tag{21}$$

This allows highlighting directly the dependence of the time to recovery from the threshold and disturbance values (Fig. 6).

If we fix the disturbance d, we can observe the invariance of TTR with the threshold: in the space of parameters (see Fig. 5), the time to recovery reaches its maximal value when the threshold is around 0.36.

The next step is the computation of the resilience regions within the two failure-recovery regions, as described in Section III.

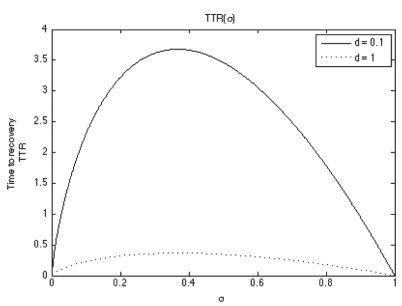


Figure 6. TTR (σ) with fixed disturbance.

Once the states x_1, x_2 enter the out-of-operation region $\bar{O}$ at a certain finite time, the system cannot recover back to the operation region O. But in the two failure-recovery regions R_1 and R_2, it is possible for the system to return to the operation region.

To find the specific resilience region, we compute a resilience curve to separate the end-to-failure and end-to-recovery parts in the failure-recovery region. The situation in R_1 is considered first, whose dynamic equations are (the coupling factors are neglected at first):

$$\begin{cases} \dot{x}_1(t) = -\lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2 x_2(t) \end{cases}. \tag{22}$$

After integration, we obtain:

$$\begin{cases} x_1(t) = 1 + (x_1(0) - 1)e^{-\lambda_1 t} \\ x_2(t) = x_2(0)e^{-\mu_2 t} \end{cases}. \tag{23}$$

From the equations above, we observe that state x_1 tends to diverge to 1 whereas state x_2 converges exponentially to 0. Therefore, there exists a set of states $M \in R_1$ which pass the point (σ_1, σ_2) at a certain time $t = T$. The set M is represented by the following state equations, with initial conditions $x_1(0)$ and $x_2(0)$:

$$\begin{cases} x_1(T) = 1 + (x_1(0) - 1)e^{-\lambda_1 T} = \sigma_1 \\ x_2(T) = x_2(0)e^{-\mu_2 T} = \sigma_2 \end{cases}. \tag{24}$$

The set of the initial states which pass the point (σ_1, σ_2) at time T is the curve described by:

$$x_1(0) = 1 + (\sigma_1 - 1)\left(\frac{x_2(0)}{\sigma_2}\right)^{\frac{\lambda_1}{\mu_2}}, \tag{25}$$

where $x_1(0) \in [0, \sigma_1]$ and $x_2(0) \in [\sigma_2, 1]$.

In R_2 where the failure is generated in S_1, the set of initial states who pass the point (σ_1, σ_2) can be identified similarly, and we have the curve:

$$x_2(0) = 1 + (\sigma_2 - 1)\left(\frac{x_1(0)}{\sigma_1}\right)^{\frac{\lambda_2}{\mu_1}}, \tag{26}$$

where $x_1(0) \in [\sigma_1, 1]$ and $x_2(0) \in [0, \sigma_2]$.

Figure 7 illustrates the resilience curves, which separate the resilience regions from the non-resilience regions within the failure-recovery region, as described by the equations (25) and (26).

When the design parameters are outside the bounds imposed by conditions (19), the system will not recover i.e., the state trajectories will always

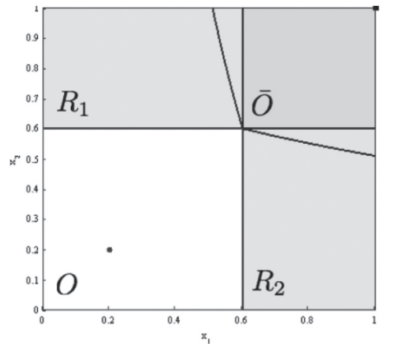


Figure 7. Four operation regions and the curves separating the resilience region and non-resilience region.

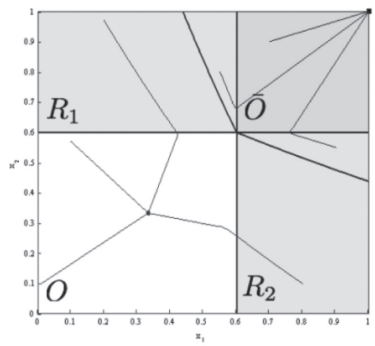


Figure 8. Resilience curve and system trajectories with different initial conditions.

converge to the (1,1) equilibrium point outside the (white) operation region as in Figure 8.

Figure 8 depicts several state trajectories for different initial conditions of the system. We observe that as long as the equilibrium point (denoted as the black dot) is inside the operation region (denoted in white) the system trajectories reside at all times in the resilience region. This means that for the design parameters fulfilling conditions (19) the system will always recover from unexpected event.

The equilibrium point locus is another important aspect for the system resilience. For example, if the equilibrium point of the operation mode resides in the failure-recovery region, we can observe a chattering behavior like the one shown in Figure 9.

Similarly with the previous case, we can determine some conditions on the model parameters such that we can a priori identify the chattering behavior:

In R_1: = $[\sigma_1, 1] \times [0, \sigma_2]$

If the equilibrium point is located in the resilience region of R_1, then:

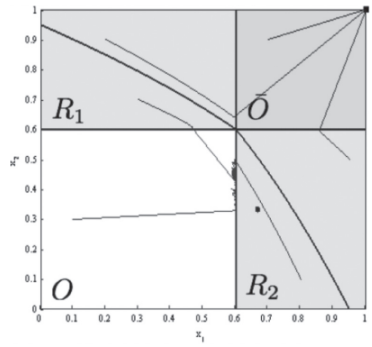


Figure 9. Chattering behavior for the system trajectories with different initial conditions.

Table 1. Parameters values.

Parameters	Resilience scenario	Chattering scenario 1	Chattering scenario 2
σ_1	0.6	0.6	0.6
σ_2	0.7	0.7	0.7
d_1	0.3	0.3	0.3
d_2	0.4	0.4	0.4
λ_1	0.1	0.1	0.1
λ_2	0.2	0.2	0.2
μ_1	[0.5,1]	0.7	[0.49,1]
μ_2	[0.57,1]	[0.55,1]	0.8

$$\begin{cases} x_{f_1} = \dfrac{d_1}{\mu_1} \\ x_{f_2} = \dfrac{d_2}{\mu_2} \end{cases}. \tag{27}$$

Then, we get the inequalities:

$$\begin{cases} 0 \le \dfrac{d_1}{\mu_1} \le 1 + (\sigma_1 - 1)\left(\dfrac{d_2}{\sigma_2 \mu_2}\right)^{\frac{\lambda_1}{\mu_2}} \\ \sigma_2 < \dfrac{d_2}{\mu_2} \le 1 \end{cases}. \tag{28}$$

In R_2: = $[\sigma_1, 1] \times [0, \sigma_2]$
We get similar results:

$$\begin{cases} \sigma_1 < \dfrac{d_1}{\mu_1} \le 1 \\ 0 \le \dfrac{d_2}{\mu_2} \le 1 + (\sigma_2 - 1)\left(\dfrac{d_1}{\sigma_1 \mu_1}\right)^{\frac{\lambda_2}{\mu_1}} \end{cases}. \tag{29}$$

The conditions (20), (28), (29) allow steering the parameters values in a way to get different scenarios of system evolution, as in Table 1.

The resilience scenario and the chattering scenario are those observed in Figures 7 and 8. To eliminate the chattering behavior, a control law can be added into the model of the interconnected system. Further work will be devoted in the future to the design of control strategies aimed at system chattering behavior elimination.

5 CONCLUSION

This paper adopts a set-theory framework for the resilience analysis of interconnected infrastructure systems. A detailed description of the system dynamics modeling is provided and invariance properties are analyzed to define and identify the resilience region, as a function of the governing parameters. This allows controlling the characteristics of the system resilience properties by design, operation and maintenance properties as represented by the values of the related parameters. An illustration of the analytical power of the framework adopted is provided on an interconnected interconnected system case study, with detailed discussions of its behavior and response to failures and/or disturbances, based on simulation results.

REFERENCES

Angelo, A. & Filippini, R. 2013. "Evaluation of Resilience of Interconnected Systems Based on Stability Analysis." Critical Information Infrastructures Security. Springer Berlin Heidelberg, 180–190.

Bloomfield, R. Buzna, L. Popov, P. Salako, K. & Wright, D. 2010, "Stochastic modelling of the effects of interdependencies between critical infrastructure," in Critical Information Infrastructures Security. Springer, pp. 201–212.

Buldyrev, S.V. Parshani, R. Paul, G. Stanley, H.E. & Havlin, S. 2010. "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025–1028.

Carlyle, G. Salmeron, M.J. & Wood, K. 2006. "Defending critical infrastructure," Interfaces, vol. 36, no. 6, pp. 530–544.

Dobson, I. 2008. "Analysis of cascading infrastructure failures," Wiley Hand-book of Science and Technology for Homeland Security.

Faraji, M. & Kiyono, J. 2012. "Infrastructure performance oriented reliability using assessment using weighed stochastic petri net," 15 WCEE, Lisboa.

Filippini, R. & Zio, E. 2013. "integrated resilience and risk analysis framework for critical infrastructures", in Proceeding of ESREL conference, pp. 2001–2008.

Murray, A.T. & Grubesic, T. H. 2007. Critical infrastructure: reliability and vulnerability. Springer Berlin, vol. 16.

Nozick, L.K. Turnquist, M.A. Jones, D.A. & Davis, J.R. 2005. "Assessing the performance of interdependent infrastructures and optimising investments," International journal of critical infrastructures, vol. 1, no. 2, pp.144–154.

O'Rourke, T.D. 2007. "Critical infrastructure, interdependencies, and resilience," Bridge-Washington-National Academy of Engineering, vol. 37, no. 1, p. 22.

Pederson, P. Dudenhoeffer, D. Hartley, S. & Permann, M. 2006. "Critical infrastructure interdependency modeling: a survey of us and international research," Idaho National Laboratory, pp. 1–20.

Reed, D.A. Kapur, K.C. & Christie, R.D. 2009. "Methodology for assessing the resilience of networked infrastructure," Systems Journal, IEEE, vol. 3, no. 2, pp. 174–180.

Rinaldi, S.M. Peerenboom, J.P. & Kelly, T.K. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies," Control Systems, IEEE, vol. 21, no. 6, pp. 11–25.

Rinaldi, S.M. 2004. "Modeling and simulating critical infrastructures and their interdependencies," in System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on. IEEE, pp. 54–61.

Svendsen, N.K. & Wolthusen, S.D. 2007. "Connectivity models of inter-dependency in mixed-type critical infrastructure networks," Information Security Technical Report, vol. 12, no. 1, pp. 44–55.

Tonmoy, F. & El-Zein, A. 2014. "Vulnerability of infrastructure to sea level rise: A combined outranking and system-dynamics approach," in Safety, Reliability and Risk Analysis: Beyond the Horizon. CRC Press.

Wolfgang, K. & Zio, E. 2011. Vulnerable systems. Springer.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A brief note on the ratio of the rectilinear and shortest distance between two arbitrary points on the 3-sphere

M.A. Odijk
Gouda, The Netherlands

P.H.A.J.M. van Gelder
Delft University of Technology, Delft, The Netherlands

ABSTRACT: In Odijk and Van Gelder (2013) we considered the length of rectilinear paths between arbitrary points on the plane, which we refer to as Flatland, relative to their straight line distance. We refer to this entity as the diversion ratio. In this note we discuss the extension of this concept to the surface of the 3-dimensional sphere, which we refer to as Planet Earth, and to the skewed case, i.e. orientations are not orthogonal, but angled instead. Considering arbitrary points, the diversion ratios become stochastic by nature. The main point of this paper is to relate the mean (skewed) diversion ratios in Flatland and on Planet Earth.

1 INTRODUCTION

In flat cultivated landscapes it is often not possible to walk in a straight line from one point to another point. Instead, paths are more or less rectilinear. Think for example of urban environments or rectangular patches of farmland, where transportation routes or pipeline infrastructure often must follow public roads. Let ρ be the length of such diversion connecting two arbitrary points relative to their straight line distance. Below we refer to this ratio as the diversion ratio. For a random variable X we denote with $\mu(X)$ its mean.

Without loss of generality we fix one of both arbitrary points and call it the origin. Then, if $x \in R^2$, with $\rho(x)$ we denote the length of the diversion that must be undertaken to move from the origin to x relative to moving in a straight line. Formally, let $L_p(x)$ be the well-known p-norm of $x = (x_1, x_2)$, i.e. $L_p(x) = (x_1^p + x_2^p)^{1/p}$, then $\rho(x) = L_1(x)/L_2(x)$. As $\rho(\alpha x) = \rho(x)$ for all $\alpha \neq 0$, we restrict ourselves to $x \in B_2$ without loss of generality, where B_2 is the boundary of the unit circle. We model arbitrariness by stipulating that x is uniformly distributed on B_2, denoted by $x \sim U(B_2)$. Hence, $\rho = \rho(X)$, where $X \sim U(B_2)$. This note extends the work by Odijk and Van Gelder (2013) in which the k-th moment and asymptotics of ρ has been investigated. In Section 2 of this note we briefly discuss the comparison between the mean value of ρ and of ρ_γ, being the diversion ratio in case the landscape is not exactly rectilinear, but skewed with angle γ instead. That is, the north-south orientation makes an angle $\gamma \in (0, \pi/2]$ with the east-west orientation. We refer to this as skewness or the skewed diversion ratio.

As over long distances the curvature of the earth influences the (skewed) diversion ratio, we discuss in Sections 3 and 4 the 3-dimensional analogues τ and τ_γ of ρ and ρ_γ.

Referring to the flat situation as Flatland, after Abott's Flatland—A romance of many dimensions from 1884 [Lindgren 2010], and to the curved situation as Planet Earth, in Section 5 we arrive at our main point we would like to make with this paper. That is we relate mean (skewed) diversion ratios in Flatland and on Planet Earth.

2 FLATLAND

Trivially, using symmetries, we have

$$\mu(\rho) = \frac{1}{2\pi}\int_0^{2\pi} |\sin(\varphi)| + |\cos(\varphi)| d\varphi = \frac{4}{\pi}\int_0^{\pi/4} \sin(\varphi) + \cos(\varphi) d\varphi = \frac{4}{\pi} \quad (1)$$

To study the skewed case, let $0 < \gamma \leq \pi/2$, and consider the basis $\{(1,0),(\cos(\gamma),\sin(\gamma))\}$ of R^2, having basis transformation matrix

$$D = \begin{pmatrix} 1 & \cos(\gamma) \\ 0 & \sin(\gamma) \end{pmatrix}^{-1} = \frac{1}{\sin(\gamma)} \begin{pmatrix} \sin(\gamma) & -\cos(\gamma) \\ 0 & 1 \end{pmatrix} \quad (2)$$

Then,

$$\mu(\rho_\gamma) = \frac{1}{2\pi\sin(\gamma)} \int_0^{2\pi} \begin{matrix} |\sin(\gamma)\cos(\varphi) - \cos(\gamma)\sin(\varphi)| \\ + |\sin(\varphi)| \, d\varphi \end{matrix}$$

$$= \frac{4}{\pi\sin(\gamma)} = \frac{\mu(\rho)}{\sin(\gamma)} \quad (3)$$

For more details and extensions, we refer to Odijk and Van Gelder (2013).

3 PLANET EARTH (SPHERICAL GEOMETRY)

In practice, Flatland approximates Planet Earth's curvature locally sufficiently accurate. Still, we could raise the question what happens with ρ and ρ_γ if we consider distances between points on Planet Earth that are so far apart that curvature does play a role.

Assume Planet Earth is a perfect sphere and let $(\phi_1, \phi_2) = (0,0$ be the spherical coordinates of the origin of Planet Earth's surface, where $\phi_1 \in [0, 2\pi]$ is the latitude ($\phi_1 = 0$ marking the Prime Meridian crossing Greenwich) and $\phi_2 \in [-\pi/2, \pi/2]$ the longitude ($\phi_2 = 0$ being the equator). Below we assume without loss of generality that $(\phi_1, \phi_2) \in [0, \pi] \times [0, \pi/2]$, i.e. (ϕ_1, ϕ_2) lies on the intersection Q of the northern and eastern hemispheres. Below assume without loss of generality that Planet Earth has radius 1.

Consider the spherical rectilinear distance between $(0,0)$ and (ϕ_1, ϕ_2) , i.e. the length of a connecting path running eastward over parallel arcs and heading north over meridian arcs. In contrast to Flatland, it matters how the path is organised. For example, the path $(0,0) \to (0, \phi_2) \to (\phi_1, \phi_2)$, i.e. first moving north and from there continuing east, has length $L_1^{\min}(\phi_1, \phi_2) = \phi_1 \cos(\phi_2) + \phi_2$, whereas the path $(0,0) \to (\phi_1, 0) \to (\phi_1, \phi_2)$, i.e. first moving east and from there continuing north, has length $L_1^{\max}(\phi_1, \phi_2) = \phi_1 + \phi_2$, which is longer. $L_1^{\min}(\phi_1, \phi_2)$ and $L_1^{\max}(\phi_1, \phi_2)$ are Flatland's analogue of the 1-norm. The superscripts min and max denote that these are the shortest and longest spherically rectilinear paths between $(0,0)$ and (ϕ_1, ϕ_2). That is, for just any path p between the origin and (ϕ_1, ϕ_2) consisting of an alternating chain of pieces of meridian arcs and pieces of parallel arcs, it is not difficult to see that its length is bounded by $L_1^{\min}(\phi_1, \phi_2)$ and $L_1^{\max}(\phi_1, \phi_2)$.

Let $\Delta(\phi_1, \phi_2) = \arccos(\cos(\phi_1)\cos(\phi_2))$ be the great circle distance between $(0,0)$ and (ϕ_1, ϕ_2), the spherical analogue of Flatland's 2-norm.

For $(\varphi_1, \varphi_2) \neq (0,0)$, let

$$\tau^{\min}(\phi_1, \phi_2) = \frac{L_1^{\min}(\phi_1, \phi_2)}{\Delta(\phi_1, \phi_2)} \quad (4)$$

and

$$\tau^{\max}(\phi_1, \phi_2) = \frac{L_1^{\max}(\phi_1, \phi_2)}{\Delta(\phi_1, \phi_2)} \quad (5)$$

be the spherical analogues of $\rho(x)$, $x \in B$. We set $\tau^{\min}(0,0) = \tau^{\max}(0,0) = 1$, which makes sense given the meaning of $\tau^{\min}(\phi_1, \phi_2)$ and $\tau^{\max}(\phi_1, \phi_2)$.

Note that $\tau^{\min}(\phi_1, \phi_2)$ and $\tau^{\max}(\phi_1, \phi_2)$ are discontinuous at $(0,0)$. To see this note that $\tau^{\min}(\phi_1, 0) = \tau^{\min}(0, \phi_2) = 1$ and that (apply l'Hopital's rule)

$$\lim_{\varphi \downarrow 0} \tau^{\min}(\varphi, \varphi) = \frac{\lim_{\varphi \downarrow 0} \cos(\varphi) - \varphi\sin(\varphi) + 1}{\lim_{\varphi \downarrow 0} 2\sin(\varphi)\cos(\varphi) \Big/ \sqrt{1 - \cos^4(\varphi)}}$$

$$= \frac{2}{\lim_{\varphi \downarrow 0} 2\cos(\varphi) \Big/ \sqrt{1 + \cos^2(\varphi)}} = \sqrt{2} \quad (6)$$

For $\tau^{\max}(\phi_1, \phi_2)$ a similar reasoning holds true.

Also, $\tau^{\max}(\phi_1, \phi_2)$ is not well defined for $\phi_2 = \pi/2$. To see this, note that this is the north pole and that $\tau^{\max}(\phi_1, \phi_2)$ is discontinuous at this point as all points $(\phi_1, \pi/2)$ map on it and $\tau^{\max}(\phi_1, \phi_2) \to 1 + 2\phi_1/\pi$ ($\phi_2 \uparrow \pi/2$). So close to the north pole, $\tau^{\max}(\phi_1, \phi_2)$ varies between 1 and 3, depending on ϕ_1. Since the point $(0, \pi/2)$ can be reached directly from the origin over a meridian, it makes sense to define $\tau^{\max}(\phi_1, \pi/2) = 1$ for all ϕ_1. To see that 3 is also the supremum of $\tau^{\max}(\phi_1, \phi_2)$, first note that on the boundaries we have $\tau^{\max}(0, \phi_2) = 1$, $\tau^{\max}(\phi_1, 0) = 1$, and $\tau^{\max}(\pi, \phi_2) = (\pi + \phi_2)/(\pi - \phi_2) \uparrow 3$ ($\phi_2 \uparrow \pi/2$). As to the interior, consider the first order condition

$$\Delta^2(\phi_1, \phi_2) \frac{\partial \tau^{\max}(\phi_1, \phi_2)}{\partial \phi_1}$$

$$= \Delta(\phi_1, \phi_2) - \frac{(\phi_1 + \varphi_2)\cos(\phi_2)\sin(\phi_1)}{\sqrt{1 - \cos^2(\phi_1)\cos^2(\phi_2)}} = 0$$

$$\Delta^2(\phi_1, \phi_2) \frac{\partial \tau^{\max}(\phi_1, \phi_2)}{\partial \phi_1}$$

$$= \Delta(\phi_1, \phi_2) - \frac{(\phi_1 + \phi_2)\cos(\phi_1)\sin(\phi_2)}{\sqrt{1 - \cos^2(\phi_1)\cos^2(\phi_2)}} = 0 \quad (7)$$

implying that local maxima on the interior of the domain of $\tau^{\max}(\phi_1,\phi_2)$ are necessarily on the line $\phi_1=\phi_2$. However, on the interior

$$\tau^{\max}(\varphi_1,\varphi_1)=\frac{2\varphi_1}{\arccos(\cos^2(\varphi_1))}<\frac{2\varphi_1}{\arccos(\cos(\varphi_1))}=2 \tag{8}$$

Therefore, we conclude that 3 is the supremum of $\tau^{\max}(\phi_1,\phi_2)$.

Finally, for $x\in Q$, let $(\phi_1(x),\phi_2(x))\in[0,\pi]\times[0,\pi/2]$ be its pole coordinates and define $\tau^{\min}=\tau^{\min}(\phi_1(X),\phi_2(X))$ and $\tau^{\max}=\tau^{\max}(\phi_1(X),\phi_2(X))$, where $X\sim U(Q)$ i.e. we randomise $\tau^{\min}$ and $\tau^{\max}$. Numerically we find $\mu(\tau^{\min})\approx 1.168$ and $\mu(\tau^{\max})\approx 1.365$. As $\mu(\rho)\approx 1.273$, we see that, loosely speaking, on average the curvature of the sphere causes the diversion ratio to deviate about 8% from the Flatland situation.

4 THE SKEWED CASE ON PLANET EARTH

Next, like in Flatland, assume the situation in which the rectilinear paths are skewed with parameter γ, where γ is the angle between the equator and the path as it starts in the origin. So, we consider paths starting in the origin, "climbing" with slope γ to the ϕ_2-parallel (below called the skewed section of the path), and then proceed over this parallel to the ϕ_1-meridian either clockwise or anti-clockwise, whichever route is shortest (below called the parallel section of the path). Like in Section 3, this is the shortest path of this kind. By moving first over the equator and starting the climb up north after that, the longest path of this kind is defined. Below we refer to these extreme variants as the shortest and longest paths.

Below we exclude throughout the cases $\gamma=0$ and $\phi_2=\pi/2$, representing situations in which the skewed path has infinite length. Whereas in Flatland it suffices to consider the northeastern part Q of Planet Earth, in the skewed case we need to consider the entire northern hemisphere H i.e. below $(\phi_1,\phi_2)\in[0,2\pi]\times[0,\pi/2]$.

As the skewed section is a loxodrome, i.e. a path over Planet Earth under constant compass direction, it is well known that the length of this section equals $\phi_2/\sin(\gamma)$. As to the length of the parallel section, consider the mercator projection of Planet Earth. It is well known that on this projection the projected distance of the ϕ_2-parallel to the equator equals $gd^{-1}(\phi_2)=\ln(\tan(\pi/4+\phi_2/2))$, where gd^{-1} is the inverse gudermannian or lambertian. Also, it is well known that the mercator projection is a conformal mapping of Planet Earth's surface, i.e. it preserves angles, and that it also preserves distances on the equator. Hence, in case of the shortest path the skewed section ends on the $gd^{-1}(\phi_2)/\tan(\gamma)$-meridian. So, the length $x_\gamma^{\min}(\phi_1,\phi_2)$ of the parallel section is equal to the shortest distance over the ϕ_2-parallel between the ϕ_1-meridian and the $gd^{-1}(\phi_2)/\tan(\gamma)$-meridian, i.e.

$$\begin{aligned}x_\gamma^{\min}(\varphi_1,\varphi_2)&\\ =\cos(\varphi_2)\min\{z_\gamma(\varphi_1,\varphi_2),2\pi-z_\gamma(\varphi_1,\varphi_2)\}&\end{aligned} \tag{9}$$

with

$$z_\gamma(\phi_1,\phi_2)=(\phi_1-gd^{-1}(\phi_2)/\tan(\gamma))\bmod(2\pi) \tag{10}$$

In case of the longest path, it is not difficult to see that, likewise

$$\begin{aligned}x_\gamma^{\max}(\phi_1,\phi_2)&=\min\{z_\gamma(\phi_1,\phi_2),2\pi-z_\gamma(\phi_1,\phi_2)\}\\&=x_\gamma^{\min}(\phi_1,\phi_2)/\cos(\phi_2)\end{aligned} \tag{11}$$

Then the shortest and longest skewed rectilinear distances between the origin and (ϕ_1,ϕ_2) read

$$L_1^{\gamma,\min}(\phi_1,\phi_2)=\frac{\phi_2}{\sin(\gamma)}+x_\gamma^{\min}(\phi_1,\phi_2) \tag{12}$$

and

$$L_1^{\gamma,\max}(\phi_1,\phi_2)=\frac{\phi_2}{\sin(\gamma)}+x_\gamma^{\max}(\phi_1,\phi_2) \tag{13}$$

so that for $(\varphi_1,\varphi_2)\neq(0,0)$ and $\varphi_2\neq\pi/2$ the shortest and longest skewed diversion ratios read

$$\tau_\gamma^{\min}(\phi_1,\phi_2)=\frac{L_{\gamma,1}^{\min}(\phi_1,\phi_2)}{\Delta(\phi_1,\phi_2)} \tag{14}$$

and

$$\tau_\gamma^{\max}(\phi_1,\phi_2)=\frac{L_{\gamma,1}^{\max}(\phi_1,\phi_2)}{\Delta(\phi_1,\phi_2)} \tag{15}$$

Like in Flatland, for $x\in H$, let $(\phi_1(x),\phi_2(x))\in[0,2\pi]\times[0,\pi/2]$ be its pole coordinates and define

$$\tau_\gamma^{\min}=\tau_\gamma^{\min}(\phi_1(X),\phi_2(X)) \tag{16}$$

and

$$\tau_\gamma^{\max}=\tau_\gamma^{\max}(\phi_1(X),\phi_2(X)) \tag{17}$$

where $X\sim U(H)$, i.e. we randomise $\tau_\gamma^{\min}$ and $\tau_\gamma^{\max}$. Note that

$$\mu(\tau_\gamma^{\min})\sin(\gamma) \to \frac{1}{2\pi}\int_0^{\pi/2}\int_0^{2\pi}\frac{\varphi_2\cos(\varphi_2)}{\Delta(\varphi_1,\varphi_2)}d\varphi_1 d\varphi_2$$
$$= \frac{4\kappa}{\pi}(\gamma \downarrow 0) \tag{18}$$

with $\kappa \approx 0.344$ and, likewise, $\mu(\tau_\gamma^{\max})\sin(\gamma) \to 4\kappa/\pi(\gamma \downarrow 0)$.

5 RELATING FLATLAND AND PLANET EARTH

First of all, recall that in the above we concluded that, loosely speaking, in the non-skewed case on average the curvature of the sphere causes the diversion ratio to deviate about 8% from the Flatland situation. More precisely,

$$\frac{\mu(\tau^{\min})}{\mu(\rho)} \approx 91.75\% \tag{19}$$

and

$$\frac{\mu(\tau^{\max})}{\mu(\rho)} \approx 107.23\% \tag{20}$$

In the skewed case we see that for $\gamma \downarrow 0$

$$\frac{\mu(\tau_\gamma^{\min})}{\mu(\rho_\lambda)} \to \kappa \approx 34.4\% \tag{21}$$

and

$$\frac{\mu(\tau_\gamma^{\max})}{\mu(\rho_\lambda)} \to \kappa \approx 34.4\% \tag{22}$$

i.e. for small values of skewness, the ratio is about 34.4% independent of taking the shortest or longest path on Planet Earth or anything in between.

Secondly, in Section 2 we derived $\mu(\rho_\gamma) = 4/\pi\sin(\gamma)$ for fixed γ. However, in landscapes where the level of skewness differs regionally, it makes sense to randomise γ as well, when considering the mean diversion ratio. To this end, for $0 < \varepsilon < \pi/2$ define $\rho_\varepsilon^{U(\gamma)} = \rho_\gamma$, where $\gamma \sim U[\varepsilon, \pi - \varepsilon]$. As to its mean, we can calculate

$$\mu(\rho_\varepsilon^{U(\gamma)}) = \frac{1}{\pi - 2\varepsilon}\int_\varepsilon^{\pi-\varepsilon}\mu(\rho_\gamma)dy$$
$$= \frac{4}{\pi}\frac{\ln(\tan(\pi/2 - \varepsilon/2))}{\pi/2 - \varepsilon}$$
$$= \mu(\rho)\frac{gd^{-1}(\pi/2 - \varepsilon)}{\pi/2 - \varepsilon} \tag{23}$$

Recalling that $\delta_\varepsilon^{mercator} = gd^{-1}(\pi/2 - \varepsilon)$ is the mercator projection the projected distance of the equator to the $(\pi/2 - \varepsilon)$-parallel and that $\delta_\varepsilon^{true} = \pi/2 - \varepsilon$ is the true distance from the equator to the $(\pi/2 - \varepsilon)$-parallel, we see that

$$\frac{\mu(\rho_\varepsilon^{U(\gamma)})}{\mu(\rho)} = \frac{\delta_\varepsilon^{mercator}}{\delta_\varepsilon^{true}} \tag{24}$$

Finally, let $\eta(\gamma)$ be the pole-to-pole distance on Planet Earth along a path with skewness γ. As this path is a loxodrome, its distance measures $\eta(\gamma) = \pi/\sin\gamma$. Also, let $\zeta = \Delta(\pi, 0) = \pi$ be the great circle distance between the poles. Then

$$\frac{\mu(\rho_\gamma)}{\mu(\rho)} = \frac{4/(\pi\sin(\gamma))}{4/\pi} = \frac{\eta(\gamma)}{\zeta} \tag{25}$$

REFERENCES

Lindgren, W.F. and Banchoff T.F., 2010. Flatland—An edition with notes and commentary, Camebridge University Press, Original by the title Flatland—A romance of many dimensions by E.A. Abbott, 1884.

Odijk, M.A. and Van Gelder, P.H.A.J.M., 2013. A note on the length, measured along fixed orientations, of a path connecting any two points relative to their straight line distance, Statistica Neerlandica, doi:10.1111/stan.12001.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A game-theoretical model to allocate security resources in a multi-modal transportation system facing adaptive adversaries

Luca Talarico & Kenneth Sörensen
Research Groups ANT/OR, Faculty of Applied Economics, University of Antwerp, Antwerp, Belgium

Genserik Reniers
Center for Corporate Sustainability (CEDON), HUB, KULeuven, Brussels, Belgium
Safety Science Group, TU Delft, Delft, The Netherlands

ABSTRACT: In this paper we present a model to allocate security resources within a chemical supply chain which is characterized by the use of different transportation modes, each having their own security features. We consider security-related risks so asto take measures against terrorist acts which could target critical transportation systems. The idea of addressing security-related issues, by supporting decisions for preventing or mitigating intentional acts on transportation infrastructure, has gainedattention in academic research only recently. The decision model presented in this paper is based on game theory. The **M**ult**I**-modal **S**ecurity-**TRA**nsportation mode**L**, that we named *MISTRAL* for short, can be employed to organize intelligence capabilities aimed at securing chemical supply chains. It enables detection and warning against impending attacks on transportation infrastructures and the subsequent adoption of security countermeasures. This is of extreme importance for preventing terrorist attacks and for avoiding (possibly huge) human and economic losses.

Keywords: multi-modal transportation; security risk analysis; game-theory; multi-attribute utility

1 INTRODUCTION

Daily shipments of dangerous goods are critical to global economies. However, these transportation activities involve a variety of security risks. In case of incidents, dangerous freights would obviously attract the attention of the general public, policy-makers and industrialists. Therefore, both for the responsible government and the private authorities, it is essential to efficiently secure these hazardous transports. Since a lot of stakeholders are involved in a chemical supply chain, it is not easy to adequately and efficiently securing it. Moreover, while the *unintentional accident* likelihood depends on (relatively) well-known parameters such as maintenance of infrastructure, speed characteristics and the presence of junctions, the *intentional accident* likelihood relates to much less known factors such as vulnerabilities, consequences, and intentions.

One of the key factors of the chemical supply chain is multi modality; i.e., the use of different transport modes, each having their own characteristics with respect to economic and environmental parameters, as well as characterized with safety and security mode-specific features. Multi-modal transportation indeed is very important and it is widely adopted in the chemical industry to transport goods, using e.g. road, railway, barges, ships, and pipelines combined together. A variety of companies are active usually within one of the available transport modi; and rarely they operate within several of the modi at the same time. Nonetheless, by transporting chemical products employing different modes, the chemical industry and its Logistics Service Providerscan probably greatly improve their security scores.

Allocating security resources is essential on both intra- and inter-modal levels. On an intra-modal dimension, the authorities or the companies responsible for the transport have to decide on which transportation routes, belonging to the same mode, available between point A and point B, security measures have to be taken. This decision regarding security resources allocations should take into account all existing and feasible uni-modal transportation routes between A and B and it should be repeated for every dangerous freight the authorities or the companies wish to investigate. On an inter-modal dimension, the different available modi for transporting a certain hazardous cargo between A and B should be investigated and security resources need to be allocated

between the different modi, which forms an extra complexity to the uni-modal security resources allocation problem. Since multi-modal planning is even more difficult than uni-modal planning an even stronger need for support by a mathematical model is present in the multi-modal case.

Three research lines are present in scientific literature regarding the development of safety decision support software in order to transport dangerous freights: (i) safety-related risk assessment software packages; (ii) route selection and vehicle scheduling software packages; and (iii) hazardous materials network design software. Note that these software packages that deal with *safety*-related transport problems are designed to guide uni-modal decisions. Among them, it is worth mentioning probabilistic tools, GIS-based tools, tools ensuring an equitable distribution of risk, tools based on the iterative application of minimum path algorithms, tools based on the generation of minimum paths, tools based on multi-objective algorithms, bi-levels programming tools (taking into account two distinct decision-makers: the government and transport companies), and tools based on heuristic algorithms.

However, the idea of developing such software packages addressing security-related issues and specifically aiming them at supporting decisions for preventing or mitigating intentional designed malicious acts on transportation infrastructure, has only very recently gained attention in the academic world.

We are aware that various conceptualisations and software packages (GIS-based or not) for dangerous freight risk assessments capturing one or several of the transport modes, have been elaborated and are explained in literature. However, as mentioned before, these software applications are aimed at safety related (nonintentional) risks and they could not be used for taking measures against intentional (terrorist) acts. In fact, to our knowledge, at present there is no model for the transportation of dangerous substances available for governmental or industrial decision makers, which is based on a multi-attribute terrorist utility and which provides recommendations on where to optimally allocate security measures and resources in a multi-modal chemical transportation network. This paper elaborates such a model and uses game theory to do so.

2 RELATED SECURITY PROBLEMS AND RESEARCH QUESTIONS

Since the terrorist attacks on 11 September 2001, game theory has been increasingly employed as a mathematical tool to deal with security decisions facing with adaptive adversaries. In particular, recent literature includes Bier et al. (2008); Dighe et al. (2009); Guikema and Aven (2010) and Zhuang et al. (2010). More specifically, gaining insights into the nature of optimal defensive investments which yield the best trade-off between investment costs and critical infrastructure security was also already subject of an important amount of scientific research, e.g., Gao et al. (2013b); Golany et al. (2009); Hausken and Levitin (2009); Hausken and Zhuang (2013); Merrick and Parnell (2011); Reniers (2010); Roy and Jomon Aliyas (2013). In order to have more details about these methods the reader is referred to an extensive survey made by Sandler and Siqueira (2009).

However, to date, no concrete attention has been paid to decision problems arising in the allocation of security resources in a multi-modal transportation network. This is thus a research subject deserving much more attention from the academic world as well as from governmental authorities.

We agree with Cox (2009) that game theory and risk analysis are mutually reinforcing in order to obtain effective risk management recommendations for allocating security resources. In case of our multi-modal transportation problem, we choose to focus on the development of an attacker-defender model based on game theory. We consider a dynamic game with incomplete information in which the defender chooses how to allocate the security resources, and then an attacker chooses which target to attack according to a multi-attribute utility function. A model focusing on multi-modal transportations of dangerous goods should make the decision process of taking security countermeasures allocations in a complex transportation network more objective and (subsequently) more justified.

In the remainder of the paper we will refer to a *strategic game* as a model in which a set of decision makers interact with each others. In recognition of the interaction, we will use the term *players* to identify the decision makers.

The research questions of this paper therefore (i) include a ranking of transportation routes and modes where to allocate security countermeasures based on certain assumptions; and (ii) provide this ranking considering both inter—and intra-modal transports of hazardous goods.

In the next section the characteristics of a multi-modal supply chain are briefly mentioned and in Section 4 a one-period $\mathcal{MISTRAL}$ model is defined. The model has been used within a solution approach in order to simulate different realistic scenarios which might affect a chemical supply chain. Detailed results will be illustrated during the conference.

3 CHARACTERISTICS OF A MULTI-MODAL CHEMICAL SUPPLY CHAIN

Supply chains used to transport hazardous materials represent a viable target for terrorist groups mainly due to two factors:

1. the physical and chemical properties of the transported material may cause a malicious release which could potentially engender public injuries to a neighbouring population and/or environmental damages;
2. the critical importance of the products may determine the disruption of operations of the whole industry along the supply chain.

In general, terrorists' actions are targeted at critical infrastructures, suggesting that attackers select their targets for strategic reasons in order to maximize the consequences of the damages. The transported material and its operating conditions (e.g. pressure, temperature, density, volume) are both crucial to determine the criticality of the supply chain. In fact the possible scenarios (e.g. explosions, toxic cloud migrations, thermal radiation effects, toxic releases), that can arise after an attack, influence the level of criticality of a certain supply chain.

In our study, we focus on four real and tangible transportation modes which are commonly encountered within chemical supply chain: inland waterways ($i = 1$), road transport ($i = 2$), railway ($i = 3$), and pipeline ($i = 4$). Considering the system structure of the different transport modes, we assume that road ($i = 2$) and pipeline ($i = 4$) have a parallel structure, whereas inland waterways ($i = 1$) and railway ($i = 3$) have a serial structure[1].

It should be noted that by enlarging the set of available transportation modes the *MISTRAL* model could be generalized and extended to other supply chains which are used for non chemical products that might be a potential target for terrorists-attackers.

4 MISTRAL MODEL

In the *MISTRAL* model, here proposed, we consider that r_i routes for each mode i are present in a chemical supply chain as described in the previous section. Therefore, there are altogether $r_1 + r_2 + r_3 + r_4$ routes in the system. For route j in mode i, we let the government's defense level be d_{ij} and let the terrorist's attack level be A_{ij}, for $i = 1, \ldots, 4$ and $j = 1, \ldots, r_i$. The probability of damage conditional on an attack happening on each route is a function of d_{ij} and A_{ij}. In particular, we apply the common ratio form contest success function (Skaperdas (1996); Tullock (1980)), that is:

$$P_{ij}(A_{ij}, d_{ij}) = \frac{A_{ij}}{A_{ij} + \beta_i \cdot d_{ij}} \tag{1}$$

where β_i is the relative defense/attack effectiveness ratio for mode i. We assume that $\beta_1 > \beta_2 > \beta_3 > \beta_4$ (i.e., the inland waterways transports are easiest to defend while pipeline transports are most difficult to defend). Note that we have $\partial P_{ij}/\partial d_{ij} \leq 0$ and $\partial P_{ij}/\partial A_{ij} \geq 0$. We define $P_{ij}(0, d_{ij}) = 0 \ \forall d_{ij}$.

Assuming performance independence among routes $j = 1, \ldots, r_i$ within a mode i, the vulnerability Q_i associated to mode i is calculated as:

$$Q_i(A_i, d_i) = \begin{cases} \prod_{j=1}^{r_i} P_{ij}(A_{ij}, d_{ij}), & \text{if } i = 2,4 \\ 1 - \prod_{j=1}^{r_i} [1 - P_{ij}(A_{ij}, d_{ij})], & \text{if } i = 1,3 \end{cases} \tag{2}$$

where $A_i = (A_{i1}, \ldots, A_{ir_i})$ and $d_i = (d_{i1}, \ldots, d_{ir_i})$. Now we consider the valuation of route i, namely the expected loss conditional on a successful attack, v_i. We consider two types of losses (financial loss fi and human loss h_i) and use the following multi-attribute utility function:

$$v_i = f_i + c \cdot h_i \tag{3}$$

In formula (3) c represents a factor translating human loss into financial terms. Furthermore, we assume that $f_2 < f_4 < f_1 < f_3$ and $h_1 < h_4 < h_2 < h_3$; in other words, road transportation and inland waterways would lead to the lowest possible financial and human losses, respectively, and railway would lead to the highest financial and human losses. These are just some assumptions that we made without loss of generality which can be easily changed by the user of the *MISTRAL* model to fulfill the requirements of a specific chemical supply chain.

We assume that the government desires to maximize the total expected averted losses, subtracting the total defense costs, while the terrorist wants to maximize the total expected damage, subtracting the total attack costs. In other words, government and terrorist maximize their utilities $u(A,d)$ and $U(A,d)$, respectively as follows:

$$\max_d u(A,d) = \sum_{i=1}^{4} \left\{ v_i \cdot [1 - Q_i(A_i, d_i)] - b \cdot \sum_{j=1}^{n_i} d_{ij} \right\} \tag{4}$$

[1]We acknowledge that this assumption on system structure depends on the scope of the security study, but we believe that these assumptions are generally reasonable.

$$\max_{A} U(A,d) = \sum_{i=1}^{4} \left[v_i \cdot Q_i(A_i,d_i) - B \cdot \sum_{j=1}^{n_i} A_{ij} \right] \qquad (5)$$

In formulae (4)-(5) b and B are unit costs for defense and attacks, respectively and $A = (A_1 \ldots, A_4)$ and $d = (d_1, \ldots, d_4)$ represent a specific set of possible actions to be adopted by the attacker and the government respectively. In particular these actions are addressed to a specific transportation mode (e.g. $A_i = (A_{i1}, \ldots, A_{in_i})$ or $d_i = (d_{i1}, \ldots, d_{in_i})$) each containing j routes. In the remainder of the paper we will refer to A and d with the term text it *strategies* to denote a specific attack (for A) and defense (for d) actions. The quality of each strategy is measured by using the *utility functions*, mentioned before, which are able to capture and quantify players' preferences.

It should be noted that in the strategic game the players' payoffs have only a ordinal significance. For example, if a player has three available (attack or defense) strategies named a, b, and c for which the resulting payoff is respectively 1, 2, and 10, the only conclusion that it is possible to draw is that the player prefers c to b and b to a. In other words the values associated to the payoff in themselves do not imply that the player's preference between c and b is stronger than his preference between a and b (see e.g., Osborne (2003)).

Below we consider two possible sequences of moves: simultaneous-move and sequential move (where the defender is the first mover). Both sequences have been studied in literature by e.g., Gao et al. (2013a), Shan and Zhuang (2013) and Bakir (2011). If the defense is public information and terrorists know the defense allocation before making the attacking decisions, a sequential-move model should be used. Otherwise, if both players make decisions at the same time, or at least they do not know the other player's choice at the time that they make their own decisions, a simultaneous-move model should be used.

Definition 1. *We call a pair* (A^*, d^*) *an equilibrium for a simulataneous-move* $\mathcal{MISTRAL}$ *game if and only if* $A^* = \arg\max_A U(A, d^*)$ *and* $d^* = \arg\max_d u(A^*, d)$.

Definition 2. *We call a pair* (A^*, d^*) *an equilibrium for a sequential-move* $\mathcal{MISTRAL}$ *game (where the government is the first mover) if and only if* $A^* = \hat{A}^*$ *and* $d^* = \arg\max_d u(\hat{A}^*, d)$, *where the best response function* $\hat{A}^*$ *is defined as* $\hat{A}^* = \arg\max_A U(A,d)$.

5 CONCLUSIONS

In this work a model which can guarantee the security of a multi-modal transportation system facing adaptive adversaries has been presented. The model, named $\mathcal{MISTRAL}$, can be used by public and private organizations in order to establish the appropriate allocation of security countermeasures for each route belonging to a specific transportation mode within a chemical supply chain.

Using theorems and concepts borrowed from game theory the $\mathcal{MISTRAL}$ model can be solved by evaluating and analysing the utilities associated to the two players with different interests that are involved in the strategic game. On one side there is the government (or a public-private institution) who intends to protect a given critical infrastructure by allocating adequate security measures on both the inter-modal and intra-modal levels, and on the other side there is the attacker whose goal is to destroy a targeted supply chain. A methodological scheme to find the equilibrium, has been applied to a variety of illustrative examples that will be presented at the conference.

When no limitations or constraints on the defensive or attack strategies are applied, the solution of the $\mathcal{MISTRAL}$ game consists of an imitation of the opponent's strategy. In other words, by using intelligence services the government should try to anticipate the terrorists' moves and guarantee appropriate security levels, which could at least counterbalance the intensity levels of the attacks. This concept is applied to specific prevention mechanisms adopted by several nations, such as those based on a "terror alert level" scale (HSAC, 2009; UK Cabinet Office, 2006).

Possible applications of the $\mathcal{MISTRAL}$ model pertain to the anticipation of potential attacks to a targeted chemical supply chain and the limitation of the consequences of these attacks thanks to an appropriate evaluation of terrorist threats. Additionally, the $\mathcal{MISTRAL}$ model can lead to a better definition and allocation of the security countermeasures for both intra-modal and inter-modal levels.

Future research will be aimed at extending the current $\mathcal{MISTRAL}$ model to incorporate the case of repeated games. In so doing, it will be possible to simulate realistic scenarios in which continuous attacks are directed to the same supply chain, e.g. the repeated attacks performed on a specific critical pipeline infrastructure Talarico et al. (2014). Moreover, additional real-life constraints can be included in the model such as a limited budged for security (or for the attacks), criticality of the infrastructures constituting the whole supply chain and so forth. Additional information about the characteristics of the transported goods can be included in the model. As a matter of fact, the hazardousness of these materials can influence the consequences of a potential attack.

REFERENCES

Bakir, N. (2011). A stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research 187*(1), 5–22.

Bier, V., N. Haphuriwat, J. Menoyo, R. Zimmerman, & A. Culpen (2008). Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis 28*(3), 763–770.

Cox, L. (2009). Game theory and risk analysis. *Risk Analysis 29*(8), 1062–1068.

Dighe, N., Z. J., & B. V.M. (2009). Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. *International Journal of Performability Engineering, special issue on System Survivability and Defense against External Impacts 5*(1), 31–43.

Gao, X., W. Zhong, & S. Mei (2013a). A game-theory approach to configuration of detection software with decision errors. *Reliability Engineering & System Safety 119*(0), 35–43.

Gao, X., W. Zhong, & S. Mei (2013b). Information security investment when hackers disseminate knowledge. *Decision Analysis 10*(4), 352–368.

Golany, B., E. Kaplan, A. Marmur, & U. Rothblum (2009). Nature plays with dice terrorists do not: allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research 192*(1), 198–208.

Guikema, S. & T. Aven (2010). Assessing risk from intelligent attacks: A perspective on approaches. *Reliability Engineering and System Safety 95*(5), 478–483.

Hausken, K. & G. Levitin (2009). Minmax defense strategy for complex multi-state systems. *Reliability Engineering and System Safety 94*(2), 577–587.

Hausken, K. & J. Zhuang (2013). The impact of disaster on the strategic interaction between company and government. *Eu-ropean Journal of Operational Research 225*(2), 363–376.

HSAC, H.S.A.C. (2009, September). Homeland security advisory system, task force report and recommendaations. Technical report, U.S. Department of Homeland Security. Merrick, J. & G. Parnell (2011). A comparative analysis of pra and intelligent adversary methods for counterterrorism risk management. *Risk Analysis 31*(9), 1488–1510.

Osborne, M. (2003). *An Introduction to Game Theory*. USA: Oxford University Press.

Reniers, G. (2010). An external domino effects investment approach to improve cross-plant safety within chemical clusters. *Journal of Hazardous Materials 117*(1–3), 167–174.

Roy, A. & P. Jomon Aliyas (2013). Terrorism deterrence in a two country framework: strategic interactions between r&d, defense and pre-emption. *Annals of Operations Research 211*(1), 399–432.

Sandler, T. & K. Siqueira (2009). Games and terrorism. *Simulation & Gaming 40*(2), 164–192.

Shan, X. & J. Zhuang (2013). Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game. *European Journal of Operational Research 228*(1), 262–272.

Skaperdas, S. (1996). Contest success functions. *Economic Theory 7*, 283–290.

Talarico, L., k. Sörensen, G. Reniers, & J. Springael (in press 2014). *Securing Transportation Systems*, Chapter Pipeline Security. New York: Springer Science and Business Media, LLC.

Tullock, G. (1980). *Efficient Rent-Seeking* (Buchanan, J.M., Tollison, R.D., and Tullock, G. ed.). Toward a Theory of the Rent-Seeking Society. College Station: Texas A. & M. University Press.

UK Cabinet Office, (2006, July). Threat levels: The system to assess the threat from international terrorism. Guidance Policy: Protecting the UK against terrorism, National security and intelligence, St Clements House, 2–16 Colegate, Nor-wich, UK.

Zhuang, J., V. Bier, & O. Alagoz (2010). Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research 203*(2), 409–418.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Assessment of the critical events sequences of systems by means of probabilistic languages

D. Ionescu, N. Brînzei & J.F. Pétin
CRAN, UMR 7039, Université de Lorraine, Vandœuvre-lès-Nancy, France
CNRS, CRAN, UMR 7039, Vandœuvre-lès-Nancy, France

ABSTRACT: In dependability studies of dynamic systems it is important to assess the probability of occurrence for the events sequences which describe the system evolution or which are critical for the mission of the system or for the humans and environment safety. In this paper we use the probabilistic languages framework in order to realize the quantitative assessment and we start by modeling the system as a finite state automaton. This is ulterior transformed in a probabilistic automaton using the embedded discrete Time Markov Chain. The determination of the languages afferents at each state of the automaton enable to calculate the probability of occurrence for every events sequence that can be subtract from these languages.

1 INTRODUCTION

Assessing the dependability of a critical system generally relies on Boolean models (Fault Trees models, Reliability block diagrams, etc.) for:

- qualitative analysis, such as the determination of the sets of component's failures that cause a critical or undesired system situation (it is defined as the *cut* set),
- quantitative analysis to evaluate the probabilities of undesired events or RAMS indicators, that can be based on the Sylvester-Poincaré Theorem or Binary Decision Diagrams technique (Dutuit & Rauzy 2005, Ibanez-Llano et al. 2010).

This paper explores the use of probabilistic languages introduced by (Garg et al. 1999) as a formal framework for qualitative/quantitative analyze of the event sequences. Before to describe the *probabilistic languages* concept, we will present some reasons that motivate the choice of *events sequences* in dependability studies.

Evaluation using *cut* analysis requires a full independence of the events involved in the *cut* set. However, this assumption cannot be stated in the case of dynamic reparable systems due to the order relationship between events occurrence:

- occurrence of event may depend on previous occurrence of other events; *e.g.* in the dynamic controlled systems event occurrence may be prohibited by its control according to a previous occurrence, or not, of some other events,
- impact of event sequence on the system failure may be different according to the scheduling of the event occurrence within the sequence; *e.g.* event e_1 followed by event e_2 leads to an undesired event while e_2 followed by e_1 has no impact.

In these cases, the value of the obtained probability, based on *cut-set* calculus, represents an overstatement of the real probability that is searched, corresponding no longer with the actual needs of dependability studies.

Moreover, the *cut*-based analysis approaches fit well to the non-reparable systems. However, in dynamic reliability context, it is necessary to take in consideration the changes between the different modes of functioning/failure or when the systems turns back into a functioning state after having passed in a failure state. In this case the systems must be considered like reparable and only dynamic models are able to capture system reconfigurations.

For all these reasons, the *cut-set* based analysis needs to be enriched by the determination and assessment of event sequences within the *cut-set*. This evolution justifies the use of state space models to capture the system dynamic and the impact of component's failures and reparation on the system state. Some approaches have been recently developed to determine the critical sequences of events and some basic properties such as minimality and consistency has been proposed for dynamic reparable system (Bouissou & Bon 2003, Chaux et al. 2013). However, these approaches are based on deterministic language theory and focus on the identification of a set of events sequences but present some limitations and divergences for

qualitative and quantitative assessment due to modeling and sequence calculus assumptions.

The paper is organized as follows. Section 2 presents the state of the art and highlights the current limitations of existing approaches for sequences assessment. Section 3 introduces the theoretical framework of the probabilistic languages (Garg et al. 1999) and the used notations. In section 4 is introduced the case study which is used like a support for the rest of the paper. Section 5 develops a theoretical framework based on probabilistic languages for quantitative assessment of events sequences. This proposed approach is illustrated using the case study in the section 6. Finally, section 7 presents the conclusions of this work and identifies some future research directions.

2 STATE OF THE ART

The existing approaches in quantitative assessment area can be classified in two categories:

- *Boolean models* where the failure of the system is expressed using the Boolean structure function;
- *state space models* where the system behavior is represented by states and transitions and his evolution is described by the associated language.

2.1 *Boolean models*

The most important Boolean models are: Event Trees and Fault Trees (classics/dynamics). *Event Trees* (Papazoglou 1998) are graphical models that can be discretized according to their possible effects or distinction in a series of simple events. In the same time *Event Trees* are adapted for modeling and assessment of the events sequences for non-reparable systems such as safety or protection systems. Instead, the reparable systems or instrumentation and control systems can not be modeled by *Event Trees*. *Fault Trees* are built according to an undesired event that is decomposed into basic events till this decomposition becomes impossible or judged useless (Dutuit & Rauzy 2005). These models are efficient for *cut*-based analysis but have limitations for *sequence*-based analysis because of the static point of view they consider.

2.2 *State space models*

The most currently used state space models in the context dependability studies are (Cassandras & Lafortune 2008): Finite State Automata and Language theory, Petri Nets and Markov chains. Other models can also be mentioned in the context of this paper. *Boolean logic Driven Markov Process* (*BDMP*) developed by Bouissou & Bon (2003) replaces the basic events of a fault tree with Markov chains; this combination introduces dynamic features to cover the order and impact of events occurrence. Events sequences are determined by exploration of the model starting with the initial state of the system (Bouissou 2006). *Stochastic Hybrid Automaton* is a stochastic temporized finite state automaton with embedded differential equations for each mode (Perez Castaneda et al. 2011); this model enables to determine sequences of events and their probabilities thanks to Monte-Carlo simulation, but it is not possible to obtain analytical solution.

All these models can be used, according to their deterministic or stochastic features for event sequences analysis (Bouissou & Bon 2003, Chaux et al. 2013) with two kinds of problem solving: *determination* and *probability assessment* of the event sequences.

For the determination problem, approaches based on the language theory are efficient to compute some event sequences leading to a given state. Calculus is possible only for coherent systems and helps to determine the minimal set of sequences aiming to reconstruct the whole failure language (Chaux et al. 2013). This approach does not allow quantitative assessment for the determined events sequences.

For the assessment of sequence probability, some limitations are encountered by the existing approaches:

- state space models such as Markov chains are efficient for determining a state probability. Consequently, a sequence needs to be assimilated to its final state that must be considered as an absorbing state. In this case, probability of this state represents the probability of the language reaching this state.
- the sequence probability calculus is based on the events occurrence probability; in existing approaches, the value of this probability remains the same whatever is the state from which the event occurs. However, in dynamic system, a given event may have different occurrence probability in different system states even if its meaning—failure or reparation of the component c_i—remains the same in all sequences.

Probabilistic Languages (Garg et al. 1999), that takes advantages from both languages theory and stochastic process theory, appears to be an interesting way towards a formal framework for the analysis of event critical sequences. The next section presents the theory foundation of the *probabilistic languages* concept.

3 PROBABILISTIC LANGUAGES FRAMEWORK

The theory of probabilistic languages was developed by Garg, Kumar & Marcus (1999) in order to model the stochastic Discrete Event Systems (DES) behavior.

To simplify the formal definition of the probabilistic language, a special event called "termination event", noted e_Δ, is used to represent the fact that the state of the system obtained after the occurrence of a sequence is a terminal state. A system state is terminal if it represents a special interest for the study (e.g. system mission achievement, dangerous failure state). Thus the system behavior is given by the set Ω of finite length sequences followed or not by the termination event:

$$\Omega = \sum^* (e_\Delta + \varepsilon) = \sum^* e_\Delta \cup \sum^* \tag{1}$$

In this equation Σ is the set of all events called alphabet, Σ* is the set of all finite events sequences of the alphabet Σ (* is the iteration operation called also Kleene-closure) and ε represents an empty sequence of events.

To determine the occurrence probability for an events sequence *s,* should be considered not only the independent occurrence of this sequence but also the occurrence of all sequences that starts with *s* (all the sequences which have *s* like prefix). The set of all the sequences having a given prefix sequence *s* is given by:

$$< s >= \{st \mid st \in \Omega\} \tag{2}$$

Definition 1 (Garg et al. 1999): Consider the measurable space (Ω,F), where $\Omega = \Sigma^*(e_\Delta + \varepsilon)$ and F is the σ-algebra generated by $\{<s>|s \in \Omega\}$. Then a *probabilistic language* (p-language) $\mathbb{P}$ is a probability measure on the measurable space (Ω,F).

Thereby *the termination probability for a sequence s* (the probability that the evolution of a system ends after the occurrence of *s*) is given by the following expression:

$$\mathbb{P}(se_\Delta) = \mathbb{P}(s) - \sum_{e\in\Sigma} \mathbb{P}(se),\ \forall s \in \sum^* \tag{3}$$

where $\mathbb{P}(s)$ represents the occurrence probability of *s* and $\Sigma_{e\in\Sigma}\ \mathbb{P}(se)$ represents the probability of continuous operation beyond *s*.

The probabilities of termination corresponding to different sequences are mutually exclusive, so the cumulative probability that the system arrives in a terminal state can be obtained by adding the individual probabilities for all possible sequences:

$$\mathbb{P}(Syst\ e_\Delta) = \sum_{s\in\Sigma^*} \mathbb{P}(se_\Delta) \tag{4}$$

Sometimes it is easier to describe a *p-language* using an associated automaton that can recognize this language.

Definition 2: A probabilistic automaton (or p-automaton) over the alphabet (set of events) Σ is defined by the following quintuple:

$$A_p = (X, \Sigma, f, \mathbb{P}, x_0) \tag{5}$$

where:

- X is a finite set of states;
- Σ is a finite set of events called alphabet;
- f: $X \times \Sigma \to X$ is the transition function that associates to each initial state and each event an arrival state;
- $\mathbb{P}$: $X \times \Sigma \times X \to [0,1]$ is the probability transition function affecting to each transition a discrete occurrence probability which satisfies the following relation:

$$\sum_{x_j\in X} \sum_{e\in\Sigma} \mathbb{P}(x_i, e, x_j) \le 1,\ \forall x_i \in X \tag{6}$$

- x_0 represents the initial state.

The evolution of a p-automaton is the following: if the system is in the state x_i, the transition e to the state x_j is done with the probability $\mathbb{P}(x_i,e,x_j)$. The probability transition function can be extended to the paths $\pi \subset X(\Sigma X)^*$ in the p-automaton A_p (a path is obtaining by concatenating the transitions, where the end state and the initial state of two consecutive transitions coincide). The probability of the paths is defined by the next equation:

$$x_j \in X : \mathbb{P}\left(\pi e x_j\right) = \mathbb{P}\left(\pi\right)\mathbb{P}\left(x \mid \pi \mid e x_j\right) \tag{7}$$

Each p-automaton defines a p-language and inversely each p-language can be represented by a p-automaton.

Definition 3 (Garg et al. 1999): The p-automaton $A_p = (X, \Sigma, f, \mathbb{P}, x_0)$ with:

$$\forall s,t \in \sum^*, e \in \sum : \mathbb{P}\left(s,e,t\right) = \begin{cases} \dfrac{L(t)}{L(S)}, \text{if t} = se \\ 0, \text{otherwise.} \end{cases} \tag{8}$$

generates a L p-language.

4 PRESENTATION OF THE CASE STUDY

In order to present the application of probabilistic languages we start by considering an oven

temperature control system (Fig. 1). It operates in the following manner: the oven temperature can be controlled by a Proportional Integral controller (PI) or by an On/Off controller.

The Proportional Integral controller (PI) has the role of keeping the temperature at a given target value and is characterized by a failure rate λ_{PI} and by a probability of failure on demand p_{refPI}. The role of On/Off controller is to maintain the temperature in a given range and is also characterized by a failure rate $\lambda_{on/off}$ and by a probability of failure on demand $p_{refon/off}$. When the controller PI fails, the On/Off controller provides the temperature control if this one is not failing on demand. In the same manner if the On/Off controller fails the PI controller will provide the temperature control (if it not fails on demand).

When either of the controllers is failed it will be repaired, the repair process being characterized by a repair rate μ_{PI} respectively $\mu_{On/Off}$. This operating mode represents the simplified operating mode (obtained by removing the continuous part of the system describing the temperature evolution) of the case study defined in (Perez et al. 2011).

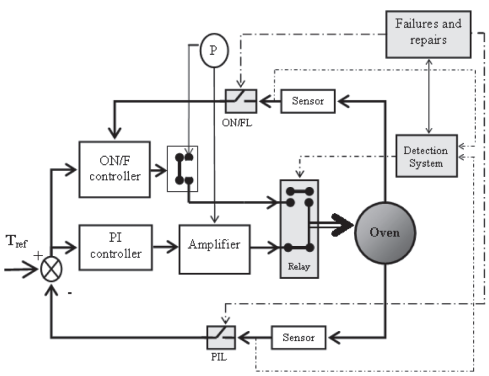


Figure 1. Structural diagram of the temperature control system of an oven.

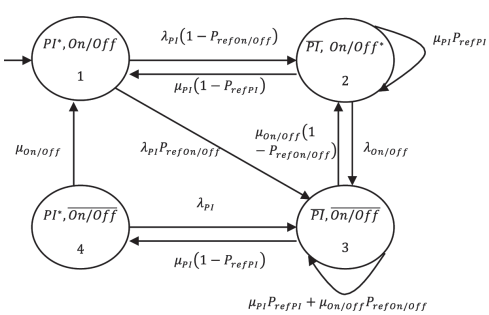


Figure 2. Continuous Time Markov Chain of the case study.

The values for the different rates that characterize the system transitions are:

$$\lambda_{PI} = 3.5 \cdot 10^{-5} h^{-1}, \lambda_{On/Off} = 2 \cdot 10^{-5} h^{-1},$$

$$\mu_{PI} = 8 \cdot 10^{-2} h^{-1}, \mu_{On/Off} = 10 \cdot 10^{-2} h^{-1},$$

$$p_{refPI} = 0.03, p_{refOn/Off} = 0.05.$$

The automaton that describes this system is presented in Figure 2.

5 PROPOSED APPROACH

The proposed approach is decomposed into four steps.

5.1 *Step 0: system modelling*

The approach based on probabilistic languages theory proposed by Garg et al. needs to give a priori the p-language (the set of sequences and for each sequence s the occurrence probability of sequences sub set that have s like prefix). In other words, the p-language is built from equation (3). This knowledge (the whole set of sequences and their probabilities) is not aware in the dependability studies. In dependability studies, the problem is rather reverse: giving a system, we need to determine the events sequences and, after that, to calculate their occurrence probabilities. Thus, we propose to work with, as initial data, the p-automaton.

5.2 *Step 1: events probability determination*

The p-automaton needs to be provided with event occurrence discrete probability for each transition (as in definition 2). As in dependability studies the probability laws describing the stochastic phenomena are rather continuous, we propose to determine discrete probabilities required by p-automata theory using embedded Discrete Time Markov Chain (DTMC) (Fig. 3) in a continous time stochastic process. This embedded DTMC is obtained by considering only the instants of transition firing between states. Using embedded DTMC ensures that the system reaches a stationnary probabilities distribution of states. Consequently, the probability p_{ij} of a transition e_{ij} that starts from a given state s_i to another state s_j is determined as the ratio between the rate of this transition and the sum of the rates for all transitions starting from state s_i. This probability is given by the following relation:

$$\mathbb{P}(e_{ij}) = p_{ij} = \lambda_{ij} / \sum_{j \neq i} (\lambda_{ij}) \quad (9)$$

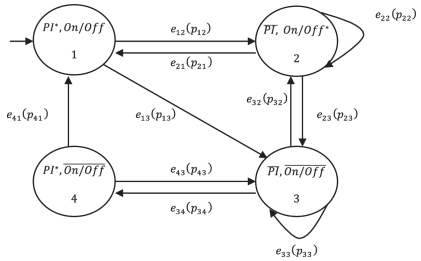


Figure 3. Discrete Time Markov Chain representing the p-automaton for the case study.

For example on the case study, the occurrence probabilities for the transitions e_{32}, e_{33} and e_{34} are:

$$\mathbb{P}(e_{32}) = p_{32} = \frac{\mu_{On/Off}\left(1 - p_{refOn/Off}\right)}{\mu_{On/Off} + \mu_{PI}}$$

$$\mathbb{P}(e_{33}) = p_{33} = \frac{(\mu_{On/Off}\, p_{refOn/Off} + \mu_{PI}\, p_{refPI})}{\mu_{On/Off} + \mu_{PI}}$$

$$\mathbb{P}(e_{34}) = p_{34} = \frac{\mu_{PI}(1 - p_{refPI})}{\mu_{On/Off} + \mu_{PI}}$$

Note that the sum off all the transitions, which can start from a given state, is equal to one.

5.3 *Step 2: sublanguages determination*

After event probability determination, next step is about probability sequence calculus.

Considering the case study, we focus on the analysis of the sequences that reach the state 3 (dangerous state). Indeed, in this state, the system is completely failed and the temperature oven is uncontrolled.

To use the equation (3), which gives the expression of the probability of these sequences, state 3 must be considered as a terminal state. Thus for a sequence, which terminates in state 3, considering first that the occurrence probability of a sequence is equal with the product between transitions probabilities (equation 7) and also considering the events e_{32}, e_{33} and e_{34}, which allowed the system to continue his evolution beyond the state 3, the termination probability for the sequence s it is:

$$\begin{aligned}
\mathbb{P}(se_{\Delta}) &= \mathbb{P}(s) - \sum \mathbb{P}(se) \\
&= \mathbb{P}(s) - \left(\mathbb{P}(se_{32}) + \mathbb{P}(se_{33}) + \mathbb{P}(se_{34})\right) \\
&= \mathbb{P}(s) - (\mathbb{P}(s)\mathbb{P}(e_{32}) + \mathbb{P}(s)\mathbb{P}(e_{33}) \\
&\quad + \mathbb{P}(s)\mathbb{P}(e_{34})) \\
&= \mathbb{P}(s) - \mathbb{P}(s)(\mathbb{P}(e_{32}) + \mathbb{P}(e_{33}) + \mathbb{P}(e_{34})) \\
&= \mathbb{P}(s) - \mathbb{P}(s)(p_{32} + p_{33} + p_{34}) \\
&= \mathbb{P}(s) - \mathbb{P}(s) \cdot 1 = 0
\end{aligned}$$

This approach is proposed in the p-languages theory and it was developed in the context of synthesis of control strategy by supervision (Wang & Ray 2004). The obtained result shows that, in dependability studies, the calculus of events sequences probability is not possible if this p-language is coupled with embedded DTMC without any cautions (if the terminal state of a sequence is not an absorbent state, its probability is always equal to zero).

To avoid this, we propose to determine firstly the whole set of events sequences of the system, that is represented by the language L_{sys}. This language can be represented as the union of sublanguages associated with the states of the system. A sublanguage associated to a state s_i is defined as the set of all events sequences, which lead the system from its initial state to the considered state.

$$L_{syys} = \bigcup_{s_i} L_i \tag{10}$$

To determine the sublanguages L_i we propose to use the theory of rational languages and more precisely the Arden lemma (Carton 2008).

Arden Lemma: Being two languages A and B and being the equation:

$$L_i = L_i A + B \tag{11}$$

where L_i represents the unknown language:

1. if $\varepsilon \notin A$, the only solution of the equation is $L_i = BA^*$.
2. if $\varepsilon \in A$, the solutions have the form $L_i = (B + C)A^*$ where $C \subseteq \Sigma^*$.

The lemma is mainly used in the case where $\varepsilon \notin A$ and the language L_i=$BA^*$is the unique solution.

For each state s_i of the system the equation (11) can be written, considering the sequences starting from all the other states $s_j \neq s_i$ and arriving in the state s_i by only one transition. The set of n equations (11) (where n is the number of system states) allow to obtain all the sublanguages L_i.

Having a system represented by a p-automaton and using this approach we can determine all the events sequences without model exploring.

5.4 *Step 3: sequences probability calculation*

Each events sequence of the system $s = e_{12}e_{23} \ldots e(n-1)n$ that starts from the initial state s_1 and arrives in the state s_n can be extracted from the language L_{syys} otained in the previous step. Using the probability for each transition of the p-automaton obtained in step 1, we propose to use the following equation in order to obtain

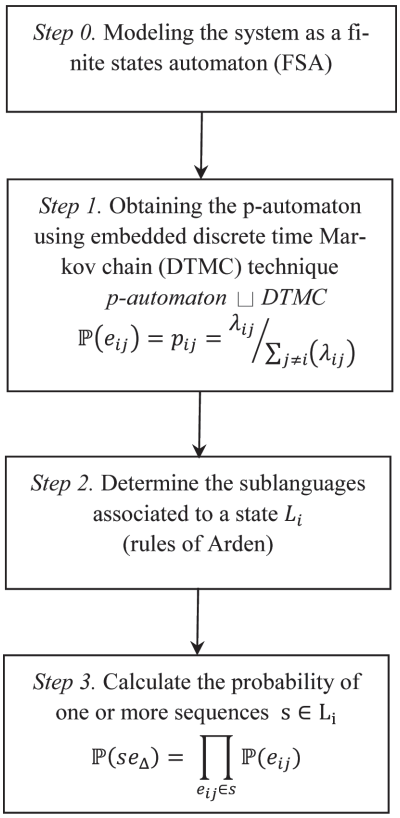


Figure 4. Approach proposed for the probabilistic assessment of events sequences.

the termination probability for the sequence $s = e_{12}e_{23} \ldots e(n-1)n$:

$$\mathbb{P}(se\Delta) = \prod_{e_{ij} \in s} \mathbb{P}(e_{ij}), \forall s \in \sum^{*} \tag{12}$$

The meaning of this equation is that the probability of a events sequence is equal with the product of the probabilities of all of its events e_{ij}.

Figure 4 summerizes the different steps of our proposed approach to formally determine the whole set of events sequences and to assess their probability using the probabilistic languages.

6 APPLICATION ON THE CASE STUDY

6.1 *Application of the proposed approach*

Step 0: Figure 3 shows the embedded Discrete Time Markov Chain representing the p-automaton of the case study.

Step 1: The transition probabilities p_{ij} are calculated using the equation (9).

Step 2: The sublanguages associated to each state represent the sub set of the sequences that lead the system from the initial state 1 to one of his states. Considering each state of the automaton as terminal state (not absorbing) we obtain the next equations:

$$L_1 = L_2e_{21} + L_4e_{41} \tag{13}$$

$$L_2 = L_1e_{12} + L_2e_{22} + L_3e_{32} \tag{14}$$

$$L_3 = L_1e_{13} + L_2e_{23} + L_3e_{33} + L_4e_{43} \tag{15}$$

$$L_4 = L_3e_{34} \tag{16}$$

For example the first equation (13) denote the sublanguage associate to state S_1 as being the all events sequences arriving in this state by only one transition: from state s_2 (all the events sequences previously terminated in s_2:L_2) followed by the transition e_{21} or from state s_4 (all the events sequences previously terminated in s_4:L_4) followed by the transition e_{41} (according to Fig. 3).

Using the Arden lemma, the equations (13–16) give the next expressions for the sublanguages:

- to state 1:

$$\begin{aligned} L_1 = {} & (e_{12} + e_{13}(e_{33} + e_{34}e_{43})^{*}e_{32}) \\ & \times (e_{22} + e_{23}(e_{33} + e_{34}e_{43})^{*}e_{32})^{*}e_{23} \\ & \times (e_{33} + e_{34}e_{43})^{*}e_{34}e_{41} \\ & \times [(e_{12} + e_{13}(e_{33} + e_{34}e_{43})^{*}e_{32})(e_{22} + e_{23} \\ & \times (e_{33} + e_{34}e_{43})^{*}e_{32})^{*}e_{21} \\ & + e_{13}(e_{33} + e_{34}e_{43})^{*}e_{34}e_{41}]^{*} \end{aligned} \tag{17}$$

- to state 2:

$$\begin{aligned} L_2 = {} & L_1(e_{12} + e_{13}(e_{33} + e_{34}e_{43})^{*}e_{32}) \\ & \times (e_{22} + e_{23}(e_{33} + e_{34}e_{43})^{*}e_{32})^{*} \end{aligned} \tag{18}$$

- to state 3:

$$L_3 = (L_1e_{13} + L_2e_{23})(e_{33} + e_{34}e_{43})^{*} \tag{19}$$

- to state 4:

$$L_4 = L_3e_{34} \tag{20}$$

Step 3: Having the sublanguage defined for each state of the considered system we can obtain firstly the probability for a sublanguage and secondly the probabilities for events sequences belonging to this sublanguage. To illustrate the sequence probabilities assessment, the results obtained for two sublanguages (L_1 and L_3) are presented in this paper.

For the simplification we will use the following notations:

$$p_{12} = p; p_{13} = 1 - p; p_{21} = p_1; p_{23} = p_2;$$
$$p_{22} = 1 - p_1 - p_2; p_{32} = p_3; p_{34} = p_4;$$
$$p_{33} = 1 - p_3 - p_4; p_{41} = p_5; p_{43} = 1 - p_5.$$

6.1.1 *Probabilities assessment for the sublanguage L_1*

Using the expression (17) we can calculate the probabilities of different iterations that compose the regular expression of the sublanguage L_1 and, after that, we obtain the final analytic expression:

$$\mathbb{P}(L_1) = \sum_{s \in \Sigma^*} \mathbb{P}(se_\Delta) = \frac{p_2 p_4 p_5}{p_2(p_3 + p_4 p_5) - p_2 p_3} = 1 \tag{21}$$

This result, the probability of the sublanguage $\mathbb{P}(L_1)$, is compliant with the expected one: indeed, for the p-automaton of the Figure 3, the probability of all sequences starting from state 1 and reaching back to state 1 must be obviously equal to one. Nevertheless, the approach is able to provide the probability of all individual sequences reaching to this state. To illustrate this fact, the occurrence probability for some particular sequences, extracted from L_1 and that lead the system in the state 1, are obtained doing the numerical calculus. Their values are presented in Table 1. Firstly we can observe that the sum of probabilities of considered events sequences is approximately equal with 1 and this corresponds to analytical solution of the sublanguage probability (eq. 21). Secondly we can identify the most relevant events sequences (by the greatest values of their probability).

Table 1. Occurrence probabilities for few sequences that lead the system in the state 1.

Sequence (s_i)	Sequence probability ($\mathbb{P}(s_i)$)
$S_1 = e_{12}e_{21}$	0.9213
$S_2 = e_{12}e_{22}e_{21}$	0.0276
$S_3 = e_{12}e_{23}e_{33}e_{32}e_{21}$	4.9961e-06
$S_4 = e_{12}e_{22}e_{23}e_{32}e_{23}e_{32}e_{21}$	4.8080e-10
$S_5 = e_{12}e_{23}e_{34}e_{43}e_{32}e_{21}$	1.8331e-08
$S_6 = e_{12}e_{22}e_{23}e_{33}e_{34}e_{43}e_{32}e_{21}$	2.2602e-11
$S_7 = e_{12}e_{23}e_{34}e_{41}$	1.0233e-04
$S_8 = e_{13}e_{34}e_{41}$	0.0215
$S_9 = e_{13}e_{33}e_{34}e_{41}$	8.8586e-04
$S_{10} = e_{13}e_{34}e_{43}e_{34}e_{41}$	3.2502e-06
$S_{11} = e_{13}e_{32}e_{21}$	0.0256
$S_{12} = e_{13}e_{33}e_{32}e_{22}e_{23}e_{32}e_{21}$	4.1624e-09
	$\mathbb{P}(L_1) = \Sigma_{s_i} \mathbb{P}(s_i) \cong 1$

6.1.1 *Probabilities assessment for the sublanguage L_3*

The sublanguage L_3 describes infinity sequences which bring the system in the failure state 3 from the initial state 1:

$$\mathbb{P}(L_3) = \frac{p_1 + p_2 - pp_1}{p_1(p_3 + p_4 p_5) + p_2 p_4 p_5} \tag{22}$$

Calculating the numerical values for some sequences we obtain the values from Table 2. The state 3 represents the dangerous state because the oven temperature is uncontrolled and thus we can identify the most critical events sequences (with the greatest values of their probability) of the system.

6.2 *Analytic validation of the results*

In order to check the validity of the results (sequences probabilities), we propose the next approach:

1. To determine the stationary distribution of states probabilities for embedded DTMC [π_1 π_2 π_3 π_4] by using the equations:

$$\pi = \pi \cdot M \text{ and } \pi \cdot \overline{1} = 1 \tag{23}$$

   where the vector π represents the state probability distribution, M is the matrix of transitions probabilities and $\overline{1}$ is a vector with all elements 1. Using the equations (23) we determined the analytic form for the state probabilities.
2. To prouve that the probabilities for different sublanguages, obtained by the equations (17–20), the following relation is to be validated:

$$\mathbb{P}(s_i) \cdot \sum_{\substack{s \in \Sigma^* \\ s \\ i \to j}} \mathbb{P}(se_\Delta) = \mathbb{P}(s_i) \cdot \mathbb{P}(L_{i \to j}) = \mathbb{P}(s_j) \tag{24}$$

It means that the probability to reach state S_j is equal to the product of the probability of the

Table 2. Occurrence probabilities for few sequences that lead the system in the state 3.

Sequence (s_i)	Sequence probability ($\mathbb{P}(s_i)$)
$S_1 = e_{12}e_{23}$	2.3744e-04
$S_2 = e_{12}e_{22}e_{21}e_{13}$	0.0014
$S_3 = e_{13}e_{33}$	0.0021
$S_4 = e_{12}e_{22}e_{23}e_{32}e_{23}e_{33}$	3.8620e-11
$S_5 = e_{12}e_{23}e_{33}e_{34}e_{43}$	1.4724e-09
$S_6 = e_{13}e_{33}e_{34}e_{43}e_{32}e_{23}$	4.0899e-11
	$\mathbb{P}(L_3) = \Sigma_{s_i} \mathbb{P}(s_i) \cong 0.0037$

initial state S_i and the probability of the sublanguage from S_i to S_j.

- for L_1: $\pi_i\mathbb{P}(L_1) = \pi_1$
- for L_2: $\pi_i\mathbb{P}(L_2) = \pi_2$
- for L_3: $\pi_i\mathbb{P}(L_3) = \pi_3$
- for L_4: $\pi_i\mathbb{P}(L_4) = \pi_4$

7 CONCLUSIONS

In this paper, we presented the use of the theory of probabilistic language for the assessment of the occurrence probability of events sequences that describe the system evolutions. In order to be able to apply this theory, for a system modelled by a finite state automaton, we proposed a 3 steps approach.

The use of the embedded Discrete Time Markov Chain in a continuous stochastic process for determining the events probability makes assumption that the system is in a stationary state characterizing by stationary distribution probabilities over its states. But the embedded DTMC is not limited to Continuous Time Markov Chain; a DTMC can also be defined from semi-Markov or under some hypothesis from more generally stochastic processes. Another advantage to use the DTMC to obtain the events probability is that the probability of an event is not the same during the system evolution, but can depends on the state where it occurs (in other words the same event can be characterized by different occurrence probabilities). The use of the Arden lemma permits to formally determine the whole set of events sequences, without model exploring. Finally, the probability occurrence for relevant or critical events sequences and for a sublanguage is determined.

The approach is applied on a control system temperature. This case study shows the ability of the proposed approach to take into account together stochastic phenomena characterized by continuous laws of probability (such as failures and reparations processes) and phenomena characterized by discrete laws of probability (such as failures on demand).

This work opens several ways of research in our future activity. First of all, it will be interesting to propose an approach that allows calculating the probabilities of events sequences in a transient system state before reaching the stationary distribution. Secondly, we are interested to apply this approach in more complex systems including components ageing with the more generally underlying stochastic continuous process. Also, an extension of the operations provided by the p-languages theory should be useful for taking in account different types of systems (non-deterministic systems, reconfigurable systems, systems composed of several sub-systems) in dependability studies.

REFERENCES

Bouissou, M. & Bon, J.L. 2003. A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov processes. *Reliability Engineering and System Safety* 82(2): 149–163.

Bouissou, M. 2006. Efficient determination of minimal failure scenario for sequential systems. *15ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2006,* Lille (France).

Carton, O. 2008. *Langages formels, calculabilité et complexité*. Paris: Ed. Vuibert.

Cassandras, C.G. & Lafortune, S. 2008. *Introduction to Discrete Event System,* Second Edition. New-York: Springer.

Chaux, P.Y, Roussel, J.M., Lesage, J.J., Deleuze, G., Bouissou, M. 2013. Towards an unified definition of Minimal Cut Sequences. *4th IFAC Workshop on Dependable Control of Discrete Systems (DCDS 2013)*, York (United Kingdom).

Dutuit, Y. & Rauzy, A. 2005. Approximate estimation of system reliability via fault trees. *Reliability Engineering and System Safety* 87(2): 163–172.

Garg, V.K., Kumar, R. & Marcus, S.I. 1999. A Probabilistic Language Formalism for Stochastic Discrete-Event Systems. *IEEE Trans. on Automatic Control* 44(2): 280–293.

Ibanez-Llano, C., Rauzy A., Melendez E. & Nieto F. 2010. A reduction approach to improve the quantification of linked fault trees through binary decision diagrams. *Reliability Engineering and System Safety* 95(12): 1314–1323.

Papazoglou, I.A. 1998. Mathematical foundations of event trees. *Reliability Engineering and System Safety* 61(3): 169–183.

Perez Castaneda, G.A., Aubry, J.F. & Brinzei, N. 2011. Stochastic hybrid automata model for dynamic reliability assessment. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability* 225(1): 28–41.

Wang, X. & Ray, A. 2004. A language measure for performance evaluation of discrete event supervisory control systems. *Applied Mathematical Modelling* no. 28: 817–833.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

RAM analysis applied to decommissioning phase: Comparison and assessment of different methods to predict future failures

E. Calixto
Genesis Oil and Gas Consultants, UK

Yizhak Bot
BQR Reliability Engineering Ltd., Israel

ABSTRACT: Reliability Engineering methods are applied throughout asset lifecycle, but the greatest challenge is in decommissioning phase, as it requires the equipment degradation after repair and its effects on system operational availability to be considered in order to better predict future equipment performance.

In order to predict future failures and define critical equipment it is necessary to take into account the positive or negative maintenance effect on equipment reliability. Therefore, the Reliability Growth Analysis (RGA) applied to a repairable system can be performed to predict the cumulative number of failures, considering the degradation effect of repairable equipment.

Despite RGA being the best approach, in some cases it is necessary to consider the system configuration modelling RBD (Reliability Block Diagram) and perform a direct simulation to predict system operational availability and expected number of future failures. Therefore, the General Renewal Model is required to define the restoration factor of each equipment item in order to take into account the degradation effect on equipment performance and apply these factors to RBD configuration in order to predict the system operational availability and future expected number of failures with respect to the degradation effect. The restoration factor is minted to give values between zero and one. In other words, a restoration level between "as bad as old" and "as good as new". The RGA model deems the restoration levels as "as bad as old" and "as good as new" and "better than as good as new". Therefore, the proposal methodology predicts the restoration factor from the RGA model, based on a likelihood method. In addition, the expected number of future failures is determined by comparing the prediction results from RGA model (Crown AMSAA Model) and direct simulation which considers the restoration factor.

The main objective of this paper is to present these particular reliability engineering methods and demonstrate the application on an asset case study in decommissioning phase. The simulation for cumulative time as well as a specific period of four months was carried out in order to predict the effect of critical failures on system operational availability during a specific range of time.

1 INTRODUCTION

The RAM analysis is a recognized management and engineering discipline for the purpose of guaranteeing the specified functionality of a system over its complete lifecycle. RAM analysis also aims to ensure the operation, maintenance and disposal costs remain below the acceptable level, by establishing the relevant performance characteristics at the beginning of the procurement cycle, and through monitoring and control of their implementation throughout all asset life cycle phases (Vozella, 2006).

The general definition of reliability used throughout industry and quoted in many engineering books published on this subject follows the example as taken from MIL-STD-785:

Reliability: the ability of an product to perform a required function under given conditions for a given time interval.

Availability: ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

Maintainability: a state in which an item can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.

Despite the RAM analysis being the most common method utilized by reliability engineers, most of time the degradation caused by equipment age and maintenance effects is not taken into account. In many cases, the reliability data are obtained from

a generic database concerning constant failure rate, and the equipment failure-rate data obtained are treated as an average (Gerbec, M. et al. 2010).

The null hypothesis of the HPP (Homogeneous Poisson Process) with the alternative being a NHPP (NonHomogeneous Poisson Process) is defined by a trend test such as the Laplace Test or the Military Handbook test (Lindqvist, et al. 2006).

The degradation effect must be taken into account to represent the increasing number of asset failures during asset wear out. Whenever this type of degradation is not represented by "Direct simulation", the equipment is considered as good as new after repair.

The RAM analysis performed concerning decommissioning phase must take into account the degradation effect in order to predict the future failures of the assets.

Indeed, nowadays many RAM analyses use data from generic databases (exponential PDF) that in most of cases will not represent the real performance of the system assessed. In addition, these databases do not consider the restoration factor or the different PDFs (probability density functions) which are more applicable to failure modes in the analysis.

This paper will discuss the importance of considering the restoration factor by comparing the reliability growth analysis (Crow AMSSA Model) and General Renewal Model when performing a RAM analysis to predict system performance by applying a case study concerning decommissioning phase.

2 RAM ANALYSIS IN DECOMMISSIONING PHASE

In order to understand the application of RAM analysis in asset decommissioning phase it is necessary to first understand the asset management concept, as well as how reliability engineering is applied during asset lifecycle.

Asset Management is defined as the best practices applied during asset lifecycle in order to achieve the best performance result. Indeed, such practices are carried out with support of a leader at different organizational levels, specifically strategic, tactical and operational.

Therefore, different reliability engineering methods must be used in different asset lifecycle phases, as shown in Figure 1. The optimal asset performance is achieved when most early life failures are eliminated during design phase, which enables excellent performance during operational phase. This is shown by the green bathtub curve in Figure 1, representing a lower failure rate, or in other words, higher reliability.

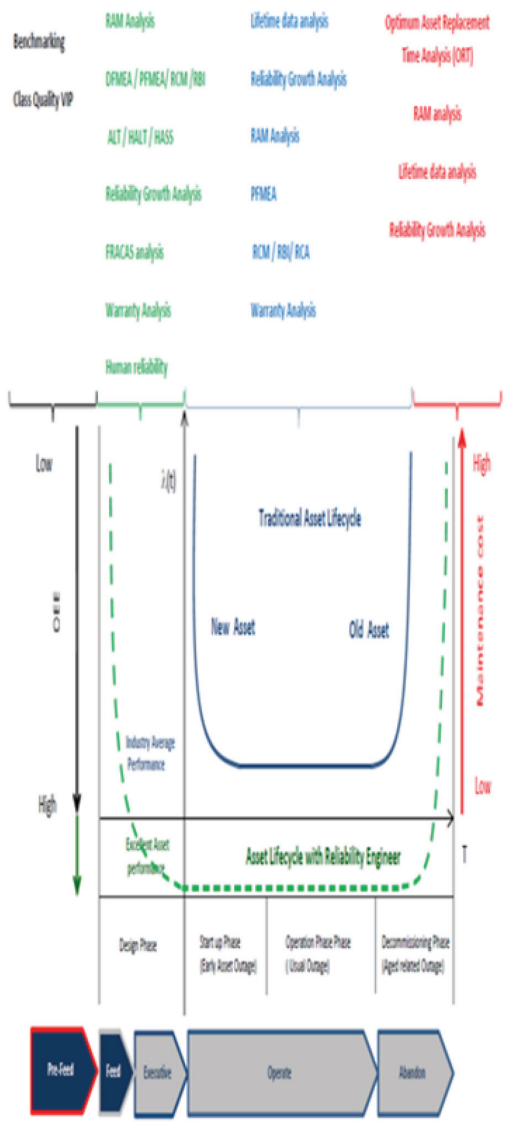


Figure 1. Asset Management Source: Calixto, E. 2014.

In order to achieve optimal performance, it is necessary to implement different methods throughout asset lifecycle. Indeed, all efforts begin in design phase, applying different qualitative (DFMEA, RCM, RBI, HALT, FRACAS, human reliability) and quantitative (RAM, ALT, Reliability Growth analysis and warranty analysis) methods. The main objective of these methods is to identify the early-life failure during design and eliminate them whenever it is possible. During operational phase, different qualitative (PFMEA,

RCM, RBI) and quantitative (Lifetime data analysis and RAM analysis) methods must be utilized to maintain asset performance until the end of asset life, when decommissioning of the equipment is defined and supported by RAM analysis, ORT (Optimum Replacement Time) and Reliability Growth analysis.

The Optimum replacement time for all equipment must be analyzed in order to reduce operational cost, maintain high availability of the system and below the acceptable risk level for failure.

The decommissioning phase is the most challenging in terms of RAM analysis because it requires different analyses to be performed, such as Reliability Growth Analysis, General Renewal Model and the usual Lifetime data analysis during the lifetime data analysis step in order to predict the future system performance.

In addition, in some cases, it is also important to carry out the Optimum Replacement Time analysis in order to define when it is best to replace equipment based on operational cost analysis.

In general terms, the RAM analysis methodology applied for decommissioning phase can be defined by the following steps represented in Figure 2.

Regarding decommissioning phase, it is very important to take into account the equipment age in order to predict future failures that will reduce system performance in decommissioning phase. Therefore, it is important to perform the Reliability Growth Analysis (RGA) using the Crow AMSAA method, as well as performing the General Renewal Model in order to accurately predict the expected number of future failures.

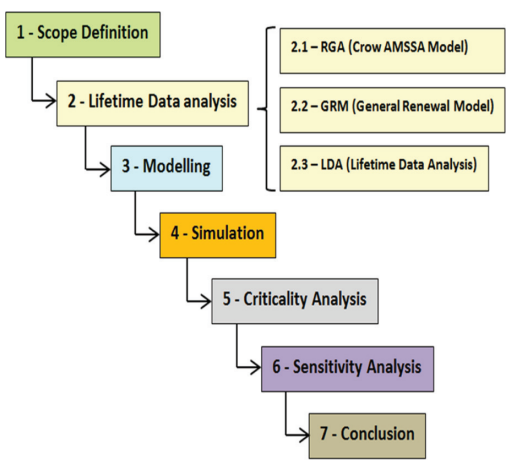


Figure 2. RAM Methodology in decommissioning phase.

Indeed, these methods are applied for single equipment and components but it is a very important result for comparison with the Monte Carlo (MC) Simulation result from RAM analysis. In fact, the best approach is to carry out RGA analysis and then adjust the MC simulation for each equipment item.

Despite a good approach, the software packages which perform system direct simulation (Monte Carlo simulation) have some limitations and are not able to predict the exact expected number of failures predicted by RGA. Indeed, it is possible to take into account the restoration factor predicted by the General Renewal Model, but it is only possible to have equipment in the state "as good as new" or "as bad as old".

Theoretically, this is the best condition that some equipment can achieve in terms of performance after preventive or corrective maintenance, but in some cases it is possible to have reliability growth. This is achieved by swapping internal components for more reliable ones or even modifications which increase equipment reliability when performed.

3 RELIABILITY GROWTH ANALYSIS

The Crow AMSAA model was introduced by Dr.Larry H. Crow in 1974 in order to be applied to product improvement assessment during design phase. Nowadays, this model is also applied during the operational phase of asset life cycle to assess the equipment degradation over time, as well as the effect of maintenance on repairable equipment in order to predict future failures.

The Crow AMSSA is a statistical model which uses the Weibull failure rate function to describe the relationship between accumulated time to failure and test time, being a Non-Homogeneous Poisson Process Model. This approach is applied in order to demonstrate the effect of corrective and preventive actions on reliability when a product is being developed or for repairable systems during operation phase (Crow, 2012). Thus, whenever improvement is implemented during test (Test-Fix-Test) or maintenance, the Crow AMSAA model is appropriated to predict reliability growth and expected cumulative number of failures. The expected cumulative number of failures is mathematically represented by the following equation:

That is approximately:

$$E(N_i) = \int_o^T \rho(t)dt \quad (1)$$

$$E(N) = \lambda T^{\beta} \quad (2)$$

The Crow AMSAA Model assumes that intensity failure is approximately Weibull failure rate, thus intensity of failure on time is:

$$\rho(t) = \frac{\beta}{\eta^{\beta}} T^{\beta-1}$$

where initial failure rate as:

$$\lambda = \frac{1}{\eta^{\beta}}$$

If cumulative failure rate is approximately failure intensity we have:

$$\lambda_i = \beta\lambda T^{\beta-1}$$

The equation above describes failure intensity during the test and depends on the β value increasing, decreasing or staying constant through time. It's very important to bear in mind that β in the Crow AMSAA Model describes intensity failure behavior and does not have same meaning as the Weibull PDF shape parameter.

An example of an application of this methodology is demonstrated in Figure 3, which shows the cumulative number of failures over time for different compressors.

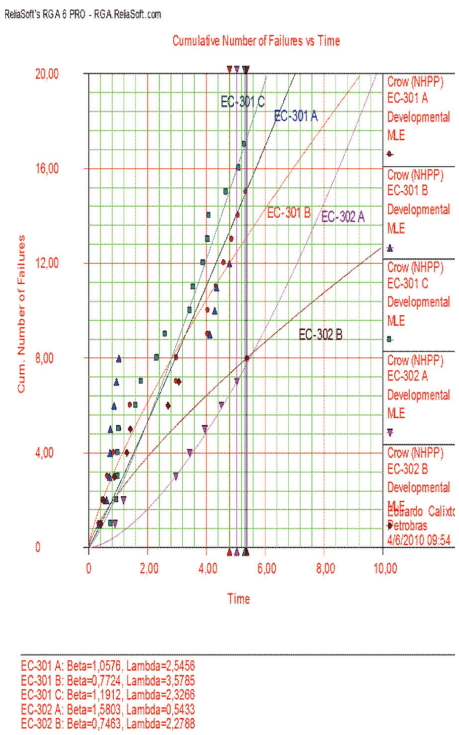


Figure 3. Reliability Growth Analysis. Source: Calixto E, 2011.

In Figure 3, for each compressor, there are different β and λ values, which describe the effect of improvement actions as well as the cumulative failure rate.

In fact, β is a shape parameter of Intensity Failure Function in the Crow AMSAA Model. Thus, in this model when $\beta > 1$, reliability decreases through time because failure intensity is increasing. In other words, corrective product actions are not improving the product. When $\beta < 1$, intensity of failure decreases through time; in other words, reliability is increasing. Therefore, corrective product actions are improving product reliability. When $\beta = 1$, there's no improvement or product reliability degradation. In this case, the product behaves as if no corrective action takes place and intensity failure is constant through time. The Growth rate in the Crow AMSAA Model is $1-\beta$.

The Crow AMSSA model is the best model to predict future failures and analyse the effect of maintenance and operational environment on equipment performance. Indeed, Power Law processes (Crow AMSAA Model) are often sufficient for simple reliability studies, but in the case of complex system, there is a need for more complex model (Verrier, V. et al. 2010).

Indeed, it is not possible to use the Crow AMSAA model to predict the expected number of future failures for different equipment in complex configurations. In this case, it is necessary to represent complex systems with an RBD model.

Once the system is represented by RBD and the direct simulation is performed to predict the expected number of future failures, it is necessary to take into account the degradation factor that will be explained in the next section.

4 GENERAL RENEWAL PROCESS

The General Renewal Model (Kijima I and II) was proposed by Kijima and Sumita in 1986. The Kijima Model, known as "General Renovation Process" or "General Renewal Process", is based on component virtual life concept. This method considers the reduction in component age when an intervention is performed; it can be described in two forms:

⇒Age re-establishment based in last intervention (Kijima I);

⇒Age re-establishment based in all intervention (Kijima II);

In first case, the "Model Kijima I" assumes that reestablishment of component age occurs only for the last repair. Therefore, the model assumes that the "ith" repair does not remove all reliability

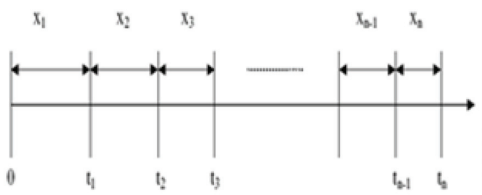


Figure 4. General renewal model.

losses until the "ith" failure. Therefore, if "t_i" is time between failures, the component age through time is represented by equation:

$$V_n = V_{n-1} + qX_n \quad (3)$$

where,

X_n = time between (n – 1)th and a nth failure
q^n = restoration factor
V_n = age in time n
V_{n-1} = age in time n–1.

In the second case, the Model Kijima II assumes that re-establishment of component age occurs for all failures throughout component life since the first repair. Thus, this model regards that the "ith" repair remove all reliability losses until "ith" failure. Therefore, the component age through time is represented by equation:

$$V_n = q\left(V_n + X_n\right) \quad (4)$$

Figure 4 graphically represents the concept of the General Renewal Model that takes into account the effect of maintenance. The Kijima factor applied in the case study was defined using the software "Weibull 9.0" based on the likelihood method applied in Crown AMSSA Model parameters.

5 LIFETIME DATA ANALYSIS

In order to define equipment, product and services reliability it is necessary to collect historical failure data and treat them statistically.

Therefore, the first step in a lifetime data analysis study is to know how failures occur through time; this is critical for definition of indexes such as failure rate, reliability, availability, reliability through time, in order to support decisions in defining best time to inspection), and maintenance, to check if equipment achieves reliability warranty requirement and to support information to new projects.

Indeed, the decisions based on reliability are based on lifetime data analysis results. This analysis requires historical data about failure modes and repair time. The failure mode is the way that the equipment or product lost part or total capacity to carry out their function.

Therefore, understanding the type of data required is the first step in the lifetime data analysis process. Essentially, the type of data sample can be grouped or not grouped, meaning that reliability is predicted based on only one equipment item or based on a group of similar equipment. In most cases, when equipment from a process plant is being assessed, the sample is not grouped because, when comparing the equipment to the sample from a similar process plant, factors such as maintenance policy, operational environment and process variation affect equipment reliability differently.

Regarding the data, it is important to understand how data are recorded. Indeed, the data can be complete, right suspension, left suspension, in interval, or a combination of such configurations.

The next step is to apply different goodness of fit methods, such as Rank regression and Maximum Likelihood, to estimate the PDF parameters as well as the best PDF which fits the data assessed.

The final product of lifetime data analysis is the PDF and its parameters that best fit the failure or repair data assessed, as shown in Figure 5.

The Probability Density Function (PDF) describes the possibility of events occurring

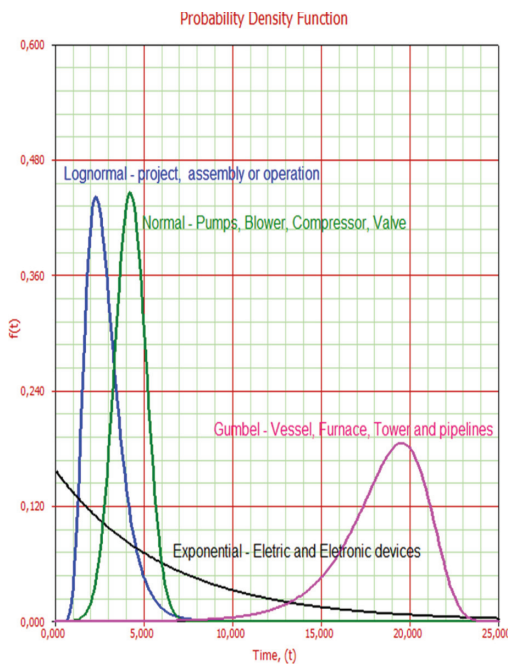


Figure 5. Oil and Gas equipment PDF. Source: Calixto E, 2012.

through time. In equipment life cycle analysis, it describes failure or repair time occurrence through time. This provides good information to a maintenance and reliability professional to make decisions regarding maintenance policy, inspection policy and failure behavior. However, in order to make these decisions, other indexes are required, such as failure rate and reliability function. Figure 6 summarizes the main steps of lifetime data analysis.

Despite a very important method, the lifetime data analysis does not consider the effect of maintenance on equipment degradation. In fact, when applying the PDF parameters to RBD models and then running the direct simulation in RAM analysis, the following events will be similar to the first one.

Therefore, it is important to take into account the degradation effect analysis which is defined by applying the General Renewal Model and Crow AMSSA model, as will be demonstrated in the next section.

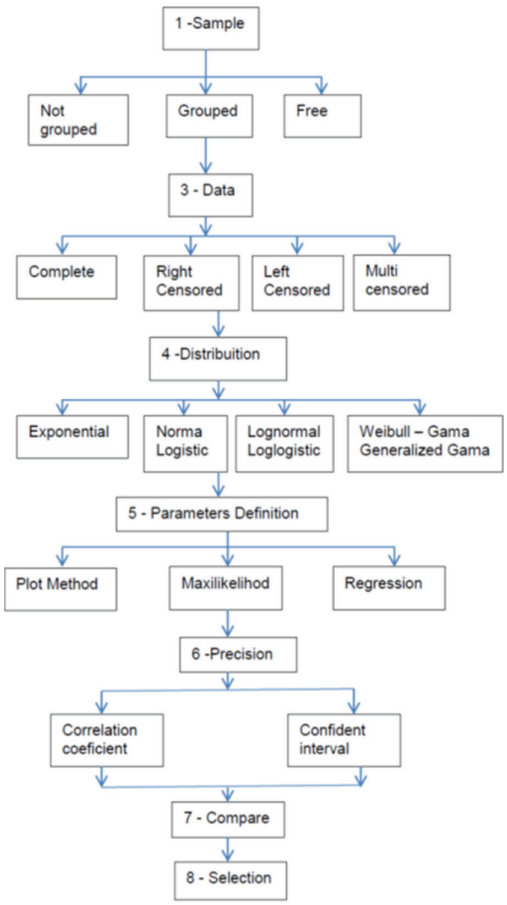


Figure 6. Lifetime data analysis steps.

6 COMPARING DIFFERENT METHODS

In order to predict future failures, it is necessary to take into account the positive or negative maintenance and environment effect on equipment reliability. Therefore, the Reliability Growth Analysis (RGA) can be performed to predict the cumulative number of failures regarding the degradation effect on repairable equipment. The second option is to perform the General Renewal Method to predict the restoration factor and apply it to the RBD for each equipment item or failure mode and run the direct simulation.

In the first case, in order to predict future failures, the Reliability Growth Analysis (Crow AMSSA Model) is applied to define the improvement or degradation in each equipment item as well as taking into account the effect of corrective and preventive maintenance.

This analysis is the most accurate in predicting future failures because it considers all positive or negative effects on equipment performance.

Certainly, the ideal situation is performing this analysis for each component, but due to a lack of precise information in the historical data archive, the analysis is carried out at the equipment level. Figure 7 shows an example of an RGA carried out for a blower.

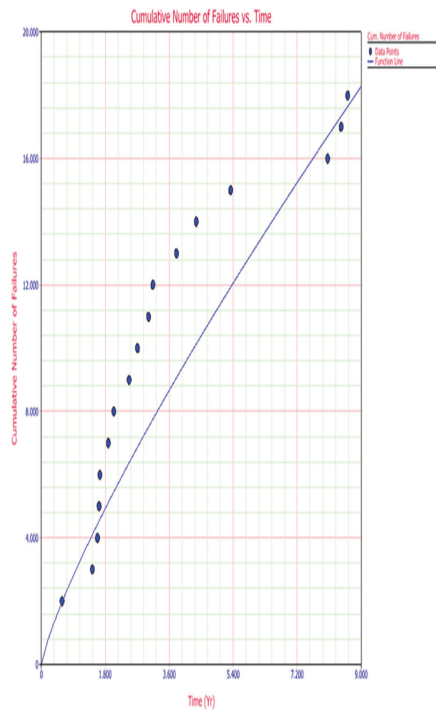


Figure 7. RGA analysis.

The cumulative number of failures during the assessed period is exactly what it is recorded on the database. In addition, the beta parameter, $\beta>1$, indicates that reliability of this Blower decreases over time ($\beta = 1.74$).

Similar analyses were carried out for other equipment in order to define the cumulative number of failures, as well as to evaluate the effect of maintenance and operational environment by assessing the beta parameter value.

Regarding the second option, the General Renewal Model which defines the type of restoration factor (Kijima I or II) can also be applied. Indeed, this analysis might be adjusted to achieve similar results provided by RGA analysis in terms of cumulative number of failures. Considering that the restoration factor is on the maximum, 1 (100% of restoration), some adjustment is necessary when adjusting the GRM based on RGA results. This adjustment is based on the assumption that the RGA represents the best prediction of future failures. Once the equipment needs to be assessed in the context of a system and not individually, it is necessary to define the PDF and restoration factor for each one and then input the values into the RBD model.

Table 1 shows an example of the final reliability data as result of the RGA, GRM an LDA analyses.

The final step is to validate the reliability database presented in Table 1 by performing individual Direct Simulations (Monte Carlo—MC) in order to check if the PDF and restoration factor were adjusted well to the RGA model prediction. Therefore, the simulation was performed for 10, 15 and 20 years. Table 2 shows an example of future predictions for some equipment, comparing the RGA and MC methods result.

Tank 1 was assessed only through the MC method because the small number of failures does not enable the RGA analysis. The pumps were assessed by both methods and achieve a similar expected number of failures.

Finally, this approach was applied to all Boiler systems. Thus, it was demonstrated that the PDF and restoration factor were accurate enough to predict future number of failures by the MC method, as the RGA method produced similar results. The next section demonstrates the Boiler system modelled by RBD (reliability diagram block) and the final direct simulation results.

7 RAM ANALYSIS IN DECOMMISSIONING PHASE CASE STUDY

In order to demonstrate the importance of all methods described in previous section, the RAM analysis performed to assess the Boiler system in decommissioning phase will be carried out. The main objective is to define the critical equipment in terms of performance and support decision about which one must to be taken place for a new one.

In this particular case, the boiler system may cause loss of production in the whole refinery in case of outage during winter time. Therefore the RAM analysis took into account the simulation for a specific range of time that in this case is winter time.

Table 1. Reliability data base.

Equipment	Failure				Repair			Kijima factor			Crow AMSSA model	
Tank 1	PDF 2	Parameter (year)			PDF	Parameter (hours)		Type	q	RF	λ	β
	Gumbel	μ	σ		Normal	μ	σ					
		7.48	0.01			120	20					
Pump 2	PDF 2	Parameter (year)			PDF	Parameter (hours)		Type	q	RF	λ	β
	Weibull	β	η	γ	Constant	Repair time						
		0.56	0.695	0.052		24		II	0	1	6.1044	1.0655
Pump 3	PDF 2	Parameter (year)			PDF	Parameter (hours)		Type	q	RF	λ	β
	Weibull	β	η	γ	Constant	Repair time						
		0.47	0.46	1.35		24		I	0	1	0.6777	0.583
Pump 4	PDF 2	Parameter (year)			PDF	Parameter (hours)		Type	q	RF	λ	β
	Weibull	β	η		Constant	Repair time						
		0.7285	0.564			24		II	0	1	0.6522	1.6522
Pump 5	PDF 2	Parameter (year)			PDF	Parameter (hours)		Type	q	RF	λ	β
	Weibull	β	η		Constant	Repair time						
		0.6363	0.8888			24		I	0	1	1.4076	0.5716

Table 2. RGA × MC.

Equipment	10 years		15 years		20 years	
Tank 1	MC	RGA	MC	RGA	MC	RGA
	1		1.99		2	
Pump 2	MC	RGA	MC	RGA	MC	RGA
	9.7	8.89	14.09	10.98	18.3	12.76
Pump 3	MC	RGA	MC	RGA	MC	RGA
	4.24	3.15	6.44	4.28	8.56	5.28
Pump 4	MC	RGA	MC	RGA	MC	RGA
	15.37	12.88	22.6	19.3	29.91	25.27
Pump 5	MC	RGA	MC	RGA	MC	RGA
	9.06	8.87	13.23	12.13	17.42	15.24

In addition, the LDA, RGA and GRM are part of "RAM model in decommissioning phase" as shown in Figure 2 and such accuracy was demonstrated on Figure 7, Table 1 and 2.

Once the lifetime data analysis step is complete the following step is to Model the RDB and perform the direct simulation.

Figure 8 shows the Boiler System RDB (RDB BQR software) which basically has two subsystem that are Hot Water Boiler and Hot Water Distribution.

The Hot Water Boiler subsystem is represented by the RBD (RDB-BQR software) in Figure 9. In this case, all equipment has standby configuration that enable a high operational availability. Despite high operational availability, the operational cost is high due to number of failures in such equipment.

Figure 10 shows the Hot Water Distribution Subsystem RBD (RDB BQR software) which has the pipes 1, 7 and 8 as the most critical in terms of boiler system unavailability.

After modeling the system the next step is to carry out the direct simulation (MC-Monte Carlo). In this particular case, for the cumulative time of 8 years the boiler has 97.48% of operational availability. The most critical equipment are the pipes 1, 7 and 8 because are those which presents the lower operational availability that is 97%, 97,1% and 97.4% respectively.

Based on simulation result, the future loss of production was predicted based on failure on critical pipes (1,7 and 8). The simulation to predict future loss of production regarded that once the pipes fails during the winter such pipes will be out until the end of the winter. That is a worse scenario as shows picture 11. From the top t the bottom, the first red line represents the pipe 1 shutdown during the winter time. The second red line show the impact of such failure in the boiler system that will be unavailable during the winter once the pipe 1 shutdown.

Based on Boiler system direct simulation, was recommended to take place those critical pipes

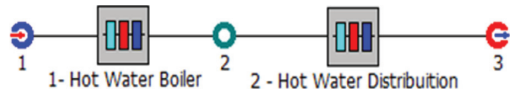


Figure 8. Boiler system.

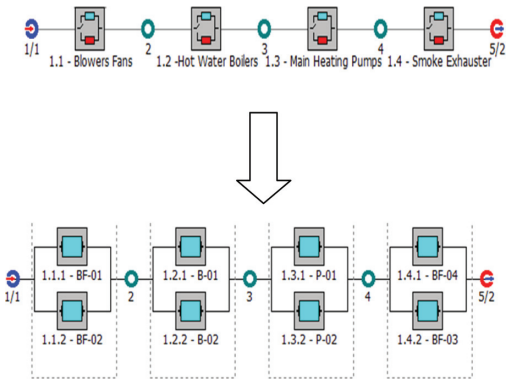


Figure 9. Hot water boiler subsystem.

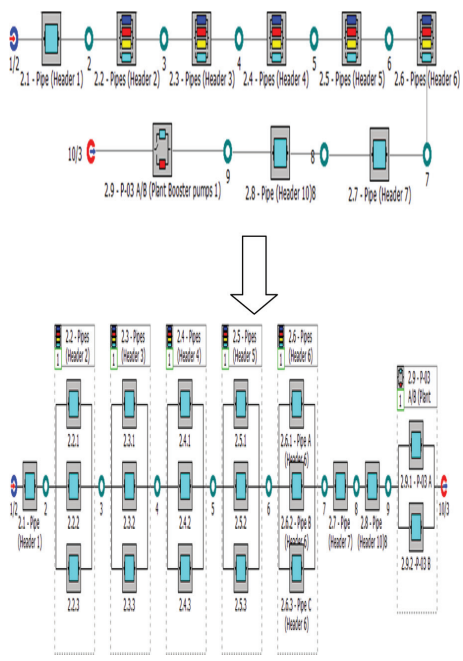


Figure 10. Hot water distribution subsystem.

because based on direct simulation prediction the chance to have such pipe failure during the winter time is 60%. Such probability regards all type of failures on pipes. In case of corrosion, the probability reduces for 10%.

The sensitivity case regarding new subsystems was carried out and in this case the operational availability will achieve 99.92% of operational availability for the next five years if the Hot Water Boiler remains the same and a new Hot Water Boiler will take place. Whether all system be replaced for a new one the operational availability will be 100% in the next 5 years.

The important aspect related decision in decommissioning phase is the Optimum Replace time assessment that defines when each equipment item must be replaced due to the increase operational cost. Regarding this analysis, the boilers must be replaced at 2.34 years because despite not cause impact on system operational availability due to standby configuration the operational cost increase on time as shows the Figure 12.

Similar OPT assessment was carry out for other equipment of Hot Water Boiler in order to define which one must to be replaced for the new one due to increasing operational cost. In this particular case, because of redundancy configuration the equipment has no impact on Hot Water Boiler operational availability but have high operational cost related to failures.

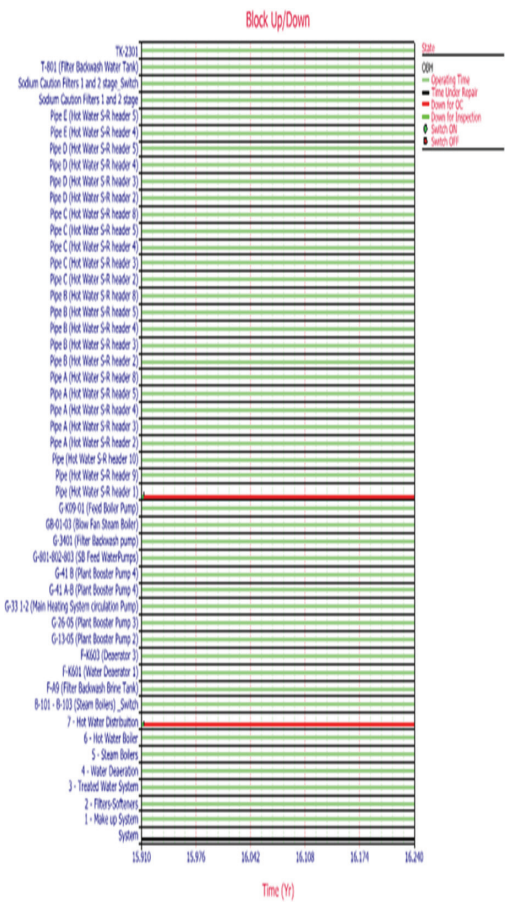


Figure 11. Loss of production during winter.

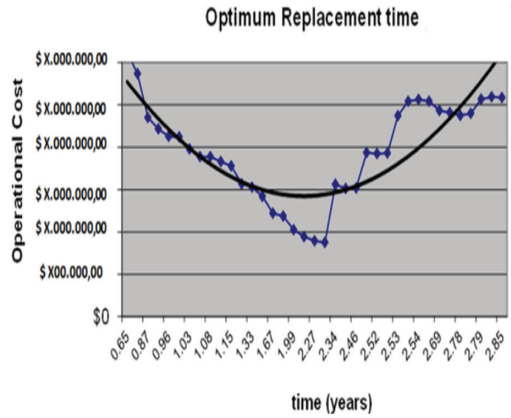


Figure 12. Optimum replace time—water boiler.

8 CONCLUSION

The main objective of this paper was to demonstrate the importance of RAM analysis to support decisions regarding asset improvement during decommissioning phase.

In addition, the paper has demonstrated the importance of restoration factors in predicting the future failures of assets that require additional models such as the General Renewal Model and Crow AMSSA model.

The Direct Simulation (MC-Monte Carlo) and CROW AMSAA model were compared and demonstrated to achieve similar results related to equipment future failure prediction. It is important to highlight that it is only possible when is regarded the restoration factor in Direct Simulation and the PDF as well as Restoration factor are adjusted to predict the similar number of failure obtained on the Crow AMSSA method.

In this particular case study, the simulation during a specific range of time (winter) allows prediction of the loss of production. These model characteristics are not present in all software packages, but must be considered as an opportunity to improve, in order to enable simulations for a specific period of time.

The Decommissioning phase is critical in the asset lifecycle and an accurate decision about which equipment must or must not be replaced should be supported by the best Reliability Engineering methods.

The Optimum Replace Time method is not applied in many cases and must be considered in decommissioning phase for all equipment, even for those that do not have a direct impact on system availability in of the event of failure. In many cases the operational cost increases with time, making the asset inefficient from an economic point of view.

REFERENCES

Bayer Technology Services Asset Life Cycle Management. www.bayertechnology.com.

Calixto, E.,.2012. Gas and Oil relibility Engineer: Modeling and Analysis. Elsevier ISBN: 9780123919144.

Calixto, E., 2014. Safety Sciencer: Methods to prevent incident and health damageson workplace. Bethamscience. (Release in July 2014). http://www.benthamscience.com/ebooks/forthcomingtitles.htm.

Gerbec, M., 2010. Case study: Reliability analysis of natural-gas pressure-regulating installation. Taylor & Francis Group, London, ISBN 978-0-415-60427-7.

Lindqvist, B.H., 2006. On the statistical modeling and analysis of repairable system, *Statistical Science*, 21, 532–551.

O'connor P.D.T., 2010. Practical Reliability Engineering. Fourth Edition. John Wiley & Sons Ltd.

Pallerosi, A.C., 2007. Confiabilidade, A quarta dimensão da qualidade. Conceitos básicos e métodos de cálculo. Reliasoft, Brasil.

Tobias, P.A., Trindade D.C., 2012. Applied Reliability. Third Edition. CRC Press.

Yang, G., 2007. Life Cycle Reliability Engineering. John Wiley & Sons Ltd.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability indices computation for a flow network with a series-parallel-reducible structure

J. Malinowski
Systems Research Institute, Polish Academy of Sciences, Poland
Warsaw School of Information Technology, Poland

ABSTRACT: A flow network with multiple inflow and outflow points, and a series-parallel-reducible structure is considered. It is composed of independent components with constant failure and repair rates. The author has defined indices that characterize the dynamically changing throughput between inflow points and a given internal point. He has also constructed an algorithm to compute these indices. The algorithm is based on the stepwise aggregation of the network structure, it operates on integer numbers, and has relatively low numerical complexity. A crucial role in the computations is played by the notions of c-importance of components and c-availability at network junctions, introduced by the author. The presented results can be applied in the reliability analysis of various types of flow networks, e.g. water supply systems, gas and/or oil pipelines, power transmission and/or distribution networks, etc.

1 INTRODUCTION

The current paper is a continuation of Malinowski (2013), where a series-parallel-reducible system characterized by its capacity defined as a function of component capacities was considered. Its subject is a flow network via which a commodity (water, gas, electric power, etc.) is delivered from inflow to outflow points. The paper can be classified as a contribution to the field of reliability of flow networks regarded as multi-state repairable systems. Multi-state systems with binary or multi-state components have been studied with increasing interest during the recent decades. A broad overview of multi-state reliability models and methods used for their analysis, along with the comprehensive survey of relevant literature can be found in Lisnianski et al. (2010) and Lisnianski & Levitin (2003). Methods of computing failure/repair frequencies, intensities, and availabilities of multi-state systems are investigated in Chang et al. (2004), Druault-Vicard & Tanguy (2006), and Korczak (2007). As far as series-parallel flow networks are concerned, the literature on this subject is rather scarce, however some interesting results, related to the topic of this paper, can be found in Klinz & Woeginger (2004) and Krumke & Zeck (2013).

A network investigated in the current paper has the following characteristics:

1. It is composed of two-state independent components: inflow nodes, transit nodes, outflow nodes, and directed links.
2. It has a series-parallel-reducible structure that can be reduced to a single component by stepwise series-parallel aggregation.
3. To the inflow nodes only outbound links are connected, to the transit nodes—both inbound and outbound links, a node to which only inbound links are connected is called terminal. An outflow node can be either a transit or a terminal one.
4. Each component has certain throughput. The throughput of a non-terminal node is the sum of its outlets' throughputs. One of the outlets of an outflow node supplies a commodity to the customer. An operable component has non-zero integer throughput, a failed one has zero throughput.
5. When a component fails its repair is started immediately. The time-to-failure and time-to-repair of each component are independent, exponentially distributed random variables.
6. The network state is defined w.r.t. a given point, as the effective throughput between this point and all the preceding inflow nodes, i.e. the residual throughput after all the outflow nodes preceding this point are supplied. This state is an integer-valued function of the throughputs and demands of individual components, determined by the system structure. It will be defined later in the paper.
7. The network is operable at an outflow node if the network state at the point just before this node is greater or equal to the node's demand.

In Fig. 1 the Reliability Block Diagram (RBD) of a small exemplary network is presented; e_1 and e_6

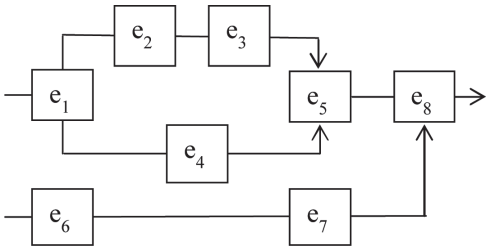


Figure 1. The RBD of a small exemplary network.

are inflow nodes, e_2, e_3, e_4, e_7—outflow nodes, and e_5, e_8—transit nodes. This network is a fragment of a bigger one, as it extends beyond e_8 which is a transit node. For simplicity, pipes are considered failure-free; otherwise, additional boxes should be inserted between the existing ones.

The above described systems can be used as reliability models of various types of flow networks with series-parallel-reducible structures. Systems of this kind are usually considered functional if the effective throughputs at given points are greater or equal to certain threshold values. Their reliability analysis is thus based on parameters related to the time-points in which theses values are reached from above or below during the system operation.

We will consider three such parameters, namely the c-availability and the two c-intensities. They correspond to analogous characteristics for two-state systems. The first parameter, denoted $A(c,t,z)$, is the probability that at time t the network state at a point z is greater or equal to c. The remaining two, denoted $\Lambda^+(c,t,z)$ and $\Lambda^-(c,t,z)$, are the intensities with which the network state crosses the level c from below or above respectively. They will be referred to as transition intensities, where a transition takes place between the states "$\geq c$" and "$<c$". It will be shown how to compute asymptotic ($t\to\infty$) values of these parameters, and how several other frequently used reliability parameters of repairable systems can be derived from the asymptotic intensities. The presented method is illustrated by the calculation of $A(c,t,z)$ for the exemplary network.

2 DETAILED ASSUMPTIONS AND NOTATION

2.1 *Regarding individual components*

e_i—the i-th component of the network; i∈ S, where S is the index set of the components set.

c_i—the throughput of the operable e_i; an integer number.

x_i—the state of e_i; $x_i = c_i$ or $x_i = 0$ depending whether e_i is operable or failed.

$\underline{x}$—the vector of x_i, i∈ S, i.e. $\underline{x} = [x_i, i\in S]$.

$X_i(t)$—the (random) state of e_i at time t.

$\underline{X}(t)$—the (random) vector of the components' states at time t, i.e. $\underline{X}(t) = [X_i(t), i\in S]$.

λ_i, μ_i—the failure or repair intensity of e_i, i.e.

$$\lambda_i = \lim_{u\to 0} \Pr[X_i(t+u) = 0 \mid X_i(t) = c_i]/u,$$
$$\mu_i = \lim_{u\to 0} \Pr[X_i(t+u) = c_i \mid X_i(t) = 0]/u \qquad (1)$$

It is assumed that both intensities are constant, i.e. they do not depend on t. Clearly, this occurs if the time-to-failure and time-to-repair of e_i are exponentially distributed.

$p_i(t)$, $q_i(t)$—the probability of e_i being operable or failed at time t, i.e.

$$p_i(t) = \Pr[X_i(t) = c_i],$$
$$q_i(t) = \Pr[X_i(t) = 0] = 1 - p_i(t) \qquad (2)$$

As shown in Barlow & Proschan (1975), the above probabilities are related to the failure/repair intensities of e_i in the following way:

$$p_i(t) = \frac{\mu_i}{\lambda_i+\mu_i} + \frac{\lambda_i}{\lambda_i+\mu_i}\exp[-(\lambda_i+\mu_i)t],$$
$$q_i(t) = \frac{\lambda_i}{\lambda_i+\mu_i} + \frac{\lambda_i}{\lambda_i+\mu_i}\exp[-(\lambda_i+\mu_i)t] \qquad (3)$$

$A_i(c,t)$—the c-availability of e_i at time t, i.e.

$$A_i(c,t) = \Pr[X_i(t)\geq c] = \begin{cases} 1, & c\leq 0 \\ p_i(t), & 0 < c \leq c_i \\ 0, & c > c_i \end{cases} \qquad (4)$$

2.2 *Regarding a two-state general system*

$\Phi(\underline{x})$—a binary function expressing the system state in relation to the states of its components; $\Phi(\underline{x}) = 1$ or $\Phi(\underline{x}) = 0$ depending whether the system is operable or failed.

A system is called coherent if Φ is non-decreasing, and each component is relevant. See Barlow & Proschan (1975) for details.

$Y(t)$—the system state at time t, i.e. $Y(t) = \Phi(\underline{X}(t))$.

$I_i^B(t)$—the Birnbaum importance of e_i at time t, defined as follows:

$$I_i^B(t) = \frac{\partial \Pr[Y(t)=1]}{\partial p_i(t)} = \Pr[Y(t)=1 \mid X_i(t)=c_i] - \Pr[Y(t)=1 \mid X_i(t)=0] \qquad (5)$$

$I_i^B(t)$ can be interpreted as the probability that the failure of e_i results in the system failure.

$A(t)$, $U(t)$—the system availability or unavailability at time t, i.e.

$$A(t) = E[Y(t)] = \Pr[Y(t) = 1],$$
$$U(t) = 1 - E[Y(t)] = \Pr[Y(t) = 0] \quad (6)$$

$N_{0,1}(s,t)$, $N_{1,0}(s,t)$—the (random) number of times the system is repaired or fails in time interval (s,t).

$V(t)$, $W(t)$—the instantaneous system repair or failure frequency at time t, i.e.

$$V(t) = \lim_{u\to 0} E[N_{0,1}(t,t+u)]/u,$$
$$W(t) = \lim_{u\to 0} E[N_{1,0}(t,t+u)]/u \quad (7)$$

$\Lambda_{0,1}(t)$, $\Lambda_{1,0}(t)$—the system repair or failure intensity at time t, i.e.

$$\wedge_{0,1}(t) = \lim_{u\to 0} \Pr[Y(t+u) = 1 \mid Y(t) = 0]/u,$$
$$\wedge_{1,0}(t) = \lim_{u\to 0} \Pr[Y(t+u) = 0 \mid Y(t) = 1]/u \quad (8)$$

Clearly, (7) and (8) hold if the respective limits exist.

2.3 *Regarding a multi-state network*

We assume that in the below definitions the defined characteristic is measured at a given junction in the network structure.

$\Psi(\underline{x})$—an integer-valued function expressing the network state in relation to the components states.

$Y(t)$—the network state at time t, i.e. $Y(t) = \Psi(\underline{X}(t))$.

$\Phi_c(\underline{x})$—a binary function indicating whether the network state exceeds or is equal to c, defined as follows:

$$\Phi_c(\underline{x}) = \begin{cases} 0, & \Psi(\underline{x}) < c \\ 1, & \Psi(\underline{x}) \geq c \end{cases} \quad (9)$$

$I_i^B(c,t)$—the Birnbaum c-importance of e_i at time t, defined as follows:

$$I_i^B(c,t) = \frac{\partial Pr[Y(t) \geq c]}{\partial p_i(t)} = Pr[Y(t) \geq c \mid X_i(t) = c_i] - Pr[Y(t) \geq c \mid \boldsymbol{X}_i(t) = 0] \quad (10)$$

$I_i^B(c,t)$ can be interpreted as the probability of the event {e_i's failure causes the network state to fall from a level $\geq c$ to a level $<c$}.

$A(c,t)$, $U(c,t)$—the network c-availability or c-unavailability at time t, i.e.

$$A(c,t) = \Pr[Y(t) \geq c],$$
$$U(c,t) = 1 - A(c,t) = \Pr[Y(t) < c] \quad (11)$$

E_c^+—the event {the network state rises from a level <c to a level $\geq c$}.

E_c^-—the event {the network state falls from a level $\geq$c to a level $<c$}.

$N_c^+(s,t)$, $N_c^-(s,t)$—the (random) number of times the event E_c^+ or E_c^- occurs in time interval (s,t].

$V(c,t)$, $W(c,t)$—the instantaneous frequency with which the event E_c^+ or E_c^- occurs at time t, i.e.

$$V(c,t) = \lim_{u\to 0} E[N_c^+(t,t+u)]/u,$$
$$W(c,t) = \lim_{u\to 0} E[N_c^-(t,t+u)]/u \quad (12)$$

$\Lambda^+(c,t)$, $\Lambda^-(c,t)$—the intensity with which the event E_c^+ or E_c^- occurs at time t, i.e.

$$\wedge^+(c,t) = \lim_{u\to 0} \Pr[Y(t+u) \geq c \mid Y(t) < 0]/u$$
$$\wedge^-(c,t) = \lim_{u\to 0} \Pr[Y(t+u) < c \mid Y(t) \geq c]/u \quad (13)$$

Clearly, (12) and (13) hold if the respective limits exist. It should also be noted that the above defined frequencies and intensities are functions of t, unlike the failure/repair intensities of single components.

3 FORMULAS FOR THE TRANSITION FREQUENCIES AND INTENSITIES

Let us first consider a two-state repairable system with independent two-state components. The instantaneous repair and failure frequencies of such a system are given by the following formulas:

$$V(t) = \sum_{i=1}^{n} \mu_i q_i(t) I_i^B(t),$$
$$W(t) = \sum_{i=1}^{n} \lambda_i p_i(t) I_i^B(t) \quad (14)$$

The system repair and failure intensities are related to the repair and failure frequencies in the following way:

$$\wedge_{0,1}(t) = V(t)/U(t), \wedge_{0,1}(t) = W(t)/A(t) \quad (15)$$

The proofs of (14) and (15) can be found in Schneeweiss (1981).

Clearly, the quantities defined in Section 2 for multi-state systems can be expressed in terms of binary systems. For this purpose it is sufficient to assume that the system fails or its repair is completed when the event E_c^- or E_c^+ occurs, and use Φ_c instead of Φ in (5), (6) and (8). In consequence, (14) and (15) are transformed to the following formulas:

$$V(c,t) = \sum_{i=1}^{n} \mu_i q_i(t) I_i(c,t),$$
$$W(c,t) = \sum_{i=1}^{n} \lambda_i p_i(t) I_i(c,t) \quad (16)$$

and

$$\wedge^+(c,t) = V(c,t)/U(c,t),$$
$$\wedge^-(c,t) = W(c,t)/A(c,t) \quad (17)$$

To apply (16) and (17) for the purpose of computing $\Lambda^+(c,t)$ and $\Lambda^-(c,t)$, it is first necessary to find $A(c,t)$, and $I_i^B(c,t)$: $i \in S$ (we assume that λ_i, μ_i, and, in view of (3), $p_i(t)$ for $i \in \underline{S}$ are known). The knowledge of $\Lambda^+(c,t)$ and $\Lambda^-(c,t)$ has a key significance, because, as will be shown in Section 5, other frequently used reliability parameters of repairable systems can be calculated based on $\Lambda^+(c,t)$, and $\Lambda^-(c,t)$. Let us also note that $A(c,t)$ and $I_i^B(c,t)$: $i \in S$, are functions of $p_i(t)$: $i \in S$, thus their asymptotic values for $t \to \infty$, denoted by $A(c)$ and $I_i^B(c)$: $i \in S$, are functions of $p_i = \lim_{t\to\infty} p_i(t)$: $i \in S$. As follows from (3), $p_i(t)$ quickly converges to p_i, hence these asymptotic values characterize, with good accuracy, the network's behavior in the long time horizon. In the next section it will be shown how to compute $A(c)$ and $I_i^B(c)$ for series-parallel-reducible structures.

4 THE SERIES-PARALLEL AGGREGATION

This technique consists in stepwise aggregation of components and/or sub-modules arranged in series or in parallel into a module subsequently regarded as one component. In the last step the whole system is aggregated into a single component. Below, the aggregation steps for the network in Fig. 1 are specified.

Step 1: e2, e3 → M1 = ser(e2, e3)
Step 2: M1, e4 → M2 = par(M1, e4)
Step 3: e1, M2, e5 → M3 = ser(e1, M2, e5)
Step 4: e6, e7 → M4 = ser(e6, e7)
Step 5: M3, M4 → M5 = par(M3, M4)
Step 6: M5, e8 → M6 = ser(M5, e8)

At each aggregation step, maximum effective throughput and c-availability of the obtained module will be calculated. The respective formulas are given in Lemmas 1–6. The first two lemmas give the formulas for maximum effective throughput of a module composed of single components connected in series or in parallel. The RBDs of such modules are shown in Figs. 2 and 3.

Let us adopt the following notation:

M—a module
$e_1,\ldots,e_k$: components of M
$c_1,\ldots,c_k$: throughputs of operable $e_1,\ldots,e_k$
$d_1,\ldots,d_k$: demands at $e_1,\ldots,e_k$ (if e_j is not a customer supply point, then $d_j = 0$)

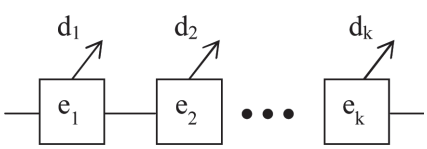


Figure 2. The RBD of ser($e_1,\ldots,e_k$).

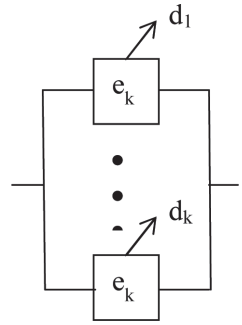


Figure 3. The RBD of par($e_1,\ldots,e_k$).

C_M: maximum (i.e. if $e_1,\ldots,e_k$ are all operable) effective throughput of M

Lemma 1
For M = ser($e_1,\ldots,e_k$) we have:

$$C_M = \min[\max(c_1 - \sum_{i=1}^{k} d_i, 0), \max(c_2 - \sum_{i=2}^{k} d_i, 0), \ldots, \max(c_k - d_k, 0)] \quad (18)$$

Lemma 2
For M = par($e_1,\ldots,e_k$) we have:

$$C_M = \sum_{j=1}^{k} \max[(c_j - d_j), 0] \quad (19)$$

The proofs of Lemmas 1 and 2 will be published in the extended version of this paper.

The two following lemmas show how to compute c-availabilities of the modules presented in Figs. 2 and 3. Let Φ_M and $A_M(c) = \Pr(\Phi_M \geq c)$ denote respectively the (random) effective throughput and the effective c-availability of the module M.

Lemma 3
For M = ser($e_1,\ldots,e_k$) it holds that

$$A_M(c) = \begin{cases} 1, & c \leq 0 \\ p_i \ldots p_k, & 1 \leq c \leq C_M \\ 0, & c \geq C_M + 1 \end{cases} \quad (20)$$

Let us note that the effective throughput of ser($e_1,\ldots,e_k$) can be equal to either 0 or C_M, where C_M is given by (18).

Lemma 4
For M = par($e_1,\ldots,e_k$) the following recursive formula holds:

$$A_{\{1,\ldots,j\}}(c) = p_j A_{\{1,\ldots,j-1\}}[c - \max(c_j - d_j, 0)] + q_i A_{\{1,\ldots,j-1\}}(c), \; j = 2,\ldots,k$$
$$A_M(c) = A_{\{1,\ldots,k\}}(c) \quad (21)$$

where

$$A_{\{1\}}(c) = \begin{cases} 1, & c \le 0 \\ p_i, & 1 \le c \le \max(c_1 - d_1, 0) \\ 0, & c \ge \max(c_1 - d_1, 0) + 1 \end{cases} \quad (22)$$

$A_M(c)$ should be computed for all integer $c \in [1, C_M]$, where C_M is given by (19).

The proofs of Lemmas 3 and 4 are based on Lemmas 1 and 2, and formulas for the distribution functions of the minimum and sum of independent, integer-valued random variables.

Finally, we give the formulas allowing to calculate the effective c-availabilities of modules composed of sub-modules rather than single components.

Lemma 5

If $M = ser(M_1,\ldots,M_k)$ then we have:

$$A_M(c) = \prod_{i=1}^{k} \Pr[\Phi_{M_i} \ge c + \sum_{j=1+1}^{k} d_{M_j}] = \\ = \prod_{i=1}^{k} A_{M_i}(c + \sum_{j=1+1}^{k} d_{M_j}) \quad (23)$$

where d_{Mj} is the total demand of all components of M_j. $A_M(c)$ should be computed for all integer c such that

$$1 \le c \le \min_{i=1,\ldots,k} \left[C_{M_i} - \sum_{j=1+1}^{k} d_{M_j} \right]$$

which is equivalent to the following condition, better suited for computational purposes:

$$A_{M_i}(c + \sum_{j=1+1}^{k} d_{M_j}) > 0, i = 1,\ldots,k$$

Lemma 6

If $M = par(M_1,\ldots,M_k)$ then the following recursive formula holds:

$$A_{M_1 \cup \ldots \cup M_j}(c) = \\ = \sum_{\beta=0}^{C_{M_j}} \Pr\left(\Phi_{M_j} = \beta\right) \Pr(\sum_{i=1}^{j-1} \Phi_{M_i} \ge c - \beta) = \\ = \sum_{\beta=0}^{C_{M_j}} \Pr\left[A_{M_j} = (\beta) - A_{M_j}(\beta+1) \right] \times \\ \times A_{M_1 \cup \ldots \cup M_{j-1}}(c - \beta), j = 2,\ldots,k \quad (24)$$

$A_M(c)$ should be computed for all integer c in the interval $[1, C_{M1} + \ldots + C_{Mk}]$.

Lemmas 5 and 6 are proved in a similar way as Lemmas 3 and 4.

To illustrate the presented method, let us find A(c) for the network presented in Fig 1. We assume that $c_1 = 9$, $c_2 = 4$, $c_3 = 3$, $c_4 = 5$, $c_5 = 4$, $c_6 = 5$, $c_7 = 4$, $c_8 = 7$, and $d_2 = 1$, $d_3 = 1$, $d_4 = 2$, $d_7 = 2$, $d_i = 0$ for i = 1, 5, 6, 8. The following calculations are performed in the successive aggregation steps:

Step 1. According to (20):
$A_{\{2,3\}}(c) = p_2p_3$, $1 \le c \le 2$
$A_{\{2,3\}}(c) = 0$, $c \ge 3$

Step 2. According to (24):
$A_{\{2,3,4\}}(c) = [A_{\{4\}}(0) - A_{\{4\}}(1)]\, A_{\{2,3\}}(c) +$
$+\ldots+ [A_{\{4\}}(3) - A_{\{4\}}(4)]\, A_{\{2,3\}}(c-3) =$
$= q_4\, A_{\{2,3\}}(c) + p_4\, A_{\{2,3\}}(c-3)$
hence
$A_{\{2,3,4\}}(1) = A_{\{2,3,4\}}(2) = q_4p_2p_3 + p_4$
$A_{\{2,3,4\}}(3) = p_4$
$A_{\{2,3,4\}}(4) = A_{\{2,3,4\}}(5) = p_4p_2p_3$
$A_{\{2,3,4\}}(c) = 0$, $c \ge 6$

Step 3. According to (23):
$A_{\{1,\ldots5\}}(c) = A_{\{1\}}(c + d_2 + d_3 + d_4) A_{\{2,3,4\}}(c) A_{\{5\}}(c)$
hence
$A_{\{1,\ldots,5\}}(1) = A_{\{1,\ldots,5\}}(2) = p_1(q_4p_2p_3 + p_4)p_5$
$A_{\{1,\ldots,5\}}(3) = p_1p_4p_5$
$A_{\{1,\ldots,5\}}(4) = p_1p_4p_2p_3p_5$
$A_{\{1,\ldots,5\}}(c) = 0$, $c \ge 5$

Step 4. According to (20):
$A_{\{6,7\}}(c) = 1$, $c \le 0$
$A_{\{6,7\}}(c) = p_6p_7$, $1 \le c \le 2$
$A_{\{6,7\}}(c) = 0$, $c \ge 3$

Step 5. According to (24):
$A_{\{1,\ldots,7\}}(c) = [A_{\{6,7\}}(0) - A_{\{6,7\}}(1)]\, A_{\{1,\ldots,5\}}(c) +$
$+\ldots+ [A_{\{6,7\}}(2) - A_{\{6,7\}}(3)]\, A_{\{1,\ldots,5\}}(c-2) =$
$= (1 - p_6p_7) A_{\{1,\ldots,5\}}(c) + p_6p_7\, A_{\{1,\ldots,5\}}(c-2)$
hence
$A_{\{1,\ldots,7\}}(1) = A_{\{1,\ldots,7\}}(2) =$
$= (1 - p_6p_7)p_1(q_4p_2p_3 + p_4)p_5 + p_6p_7$
$A_{\{1,\ldots,7\}}(3) = (1 - p_6p_7)p_1p_4p_5 +$
$+ p_6p_7p_1(q_4p_2p_3 + p_4)p_5$
$A_{\{1,\ldots,7\}}(4) = (1 - p_6p_7)p_1p_4p_2p_3p_5 +$
$+ p_6p_7p_1(q_4p_2p_3 + p_4)p_5$
$A_{\{1,\ldots,7\}}(5) = p_6p_7p_1p_4p_5$
$A_{\{1,\ldots,7\}}(6) = p_6p_7p_1p_4p_2p_3p_5$
$A_{\{1,\ldots,7\}}(c) = 0$, $c \ge 7$

Step 6. According to (23):
$A_{\{1,\ldots,8\}}(c) = A_{\{1,\ldots,7\}}(c)\, A_{\{8\}}(c)$
hence
$A_{\{1,\ldots,8\}}(c) = A_{\{1,\ldots,7\}}(c)p_8$, $1 \le c \le 6$
$A_{\{1,\ldots,8\}}(c) = 0$, $c \ge 7$

Once A(c) is computed, $I_i^B(c)$ can be found from the following equality:

$$I_i^B(c) = A(c)|_{p_i=1} - A(c)|_{p_i=0} \quad (25)$$

which is a direct consequence of (10) and (11). Thus, to obtain the c-importance of e_i, one has to find $A(c)$ for $p_i = 1$ and $p_i = 0$, p_j being fixed for $j \ne i$, and apply (25). Subsequently, $\Lambda^+(c)$, and $\Lambda^-(c)$ can be calculated from (16) and (17).

Let us note that if e_8 were a terminal node with $d_8 = c \le 6$, then the network would be operable at e_8 for $\Phi_{\{1,\ldots,7\}} \ge c$. Also note that the c-availability at, for example, e_3 is equal to $A_{\{1,2\}}(c)$, where c_1 has

to be replaced with the capacity of the outlet from e_1 towards e_2.

We conclude this section with one important remark: in case of a larger network it is possible to compute only the numerical values of $A(c)$ and $I_i^B(c)$. It is clear that deriving a closed formula, as in the given example, would be too complex a task.

5 OTHER RELIABILITY PARAMETERS EXPRESSED BY THE C-INTENSITIES

It turns out that, using the intensities $\Lambda^+(c)$ and $\Lambda^-(c)$, it is possible to compute other important reliability parameters characterizing the network state fluctuations.

Let us first define a stochastic process Y_c as follows

$$Y_c(t) = \begin{cases} 1, & Y(t) \geq c \\ 0, & Y(t) < c \end{cases} \tag{26}$$

Let, by definition

T_k—the length of the k-th period in which $Y_c(t) = 1$,

R_k—the length of the k-th period in which $Y_c(t) = 0$,

τ_k, ρ_k—the expected lengths T_k and R_k respectively,

$n_c^-(t)$, $n_c^+(t)$—the expected number of occurrences of the event E_c^- or E_c^+ respectively in a time interval of length t (e.g., in a month), provided that the system has long been in operation at the beginning of this interval.

It was shown in Malinowski (2013) that T_k and R_k have asymptotically ($k \to \infty$) exponential distributions with the parameters $\Lambda^-(c)$ and $\Lambda^+(c)$ respectively, hence it holds that

$$\begin{aligned} \tau_c &= \lim_{k\to\infty} \tau_k = 1/\wedge^-(c), \\ \rho_c &= \lim_{k\to\infty} \rho_k = 1/\wedge^+(c) \end{aligned} \tag{27}$$

Ibidem, it was also shown that

$$n_c^-(t) = n_c^+(t) = \frac{t}{\dfrac{1}{\wedge^+(c)} + \dfrac{1}{\wedge^-(c)}} = \frac{t}{\rho_c + \tau_c} \tag{28}$$

It is important to consistently use the same units of time for the parameters in (27) and (28). For example, if $\Lambda^-(c)$ and $\Lambda^+(c)$ are given in h^{-1} (hour to the power –1), then $n_c^-(t)$ is the expected number of occurrences of E_c^- in t hours. In such a case the expected number of occurrences of E_c^- in a year is equal to $n_c^-(8760)$.

6 CONCLUSION

A flow network with directed links, multiple inflow and outflow points, and a structure that can be reduced to a single component by series-parallel aggregation was considered. For such a network three basic reliability parameters were defined: c-availability—the probability with which the network's effective throughput is greater or equal to c, denoted A(c), and two c-intensities with which that throughput is reached from below or above in the course of the failure-repair process, denoted $\Lambda^+(c)$, $\Lambda^-(c)$ respectively. Assuming that the individual components' throughputs are integer valued, a method of computing these parameters was developed. This method has rather low numerical complexity compared to most known methods for network reliability calculation. It was also demonstrated how other parameters, frequently used in the reliability analysis of flow networks, can be found using A(c), $\Lambda^+(c)$ and $\Lambda^-(c)$. The obtained results can be applied to water supply, pipeline (oil or gas), power networks, etc.

REFERENCES

Barlow, R.E. & Proschan, F., 1975. *Statistical theory of reliability and life testing*. New York: Holt, Rinehart and Winston.

Chang, Y.-R., et al., 2004. Computing System Failure Frequencies and Reliability Importance Measures Using OBDD. *IEEE Transactions on Computers,* 53(1): 54–68.

Druault-Vicard, A. & Tanguy, C., 2006. Exact Failure Frequency Calculations for Extended Systems. http://arxiv.org/abs/cs/0612141

El-Damcese, M.A. & Temraz N.S., 2011. Availability and Reliability Measures for Multi-State System by Using Markov Reward Model. *Reliability: Theory & Applications,* 6(3): 68–85.

Klinz, B. & Woeginger, G.J., 2004. Minimum cost dynamic flows: the series-parallel case. *Networks,* 43(3): 153–162.

Korczak, E., 2007. New formula for the failure/repair frequency of multi-state monotone systems and its applications. *Control and Cybernetics,* 36(1): 219–239.

Krumke, S.O. & Zeck, C., 2013. Generalized max flow in series-parallel graphs. *Discrete Optimization,* 10: 155–162.

Lisnianski, A., et al., 2010. *Multi-State System Reliability Analysis and Optimization for Engineers and Industrial Managers*. Springer.

Lisnianski, A. & Levitin, G., 2003. *Multi-State System Reliability*: *Assessment, Optimization and Applications*. Singapore: World Scientific.

Malinowski, J., 2013. A method of computing the interstate transition intensities for multi-state series-parallel systems. *Safety, Reliability and Risk Analysis: Beyond the Horizon. Proceedings of the European Safety and Reliability Conference, ESREL 2013*:1213–1219.

Schneeweiss, W.G., 1981. Computing failure frequency, MTBF & MTTR via mixed products of availabilities and unavailabilities. *IEEE Trans. Reliability*, R-30: 362–363.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Minimal cut sets and direct partial logic derivatives in reliability analysis

M. Kvassay, E. Zaitseva & V. Levashenko
University of Zilina, Zilina, Slovakia

ABSTRACT: A Multi-state system is a mathematical model in reliability engineering, which allows considering some performance level in the system reliability behavior. The principal problem in reliability engineering is identification of system components that have the most influence on the system reliability. direct partial logic derivatives are one of possible approaches. In this paper, the development of direct partial logic derivatives to identify minimal cut sets (or minimal cut vectors) is considered. This development is used for calculation of the Fussell-Vesely importance measure.

1 INTRODUCTION

A system failure is investigated in reliability engineering mostly. But analysis of other system states before a failure is important problem too, that permits to investigate the system performance levels which cause a system failure. A *Multi-State System* (MSS) is one of mathematical models in reliability analysis that allows estimating some performance levels from complete failure to the perfect functioning (Lisnianski & Levitin 2003). This mathematical model is exploited in reliability analysis for detail estimation of a system instead of a *Binary-State System* (BSS) that allows defining only two states for a system and its components: failure and functioning.

Investigation of a MSS is based on the calculation of different reliability indices and measures. The group of *Importance Measures* (IMs) is used for the estimation of the influence of the fixed component state change on the system performance level change (Kuo & Zhu 2012). There are some mathematical approaches for the calculation of these measures. Most of them are based on generalization of methods that have been proposed and used for a BSS analysis. For example, Lisnianski & Levitin (2003) proposed methods for a MSS importance analysis based on the Universal Generating Function. These methods have been developed by Ramirez-Marquez & Coit (2005). In papers Zaitseva 2003, Zaitseva & Levashenko 2013 the Logic Differential Calculus has been used for calculation of IMs. In particular, the Direct Partial Logic Derivatives have been considered as the background for the definition and calculation of IMs. The Direct Partial Logic Derivatives permit to investigate the correlation between the system performance level change and the system component state change. New algorithms for the calculation of the Birnbaum IM and some other measures based on the application of these derivatives have been proposed by Zaitseva 2012 and Zaitseva & Levashenko 2013. But the definition of the Fussell-Vesely IM in terms of Direct Partial Logic Derivatives has not been considered yet. The Fussell-Vesely IM is defined by the conception of Minimal Cut Sets (Kuo & Zhu 2012). Therefore the correlation between Direct Partial Logic Derivatives and Minimal Cut Sets has to be defined.

In this paper, the development of the Direct Partial Logic Derivatives application in reliability analysis is considered and new definitions of the derivatives that are named as the union and the merge of unions of Direct Partial Logic Derivatives are proposed. The new definitions allow uniting two conceptions: the Direct Partial Logic Derivatives and the Minimal Cut Sets. Based on these Direct Partial Logic Derivatives, new definition and algorithms for calculation of IMs as the Structural Importance, Birnbaum Importance and Fussell-Vesely Importance are proposed in this paper.

2 BOUNDARY STATES

2.1 *Structure function of MSS*

The structure function defines the system state (system reliability/performance level) depending on the system components states (Zaitseva 2012):

$$\phi(\boldsymbol{x}) = \phi(x_1, \ldots, x_n):$$
$$\{0, \ldots, m_1 - 1\} \times \ldots \times \{0, \ldots, m_n - 1\} \rightarrow \{0, \ldots, M - 1\}, \quad (1)$$

where $\phi(\boldsymbol{x})$ is the system state from failure ($\phi(\boldsymbol{x}) = 0$) to perfect functioning ($\phi(\boldsymbol{x}) = M - 1$); $\boldsymbol{x} = (x_1, \ldots, x_n)$ is a state vector; x_i is the i-th component state that

changes from failure ($x_i = 0$) to perfect functioning ($x_i = m_i - 1$).

Every system component is characterized by the probabilities of its state:

$$p_{i,s} = \Pr\{x_i = s\},\ s = 0,\ \ldots,\ m_i - 1. \quad (2)$$

Note that the structure function of a MSS (1) is transformed into the structure function of a BSS if $m_i = m_j = M = 2$ (for all $i, j \in \{1, \ldots, n$ where $i \neq j$):

$$\phi(\boldsymbol{x}) = \phi(x_1, ..., x_n) : \{0,1\}^n \to \{0,1\} \quad (3)$$

A MSS reliability and unreliability based on the conception of the structure function (1) are defined as follows (Lisnianski & Levitin 2003):

$$R(j) = \Pr\{\phi(\boldsymbol{x}) \geq j\},\ j = 1,\ldots,\ M - 1, \quad (4)$$

$$U = \Pr\{\phi(\boldsymbol{x}) = 0\}. \quad (5)$$

We will consider a coherent system in this paper. Such system has two principal assumptions for the structure function (Lisnianski & Levitin 2003): (a) the structure function (1) and (3) is monotone (the system component state decrease does not improve the system reliability), and (b) the system components states are s-independent.

2.2 *Boundary states of a MSS*

The boundary state is important conception in the reliability analysis. We consider the boundary states as states for which the change of one system component causes the change of the system performance level. But this system performance level change can be caused by any component or fixed component. Therefore, two types of boundary states are considered. The first type is a boundary state for which the system state change is caused by the change of the fixed component state. These types of states are named as exact boundary states. The second type is boundary state for which the change of any system component state results change in the system state. This type is known as Minimal Cut Set.

2.2.1 *Exact boundary vector*

The exact boundary states have been considered in paper (Zaitseva 2003). These states are system states for which the change of the i-th component state from s to $\tilde{s}$ causes the system performance level change from j to $\tilde{j}$ ($s, \tilde{s} \in \{0,\ldots, m_i - 1\}$, $s \neq \tilde{s}$ and $j, \tilde{j} \in \{0,\ldots, M - 1\}$, $j \neq \tilde{j}$). The exact boundary state is defined by the exact boundary vector unambiguously. Illustrate the correlation of a system exact boundary state and an exact boundary vector by the example.

For example, consider a simple service system (Fig. 1) in a region that consists of three components (n = 3)—service point 1 (x_1—component 1), service point 2 (x_2—component 2) and infrastructure (x_3—component 3). This system has four performance levels: 0—non-operational (no customer is satisfied), 1—partially operational (some customers are satisfied), 2—partially non-operational (some customers are not satisfied), 3—fully operational (all customers are satisfied). Next, we assume that the service points are only functional (state 1) or dysfunctional (state 0). The infrastructure can be modelled by 4 quality levels, i.e. from 0 (the quality of the infrastructure is poor) to 3 (the quality is perfect). The structure function of this system is defined in Table 1 ($m_1 = m_2 = 2$, $m_3 = 4$ and $M = 4$) and components states probabilities are in Table 2.

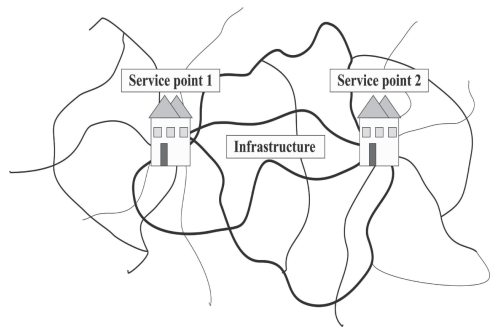


Figure 1. A simple service system.

Table 1. The structure function of the simple service system.

Components states		x_3			
x_1	x_2	0	1	2	3
0	0	0	0	0	0
0	1	0	1	1	2
1	0	0	1	1	2
1	1	0	2	3	3

Table 2. The components states probabilities of the simple service system.

	Components states							
	x_1		x_2		x_3			
	0	1	0	1	0	1	2	3
$p_{i,s}$	0.3	0.7	0.2	0.8	0.2	0.6	0.1	0.1

Determine the exact boundary states of this service system for which the failure of the first component causes the system failure as the change of the system performance level from state "1" to "0". According to Table 1, there are two situations that agree to this condition. They are possible for the failure of the second component and the third component state "1"or "2". These exact boundary states can be presented as vector states: $\boldsymbol{x} = (x_1, x_2, x_3) = (1 \rightarrow 0,0,1)$ and $\boldsymbol{x} = (x_1, x_2, x_3) = (1 \rightarrow 0,0,2)$. Note that the boundary state $\boldsymbol{x} = (x_1, x_2, x_3) = (1 \rightarrow 0,0,3)$ does not satisfy the condition because the system performance level changes from "1" to "2" depending on the failure of the first component in this case.

2.2.2 *Minimal cut vectors*

There are a lot of methods in reliability analysis that use conception of *Minimal Cut Sets* (MCSs). For example, some of them are presented by Choi & Cho (2007) and Yeh (2008). These methods have been proposed for BSS reliability analysis firstly (Shooman 1968, Rosenberg 1996).

Shooman (1968) defined a cut set of a BSS as the system components set whose simultaneous failure leads into the failure of the system (if the system has been functional). A cut set is minimal, if no component can be removed from it without losing its status as a cut set.

In the terms of the structure function, a (minimal) cut set can be interpreted by a special state vector, which is known as a (*Minimal*) *Cut Vector*. According to the definition of a cut set, the system state for a state vector covered by a cut set is zero. Therefore, *state vector* $\boldsymbol{x}$ *is a cut vector if* $\phi(\boldsymbol{x}) = 0$.

A state vector that coincides with a MCS is a *Minimal Cut Vector* (MCV). A *cut vector* $\boldsymbol{x}$ *is minimal if* $\phi(\boldsymbol{y}) = 1$ *for any* $\boldsymbol{y} > \boldsymbol{x}$, where $\boldsymbol{y}$ is state vector, for which $y_i \geq x_i$ $(i = 1, \ldots, n)$ and there exists at least one i such that $y_i > x_i$.

So, if all components of a cut set are failed and components out of the cut set are functioning, then the system is failed.

Butler (1979) generalized the definition of a MCS for MSSs and its other developments have been considered in (Aven 1985, Lisnianski & Levitin 2003, Soh & Rai 2005). Boedigheimer & Kapur (1994) proposed a conception of lower (upper) boundary points for level j ($j = 1, \ldots, M - 1$) that is similar to MCVs. Yeh (2002) and (2008) proposed to use MCVs for a network system that is interpreted as a MSS. However, those algorithms assume that source-sink cuts (in the sense of graph theory) of a network are known and therefore they cannot be used to find MCVs in other types of systems.

The generalization of MCV definition for a MSS takes into account that components of a MSS have more than two states. This extension is based on the assumption that a MCV is defined for every relevant system state, i.e. for states $1,\ldots, M-1$. According to (Aven 1985, Lisnianski & Levitin 2003), a MCV of a MSS is defined as follows: *a state vector* $\boldsymbol{x}$ *is a cut vector for demand state* j *of the system if* $\phi(\boldsymbol{x}) < j$. *A cut vector* $\boldsymbol{x}$ *is minimal if* $\phi(\boldsymbol{y}) \geq j$ *for any* $\boldsymbol{y} > \boldsymbol{x}$.

For example, consider the service system in Table 1. This system has 2 MCVs for level "1", 4 for level "2" and 3 for level "3" (Table 3).

Table 3. MCVs of the simple service system.

System state	MCVs
1	(0,0,3) (1,1,0)
2	(0,0,3) (0,1,2) (1,0,2) (1,1,0)
3	(0,1,3) (1,0,3) (1,1,1)

3 DIRECT PARTIAL LOGIC DERIVATIVES FOR CALCULATION OF BOUNDARY STATES

The mathematical tool of Direct Partial Logic Derivatives has been proposed in (Zaitseva 2003) for calculation of an exact boundary states of a MSS. The Direct Partial Logic Derivative with respect to variable x_i for the structure function (1) permits to analyze the system performance level change from j to $\tilde{j}$ when the i-th component state changes from s to $\tilde{s}$ (Zaitseva 2012, Zaitseva & Levashenko 2013):

$$\partial\phi(j \rightarrow \tilde{j}) / \partial x_i(s \rightarrow \tilde{s}) = \begin{cases} 1, & \text{if } \phi(s_i, \boldsymbol{x}) = j \text{ and } \phi(\tilde{s}_i, \boldsymbol{x}) = \tilde{j} \\ 0, & \text{other} \end{cases} \quad (6)$$

where $\phi(s_i, \boldsymbol{x}) = \phi(x_1,\ldots, x_{i-1}, s, x_{i+1},\ldots, x_n)$; $\phi(\tilde{s}, \boldsymbol{x}) = \phi(x_1,\ldots, x_{i-1}, \tilde{s}, x_{i+1},\ldots, x_n)$; $s, \tilde{s} \in \{0,\ldots, m_i - 1\}$, $s \neq \tilde{s}$ and $j, \tilde{j} \in \{0,\ldots, M-1\}$, $j \neq \tilde{j}$.

The Direct Partial Logic Derivative (6) allows investigating boundary states of a MSS for which component state x_i change from s to $\tilde{s}$ causes the system performance level change from j to $\tilde{j}$. Therefore, this derivative allows calculating exact boundary states that agree to state vectors $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$.

For example, consider the service system with the structure function in Table 1. The calculation of the Direct Partial Logic Derivative $\partial\phi(1\rightarrow0)/\partial x_1(1\rightarrow0)$ according to (6) is presented in Figure 2 (Zaitseva 2003). The exact boundary states agree to nonzero values of the derivative: $\boldsymbol{x} = (x_1, x_2, x_3) = (1 \rightarrow 0,0,1)$ and $\boldsymbol{x} = (x_1, x_2, x_3) = (1 \rightarrow 0,0,2)$.

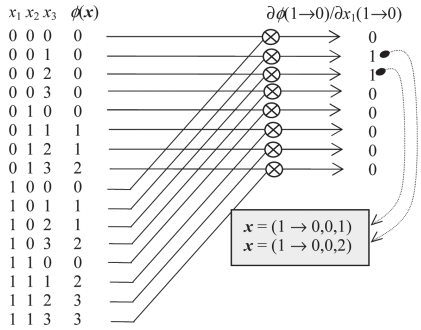


Figure 2. Calculation of the direct partial logic derivative $\partial\phi(1 \to 0)/\partial x_1(1 \to 0)$.

There is one more type of the Direct Partial Logic Derivatives that allows investigating the influence of all changes of the component to the system reliability. It is the union of all Direct Partial Logic Derivatives $\partial\phi(j \to \tilde{j})/\partial x_i(s \to (s+1))$. This union of derivatives identifies all situations in which the improvement of the fixed component state results into the transition of the system from state less than j to state greater than or equal to j:

$$\frac{\partial\phi(\uparrow\ j\uparrow)}{\partial x_i(s \to s+1)} = \bigcup_{w=0}^{j-1}\left(\bigcup_{v=j}^{M-1}\frac{\partial\phi(w \to v)}{\partial x_i(s \to s+1)}\right) \tag{7}$$

for $s = 0, \ldots, m_i - 2$ and $j = 1, \ldots, M-1$.

The Direct Partial Logic Derivative union (7) can be defined as:

$$\partial\phi(\uparrow j\uparrow)/\partial x_i(s \to s+1) = \begin{cases} 1, & \text{if } \phi(s_i, \boldsymbol{x}) < j \text{ and } \phi((s+1)_i, \boldsymbol{x}) \geq j \\ 0, & \text{other} \end{cases} \tag{8}$$

for $s = 0, \ldots, m_i - 2$ and $j = 1, \ldots, M-1$.

The dimension of the Direct Partial Logic Derivative with respect to the variable x_i is defined as $m_{1\ldots}\ m_{i\ -1} m_{i\ +1\ldots} m_n$ (Tapia et al 1991). Therefore the Direct Partial Logic Derivative union (7) and (8) for the i-th variable has dimension $m_{1\ldots}\ m_{i\ -1}\ m_{i\ +1\ldots} m_n$ too. But, the structure function investigation supposes the analysis of the all possible system states. Therefore the Direct Partial Logic Derivative union (7) and (8) has to be transformed for dimension $m_{1\ldots} m_n$ in the following way:

$$\partial\phi(\uparrow j\uparrow)/\partial x_i(s \to s+1) = \begin{cases} 1 & \text{if } x_i = s \text{ and } \phi(s_i, \boldsymbol{x}) < j \text{ and } \phi((s+1)_i, \boldsymbol{x}) \geq j \\ 0 & \text{if } x_i = s \text{ and } \left(\phi(s_i, \boldsymbol{x}) \geq j \text{ or } \phi((s+1)_i, \boldsymbol{x}) < j\right) \\ * & \text{if } x_i \neq s \end{cases}. \tag{9}$$

Table 4. The intersection of two merges of unions of direct partial logic derivatives.

$(\partial\phi\uparrow j\uparrow/\partial x_i)$	*	0	1
*	*	0	1
0	0	0	0
1	1	0	1

The merge (union) of unions (9) of Direct Partial Logic Derivatives has to be computed to identify all situations in which any improvement of a given component causes the transition of the system from state less than j to state greater than or equal to j:

$$\frac{\partial\phi(\uparrow j\uparrow)}{\partial x_i} = \bigcup_{s=0}^{m_i-2}\frac{\partial\phi(\uparrow j\uparrow)}{\partial x_i(s \to s+1)}. \tag{10}$$

The intersection of two merges (10) of two different variables (components) is defined in Table 4. This intersection identifies state vectors in which the change of states of both components (if component state can be changed) results the change of the system state from value less than j to value greater than or equal to j. In Table 4, symbol "1" means that at least state of one component from components i_1 and i_2 can be changed and all those changes result the required change of the system state (from state less than j to state greater than or equal to j). Symbol "0" identifies those state vectors in which at least one component change does not cause the required change of the system state. Finally, symbol "*" correlates with those situations, when neither component i_1 nor component i_2 can be changed from state s to state $s+1$, because both components are in state $m_{i_1} - 1$, $m_{i_2} - 1$, respectively.

The intersection of two merges of extended unions of Direct Partial Logic Derivatives identifies state vectors, in which the improvement of both components (if component can be repaired, i.e. if component is not in state $M-1$) results in the improvement of the system from state less than j to state greater than or equal to j.

The merge (10) of extended unions of Direct Partial Logic Derivatives has to be computed for all components of the system and then their "intersection" allows identifying MCVs for system state j.

4 IMPORTANCE MEASURES

Direct Partial Logic Derivative is one of possible approaches for the calculation of *Importance*

Measures (IMs) (Zaitseva 2012). The importance analysis is a part of reliability analysis that allows investigating the structural and topological aspects of the system from the reliability point of view. The IMs permit to discover the system component with maximal/minimal influence on the MSS performance level. In this paper, the applications of Direct Partial Logic Derivative are used for the computation of IMs, such as the *Structural Importance* (SI), *Birnbaum Importance* (BI), *Fussell-Vesely Importance* (FVI). The basic charcteristics of these measures are in Table 5 (Lisnianski and Levitin 2003, Zaitseva 2012).

According to (Zaitseva 2012), the Direct Partial Logic Derivative has been used for calculation of the SI and BI. The FVI definition is based on the MCS that is calculated based on the Direct Partial Logic Derivative (10) too.

In this a paper, we propose unifying method for calculation of the IMs based on the Direct Partial Logic Derivative (6) and (10).

4.1 *The Structural importance*

The SI is one of the simplest measures of the component importance. This measure focuses on the topological aspects of the system. According to the definition in paper (Armstrong 1997), this measure determines the proportion of working states of the system in which the working of the *i*-th component makes the difference between system failure and its working:

$$IS_i^{s,j} = \frac{\rho_i^{s,j}}{\rho_j} \tag{11}$$

Table 5. Importance measures.

Short name	Description
SI	The SI concentrates on the topological structure of the system and determines the proportion of working states of the system in which the working of the *i*-th component makes the difference between system failure and working state.
BI	The BI of a given component is defined as the probability that such a component is critical to MSS functioning and represents loss in MSS when the *i*-th component fails.
FVI	The FVI quantifies the maximum decrement in MSS reliability caused by the *i*-th system component state deterioration and it also allows estimating system performance level decrease for full unreliability of the *i*-th system component.

where $\rho_i^{s,j}$ is a number of system states when the change of component state from s to $s-1$ results in the system reliability change from j to h (for $h < j$); ρ_j is number of the states for which $\phi(\boldsymbol{x}) = j$ and is calculated by the structure function.

The number $\rho_i^{s,j}$ can be computed as the number of nonzero values of the Direct Partial Logic Derivative (6).

For example, the Direct Partial Logic Derivatives for the structure function in Table 1 with respect to the first variable are in Table 6. Based on these derivatives, we define the SI according to (11). Values of this measure for the first variable are shown Table 6 too. These values indicate that the failure of the first component does not cause the system skip down if the system has performance level 3. The probability of the system failure from performance level 2 and 1 depending on the first component failure is 0.3 and 0.5 accordingly. The degradation of the system performance level 3 has probability 0.5. And degradation of the performance level is possible with probability 0.3.

4.2 *The Birnbaum importance*

Note the SI (11) investigates correlation and influence of system component from the topological point of view. But this measure does not take into account the probabilities of states of system components. This disadvantage is eliminated in the calculation of another IM that is known as the BI. The BI of a given component is defined as the probability that system is sensitive to inoperative of the *i*-th system component (Lisnianski and Levitin 2003). Let us consider the Direct Partial Logical Derivatives for calculation of the BI. In paper (Zaitseva 2012), the BI has been defined as

$$IB_i^{s,j} = \Pr\{\partial\phi(j \to h)/\partial x_i(s \to s-1) \neq 0\} \tag{12}$$

Table 6. Direct Partial Logic Derivatives and SI for the first component of the simple service system.

x_2		
x_3	0 0 0 0 1 1 1 1	
$\partial\phi(j \to h)/\partial x_1(1 \to 0)$	0 1 2 3 0 1 2 3	$IS_1^{1,j}$
$\partial\phi(1 \to 0)/\partial x_1(1 \to 0)$	0 1 1 0 0 0 0 0	0.5
$\partial\phi(2 \to 0)/\partial x_1(1 \to 0)$	0 0 0 1 0 0 0 0	0.3
$\partial\phi(3 \to 0)/\partial x_1(1 \to 0)$	0 0 0 0 0 0 0 0	0
$\partial\phi(2 \to 1)/\partial x_1(1 \to 0)$	0 0 0 0 0 1 0 0	0.3
$\partial\phi(3 \to 1)/\partial x_1(1 \to 0)$	0 0 0 0 0 0 1 0	0.5
$\partial\phi(3 \to 2)/\partial x_1(1 \to 0)$	0 0 0 0 0 0 0 1	0.5

The equation (12) supposes the BI calculation as the probabilities of non-zero values of Direct Partial Logic Derivative $\partial\phi(j \to h)/\partial x_i(s \to s-1)$.

For example, consider the BI for the first component of the system with structure function in Table 1. According to (12) this measure is calculated as probability of nonzero values of Direct Partial Logic Derivatives (see Table 6). Therefore the BI for this system failure depending on the failure of the first system component is defined as:

$$\begin{aligned} IB_1^{1,1} &= \Pr\{\partial\phi(1\to 0)/\partial x_i(1\to 0)\neq 0\} \\ &= \Pr\{\{x_2=0 \text{ and } x_3=1\} \text{ OR } \{x_2=0 \text{ and } x_3=2\}\} \\ &= p_{2,0}\cdot p_{3,1} + p_{2,0}\cdot p_{3,2} \end{aligned}$$

The calculation of other measures is similar.

4.3 *The Fussell-Vesely importance*

There is one more measure that allows investigating the influence of the component state change on the system performance level. It is the FVI that represents the contribution of each component to the system failure probability and, for a BSS; it is calculated by the next equation (Meng 2009):

$$IFV_i = \frac{F_{\min\,\text{cut}}(x_i)}{Q} \tag{13}$$

where $F_{\min\,\text{cut}}(x_i)$ is the probability that at least one minimal cut set that includes the *i*-th system component is failed and Q is the function of the system unreliability (Meng 2009):

$$Q = \Pr\{\phi(\boldsymbol{x}) = 0\}. \tag{14}$$

Now, consider definition (13) of the FVI for a BSS in terms of MCVs. Every MCS can be transformed into a MCV using the following rules (Kvassay et al 2014):

a. every system component that exists in the considered MCS has value 0 in the corresponding MCV,
b. every system component that does not appear in the MCS is represented by value 1 in the corresponding MCV.

Then, the probability that at least one minimal cut set that includes the *i*-th system component is failed can be expressed as follows:

$$F_{\min\,\text{cut}}(x_i) = \Pr\{\boldsymbol{x} \le MCV_i\}, \tag{15}$$

where MCV_i denotes set of all MCVs of the system that have value 0 at the position of the *i*-th component and event $\{\boldsymbol{x} \le MCV_i\}$ means that there is at least one MCV for component *i* that is greater than or equal to arbitrary state vector $\boldsymbol{x}$.

Using (15), the FVI (13) of the *i*-th component for a BSS can be defined as follows:

$$IFV_i = \frac{\Pr\{\boldsymbol{x} \le MCV_i\}}{\Pr\{\phi(\boldsymbol{x})=0\}} = \frac{\Pr\{\boldsymbol{x} \le MCV_i\}}{1-R(1)}. \tag{16}$$

Definition (16) of the FVI for a BSS uses MCVs instead of MCSs and therefore, it is easier to extend it on MSSs.

In a BSS, MCVs exist for one working performance level of the system only, i.e. $\phi(\boldsymbol{x}) = 1$. However, a MSS has more than one working performance level and MCVs are defined for all these levels, i.e. for levels 1, 2,…, $m-1$. Therefore, we use MCV^j to denote MCVs for system performance level *j*.

In addition, MCVs for BSS with respect to component *i* have $x_i = 0$ always, because a BSS component has only two possible states. However, a MSS allows defining more than two states of any component, therefore, we denote MCVs for system state *j* with respect to state *s* of the *i*-th component as $MCV_i^{s,j}$. $MCV_i^{s,j}$ is a subset of MCV^j that contains those MCVs for system state *j* that have value $s-1$ at position *i* in a MCV. So, $MCV_i^{s,j}$ represent situations in which the repair of any damaged component different from component *i* results improvement of the MSS to state *j* or greater and transition of the *i*-th component from state $s-1$ to state *s* (minor improvement of component *i*) causes the similar improvement of MSS performance level.

Now, define the FVI of given component for a MSS in the following way:

$$IFV_i^{s,j} = \frac{\Pr\{\boldsymbol{x} \le MCV_i^{s,j}\}}{1-R(j)} = \frac{\Pr\{\boldsymbol{x} \le MCV_i^{s,j}\}}{\Pr\{\phi(\boldsymbol{x}) < j\}}, \tag{17}$$

where event $\{\boldsymbol{x} \le MCV_i^{s,j}\}$ means that there is at least one MCV for system state *j* and component state *s* which is greater than arbitrary state vector $\boldsymbol{x}$.

Clearly, event $\{\boldsymbol{x} \le MCV_i^{s,j}\}$ is a subset of event $\{\boldsymbol{x} \le MCV^j\}$. Therefore, the FVI (17) can be interpreted as the contribution of the *i*-th component transition from state *s* to state $s-1$ to system unreliability with respect to system state *j* and this is very closely to meaning of the FVI for a BSS (13).

Now, assume that we want to compute the FVIs of individual components of the simple service system defined in Table 1 and identify which component has the most influence on the system state "1". Firstly, we have to compute MCVs of the system. According to the previous section,

Direct Partial Logic Derivatives can be used for this task. In Table 7, there are computed unions (10) of Direct Partial Logic Derivatives (the white columns) and their intersection (the gray columns). Value "1" in the gray columns identifies MCVs for system state "1". According to Table 7, set MCV^1 consists of two state vectors: (1,1,0) and (0,0,3). As we can see, the found MCVs for system state "1" are same as in Table 3.

Next, we identify sets $MCV_i^{s,1}$ from MCV^1 for individual system components and their states (Table 8).

According to Table 8, there exists no MCV for states "2" or "3" of the third component of the simple service system. It means, when the third component is in state "2" or "3", then its minor failure (by one state) does not contribute to system failure.

Using Table 8, we can compute the FVI (17) for system state "1". The calculated FVI are in Table 9.

As we can see from Table 9, state "1" of the third component has the most contribution to system failure. This implies that the majority of situations in which the system fails coincide with the total failure of the 3-rd component.

Table 7. The merges of unions of direct partial logic derivatives and their intersection for state "1" of the service system.

Components states		x_3			
x_1	x_2	0	1	2	3
0	0	0 0 0 0	1 1 0 0	1 1 0 0	1 1 * 1
0	1	0 * 1 0	0 * 0 0	0 * 0 0	0 * * 0
1	0	* 0 1 0	* 0 0 0	* 0 0 0	* 0 * 0
1	1	* * 1 1	* * 0 0	* * 0 0	* * * *

Table 8. Sets $MCV_i^{s,1}$ for the service system components.

Component (i)	x_1	x_2	x_3		
Component state (s)	1	1	1	2	3
$MCV_i^{s,1}$	(0,0,3)	(0,0,3)	(1,1,0)	–	–

Table 9. The computed FVI for state 1 of the service system.

Component (i)	x_1	x_2	x_3		
Component state (s)	1	1	1	2	3
$IFV_i^{s,1}$	0.2419	0.2419	0.8065	0	0

5 CONCLUSIONS

The principal result of this paper is development of mathematical approach of Direct Partial Logic Derivatives for the calculation of MCVs of a MSS. Mathematical background for this development is considered and used for new definition of FVI measure of a MSS. New method application is presented based on the hand calculation example (it is the system in Fig. 1). The next step of the investigation will be implemented for the comparison of proposed methods and other calculation methods for the FVI measure of a MSS that are considered by Kuo & Zhu (2012) and Ramirez-Marquez & Coit (2005).

ACKNOWLEDGMENT

This work was supported by the grant of 7th RTD Framework Program No 610425 (RASimAs) and grant of Slovak Research and Development Agency SK-PL-0023-12.

REFERENCES

Armstrong, M. 1997. Reliability-importance and dual failure-mode components. *IEEE Trans. on Reliability* 46(2): 212–221.

Aven, T. 1985. *Reliability evaluation of multistate systems with multistate components. IEEE Transactions on Reliability* R-34(5): 473–479.

Boedigheimer, R., Kapur, K. 1994. Customer-Driven Reliability Models for Multistate Coherent Systems. *IEEE Trans. Reliability* 43(1): 46–50.

Butler, D.A. 1979. A complete importance ranking for components of binary coherent systems with extensions to multi-state systems. *Naval Research Logistics* 4: 565–578.

Choi, J.S., Cho, N.Z. 2007. A practical method for accurate quantification of large fault trees. *Reliability Engineering & System Safety* 92(7): 971–982.

Kvassay, M., Zaitseva, E., Levashenko V. 2014. Minimal Cut Vectors and Logical Differential Calculus. *Proc. of the 44th IEEE International Symposium on Multiple-Valued Logic*, Bremen, Germany.

Kuo, W., Zhu, X. 2012. *Importance Measures in Reliability, Risk, and Optimization: Principles and Applications.* Chichester, UK: Wiley.

Lisnianski, A., Levitin, G. 2003. Multi-state System Reliability. Assessment, Optimization and Applications. Singapore, SG: World Scientific.

Meng, F.C. 2009. On some structural importance of system components. *Journal of Data Science* 7: 277–283.

Ramirez-Marquez, J.E., Coit, D.W. 2005. Composite Importance Measures for Multi-State Systems with Multi-State Components. *IEEE Trans. on Reliability* 54: 517–529.

Rosenberg, L. 1996. Algorithm for finding minimal cut sets in a fault tree. *Reliability Engineering & System Safety* 53(1): 67–71.

Shooman, M. L. 1968. *Probabilistic Reliability: An Engineering Approach*. New York, NY: McGraw-Hill, 1968.

Soh, S., Rai, S. 2005. An efficient cutset approach for evaluating communication-network reliability with heterogeneous link-capacities. *IEEE Transactions on Reliability* 54(1): 133–144.

Tapia, M.A., Guima, T.A., Katbab, A. 1991. Calculus for a multivalued-logic algebraic system. *Applied Mathematics and Computation* 42: 255–285.

Yeh, W. 2002. A new approach to the d-MC problem. *Reliability Engineering & System Safety* 77(2): 201–206.

Yeh, W. 2008. An improved algorithm for searching all minimal cuts in modified networks. *Reliability Engineering & System Safety* 93(7): 1018–1024.

Zaitseva, E. 2003. Dynamic Reliability Indices for Multi-State System. *Proc. of the IEEE 33th Int. Symp. on Multiple-Valued Logic,* Tokyo, Japan: 287–292.

Zaitseva, E. 2012. Importance analysis of a multi-state system based on multiple-valued logic methods. In: Lisnianski A. and Frenkel I. (eds) *Recent Advances in System Reliability: Signatures, Multi-state Systems and Statistical Inference.* London: Springer: 113–134.

Zaitseva, E, Levashenko, V. 2013. Multiple-valued logic mathematical approaches for multi-state system reliability analysis. *Journal of Applied Logic* 11(3): 350–362.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On the probability of escaping a cell—in wireless networks

Christian Tanguy
Orange Labs Networks (ONL/NMP/TRM), Issy-les-Moulineaux, France

ABSTRACT: The availability and Quality of Service (QoS) of wireless network connections are crucial for telecommunications companies. The network is constituted by emitters, each devoted to a specific area called "cell". When a user moves from one cell to a neighbouring one, a "handover" (also called "hand-off") procedure must take place for the call to proceed seamlessly. Such a procedure requires network resources, also used for the establishment of new calls. If these resources are not sufficient, the forced termination probability (a call is not completed because of an unsuccessful handover attempt) and the call blocking probability (a new connection request is rejected) may be too large. Our aim is to provide simple, analytical expressions to calculate the above-mentioned probabilities of failure.

In this work we address the probability for a mobile to leave a cell represented by a few n-regular polygons, such as can be used for a two-dimensional tiling/coverage, thereby generalizing existing results on disks and rectangles. We provide the full distributions of probabilities of escaping the cell as a function of displacement, for triangles, squares, hexagons and octagons, along with the asymptotic limit for the disk. The connection with the distance distribution function is also given, along with the asymptotic average distance $\ell(n)$. These formulas could be useful for the reliability practitioner.

1 INTRODUCTION

Cellular networks have been investigated for several decades (Mac Donald 1979). Quite naturally, the advances of wireless communications have made necessary the consideration of several aspects linked to reliability. How can one ensure that communications are indeed made possible, and are not untimely terminated ? Failure protection and Quality of Service are very important issues for network operators, which are constrained by a few factors. For instance, the range of each base station is limited, so that the radius of each "cell" does not extend infinitely. When a user moves to another cell, he/she expects the call to proceed seamlessly. Resources for such a continuation of the call are required, which are also used to process new calls. Cell switching (and the associated handover procedures) also consume some of the resources. A proper optimization of resources is therefore crucial, to say nothing of financial aspects.

Handovers may lead to cut calls, which in turn can lead to customer dissatisfaction. Knowing the probability of escapes from cells is therefore one of the key aspects of wireless network management. Our aim in this work is to show very simply how to compute this probability of escape, which depends on the geometry of the cell, for several regular polygons, which as can be used for a two-dimensional covering.

Our paper is organized as follows. After a quick survey of the literature in Section 2, we introduce in Section 3 a simple way to compute the probability of staying in the initial cell, assuming that that positions at which calls are initiated are uniformly distributed, while the direction of movement of the mobile user is isotropic. We then devote the next Section to the catalog of fully analytical expressions valid for regular polygons such as equilateral triangles, squares, hexagons and octagons (they can pave the two-dimensional space when used with smaller squares). In Section 5 we link the obtained expressions to the more traditional chord length and distance density distributions, which have been studied since the nineteenth century in the field of stochastic geometry and for which considerable progress has been made in very recent years.

2 STATE OF THE ART

Traffic models and performance analysis have long been considered in cellular radio systems (Hong & Rappaport 1986, Guérin 1987). When the mobile user crosses the boundary between a cell and the next one while the call is in progress, the call requires a new base station and a new channel frequency. The procedure that allows to provide the new channel is called handover (or handoff, depending

on the source). Hong & Rappaport (1986) chose to replace a hexagonal cell by an effective circular one, because computations are easier. Their assumption is that the mobile user is moving in any direction, and that the direction remains constant throughout the call. Guérin (1987) considered hexagonal networks too, but limited the directions followed by the use to only four—north, south, east and west—in his assessment of the channel occupancy time in a cellular radio system.

More recent studies have been devoted to the channel occupancy times, handover rates for mobile computing and outage probabilities (Nanda 1993, Fang, Chlamtac, & Lin 1998, Fang & Chlamtac 2002, Zhang, Shao, & Fujise 2005, Trajanov, Filiposka, & Grnarov 2005, Tanbourgi & Sand 2010, Jain & Gupta 2011, Khan, Abbas, & Khan 2011). Note that the successive versions—going from 2.5G to 5G—of smartphones require to adapt the procedures, and the associated outage probabilities. Various mathematical frameworks are being used, from Monte Carlo simulations to renewal theory; queueing theory is also well represented, with Markov systems at the forefront.

A few other studies go beyond the mere calculation of outage probabilities is order to provision adequate resources, for instance in the future network LTE (Blogowski, Klopfenstein, & Renard 2012) and design adaptative resource allocation for prioritized call admission (Yu & Leung 1997).

Of course, the mobility of the user is a crucial parameter of the problem. This issue has been quite investigated by numerous authors (Zonoozi & Dassanayake 1997, Navidi & Camp 2004, Bettstetter 2001, Bettstetter, Hartenstein, & Pérez-Costa 2002, Bettstetter, Resta, & Santi 2003, Bettstetter, Hartenstein, & Pérez-Costa 2004, Hyytiä, Lassila, &Virtamo 2006, Hyytiä & Virtamo 2007, Le Boudec 2005a, Le Boudec 2005b). One may observe, under certain conditions, steady-state regimes for the position and velocity of the mobile user. Note that the "equilibrium" position distribution is not uniform anymore (see also (Miller 2001)). The velocity distribution, for instance, should not include the null velocity.

A few authors have been also able to show that under such conditions, simple geometric parameters are extremely useful, since they essentially provide the main result. For instance, the average chord length and the average distance $\overline{\ell}$ between points of the same cell appear quite naturally in the picture. Note that this is not only confined to cellular network studies: it also appears in models for efficient flight schedules in the fight against fires (Greulich 2008).

The calculation of the average distance between random points in a cell has been studied for many years by experts in probabilistic geometry (Santaló 1976, Lazoff & Sherman 1994, Mathai, Moschopoulos, & Pederzoli 1999) (The values of $\overline{\ell}$ for the disk, the square and the equilateral triangle are indeed given in page 49 of (Santaló 1976)). Recently, huge progress has been made which has led to new results for regular polygons or more general cells (Harutyunyan & Ohanyan 2009, Zhuang & Pan 2011, Zhuang & Pan 2012b, Aharonyan 2012, Bäsel 2012b, Bäsel 2012a). In turn, these results have been applied to very practical issues such as the minimization of energy consumption in wireless sensor networks (Zhuang, Pan, & Cai 2010) or the definition of network performance metrics (Zhuang & Pan 2012a). A nice overview of these very active fields can be found in (Moltchanov 2012).

Let us now turn to our calculation of the probability of escaping a cell, which is a major ingredient of the aforementioned calculations.

3 GEOMETRICAL METHOD

3.1 *A simple case: The circular cell*

As is usually done, we consider that the calls originate at random in the cell, and that the direction followed by the mobile user is arbitrary (and uniformly distributed). After some time t, the user has moved by some distance d, given by $d = vt$, where v is its (constant) velocity. These assumptions make the calculation quite easy, since it boils down to the assessment of the surface of the set of points belonging to both the original cell and the displaced one. In the case of a circular cell, this is very easy, since all directions are equivalent (see Figure 1).

The corresponding expression for the probability of staying in the disk is therefore easy to calculate; it has been reproduced in various papers and

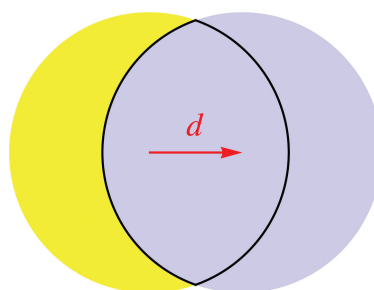


Figure 1. Circular cell and its displaced self. The area of the intersection, when divided by the area of the original disk, is nothing but the probability P_r of staying in the cell after a displacement d. The escape probability is given by $P_e = 1 - P_r$.

books (Trajanov, Filiposka, Makraduli, & Grnarov 2004, Blogowski, Klopfenstein, & Renard 2012). We now turn to more realistic cells, used in tiling the two-dimensional plane.

3.2 *A case study: The octagon*

In the case of an n-regular polygon of radius a, the invariance by rotation is broken, even though some amount of symmetry is preserved (a rotation by π/n leaves the structure unchanged). The area of the intersection of the initial and displaced cell will vary with each angle ϕ and displacement d, as shown in Figures 2–4.

We see in Figures 2–4 that the shape of the intersection goes from octagon to hexagon to lozenge. Each of the areas can be obtained effortlessly, leading to a probability of staying $P_r(d,\phi)$. For each stage, we have a specific area, namely $A_1(d,a,\phi)$, $A_2(d,a,\phi)$, and $A_3(d,a,\phi)$. Going from stage 1 to stage 2 implies a constraint on d and ϕ. This is also true for the transition from stage 2 to stage 3. When d is larger that the diameter of the octagon, namely $D = 2a$, the area of the intersection is zero, meaning that the probability of escape is equal to one.

We have to average $P_r(d,\phi)$ over ϕ, which then gives $\overline{P}_r(d)$. Because of symmetry, we need only consider $0 \le \phi \le \pi/8$. However, the constraints translate into conditions on ϕ for the integration. We have reproduced in Figure 5 the various conditions.

For instance, if $0 \le d \le 2a\sin\frac{\pi}{8}$, the average probability is given by

$$\overline{P}_r(0 \le d \le 2a\sin\frac{\pi}{8}) = \frac{8}{\pi A_0}\int_0^{\frac{\pi}{8}} A_1(d,a,\phi)\,d\phi, \tag{1}$$

Where A_0 is the area of the initial cell, namely $2\sqrt{2}\,a^2$.

For $2a\sin\frac{\pi}{8} \le d \le 2a\sin\frac{\pi}{4}$, we have

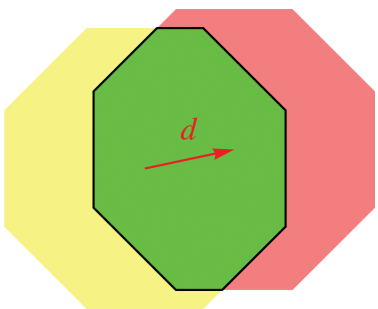


Figure 2. First stage of the displacement of the octagon.

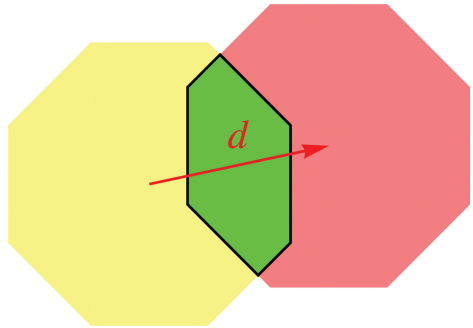


Figure 3. Second stage of the displacement of the octagon.

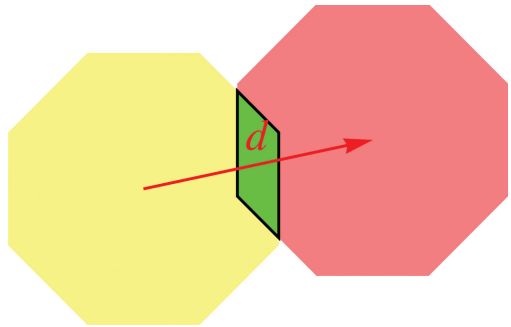


Figure 4. Third stage of the displacement of the octagon.

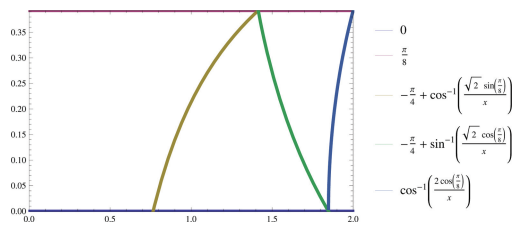


Figure 5. Various boundary functions for integrations over ϕ in the case of the octagon.

$$\overline{P}_r(0 \le d \le 2a\sin\frac{\pi}{8}) = \frac{8}{\pi A_0}\left(\int_0^{h_3} A_2(d,a,\phi)\,d\phi + \int_{h_3}^{\frac{\pi}{8}} A_1(d,a,\phi)\,d\phi\right), \tag{2}$$

with

$$h_3 = \arccos\left(\frac{\sqrt{2}\,a\sin\frac{\pi}{8}}{d}\right) - \frac{\pi}{4}. \tag{3}$$

The limits of the various integration ranges are actually $2a\sin\frac{m\pi}{8}$ $(0 \le m \le 4)$. Note that

integrations are easy—and tedious—to perform, since the $A_i(d,a,\phi)$ are simple expressions of $\cos\phi$, $\sin\phi$, plus constant terms.

The complete results are detailed in the following Section.

4 CATALOG OF ESCAPE PROBABILITIES

We provide a simple list of exact results for the escape probability $\overline{P}_e(x)$, where $x = d/a$ is a dimensionless parameter, for various configurations.

4.1 *Disk*

$$\overline{P}_e(x) = 1 - \frac{2\left(\cos^{-1}(x) - x\sqrt{1-x^2}\right)}{\pi} \quad (0 \le x \le 1) \tag{4}$$

4.2 *Equilateral triangle*

$$\begin{aligned}\overline{P}_e(x) &= \frac{4x\left(1-\frac{1}{36}\left(3\sqrt{3}+2\pi\right)x\right)}{\pi} \quad \left(0 \le x \le \frac{3}{2}\right)\\ &= \frac{6\left(\left(\frac{2x^2}{9}+1\right)\cos^{-1}\left(\frac{3}{2x}\right) - \sqrt{x^2-\frac{9}{4}}\right)}{\pi}\\ &\quad + \frac{4x\left(1-\frac{1}{36}\left(3\sqrt{3}+2\pi\right)x\right)}{\pi}\\ &\quad \left(\frac{3}{2} \le x \le \sqrt{3}\right).\end{aligned} \tag{5}$$

4.3 *Square*

Let us remember here, in order to avoid confusion with previously published results, that a represents the square's *radius* a, not the length of its sides.

$$\begin{aligned}\overline{P}_e(x) &= \frac{4\left(1-\frac{x}{4}\right)x}{\pi} \quad (0 \le x \le 1)\\ &= \frac{4\left(\frac{x^2}{4} - \sqrt{x^2-1} + \cos^{-1}\left(\frac{1}{x}\right) + \frac{1}{2}\right)}{\pi}\\ &\quad (1 \le x \le \sqrt{2})\end{aligned} \tag{6}$$

4.4 *Hexagon*

$$\begin{aligned}\overline{P}_e(x) &= -\frac{x^2}{\sqrt{3}\pi} + \frac{x^2}{9} + \frac{4x}{\sqrt{3}\pi} \quad (0 \le x \le 1)\\ &= -\frac{x^2}{3} + \frac{\sqrt{12x^2-9}}{\pi} + \frac{\left(4x^2+6\right)\sin^{-1}\left(\frac{\sqrt{3}}{2x}\right)}{3\pi}\\ &\quad -\frac{2}{3} \quad (1 \le x \le \sqrt{3})\\ &= \frac{x^2}{\sqrt{3}\pi} - \frac{x^2}{9} - \frac{10\sqrt{3x^2-9}}{3\pi} - \frac{1}{3}\\ &\quad + \frac{\left(2x^2+24\right)\cos^{-1}\left(\frac{\sqrt{3}}{x}\right)}{3\pi} + \frac{2\sqrt{3}}{\pi}\\ &\quad (\sqrt{3} \le x \le 2)\end{aligned} \tag{7}$$

4.5 *Octagon*

$$\begin{aligned}\overline{P}_e(x) &= \frac{(\pi-4)x^2}{4\sqrt{2}\pi} + \frac{4\sqrt{2}x\sin\left(\frac{\pi}{8}\right)}{\pi}\\ &\quad \left(0 \le x \le 2\sin\frac{\pi}{8}\right)\\ &= \frac{1}{8}\left(3\sqrt{2}x^2 + 4\sqrt{2} - 4\right)\\ &\quad + \frac{3\left(\sqrt{2}-1\right)\sqrt{\left(2+\sqrt{2}\right)x^2-1}}{\pi}\\ &\quad - \frac{\left(\sqrt{2}x^2 + 2\sqrt{2} - 2\right)\cos^{-1}\left(\frac{1}{\sqrt{2+\sqrt{2}}x}\right)}{\pi}\\ &\quad \left(2\sin\frac{\pi}{8} \le x \le \sqrt{2}\right)\\ &= \frac{1}{8}\left(\sqrt{2}x^2 + 4\right)\\ &\quad - \frac{\left(\sqrt{2}x^2 + 2\sqrt{2} + 2\right)\cos^{-1}\left(\frac{1}{2x\sin\frac{\pi}{8}}\right)}{\pi}\\ &\quad + \frac{3\left(1+\sqrt{2}\right)\sqrt{\left(2-\sqrt{2}\right)x^2-1}}{\pi}\\ &\quad \left(\sqrt{2} \le x \le 2\sin\frac{3\pi}{8}\right)\\ &= -\frac{\sqrt{2}\pi x^2 - 4\sqrt{2}x^2 + 4\sqrt{2}\pi - 16\left(1+\sqrt{2}\right)}{8\pi}\\ &\quad + \frac{\left(\sqrt{2}x^2 + 4\sqrt{2} + 8\right)\cos^{-1}\left(\frac{2\cos\left(\frac{\pi}{8}\right)}{x}\right)}{\pi}\\ &\quad - \frac{\left(1+2\sqrt{2}\right)\sqrt{x^2-\sqrt{2}-2}\csc\left(\frac{\pi}{8}\right)}{\pi}\\ &\quad \left(2\sin\frac{3\pi}{8} \le x \le 2\right)\end{aligned} \tag{8}$$

We have represented in Figure 6 the behavior of these escape probabilities. We see that the approach to the boundary manifests itself with

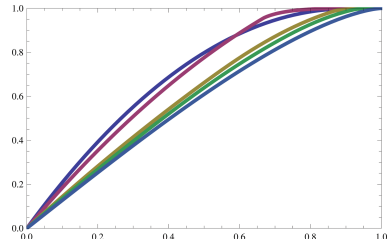


Figure 6. Comparison of the rescaled escape probabilities of the configurations detailed in Section 4 as a function of the displacement x^*, so that these probabilities are equal to 1 for $x^* = 1$. The general trend for the curves is a rightward move as n increases, with the exception of $n = 4$ (violet curve).

quite noticeable differences between the disk and other cell geometries. This is of the utmost importance, because most outages correspond to mobile users about to cross the boundary and change cells. This means that using "effective" circular cells may be not so accurate for subsequent numerical assessments of failure probabilities.

5 LINK WITH STOCHASTIC GEOMETRY

As mentioned in Section 2, there is a large body of work in stochastic geometry concerning the chord length and distance density distributions. New results have been proposed quite recently for regular n-polygons (Bäsel 2012b, Harutyunyan & Ohanyan 2009). These functions have been, in some instances, given explicitly (Zhuang & Pan 2011, Zhuang & Pan 2012b, Aharonyan 2012). The (normalized) distance density of probability is often defined as $g(l)$, so that the average distance $e\ell$ is given quite generally by

$$\bar{\ell} = \int_0^D g(l)\,dl. \tag{9}$$

where D is again the diameter of the cell.

Actually, the probability of remaining in the cell, $\overline{P}_r(l) = 1 - \overline{P}_e(l)$ is very closely connected to $g(l)$. We have

$$g(d) = \frac{2\pi d}{A_0}\overline{P}_r(d). \tag{10}$$

This means that we can recover the average length already obtained by other groups in a simple way:

$$\bar{\ell} = \int_0^D \frac{2\pi l^2}{A_0}\overline{P}_r(l)\,dl. \tag{11}$$

An analytical value is actually obtained for $\bar{\ell}(8) = 0.860007978015497247289475476698a$ for the octagon, but its expression is rather lengthy, and will not be given here It is in agreement with the value given in (Hsu 1990), once proper rescaling has been performed. In this reference, the author remarks that Monte Carlo simulations could not give information about the way the average distance in a n-regular polygon approaches that of the disk. We decided to give it a try, and numerically obtained the following asymptotic expansion, which is

$$\bar{\ell}_{\text{approx}}(n) \approx \frac{128a}{45\pi}\left(1 - \frac{1}{3}\frac{\pi^2}{n^2} + \frac{19}{360}\frac{\pi^4}{n^4} + \cdots\right). \tag{12}$$

Considering $n = 8$ in equation (12), we get $\bar{\ell}_{\text{approx}}(8) \approx 0.8600090923$, which is already satisfactory. By contrast, the average of the *s*quare of the distance is simply

$$\overline{\ell^2}(n) = \frac{2 + \cos\frac{2\pi}{n}}{3}a^2. \tag{13}$$

6 CONCLUSION

We have provided the full distributions of probabilities of escaping the cell as a function of displacement for triangles, squares, hexagons and octagons, along with their asymptotic limit: the disk. This catalog of formulas could be useful for the reliability practitioner. Besides, they show the notable difference between polygons and the limiting circle, especially close to the boundary, which is the region where hand-over procedures are most likely to occur. We have also shown that the probability of staying in such cells is closely related to the distance distribution of uniformly distributed points, which has recently been addressed for regular n-polygons (but not only) by several authors working in statistical geometry. We have also given an asymptotic expansion of the average distance $\bar{\ell}(n)$, which is an important parameter when using the random way-point mobility model for the performance assessment of mobile ad hoc networks (MANETs). After inclusion of relevant traffic and mobility data, our results will allow an efficient provisioning and optimization of network resources: cell area, energy consumption of emitters (in a green context), etc. Note that these calculations may be used, not only for wireless networks, but in a wide range of applications, such as vehicular technologies and mobile systems.

REFERENCES

Aharonyan, N. (2012). Mean distance between two points in a domain. *Proceedings of the Yerevan State University 2012*(3), 3–9.

Bäsel, U. (2012a). The distribution function of the distance between two random points in a right-angled triangle. *arXiv preprint arXiv:1208.6228v2*.

Bäsel, U. (2012b). Random chords and point distances in regular polygons. *arXiv preprint arXiv:1204.2707v2*.

Bettstetter, C. (2001, July). Mobility modeling in wireless networks: categorization, smooth movement, and border effects. *SIGMOBILE Mob. Comput. Commun. Rev. 5*(3), 55–66.

Bettstetter, C., G. Resta, & P. Santi (2003). The node distribution of the random waypoint mobility model for wireless ad hoc networks. *IEEE Transactions on Mobile Computing 2*(3), 257–269.

Bettstetter, C., H. Hartenstein, & X. Pérez-Costa (2002). Stochastic properties of the random waypoint mobility model: epoch length, direction distribution, and cell change rate. In *Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*, MSWiM '02, New York, NY, USA, pp. 7–14. ACM.

Bettstetter, C., H. Hartenstein, & X. Pérez-Costa (2004). Stochastic properties of the random waypoint mobility model. *Wireless Networks 10*(5), 555–567.

Blogowski, A., O. Klopfenstein, & B. Renard (2012). Dimensioning X2 backhaul link in LTE networks. In *IEEE International Conference on Communications (ICC 2012)*, pp. 2768–2773.

Fang, Y. & I. Chlamtac (2002). Analytical generalized results for handoff probability in wireless networks. *IEEE Transactions on Communications 50*(3), 396–399.

Fang, Y., I. Chlamtac, & Y.-B. Lin (1998). Channel occupancy times and handoff rate for mobile computing and PCS networks. *IEEE Transactions on Computers 47*(6), 679–692.

Greulich, F.E. (2008). Modeling airtanker flight distance between concurrent fires: The development and use of statistical distribution parameters. *Forest Science 54*(1), 47–57.

Guérin, R.A. (1987). Channel occupancy time distribution in a cellular radio system. *IEEE Transactions on Vehicular Technology 36*(3), 89–99.

Harutyunyan, H.S. & V.K. Ohanyan (2009). The chord length distribution function for regular polygons. *Advances in Applied Probability 41*(2), 358–366.

Hong, D. & S.S. Rappaport (1986). Trafic model and performance analysis for cellular mobile radio telephone systems with prioritized and nonprioritized handoff procedures. *IEEE Transactions on Vehicular Technology 35*(3), 77–92.

Hsu, A.C. (1990, January). The expected distance between two random points in a polygon. Master's thesis, MIT.

Hyytiä, E., P. Lassila, & J. Virtamo (2006). Spatial node distribution of the random waypoint mobility model with applications. *IEEE Transactions on Mobile Computing 5*(6), 680–694.

Hyytiä, E. & J. Virtamo (2007). Random waypoint mobility model in cellular networks. *Wireless Networks 13*(2), 177–188.

Jain, P. & S.C. Gupta (2011). Hybrid mixed handover for call blocking probability analysis in wireless ATM network. *Journal of Engineering and Computer Innovations 2*(4), 68–77.

Khan, J., A. Abbas, & K. Khan (2011). Cellular handover approaches in 2.5G to 5G technology. *International Journal of Computer Applications 21*(2), 28–37.

Lazoff, D.M. & A.T. Sherman (1994, July). An exact formula for the expected wire length between two randomly chosen terminals. Technical report, University of Maryland Baltimore County. Technical Report TR CS-98-04, Computer Science Department.

Le Boudec, J.-Y. (2005a). On the stationary distribution of speed and location of random waypoint. *IEEE Transactions on Mobile Computing 4*(4), 404–405.

Le Boudec, J.-Y. (2005b, June). Understanding the simulation of mobility models with Palm calculus. Technical Report IC/2005/033, EPFL.

Mac Donald, V.H. (1979). Advanced mobile phone service: The cellular concept. *The Bell System Technical Journal 58*(1), 15–41.

Mathai, A., P. Moschopoulos, & G. Pederzoli (1999). Random points associated with rectangles. *Rendiconti del Circolo Matematico di Palermo 48*(1), 163–190.

Miller, L.E. (2001). Distribution of link distances in a wireless network. *Journal of Research of the National Institute of Standards and Technology 106*(2), 401–412.

Moltchanov, D. (2012). Distance distributions in random networks. *Ad Hoc Networks 10*(6), 1146–1166.

Nanda, S. (1993). Teletraffic models for urban and suburban microcells: cell sizes and handoff rates. *IEEE Transactions on Vehicular Technology 42*(4), 673–682.

Navidi, W. & T. Camp (2004). Stationary distributions for the random waypoint mobility model. *IEEE Transactions on Mobile Computing 3*(1), 99–108.

Santaló, L.A. (1976). *Integral geometry and geometric probability*. London: Addison-Wesley.

Tanbourgi, R. & S. Sand (2010). Evaluation of handover rates and outage probability for the macrocellular environment. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2010)*, pp. 1–5.

Trajanov, D., S. Filiposka, J. Makraduli, & A. Grnarov (2004). Connection resilience to nodes failures in ad hoc networks. In *Proceedings of the 12th IEEE Mediterranean on Electrotechnical Conference (MELECON 2004)*, Volume 2, pp. 579–582.

Trajanov, D.R., S.V. Filiposka, & A.L. Grnarov (2005). Node density influence on link expiration time in ad hoc networks. In *Proceedings of the International Conference on Computer as a Tool (EUROCON 2005)*, Volume 2, pp. 1838–1841.

Yu, O.T.W. & V.C.M. Leung (1997). Adaptive resource allocation for prioritized call admission over an ATM-based wireless PCN. *IEEE Journal on Selected Areas in Communications 15*(7), 1208–1225.

Zhang, Y., Z. Shao, & M. Fujise (2005). Handoff probability in wireless mobile networks. In *Proceedings of the IEEE International Conference on Communications (ICC 2005)*, Volume 5, pp. 3407–3411.

Zhuang, Y. & J. Pan (2011). Random distances associated with hexagons. Technical report.

Zhuang, Y. & J. Pan (2012a). A geometrical probability approach to location-critical network performance metrics. In *Proceedings of IEEE INFOCOM 2012*, pp. 1817–1825.

Zhuang, Y. & J. Pan (2012b). Random distances associated with equilateral triangles. Technical report.

Zhuang, Y., J. Pan, & L. Cai (2010). Minimizing energy consumption with probabilistic distance models in wireless sensor networks. In *Proceedings of IEEE INFOCOM 2010*, pp. 2453–2461.

Zonoozi, M. & P. Dassanayake (1997). User mobility modeling and characterization of mobility patterns. *IEEE Journal on Selected Areas in Communications 15*(7), 1239–1252.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability analysis of ship-rope transporter with dependent components

A. Blokus-Roszkowska & K. Kołowrocki
Maritime University, Gdynia, Poland

ABSTRACT: In the paper, an innovative model of combination of the influence of complex systems' inside-dependences and the influence coming from their outside-dependencies on their reliability are presented. Further, the model is practically applied to the reliability evaluation of the ground ship-rope transporter operating in a shipyard at variable operation conditions and changing in time its reliability structure, its components' reliability parameters and among its components and subsystems dependencies. As a result of this application, the multi-state reliability function of the shipyard transportation system is determined in case when its components have exponential reliability functions with interdependent departures rates from the subsets of their reliability states. At the end, discussion of how changing the reliability structure, components' reliability parameters and inside and outside this transportation system dependencies result in changes of its reliability characteristics is performed.

1 INTRODUCTION

Currently, newest trends in the reliability analysis of technical systems are directed to the complex systems. These are complex systems that significant features are inside-system dependencies and outside-system dependencies, that in case of damage have significantly destructive influence on safety of the environment where they are operating. These systems are made of large number of interacting components and even small perturbations can trigger large scale consequences. For above reason, as an extended failure within one of the complex system may result in critical incapacity or destruction and can significantly damage many aspects of human life. This development of suitable tools for their reliability analysis is of great value.

From the point of view of more precise reliability analysis, developed methods should be based on a multi-state approach (Kołowrocki 2014, Kołowrocki & Soszyńska-Budny 2011, Xue 1985, Xue & Yang 1995a, b, Yu et al. 1994) instead of normally used two-state approach. This will enable different complex system's inside and outside reliability states to be distinguished, such that they ensure a demanded level of system operation effectiveness with accepted consequences of their dangerous accidents.

In most reliability analyses, it is assumed that components of a system are independent. But in reality, especially in case of complex systems, this assumption is not true, so that dependencies among the complex systems' components and subsystems should be assumed and considered. It is a natural assumption, as after decreasing the reliability state by one of components in a subsystem, inside interactions among remaining components may cause further components reliability states decrease (Blokus-Roszkowska 2007a, Pradhan et al. 2003, Pradhan & Hansen 2005).

To tie results of investigations of complex systems inside-dependences together with results coming from assumed their outside-dependencies, the semi-Markov model (Grabski 2002, Kołowrocki 2013, Limnios & Oprisan 2005) can be used to describe those systems operation processes. This linking of inside and outside of complex systems dependencies under assumed their structures multi-state models, is the main idea of the systems' reliability analysis methodology presented in the paper.

2 RELIABILITY ANALYSIS OF SYSTEMS WITH DEPENDENT COMPONENTS

2.1 *Multi-state "m out of n" system*

In the multi-state reliability analysis to define a system with degrading components, we assume that (Kołowrocki 2004):

- n is a number of system components,
- E_i, $i = 1,2, \ldots, n$, are components of a system,
- all components and a system under consideration have the reliability state set $\{0,1, \ldots, z\}$, $z \geq 1$,

– the reliability states are ordered, the reliability state 0 is the worst and the reliability state z is the best,
– $T_i(u)$, $i = 1,2, \ldots, n$, are independent random variables representing lifetimes of components E_i in the reliability state subset $\{u, u+1, \ldots, z\}$, while they were in the reliability state z at the moment $t = 0$,
– $T(u)$ is a random variable representing lifetime of a system in the reliability state subset $\{u, u+1, \ldots, z\}$ while it was in the reliability state z at the moment $t = 0$,
– the system states degrades with time t,
– $E_i(t)$ is a component E_i reliability state at the moment t, $t \in < 0,\infty)$, given that it was in the reliability state z at the moment $t = 0$.

In a multi-state "m out of n" system with dependent components we may consider the dependency of changes of their ageing reliability states and assume that after changing the reliability state subset by one of system components to the worse reliability state subset, lifetimes of remaining system components in this reliability state subset decrease (Blokus-Roszkowska 2007b, Kołowrocki 2013). More exactly, we assume that if anyone of system components gets out of the reliability state subset $\{u, u+1, \ldots, z\}$, then the reliability of remaining ones is getting worse so that their mean values of lifetimes $T_i'(u)$ in reliability state subset $\{u, u+1, \ldots, z\}$ become less according to the formula

$$E[T_i'(u)] = c(u)\frac{n-1}{n}E[T_i(u)], i = 1, \ldots, n, u = 1, \ldots, z, \tag{1}$$

where $c(u)$ are component stress proportionality correction coefficients (Kołowrocki 2013).

Generalizing, if $\upsilon, \upsilon = 0,1,2, \ldots, n-1$, components of a system are out of the reliability state subset $\{u, u+1, \ldots, z\}$, the mean values of the lifetimes $T_i'(u)$ in the reliability state subset $\{u, u+1, \ldots, z\}$ of system remaining components are given by

$$E[T_i'(u)] = c(u)\frac{n-\upsilon}{n}E[T_i(u)], i = 1, \ldots, n, u = 1, \ldots, z. \tag{2}$$

Hence, for case when considered system is homogeneous with components having exponential reliability functions of the form

$$R_i(t,\cdot) = [1, R_i(t,1), \ldots, R_i(t,z)], \quad t \in < 0,\infty), i = 1,2, \ldots, n, \tag{3}$$

where

$$R_i(t,u) = \begin{cases} 1, & t < 0 \\ \exp[-\lambda(u)t], & t \geq 0, \ i = 1, \ldots, n, \end{cases} \tag{4}$$

with intensity of departure $\lambda(u) \geq 0$ from the reliability state subset $\{u, u+1, \ldots, z\}$, according to the well known relationship between the lifetime mean value in this reliability state subset and intensity of departure from this reliability state subset of the form

$$E[T_i(u)] = \frac{1}{\lambda(u)}, i = 1,\ldots,n, u = 1,\ldots,z,$$

we get following formula for intensities of departure from this reliability state subset of remaining components

$$\lambda^{(\upsilon)}(u) = \frac{1}{c(u)}\frac{n}{n-\upsilon}\lambda(u) \quad \upsilon = 0,1, \ldots, n-1, u = 1, \ldots, z. \tag{5}$$

With this simple approach to inside dependencies of complex systems with homogeneous components we can find analytical solutions for reliability characteristics of selected reliability structures. The main theoretical result presented below in the form of Proposition 1 is a generalization of the results given in (Blokus-Roszkowska 2007b, Kołowrocki 2013).

Proposition 1. If in a homogeneous multi-state "m out of n" system

i. components have exponential reliability function given by (3)–(4),
ii. components are dependent,
iii. intensities of departure from the reliability state subsets of components are given by (5),

then the multi-state system reliability function is given by the formula

$$\boldsymbol{R}(t,\cdot) = [1, \boldsymbol{R}(t,1), \ldots, \boldsymbol{R}(t,z)], \tag{6}$$

where

$$\boldsymbol{R}(t,u) = \sum_{\upsilon=0}^{n-m} \frac{\left[\frac{n\lambda(u)}{c(u)}t\right]^{\upsilon}}{\upsilon!} \times \exp\left[-\frac{n\lambda(u)}{c(u)}t\right], t \geq 0, u = 1, \ldots, z. \tag{7}$$

Proof: We denote by $N(t,u)$ a number of components that got out of the reliability state subset $\{u, u+1, \ldots, z\}$ up to the moment t, $t \geq 0$. Then the number $N(t,u)$ is a process with states

0,1,2, …, n, and probability of its particular state is given by

$$P_\upsilon(t,u) = P(N(t,u) = \upsilon), \upsilon = 0,1,2, \ldots, n, u = 1, \ldots, z.$$

The above definition and formula (5) mean that the process $N(t,u)$ is a Markov process with the transition rates

$$\lambda_{ij}(u) = \begin{cases} -\dfrac{n\lambda(u)}{c(u)}, & j = i, \\ \dfrac{n\lambda(u)}{c(u)}, & j = i+1, \\ 0, & j \neq i \wedge j \neq i+1, i = 0,1, ..., n. \end{cases}$$

Since a "m out of n" system is out of the reliability state subset $\{u, u+1, \ldots, z\}$ if at least m its components are in the reliability state subset $\{u, u+1, \ldots, z\}$, i.e. the system is out of this reliability state subset when the process $N(t,u)$ is at the state $n-m+1$. Then the state $n-m+1$ is an absorbing state and the matrix of transition rates between states takes the following form

$$\begin{array}{c} state \\ 0 \\ 1 \\ \vdots \\ n-m \\ n-m+1 \\ \vdots \\ n \end{array} \begin{array}{c} \begin{array}{ccccccccc} 0 & 1 & 2 & \ldots & n-m & n-m+1 & \ldots & n \end{array} \\ \begin{bmatrix} -\dfrac{n\lambda(u)}{c(u)} & \dfrac{n\lambda(u)}{c(u)} & 0 & \ldots & 0 & 0 & 0 \ldots & 0 \\ 0 & -\dfrac{n\lambda(u)}{c(u)} & \dfrac{n\lambda(u)}{c(u)} & \ldots & 0 & 0 & 0 \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ \vdots \ \vdots & \\ 0 & 0 & 0 & \ldots & -\dfrac{n\lambda(u)}{c(u)} & \dfrac{n\lambda(u)}{c(u)} & 0 \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ \vdots \ \vdots & \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \ldots & 0 \end{bmatrix} \end{array} \tag{8}$$

Thus, the distribution function of system lifetime in the state subset $\{u, u+1, \ldots, z\}$ is given by

$$\begin{aligned} \boldsymbol{F}(t,u) &= P(T(u) < t) \\ &= P(N(t,u) = n-m+1) = P_{n-m+1}(t,u) \end{aligned}$$

for $t \geq 0$, $u = 1,\ldots,z$,

and the suitable reliability function component of this system is of the form

$$\boldsymbol{R}(t,u) = 1 - P_{n-m+1}(t,u), t \geq 0, u = 1, \ldots, z. \tag{9}$$

From the stochastic processes theory it follows that having given the matrix (8) of transition rates between states, it is possible to find the probability $P_{n-m+1}(t,u)$ from following system of differential equations:

$$\begin{cases} P_0'(t,u) = -\dfrac{n\lambda(u)}{c(u)} P_0(t,u) \\ P_1'(t,u) = \dfrac{n\lambda(u)}{c(u)} P_0(t,u) - \dfrac{n\lambda(u)}{c(u)} P_1(t,u) \\ P_2'(t,u) = \dfrac{n\lambda(u)}{c(u)} P_1(t,u) - \dfrac{n\lambda(u)}{c(u)} P_2(t,u) \\ \quad \vdots \\ P_{n-m}'(t,u) = \dfrac{n\lambda(u)}{c(u)} P_{n-m-1}(t,u) - \dfrac{n\lambda(u)}{c(u)} P_{n-m}(t,u) \\ P_{n-m+1}'(t,u) = \dfrac{n\lambda(u)}{c(u)} P_{n-m}(t,u) \end{cases} \tag{10}$$

for $t \geq 0$, $u = 1,\ldots,z$.

It is supposed that all components of analyzed system at the beginning are in the state subset $\{u, u+1, \ldots, z\}$, and therefore at the moment $t = 0$ the process $N(t,u)$ $u = 1,2, \ldots, z$, is at the state 0. It means that probability of its particular states $\upsilon = 0,1,2, \ldots, n-m+1$, of the process $N(t,u)$, $u = 1,2, \ldots, z$, at the moment $t = 0$ are given by

$$P_0(0,u) = 1, P_\upsilon(0,u) = 0, \upsilon = 1,2, \ldots, n-m+1, \quad u = 1, \ldots, z. \tag{11}$$

Applying Laplace's transform to the system of equations (10) with the initial conditions (11), we obtain

$$\begin{cases} s\boldsymbol{P}_0(s,u) - 1 = -\dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_0(s,u) \\ s\boldsymbol{P}_1(s,u) = \dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_0(s,u) - \dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_1(s,u) \\ \quad \vdots \\ s\boldsymbol{P}_{n-m}(s,u) = \dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_{n-m-1}(s,u) - \dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_{n-m}(s,u) \\ s\boldsymbol{P}_{n-m+1}(s,u) = \dfrac{n\lambda(u)}{c(u)} \boldsymbol{P}_{n-m}(s,u), \end{cases}$$

where

$$\boldsymbol{P}_\upsilon(s,u) = \int_0^\infty P_\upsilon(t,u) \exp[-st] dt, \upsilon = 1,2, \ldots, n-m+1, \quad u = 1,2, \ldots, z,$$

is a transform of the probability $P_\upsilon(t,u)$ of its particular states $\upsilon = 1,2, \ldots, n-m+1$.

Further, for $u = 1,2, \ldots, z$, we have

$$\begin{cases} \boldsymbol{P}_0(s,u) = \dfrac{c(u)}{s\cdot c(u)+n\lambda(u)} \\ \boldsymbol{P}_1(s,u) = \dfrac{n\lambda(u)}{s\cdot c(u)+n\lambda(u)}\boldsymbol{P}_0(s,u) \\ \quad\vdots \\ \boldsymbol{P}_{n-m}(s,u) = \dfrac{n\lambda(u)}{s\cdot c(u)+n\lambda(u)}\boldsymbol{P}_{n-m-1}(s,u) \\ \boldsymbol{P}_{n-m+1}(s,u) = \dfrac{n\lambda(u)}{s\cdot c(u)}\boldsymbol{P}_{n-m}(s,u). \end{cases}$$

From this system of equations we conclude that transforms of the probability $\boldsymbol{P}_{n-m+1}(s,u)$ are equal

$$\boldsymbol{P}_{n-m+1}(s,u) = \frac{[n\lambda(u)]^{n-m+1}}{s[s\cdot c(u)+n\lambda(u)]^{n-m+1}}, u = 1, \ldots, z,$$

which may be written in the form of following series

$$\boldsymbol{P}_{n-m+1}(s,u) = \frac{1}{s} - \sum_{\upsilon=0}^{n-m} \frac{\left[\dfrac{n\lambda(u)}{c(u)}\right]^{\upsilon}}{\left[s+\dfrac{n\lambda(u)}{c(u)}\right]^{\upsilon+1}}, u = 1, \ldots, z.$$

After application of inverse Laplace's transform to above equation, we have

$$P_{n-m+1}(t,u) = 1 - \sum_{\upsilon=0}^{n-m} \frac{\left[\dfrac{n\lambda(u)}{c(u)}t\right]^{\upsilon}}{\upsilon!}\exp\left[-\frac{n\lambda(u)}{c(u)}t\right], t \geq 0,$$
$$u = 1, \ldots, z.$$

Taking into account the last result and (9) we get (7), which completes the proof. #

2.2 *Multi-state "m out of l"-series system*

To define a "*m* out of *l*"-series system, we assume that (Kołowrocki 2004):

- k is a number of "*m* out of *l*" subsystems of a system,
- l is a number of components of "*m* out of *l*" subsystems,
- E_{ij}, $i = 1,2, \ldots, k$, $j = 1,2, \ldots, l$, $k, l \in N$, are components of a system,
- all components E_{ij} have the same reliability state set as before $\{0,1, \ldots, z\}$,
- $T_{ij}(u)$, $i = 1,2, \ldots, k$, $j = 1,2, \ldots, l$, $k, l \in N$, are random variables representing lifetimes of components E_{ij} in the reliability state subset $\{u, u+1, \ldots, z\}$, while they were in the reliability state z at the moment $t = 0$.

Then we can consider a multi-state "*m* out of *l*"-series system defined in (Kołowrocki 2004) and its multi-state reliability function in case its components are dependent. To this end, we assume similarly as in formula (2) for a "*m* out of *n*" system that if $\upsilon, \upsilon = 0,1,2, \ldots, l-1$, components of each "*m* out of *l*" subsystem of a system are out of the reliability state subset $\{u, u+1, \ldots, z\}$, the mean values of lifetimes $T_{ij}'(u)$ in the reliability state subset $\{u, u+1, \ldots, z\}$ of this subsystem remaining components are given by

$$E[T_{ij}'(u)] = c(u)\frac{l-\upsilon}{l}E[T_{ij}(u)] \tag{12}$$

for $i = 1,2, \ldots, k$, $j = 1,2, \ldots, l$, $u = 1,2, \ldots, z$, where $c(u)$ are component stress proportionality correction coefficients (Kołowrocki 2013).

Hence, in case subsystem components have exponential reliability functions with intensity of departure $\lambda(u)$ from the reliability state subset $\{u, u+1, \ldots, z\}$, according to the well known relationship between the lifetime mean value in this reliability state subset and the intensity of departure from this reliability state subset we get following formula for intensities of departure from this reliability state subset of subsystem remaining components

$$\lambda^{(\upsilon)}(u) = \frac{1}{c(u)}\frac{l}{l-\upsilon}\lambda(u) \tag{13}$$

for $\upsilon = 0,1,2, \ldots, l-1$, $u = 1,2, \ldots, z$.

Proposition 1 slight extension yields the following result.

Proposition 2. If in a homogeneous multi-state "*m* out of *l*"-series system.

i. components have exponential reliability function given by

$$R_{ij}(t,\cdot) = [1, R_{ij}(t,1), \ldots, R_{ij}(t,z)] \tag{14}$$

where

$$R_{ij}(t,u) = \begin{cases} 1, & t < 0, \\ \exp[-\lambda(u)t], & t \geq 0, \end{cases} \tag{15}$$

for $u = 1,2, \ldots, z$, $i = 1,2, \ldots, k$, $j = 1,2, \ldots, l$, with intensity $\lambda(u) \geq 0$ of departure from the reliability state subset $\{u, u+1, \ldots, z\}$,

ii. components are dependent,

iii. intensities of departure from the reliability state subsets of components are given by (13),

then the multi-state system reliability function is given by the formula

$$\boldsymbol{R}(t,\cdot) = [1, \boldsymbol{R}(t,1), \ldots, \boldsymbol{R}(t,z)], \tag{16}$$

where

$$\boldsymbol{R}(t,u)=\left[\sum_{v=0}^{l-m}\frac{\left[\frac{l\lambda(u)}{c(u)}t\right]^{v}}{v!}\exp\left[-\frac{l\lambda(u)}{c(u)}t\right]\right]^{k} \tag{17}$$

for $t \geq 0$, $u = 1, \ldots, z$.

3 RELIABILITY OF A GROUND SHIP-ROPE TRANSPORTER

3.1 *System's description*

The ground ship-rope transporter is used to transfer ships coming to a shipyard for repairs from a platform to a repair post and back from a repair post to a platform. First during ship docking a ship settled in special supporting carriages on the platform is raised to the wharf level, then a ship is transferred from the platform with rope broaching machines on a traverser. Next a ship with the traverser, on which a ship is settled, is shifted in the repair post direction. After some repair measures, a ship is transferred back to the traverser and next on the platform. Finally, during undocking a ship on the platform is moved down to the water.

There are nine repair posts, denoted by symbols R1–R9. First repair post R1 can be lengthening to the post R1/B1 for long ships. There are also available two repair depots denoted by symbols B and D. Generally all kind of repairs can be carried out in any repair post. The repair posts R1 and R2 are equipped in a crane. Submarines are repaired in the depot. Additionally large vessels are transferred to the repair post R1/B1. The scheme of a plan of repair post placing is given in Figure 1.

The ground ship-rope transporter is composed of three broaching machines working independently

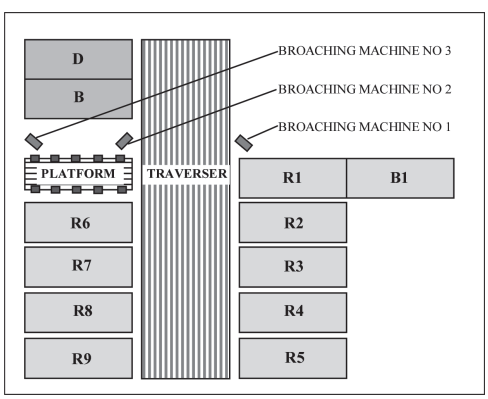


Figure 1. The scheme of a plan repair post placing.

equipped in steel ropes. The ground ship-rope transporter reliability depends strongly on a tonnage of transferred ships and the place where a ship should be transferred. These broaching machines in the transportation system are numbered 1, 2, 3. There is used one or there are used two or possibly three broaching machines depending on weight and length of a ship and on which repair post a ship should be transferred. All three broaching machines are working in extreme situation when large vessel over 1800 tons is transferred.

3.2 *System's operation process*

We analyze the ground ship-rope transporter taking into account the system operation process and its varying in time reliability structures. Considering weight and size of vessels i.e. the system's loading and the place where the ship is transferred, that has influence on the decision which broaching machines are used we can distinguish following eight operation states:

- an operation state z_1, the system is without loading, the time of waiting for a ship,
- an operation state z_2, a ship with a tonnage up to 1300 tons is transferred from the platform to the traverse, from the traverse to the repair posts R1-R5 and from the repair posts R6-R9 to the traverse (the broaching machine no. 1 is used),
- an operation state z_3, a ship with a tonnage up to 1300 tons is transferred from the traverse to the repair posts R6-R9, from the repair posts R1-R5 to the traverse and from the traverse to the platform (the broaching machine no. 3 is used),
- an operation state z_4, a ship with a tonnage up to 1300 tons is transferred from the repair posts R1-R5 to the traverse and the access to the broaching machine number 3 is difficult (the broaching machine no. 2 is used),
- an operation state z_5, a ship with a tonnage over 1300 up to 1800 tons is transferred from the platform to the traverse, from the traverse to the repair posts R1-R5 or from the repair posts R6-R9 to the traverse (the broaching machines 1 and 3 are used),
- an operation state z_6, a ship with a tonnage over 1300 up to 1800 tons is transferred from the platform to the traverse, from the traverse to the repair posts R1-R5 or from the repair posts R6-R9 to the traverser and the access to the broaching machine number 3 is difficult (the broaching machines 1 and 2 are used),
- an operation state z_7, a ship with a tonnage over 1300 up to 1800 tons is transferred from the traverse to the repair posts R6-R9, from the repair posts R1-R5 to the traverse or from the traverse to the platform (the broaching machines 2 and 3 are used),

– an operation state z_8, a ship with a tonnage over 1800 tons is transferred (all broaching machines 1, 2 and 3 are used).

From the operation process analysis and its statistical identification presented in (Blokus-Roszkowska & Kołowrocki 2009a) we obtain limit values of transient probabilities $p_b(t)$ at particular operational states z_b, $b = 1,2, \ldots, 8$, that respectively amount:

$$p_1 = 0.9790,\ p_2 = 0.0064,\ p_3 = 0.0065,\ p_4 = 0,$$
$$p_5 = 0.0009,\ p_6 = 0, p_7 = 0.0042,\ p_8 = 0.0030. \tag{18}$$

3.3 *System's reliability*

The system consists of three broaching machines subsystems S_1, S_2, S_3 linked in series. Each broaching machine S_1, S_2, S_3 is equipped with one rope that is composed of 6 identical strands. Each strand consists of 36 wires with a webbing core. We consider wires as basic components of the system.

According to rope reliability data given in their technical certificates and experts' opinions, based on nature of wire failures, following reliability states of the ropes' components have been distinguished:

– a reliability state 3, the wire is new, without any defects,
– a reliability state 2, the corrosion of wire is greater than 0% and less than 25%,
– a reliability state 1, the corrosion of wire is greater than or equal to 25% and less than 50%,
– a reliability state 0, otherwise (a wire is failed).

A rope is in the reliability state subset {1,2,3}, {2,3}, {3}, if all 6 strand are in this subset, so it is a series system. After some consultations with experts we assume that a strand does not satisfy technical conditions after breaking 6 of its 36 wires. With this assumption we conclude that a rope is in the reliability state subset {1,2,3}, {2,3}, {3}, when all six strands of a rope are in this state subset and each of strands is in the reliability state subset {1,2,3}, {2,3}, {3}, if at least 30 out of its 36 wires are in this state subset. Thus, we obtain that a rope is a regular 4-states "30 out of 36"-series system composed of $k = 6$ series-linked strands with $l = 36$ parallel-linked components (wires). As each broaching machine has only one rope we can say that broaching machines i.e. subsystems S_1, S_2, S_3, are also regular 4-state "30 out of 36"-series systems.

Further assuming that the ground ship-rope transporter is in the reliability state subset {1,2,3}, {2,3}, {3}, when all its subsystems are in this subset of reliability states, we conclude that the ground ship-rope transporter is a series system of subsystems S_1, S_2, S_3. In our further analysis considering broaching machines we will discuss reliability of rope system only, so we say that the broaching machine is in the reliability state subset {1,2,3}, {2,3}, {3}, if the rope in this broaching machine is in this state subset.

The ground ship-rope transporter and its operation process is widely described and illustrated in (Blokus-Roszkowska & Kołowrocki 2009a). At system operational state z_1 the system is composed of subsystems S_1, S_2 and S_3 linked in series. At the operational states z_2, z_3 and z_4 a ship is transferred using one broaching machine, so the system is composed of one of subsystems S_1, S_2, S_3. At the operational states z_5, z_6 and z_7 a ship is transferred using two broaching machines, so the system is composed of two of subsystems S_1, S_2, S_3 linked in series. At the operational state z_8 a ship is transferred using all three broaching machines, so the system is composed of subsystems S_1, S_2 and S_3 linked in series.

Moreover we assume that subsystems S_1, S_2, S_3 of the ground ship-rope transporter are composed of identical 4-state components (wires), having the multi-state conditional reliability functions

$$R^{(b)}(t,\cdot) = [1, R^{(b)}(t,1), R^{(b)}(t,2), R^{(b)}(t,3)],$$

with following exponential co-ordinates $R^{(b)}(t,1)$, $R^{(b)}(t,2)$ and $R^{(b)}(t,3)$ different in various operation states z_b, $b = 1,2, \ldots, 8$.

These are, at the system operational state z_1:

$$R^{(1)}(t,1) = \exp[-0.0097t],\ R^{(1)}(t,2) = \exp[-0.0147t],$$
$$R^{(1)}(t,3) = \exp[-0.0278t],\ t \geq 0,$$

at the operational states z_2, z_3 and z_4:

$$R^{(b)}(t,1) = \exp[-0.0158t],\ R^{(b)}(t,2) = \exp[-0.0235t],$$
$$R^{(b)}(t,3) = \exp[-0.0388t],\ t \geq 0, b = 2,3,4,$$

at the operational states z_5, z_6 and z_7:

$$R^{(b)}(t,1) = \exp[-0.0175t],\ R^{(b)}(t,2) = \exp[-0.0361t],$$
$$R^{(b)}(t,3) = \exp[-0.0551t],\ t \geq 0, b = 5,6,7,$$

at the system operational state z_8:

$$R^{(8)}(t,1) = \exp[-0.0215t],\ R^{(8)}(t,2) = \exp[-0.0394t],$$
$$R^{(8)}(t,3) = \exp[-0.0607t],\ t \geq 0.$$

In case system operation time is large enough, coordinates of the system unconditional reliability function is given by (Soszyńska 2007)

$$\boldsymbol{R}(t,u) \cong \sum_{b=1}^{v} p_b [\boldsymbol{R}(t,u)]^{(b)}, \; t \geq 0, \tag{19}$$

where $[\boldsymbol{R}(t,u)]^{(b)}$, $u = 1,2,3$, $b = 1,2, \ldots, 8$, are coordinates of the system conditional reliability functions and p_b are limit transient probabilities of the system operation process at the operation state z_b, $b = 1,2, \ldots, 8$, given by (18).

In reliability analysis of the ground ship-rope transporter with dependent components at variable operation conditions we assume that both intensities of departure $\lambda(u)$, $u = 1,2,3$, from the reliability state subset $\{1,2,3\}$, $\{2,3\}$, $\{3\}$, and component stress proportionality correction coefficients $c(u)$, $u = 1,2,3$, are influenced by changes of the system operation process states and their values can differ at various operation states z_b, $b = 1,2, \ldots, 8$.

Then assuming system components' dependence defined by (13) and applying directly the formulae (16)–(17) and (19), we get the system reliability function

$$\boldsymbol{R}(t,\cdot) = [1, \boldsymbol{R}(t,1), \boldsymbol{R}(t,2), \boldsymbol{R}(t,3)], \; t \geq 0, \tag{20}$$

where

$$\begin{aligned}
\boldsymbol{R}(t,1) &\cong \sum_{b=1}^{v} p_b \left[\sum_{\upsilon=0}^{l-m} \frac{[(l[\lambda(1)]^{(b)}/[c(1)]^{(b)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(l[\lambda(1)]^{(b)}/[c(1)]^{(b)})t] \right]^{k} \\
&= 0.979 \left[\sum_{\upsilon=0}^{6} \frac{[(0.3492/[c(1)]^{(1)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.3492/[c(1)]^{(1)})t] \right]^{18} \\
&\quad + 0.0064 \left[\sum_{\upsilon=0}^{6} \frac{[(0.5688/[c(1)]^{(2)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.5688/[c(1)]^{(2)})t] \right]^{6} \\
&\quad + 0.0065 \left[\sum_{\upsilon=0}^{6} \frac{[(0.5688/[c(1)]^{(3)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.5688/[c(1)]^{(3)})t] \right]^{6} \\
&\quad + 0.0009 \left[\sum_{\upsilon=0}^{6} \frac{[(0.63/[c(1)]^{(5)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.63/[c(1)]^{(5)})t] \right]^{12} \\
&\quad + 0.0042 \left[\sum_{\upsilon=0}^{6} \frac{[(0.63/[c(1)]^{(7)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.63/[c(1)]^{(7)})t] \right]^{12} \\
&\quad + 0.003 \left[\sum_{\upsilon=0}^{6} \frac{[(0.774/[c(1)]^{(8)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.774/[c(1)]^{(8)})t] \right]^{18}, \; t \geq 0,
\end{aligned} \tag{21}$$

$$\begin{aligned}
\boldsymbol{R}(t,2) &\cong \sum_{b=1}^{v} p_b \left[\sum_{\upsilon=0}^{l-m} \frac{[(l[\lambda(2)]^{(b)}/[c(2)]^{(b)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(l[\lambda(2)]^{(b)}/[c(2)]^{(b)})t] \right]^{k} \\
&= 0.979 \left[\sum_{\upsilon=0}^{6} \frac{[(0.5292/[c(2)]^{(1)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.5292/[c(2)]^{(1)})t] \right]^{18} \\
&\quad + 0.0064 \left[\sum_{\upsilon=0}^{6} \frac{[(0.846/[c(2)]^{(2)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.846/[c(2)]^{(2)})t] \right]^{6} \\
&\quad + 0.0065 \left[\sum_{\upsilon=0}^{6} \frac{[(0.846/[c(2)]^{(3)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(0.846/[c(2)]^{(3)})t] \right]^{6} \\
&\quad + 0.0009 \left[\sum_{\upsilon=0}^{6} \frac{[(1.2996/[c(2)]^{(5)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.2996/[c(2)]^{(5)})t] \right]^{12} \\
&\quad + 0.0042 \left[\sum_{\upsilon=0}^{6} \frac{[(1.2996/[c(2)]^{(7)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.2996/[c(2)]^{(7)})t] \right]^{12} \\
&\quad + 0.003 \left[\sum_{\upsilon=0}^{6} \frac{[(1.4184/[c(2)]^{(8)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.4184/[c(2)]^{(8)})t] \right]^{18}, \; t \geq 0,
\end{aligned} \tag{22}$$

$$\begin{aligned}
\boldsymbol{R}(t,3) &\cong \sum_{b=1}^{v} p_b \left[\sum_{\upsilon=0}^{l-m} \frac{[(l[\lambda(3)]^{(b)}/[c(3)]^{(b)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(l[\lambda(3)]^{(b)}/[c(3)]^{(b)})t] \right]^{k} \\
&= 0.979 \left[\sum_{\upsilon=0}^{6} \frac{[(1.0008/[c(3)]^{(1)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.0008/[c(3)]^{(1)})t] \right]^{18} \\
&\quad + 0.0064 \left[\sum_{\upsilon=0}^{6} \frac{[(1.3968/[c(3)]^{(2)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.3968/[c(3)]^{(2)})t] \right]^{6} \\
&\quad + 0.0065 \left[\sum_{\upsilon=0}^{6} \frac{[(1.3968/[c(3)]^{(3)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.3968/[c(3)]^{(3)})t] \right]^{6} \\
&\quad + 0.0009 \left[\sum_{\upsilon=0}^{6} \frac{[(1.9836/[c(3)]^{(5)})t]^{\upsilon}}{\upsilon!} \cdot \exp[-(1.9836/[c(3)]^{(5)})t] \right]^{12}
\end{aligned}$$

$$+ 0.0042\left[\sum_{\upsilon=0}^{6}\frac{[(1.9836/[c(3)]^{(7)})t]^{\upsilon}}{\upsilon!}\cdot\exp[-(1.9836/[c(3)]^{(7)})t]\right]^{12}$$

$$+ 0.003\left[\sum_{\upsilon=0}^{6}\frac{[(2.1852/[c(3)]^{(8)})t]^{\upsilon}}{\upsilon!}\cdot\exp[-(2.1852/[c(3)]^{(8)})t]\right]^{18}\quad t\geq 0, \tag{23}$$

Approximate graphs of coordinates of the complex system reliability function are presented in Figure 2.

The expected values and standard deviations of the shipyard rope transportation system unconditional lifetimes in the reliability state subsets {1,2,3}, {2,3}, {3}, calculated from results given by (20)–(23), according to formula given in (Soszyńska 2007), for $[c(u)]^{(b)} = 1$, $u = 1,2,3$, $b = 1, \ldots, 8$, respectively are:

$$\mu(1) = \sum_{i=1}^{8} p_i \mu_i(1) \cong 8.7945, \sigma(1) \cong 2.2375 \text{ years}, \tag{24}$$

$$\mu(2) = \sum_{i=1}^{8} p_i \mu_i(2) \cong 5.7981, \sigma(2) \cong 1.4870 \text{ years}, \tag{25}$$

$$\mu(3) = \sum_{i=1}^{8} p_i \mu_i(3) \cong 3.0731, \sigma(3) \cong 0.7804 \text{ years}. \tag{26}$$

and further, considering (24)–(26), the mean values of unconditional lifetimes in particular reliability states 1, 2, 3, (Soszyńska 2007) for $[c(u)]^{(b)} = 1$, $u = 1, 2, 3$, $b = 1, \ldots, 8$, respectively are:

$$\begin{aligned}\bar{\mu}(1) &= \mu(1) - \mu(2) = 2.9964,\\ \bar{\mu}(2) &= \mu(2) - \mu(3) = 2.725,\\ \bar{\mu}(3) &= \mu(3) = 3.0731 \text{ years}.\end{aligned} \tag{27}$$

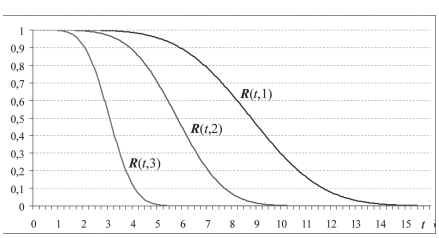


Figure 2. The graph of coordinates of the ground shiprope transporter reliability function $\boldsymbol{R}(t,\cdot)$ for $[c(u)]^{(b)} = 1$, $u = 1,2,3$, $b = 1, \ldots, 8$.

Since the critical reliability state is $r = 2$, then the system risk function, according to definition presented in (Kołowrocki 2004), is given by

$$\boldsymbol{r}(t) = 1 - \boldsymbol{R}(t,2)$$

where coordinate of the system unconditional reliability function $\boldsymbol{R}(t,2)$ is given by (22).

Hence, the moment when the system risk function exceeds a permitted level, for instance $\delta = 0.05$, for $[c(2)]^{(b)} = 1$, $b = 1, \ldots, 8$, is:

$$\tau = \boldsymbol{r}^{-1}(\delta) \cong 3.35 \text{ years} \cong 3 \text{ years } 128 \text{ days}. \tag{28}$$

Assuming different values of component stress proportionality correction coefficients $[c(u)]^{(b)}$, $u = 1, 2, 3$, $b = 1, \ldots, 8$, at variable operation conditions we can observe changes of expected values and standard deviations of the shipyard rope transportation system unconditional lifetimes in the reliability state subsets {1,2,3}, {2,3}, {3}. In case:

$$\begin{aligned}&[c(1)]^{(1)} = 1.0, [c(1)]^{(b)} = 0.7, b = 2,3,4,\\ &[c(1)]^{(b)} = 0.4, b = 5,6,7, [c(1)]^{(8)} = 0.2,\end{aligned} \tag{29}$$

$$\begin{aligned}&[c(2)]^{(1)} = 1.0, [c(2)]^{(b)} = 0.7, b = 2,3,4,\\ &[c(2)]^{(b)} = 0.4, b = 5,6,7, [c(2)]^{(8)} = 0.3,\end{aligned} \tag{30}$$

$$\begin{aligned}&[c(3)]^{(1)} = 0.9, [c(3)]^{(b)} = 0.8, b = 2,3,4,\\ &[c(3)]^{(b)} = 0.5, b = 5,6,7, [c(3)]^{(8)} = 0.4,\end{aligned} \tag{31}$$

we obtain following values:

$$\begin{aligned}&\mu(1) \cong 8.7409, \mu(2) \cong 5.7671, \mu(3) \cong 2.7565 \text{ years},\\ &\sigma(1) \cong 2.3251, \sigma(2) \cong 1.5373, \sigma(3) \cong 0.7156 \text{ years}.\end{aligned}$$

For following values of component stress proportionality correction coefficients:

$$\begin{aligned}&[c(1)]^{(1)} = 0.9, [c(1)]^{(b)} = 0.7, b = 2,3,4,\\ &[c(1)]^{(b)} = 0.4, b = 5,6,7, [c(1)]^{(8)} = 0.2,\end{aligned} \tag{32}$$

$$\begin{aligned}&[c(2)]^{(1)} = 0.9, [c(2)]^{(b)} = 0.7, b = 2,3,4,\\ &[c(2)]^{(b)} = 0.4, b = 5,6,7, [c(2)]^{(8)} = 0.3,\end{aligned} \tag{33}$$

$$\begin{aligned}&[c(3)]^{(1)} = 0.9, [c(3)]^{(b)} = 0.7, b = 2,3,4,\\ &[c(3)]^{(b)} = 0.5, b = 5,6,7, [c(3)]^{(8)} = 0.3,\end{aligned} \tag{34}$$

we obtain expected values and standard deviations:

$$\begin{aligned}&\mu(1) \cong 7.8746, \mu(2) \cong 5.1954, \mu(3) \cong 2.7523 \text{ years},\\ &\sigma(1) \cong 2.0802, \sigma(2) \cong 1.3758, \sigma(3) \cong 0.7190 \text{ years}.\end{aligned}$$

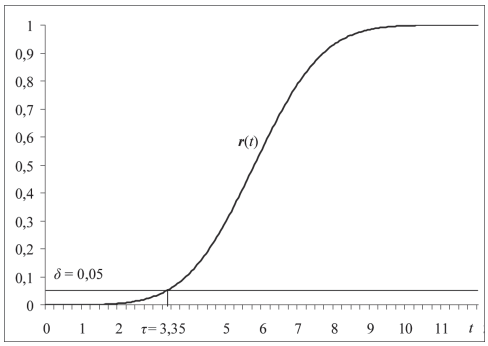


Figure 3. The graph of the ground ship-rope transporter risk function $\boldsymbol{r}(t)$ for $[c(2)]^{(b)} = 1$, $b = 1, \ldots, 8$.

Then the moment when the system risk function exceeds a permitted level $\delta = 0.05$, for values of component stress proportionality correction coefficients given by (29)–(31), is:

$$\tau = \boldsymbol{r}^{-1}(\delta) \cong 3.267 \text{ years} \cong 3 \text{ years } 97 \text{ days}$$

and for values of component stress proportionality correction coefficients given by (32)–(34), equivalently:

$$\tau = \boldsymbol{r}^{-1}(\delta) \cong 2.965 \text{ years} \cong 2 \text{ years } 352 \text{ days}.$$

4 CONCLUSIONS

Many technical systems belong to the class of complex systems as a result of large number of interacting components and subsystems they are built of and their complicated operating processes having significant influence on their reliability. In the paper we present an analytical model of reliability analysis of complex systems and their reliability characteristics evaluation considering the influence of the inside-system and outside-system dependencies. The multi-state reliability function of homogeneous multi-state "*m* out of *n*" and "*m* out of *l*"-series systems are determined in case when the systems' components have exponential reliability functions with interdependent departures rates from the subsets of their reliability states.

The ship-rope transporter is analyzed at variable operation conditions and its changing in time reliability structure, its components' reliability parameters and among its components dependability are considered. The influence of changing at operation states intensities of departure from the reliability state subset, as well as components' stress proportionality correction coefficients on mean values and standard deviations of the ship-rope transporter unconditional lifetimes states is investigated. Obtained results illustrate that after decreasing the reliability state by some of components, the inside interactions among remaining components may cause further components reliability states decrease.

REFERENCES

Blokus-Roszkowska, A., 2007a. On component failures' dependency influence on system's lifetime. *Int J of Reliab, Quality and Safety Eng. Special Issue: System Reliability and Safety,* 14(6): 1–19.

Blokus-Roszkowska, A., 2007b. *Reliability analysis of homogenous large systems with component dependent failures*. PhD Thesis, Gdynia Maritime University—System Research Institute Warsaw (*in Polish*).

Blokus-Roszkowska, A. & Kołowrocki, K., 2009a. Reliability and availability of a ground ship-rope transporter in variable operation conditions. *Electronic Journal of Reliability & Risk Analysis: Theory & Application,* 2(4): 82–96.

Blokus-Roszkowska, A. & Kołowrocki, K., 2009b. Reliability and risk analysis of a ground ship-rope transporter in variable operation conditions. *Proc. European Safety and Reliability Conference—ESREL 2009*, Czech Republic, Prague: 1643–1648.

Grabski, F., 2002. *Semi-Markov Models of Systems Reliability and Operations Analysis*. System Research Institute, Polish Academy of Science (*in Polish*).

Kołowrocki, K. 2014. *Reliability of Large and Complex Systems*. Elsevier.

Kołowrocki, K., 2013. On safety of critical infrastructures. *Journal of Polish Safety and reliability Association, Summer Safety and Reliability Seminars*, 4(1): 51–72.

Kołowrocki, K. & Soszyńska-Budny, J., 2011. *Reliability and Safety of Complex Technical Systems and Processes: Modeling—Identification—Prediction—Optimization*. Springer.

Limnios, N. & Oprisan, G., 2005. *Semi-Markov Processes and Reliability*. Birkhauser: Boston.

Pradhan, S. & Chakrabarti, Bikas K., 2003. Failure properties of fiber bundles. *Int. J. Mod. Phys. B,* 17: 5565.

Pradhan, S. & Hansen, A., 2005. Failure properties of fiber bundle model having lower cutoff in fiber threshold distribution. *Phys. Rev. E.,* 72: 026111.

Soszyńska, J., 2007. *Systems reliability analysis in variable operation conditions.* PhD Thesis, Gdynia Maritime University-System Research Institute Warsaw (*in Polish*).

Xue, J., 1985. On multi-state system analysis. *IEEE Trans on Reliab.,* 34: 329–337.

Xue, J. & Yang, K., 1995. Dynamic reliability analysis of coherent multi-state systems. *IEEE Trans on Reliab.,* 4(44): 683–688.

Xue, J. & Yang, K., 1995. Symmetric relations in multi-state systems. *IEEE Trans on Reliab.,* 4(44): 689–693.

Yu, K., Koren, I. & Guo, Y., 1994. Generalised multistate monotone coherent systems. *IEEE Trans on Reliab.,* 43: 242–250.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Maritime traffic flow simulation in the Intelligent Transportation Systems theme

A. Blokus-Roszkowska & L. Smolarek
Maritime University, Gdynia, Poland

ABSTRACT: The paper proposes safety analysis of waterways' crossings in restricted area using simulation and describes maritime traffic phenomena with application of cellular automata. There is presented a cellular automaton model with introduced rules of vessels movement and collision avoidance manoeuvre. This model is able to describe different types of vessels evolving different type of intersections and provides the basis for simulation. In simulation there is considered simple crossing with distinguished main flow having priority and a roundabout with three different priority scenarios. As a result of simulation there are given probabilities of transitions between system safety states and probabilities of system's being in particular safety states during simulation time. Analysis and comparison of simulation results for various crossing's geometry and priority traffic schemes can potentially affect the tasks and decisions of authorities related to maritime transport and traffic in area with developed vessel traffic management including vessel traffic services.

1 INTRODUCTION

Permanent development of transportation systems and its infrastructure has influence on increasing demand on Vessel Traffic Management and Information Systems to improve safety and effectiveness of maritime transportation. Intelligent Transport Systems (ITS), using a range of information and communication technologies, can face problems associated with maritime traffic management and safety improvement (Perera et al. 2012, Pietrzykowski 2011). One of maritime safety tasks is to reduce the risk of collisions at waterways' crossings. In this paper there is presented simulation approach to this topic with application of cellular automaton model.

Using mathematical models we can simulate real-life situations. In this paper a cellular automaton model is applied to simulate maritime traffic at waterways' crossing in VTS (Vessel Traffic Services) area. With simulation model representing both vessels and waterway organization it is possible to analyze the effects of changing waterway priority, vessel type and human behaviour. Vessels are classified by their type, departure port and destination (input and output flow). Each type of vessel is characterized by its velocity, size, acceleration, maneuverability, probability of taking evasive action. With development and improvement of models reproducing maritime traffic features including waterways, vessels and humans we can simulate and plan more efficient ITS systems. Simulation models can support analysis and understanding of likely impacts and effects of some maritime traffic features. Thus ITS can be applied in the domain of transport to improve system performance, transport safety and efficiency (Jamroz & Krystek 2006, Wibowo & Deng 2012).

2 A CELLULAR AUTOMATON MODEL FOR MARITIME TRAFFIC

This paper presents cellular approach to analysis of influence of maritime traffic organization on the collision risk. Cellular automata are often applied to road traffic simulation and are very useful in emulating priority rules of the road are supposed to work in traffic (Maerivoet & De Moor 2005, Wolfram 1986), especially in a roundabout (Chen et al. 2006). However, this approach has not been used for describing vessels motion. The problem of traffic simulation in an intersection can be solved by multi-agent system approach (Doniec et al. 2008). Specifically, a multi-agent model using priority relations allows for simulating traffic at road junction for different priority scenarios. Then, agents approaching an intersection coordinate their actions in order to avoid collision. Similar approach is presented in this paper to describe vessel dynamic and behavior at waterways' crossing including various priority scenarios at restricted area. Detailed analysis of simulation results for different traffic schemes can be effectively used in

evaluation of maritime traffic organization and optimization at waterways in VTS area.

As we focus on simulation of waterways' crossing, we do not consider overtaking rule. The rule of vessel movement is introduced and a set of rules is applied to provide collision avoidance manoeuvre.

2.1 *Movement rule*

To describe main features of maritime traffic we use Nagel-Schreckenberg model with some modifications (Nagel & Schreckenberg 1992). Vessels usually move with constant velocity, thus we can adapt to our model following modification of movement rule:

$$x_i^{(t+\Delta t)} = x_i^{(t)} + v_i \,, \tag{1}$$

if ith vessel is not performing an avoidance manoeuvre, where $x_i^{(t)}$ is the position of ith vessel at time t, $t \geq 0$, v_i is velocity of ith vessel and Δt is a time step.

Velocity of a vessel does not depend on parameter t as we assume that in considered distance of lanes' crossing vessels move with constant velocity. However we can consider extension of presented model by taking into account speed interval for each type of vessel and observing some speed alteration while vessel movement with assumed a priori lower and upper bound.

2.2 *Collision avoidance rules*

As a next step, we add to our model collision avoidance rule. In maritime traffic the distance between vessels being on collision courses (the number of empty cells between two vessels) must be known in order to perform collision avoidance manoeuvre. The necessary distance to take evasive action depends on vessel size, velocity and maneuverability. Thus, for vessels performing an avoidance manoeuvre we can implement some collision avoidance rules depending on vessel size, velocity, type (maneuverability) and distance to lanes' crossing.

A collision avoidance manoeuvre should be preceded by starting evasive action rule that determine whether a vessel starts collision avoidance manoeuvre taking into account distance between vessels and probability of taking evasive action by give-way and stand-on vessel.

Starting evasive action rule:

(if the vessel is on collision course) and (distance between vessels $d < 3704$ m) and ($rand < p_{EA}$) then (start evasive action),

where p_{EA} denotes probability of taking evasive action by the vessel and *rand* is a variable with generated random positive decimal value that ranges between 0.0 and 1.0. The third condition in this rule means that taking evasive action occurs randomly with assumed probability p_{EA}, even if the first two conditions are met.

Described in this paper rules can be applied for all vessels, however for different type of vessels rules are used with different parameters affecting probability of taking evasive action, time of performing collision avoidance manoeuvre as well as velocity in movement rule. Another factor that influence the decision of taking evasive action and its performance is vessel priority.

The decision of taking collision avoidance manoeuvre by the vessel i.e. determining probability p_{EA}, can be described by following rule:

if (the vessel is a give-way vessel)
  if ($d \geq 2$ nm) then $p_{EA} = 0$
    else if ($d \geq d_3$) then $p_{EA} = 0.5 p_{EA_GW}$
    else if ($d \geq d_1$) then $p_{EA} = p_{EA_GW}$
    else ($d < d_1$) there is a collision
if (the vessel is a stand-on vessel)
  if ($d \geq d_3$) then $p_{EA} = 0$
    else if ($d \geq d_2$) then $p_{EA} = p_{EA_SO}$
    else if ($d \geq d_1$) then
      $p_{EA} = 2p_{EA_SO}$ if $p_{EA_SO} < 0.5$
      $p_{EA} = 1$ if $p_{EA_SO} \geq 0.5$
    else ($d < d_1$) there is a collision

where p_{EA_GW} denotes probability of taking evasive action by give-way vessel and p_{EA_SO} by stand-on vessel, respectively. These probabilities can be assumed a priori (as a value or interval) for different type of vessels depending on their size, velocity, maneuverability. In simulation we randomly choose from fixed interval the probability p_{EA_GW} and p_{EA_SO} on basis of modelling of vessel behaviour presented in (Chauvin & Lardjane 2008).

We assume a navigator during encountered crossing situation perform collision avoidance manoeuvre in a proper way at safe distance without deceleration and a vessel while taking evasive action is safe and can not cause collision with other vessels on its scheduled destination waterway. We distinguish two types of collision avoidance rule:

I case—a collision avoidance rule by changing vessel velocity (vessel acceleration),
II case—a collision avoidance rule by changing vessel course.

In simulation program we consider eight major ship types. The simulation is carried out with randomly generated initial configuration on vessel parameters and behaviour (vessels type, size and velocity, maneuverability, probability of taking evasive action). For each class of vessels these data are taken into model with different conditions and initial values. Further, we divide ship types into two groups with respect to model of collision

avoidance group. Some types of vessels can reach much higher velocities than limit value in restricted area and in collision situation they can speed up to 20 knots i.e. 10 m/s, in case of fast ferry can reach speed even over 30 knots i.e. 15 m/s. These vessels constitute first group: a container carrier, a RoPax, a passenger ship, a reefer and a fast ferry. The second group of vessels is made by a tanker, a bulk carrier and a general cargo ship.

Collision avoidance rule in first case takes form:

if (vessel_type is container carrier or RoPax or passenger ship or reefer or fast ferry) and ($v_i < 8$ m/s) and ($d_{EA} > 556$ m) then

$$x_i^{(t+\Delta t)} = x_i^{(t)} + v_{i_A}, \tag{2}$$

where v_{i_A} is velocity of a vessel after acceleration and d_{EA} denotes minimal distance between target vessel and collision point in a moment home ship leaves waterways' crossing and can be estimated from formula:

$$d_{EA} = d_{C_other} - \frac{d_C + LOA_i}{v_{i_A}} \cdot v_{i_other} \tag{3}$$

where:
v_{i_other}—velocity of a vessel being on collision course,
LOA_i—length of home ship,
d_c—distance between home ship and collision point,
d_{C_other}—distance to collision point on a route of target ship.

Time during that vessels move with higher speed t_A can be estimated from formula:

$$t_A = \frac{d_c - \frac{1}{6}v_i}{v_i + 4} \tag{4}$$

and time to reach collision point by target ship t_{C_other} is counted from formula:

$$t_{C_other} = \frac{d_{C_other} - d_T}{v_{i_other}}, \; d_T = \max\{370\ m; 2LOA_{other}\}, \tag{5}$$

where LOA_{other} denotes length of target vessel.

Following rule defines when collision avoidance manoeuvre by vessels acceleration can be used.

$$\text{If } ((t_A + 600s) < t_{C_other}) \text{ then} \tag{6}$$

(it is possible to avoid collision by vessel acceleration assuming that after a period of time equal 10 minutes a vessel will accelerate about 2 m/s) else (a vessel should perform collision avoidance manoeuvre by course changing).

Taking into account that any change of vessel velocity takes time and do not influence on distance between vessels significantly, a collision avoidance manoeuvre by vessel acceleration can be performed in larger distance from collision point. What is more, as this procedure is not recommended as navigation rule is rarely used. In simulation program we assume that collision avoidance manoeuvre by vessel acceleration is used in less than 10% cases (with probability under 10%) assuming that condition (6) holds and distance of a vessel to collision point is larger than 3704 m.

As in our model we focus on safety analysis of waterways' crossing the exact trajectory of a vessel does not play a key role, and we are only interested in the moment when the vessel is at the point of collision. Some deviations from the vessel trajectory and drift angle affecting the time to reach the waterways' crossing can be included i.e. simulated by generating the velocity from a fixed interval instead of adopting a constant velocity of a vessel. Similarly, in second model of collision avoidance rule we can assume it is not important the exact vessel collision avoidance manoeuvre trajectory but time of performing evasive action and place where the vessel will be after ending collision avoidance manoeuvre. Considering this we can implement following rule for collision avoidance manoeuvre:

$$x_i^{(t+\Delta t)} = x_i^{(t)} + v_{i_EA}, \tag{7}$$

if ith vessel is performing avoidance manoeuvre,

where v_{i_EA} is vessel velocity, if a vessel would move on scheduled route during time equivalent to time of performing collision avoidance manoeuvre, moving on collision avoidance route with velocity v_i. We assume a ship is performing turning motion moving at constant speed and at constant rudder angle. Vessel velocity is expressed in cells per time step Δt. Then the velocity v_{i_EA} can be determined by the formula:

$$v_{i_EA} = \frac{S_{i_EA} \cdot \Delta t}{T_{i_EA} \cdot CS \cdot 60}, \tag{8}$$

where S_{i_EA} denotes a distance on scheduled course line during performing collision avoidance manoeuvre expressed in m, T_{i_EA} is time of performing collision avoidance manoeuvre expressed in minutes and CS denotes a cell size in m.

For simulation simplification, we assume time of navigational restore is equal to time of collision avoidance (Fig. 1). Under assumption that vessels move with constant speed and at constant turning angle, we can also assume that a dis-

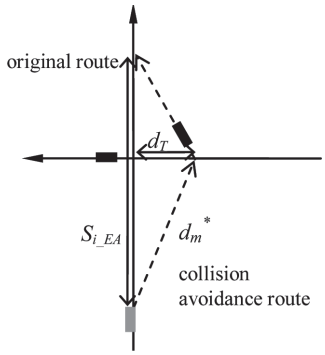


Figure 1. Navigational restore manoeuvre.

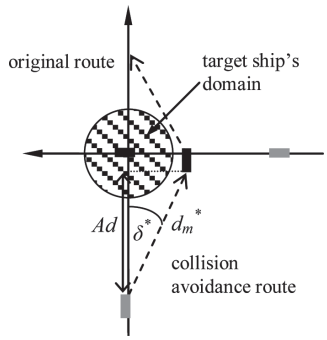


Figure 2. Collision avoidance manoeuvre including constraints.

tance from the beginning of turning to restoring is equal to a distance of restoring of scheduled course line (to the end of collision avoidance manoeuvre).

We have $S_{i_EA} = 2Ad$, where the advance for performed manoeuvre can by counted from:

$$Ad = d_m^* \cdot \cos\delta^*, \tag{9}$$

and

$$T_{i_EA} = 2t_m^*, \tag{10}$$

where d_m* is a distance after collision avoidance before starting navigational restore and t_m* is navigational time after collision avoidance i.e. time of evasive action not including time of navigational restore. A turning angle δ* (Fig. 2) allows to determine required advance for collision avoidance in order to avoid entering target ship domain (Fujii & Tanaka 1971).

Further, taking into account constraints for turning angle δ* we assume staring rudder angle δ_0 for example $\delta_0 = 10°$ or $\delta_0 = 5°$ in case a vessel starts evasive action in long distance from collision point. This rudder angle must be verified by real situation and the upper bound of turning angle. In (Su et al. 2012) authors assume that the shortest required advance to prevent a collision and perform turning motion can be obtain for full rudder equal to 35°. However full rudder angle 35° is practiced only for slowly moved unit with speed around 3 m/s or in extremely dangerous collision situation. This is caused by the fact that vessels during course changing over 10° lose their velocities. In presented simulation model, we assume the upper bound of turning angle depending on vessel type and its manoeuvring characteristics. We denote it by $\delta_{full}^{(c)}$ for each of vessel class c. In case a distance between home ship and collision point is short, it could be required larger rudder angle δ than δ_0. Then, real turning angle δ* can be defined by:

$$\delta^* = \min\left\{\max\left\{\delta_0;\delta\right\};\delta_{full}^{(c)}\right\}, \tag{11}$$

where rudder angle δ is determined form the condition not to cross target vessel domain and taking into account experts' opinion that a vessel usually passes target vessel in a distance not shorter than 2 cables (370 m) in restricted area:

$$\delta = \arcsin\frac{d_T}{d_m^*},\ d_T = \max\left\{370m;\ 2LOA_{other}\right\}. \tag{12}$$

As shown in Figure 3, the distance d_m after collision avoidance before starting navigational restore (before taking into account constraint conditions) can be determined as:

$$d_m = \frac{d_C}{\cos\delta_0}, \tag{13}$$

where d_c is a distance between home ship and collision point and δ_0 denotes starting rudder angle.

By t_{C_max} we denote maximum time to reach collision point by target ship:

$$t_{C_\max} = \frac{d_{C_other}}{v_{\min_other}}, \tag{14}$$

where v_{min_other} is minimum velocity of target ship.

Further, the distance d_m* after collision avoidance before starting navigational restore can by given by:

$$d_m^* = t_m^* \cdot v_i. \tag{15}$$

Including constraint conditions, presented in (Tsou & Hsueh 2010), time after collision avoidance

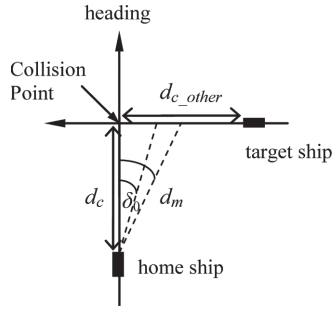


Figure 3. Starting position of evasive action.

and navigational restore time should not exceed 60 minutes and should be at least larger than time of closest point of approach. Then, we can determine navigational time after collision avoidance t_m* by formula:

$$t_m^* = \min\left\{\max\left\{\frac{d_m}{v_i}, t_{C_\max}\right\}, 3600s\right\}. \quad (16)$$

Time of taking evasive action can be also affected by many other factors including ship type and basic manoeuvring performance characteristics. Then, we can modify formula (16) to make it more realistic by:

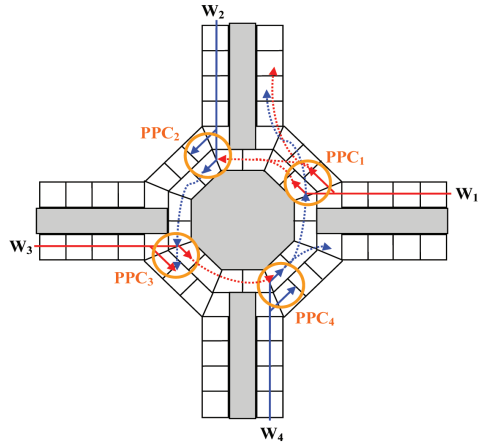
$$t_m^* = \min\left\{\max\left\{\frac{d_m}{v_i} + t_{RA}, t_{C_\max}\right\}, 3600s\right\}, \quad (17)$$

where t_{RA} is time required for a ship to turn its heading by rudder angle. Maneuverability of a ship can be expressed by measures such as Turning Ability, Initial Turning Ability, Course Changing and Yaw Checking Ability. Details for these measures and rating system taking into account requirements of the IMO standards can be found in (ABS Guide 2006).

3 SIMULATION RESULTS AND ITS ANALYSIS

3.1 *Crossing's situation*

In simulation we consider simple crossing and a roundabout as a junction of four routes with four point of potential collision (Fig. 4). We assume traffic lanes 1 and 3 are main routes on that there are usually large vessels with less maneuverability. The vessels are observed in lanes entering the roundabout-lane with a distance 4 nautical mile and we assume distances between collision points



W_1, W_2, W_3, W_4 – enter lines for roundabout

PPC_1, PPC_2, PPC_3, PPC_4 – Potential Points of Collision

Figure 4. The scheme of grade roundabout crossing.

are equal to 1 nautical mile i.e. 1852 m. A crossing's geometry for considered situation is widely described in (Blokus-Roszkowska & Smolarek 2012a, 2013).

In maritime traffic scenario with a roundabout we consider three different priority scenarios (Blokus-Roszkowska & Smolarek 2012b). First case, when a vessel having another vessel on her own starboard side shall keep out of the way. Second scenario, when a vessel being on a roundabout-lane has priority and a vessel entering a roundabout crossing is directed to keep out of the way. And third case—a roundabout with distinguished main flow having priority. Then, we assume that traffic lanes 1 and 3 are main routs with stand-on vessels and on routs 2 and 4 moves give-way vessels that should keep out of the way of vessels being on routs 1 and 3.

According to the rule 15, in case of risk collision during crossing situation, the vessel which has another vessel on her own starboard side shall keep out of the way and shall avoid crossing ahead of another vessel. However, considering roundabout crossing, we distinguish some situation when the vessel being on the roundabout-lane has priority. When the vessel on the roundabout is very large and with less maneuverability we assume it has priority and the vessel entering roundabout crossing is directed to keep out of the way of vessel being on the roundabout-lane. Considered priority scenarios and performed traffic simulation at waterways' crossing are not devoted to change rules on the level of vessel navigation. They can be applied during creating concepts of maritime traffic organization and management in restricted area.

3.2 *Assumptions and simulation results*

We take into consideration following four states corresponding to risk levels depending on mutual distance of vessels that are on collision courses in restricted area:

– state 3 (negligible risk of collision)—both ships being in cells are in safety distance defined in simulation program as 1852 m, i.e. the number of cells between two ships being in state 3 is equal at least d_3, determined from the formula:

$$d_3 = \left\lceil \frac{1852}{CS} \right\rceil, \tag{18}$$

where $\lceil d \rceil$ denotes the smallest integer number not lower than d and CS is a cell size depending on flow intensities, velocities and lengths of vessels (Blokus-Roszkowska & Smolarek 2013);

– state 2 (low risk of collision)—both ships being in cells are in a distance of passing clear, assumed to be equal to 926 m; it means that the number of cells between two ships being in state 2 is equal at least d_2, were d_2 is given by the formula:

$$d_2 = \left\lceil \frac{926}{CS} \right\rceil; \tag{19}$$

– state 1 (high risk of collision)—both ships being on collision courses are in cells in a distance concerned with their lengths and number of cells between two ships being in state 1 is equal at least d_1, where d_1 is defined by the formula:

$$d_1 = \left\lceil \frac{2LOA_{\max}}{CS} \right\rceil, \tag{20}$$

where $LOA_{max} = \max\{LOA_M, LOA_L\}$ and LOA_M is a length of a vessel moving on main waterway, LOA_L is a length of a vessel being on collision lateral waterway;

– state 0 (collision alert)—the number of cells between two ships being in state 0 is lower than d_1 defined by (20).

In simulation we compare time to point of collision expressed in time steps. If time of vessels being on collision courses is shorten than time of vessels reaching collision point and none of vessels take evasive action at this moment, we check the distance between vessels. Then, we compare obtained distance with the threshold values of safety states defined before and according to this definition we assign the proper state of the vessel. If the vessel status state has changed, this information is saved along with time after that transition has occurred, i.e. time during which ship was in the previous safety state.

Simulation run under various crossing's geometric conditions for fixed, on the basis of results presented in (Montewka et al. 2010) and (Blokus-Roszkowska et al. 2012), traffic flow parameters. For the simulation, we assume starting times of vessels on main waterway follow normal distribution with mean value 2.21 h and standard deviation 0.52 h. On lateral waterways we assume Erlang distribution with mean time between ships departing equal to 1.21 h and standard deviation 0.95 h and 1.03 h, equivalently for both directions. Following these, numbers of system's transitions between the states, obtained during simulation time equivalent to four months of real time, are derived for introduced three different models of priority in a roundabout.

I scenario—a vessel having another vessel on her own starboard side shall keep out of the way.

Matrix of transitions' numbers between states is the following:

$$[n_{ij}]^I = \begin{bmatrix} 0 & 0 & 1 & 33 \\ 32 & 0 & 1 & 89 \\ 0 & 110 & 0 & 747 \\ 2 & 12 & 855 & 0 \end{bmatrix}, \; i, j = 0, 1, 2, 3, \tag{21}$$

and the vector of total numbers of transitions from each state:

$$[n_0, n_1, n_2, n_3]^I = [34, 122, 857, 869].$$

On the basis of obtained form simulation program number of system's transitions between states (21) we can estimate the matrix of transitions' probabilities:

$$[p_{ij}]^I = \begin{bmatrix} 0 & 0 & 0.0294 & 0.9706 \\ 0.2623 & 0 & 0.0082 & 0.7295 \\ 0 & 0.1284 & 0 & 0.8716 \\ 0.0023 & 0.0138 & 0.9839 & 0 \end{bmatrix}, \tag{22}$$

$$i, j = 0, 1, 2, 3.$$

Analysing probabilities of transitions between states (22) we can conclude that the most of observed transition during simulation time is from ship safety state 3 (negligible risk of collision) to safety state 2 (low risk of collision) and from state 2 to state 3. This relationship can be observed in all cases. Quite frequent are also transitions from state 2 to state 1 (high risk of collision). From state 1 transitions the most often appeared to state 3. This could be caused by the fact that in a situation of high risk of collision both vessels i.e. stand-on and give-way vessels take evasive action with high

probability. However, there are situations in which vessels did not take evasive action and transitions form state 1 to state 0 occurred.

Simulation requires modeling of human behaviour, namely the reaction to information that represents the choice between different alternatives. In this paper, we assume a priori probability of taking evasive action by give-way and stand-on vessels according to modeling of vessel behaviour conducted in (Chauvin & Lardjane 2008, Blokus-Roszkowska & Smolarek 2013). This probability is randomly chosen from fixed interval depending on vessel type and velocity in case it is stand-on and give-way vessel. Taking into account results of simulation, the probability of taking action by give-way and stand-on vessels should be verified a posteriori by real data. We assume that in case the risk of collision is negligible, give-way vessel will take evasive action with probability $0.5p_{EA_GW}$, otherwise with probability p_{EA_GW}. In case the risk of collision is high, we assume stand-on vessel will start evasive action with higher probability than mentioned before i.e. $2p_{EA_SO}$ if $p_{EA_SO} < 0.5$ and 1 if $p_{EA_SO} \geq 0.5$, otherwise with probability p_{EA_SO}. Figure 5 illustrates the behaviour of stand-on and give-way vessel in terms of manoeuvring.

From simulation we also obtain realizations of conditional sojourn times at the state until transition to another state. From these results there is determined a vector of probabilities of system's being in particular states during simulation time. Namely, from simulation there are given both probabilities of ship collision alert and probabilities of occurrence high, low or negligible risk of collision. Figure 6 presents the output window showing the results of simulation, i.e. probabilities of vessels being in safety states, in a bar chart. In first scenario of priority, these probabilities are as follows (Fig. 6):

$$p(0) = 0.0001,\ p(1) = 0.0006,$$
$$p(2) = 0.0171,\ p(3) = 0.9822.$$

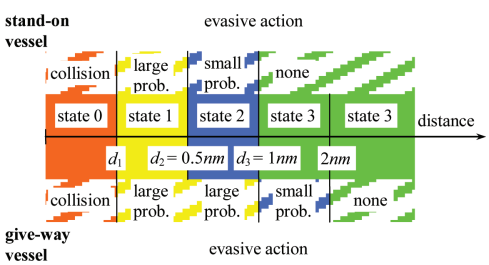


Figure 5. The probability of taking evasive action by give-way and stand-on vessels in restricted area assumed in simulation.

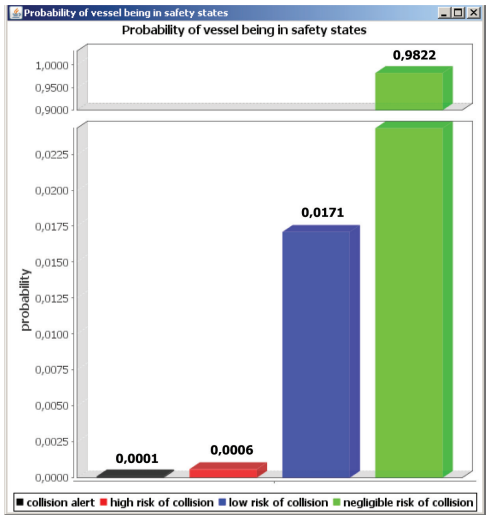


Figure 6. Probability of vessels being in safety states obtained from simulation for a roundabout with I priority scenario.

II scenario—a vessel being on a roundabout-lane has priority and vessel entering roundabout crossing is directed to keep out of the way. In this scenario of traffic organization the matrix of transitions' numbers between states takes form:

$$[n_{ij}]^{II} = \begin{bmatrix} 0 & 0 & 2 & 52 \\ 52 & 0 & 2 & 71 \\ 1 & 118 & 0 & 731 \\ 1 & 7 & 846 & 0 \end{bmatrix},\ i,\ j = 0, 1, 2, 3, \quad (23)$$

and the vector of total numbers of transitions:

$$[n_0, n_1, n_2, n_3]^{II} = [54, 125, 850, 854].$$

Then, the matrix of transitions' probabilities is:

$$[p_{ij}]^{II} = \begin{bmatrix} 0 & 0 & 0.0370 & 0.9630 \\ 0.4160 & 0 & 0.0160 & 0.5680 \\ 0.0012 & 0.1388 & 0 & 0.8600 \\ 0.0012 & 0.0082 & 0.9906 & 0 \end{bmatrix}, \quad (24)$$
$$i,\ j = 0, 1, 2, 3.$$

In second scenario, probabilities of ship collision alert, occurrence of high, low or negligible risk of collision are equal equivalently:

$$p(0) = 0.0003,\ p(1) = 0.0006,$$
$$p(2) = 0.0118,\ p(3) = 0.9873.$$

III scenario—a roundabout with distinguished main flow having priority.

In last model of traffic organization for a roundabout, the matrix of transitions' numbers between states is:

$$[n_{ij}]^{III} = \begin{bmatrix} 0 & 0 & 0 & 32 \\ 32 & 0 & 2 & 95 \\ 0 & 122 & 0 & 705 \\ 0 & 7 & 825 & 0 \end{bmatrix}, \; i, j = 0, 1, 2, 3, \quad (25)$$

and the vector of total numbers of transitions:

$$[n_0, n_1, n_2, n_3]^{III} = [32, 129, 827, 832].$$

Then, the matrix of transitions' probabilities takes values:

$$[p_{ij}]^{III} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0.2481 & 0 & 0.0155 & 0.7364 \\ 0 & 0.1475 & 0 & 0.8525 \\ 0 & 0.0084 & 0.9916 & 0 \end{bmatrix}, \quad (26)$$
$$i, j = 0, 1, 2, 3.$$

The worst results from simulation, for assumed parameters of flows, are given for a model of roundabout traffic organization in which a roundabout-lane has priority. The results are comparable in case of a roundabout with distinguished main flow having priority and for a roundabout, when a vessel having another vessel on her own starboard side shall keep out of the way. Besides, the number of transitions to state 0 (collision alert) is the lowest for a roundabout with distinguished main flow having priority. This can suggest that in this maritime traffic scenario the performance of collision avoidance manoeuvre, according to rules presented in Section 2 of this paper, is the most effective.

In third case, probabilities of being in particular safety states, defined before, are:

$$p(0) = 0.0002, \; p(1) = 0.0006,$$
$$p(2) = 0.0125, \; p(3) = 0.9867.$$

In case of simple crossing with distinguished main flow having priority we obtain results presented below. Simulation was also performed in time equivalent to four months of real time observation.

Then, the matrix of transitions' numbers between states is given by:

$$[n_{ij}]^{II} = \begin{bmatrix} 0 & 3 & 0 & 35 \\ 33 & 0 & 4 & 77 \\ 0 & 83 & 0 & 347 \\ 5 & 28 & 426 & 0 \end{bmatrix}, \; i, j = 0, 1, 2, 3, \quad (27)$$

and the vector of total numbers of transitions:

$$[n_0, n_1, n_2, n_3]^{II} = [38, 114, 430, 459].$$

Matrix of transitions' probabilities is the following:

$$[p_{ij}]^{II} = \begin{bmatrix} 0 & 0.0789 & 0 & 0.9211 \\ 0.2895 & 0 & 0.0351 & 0.6754 \\ 0 & 0.1930 & 0 & 0.8070 \\ 0.0109 & 0.0610 & 0.9281 & 0 \end{bmatrix}, \quad (28)$$
$$i, j = 0, 1, 2, 3.$$

Then, probabilities of system's being in particular safety states during simulation time are:

$$p(0) = 0.0002, \; p(1) = 0.0007,$$
$$p(2) = 0.1736, \; p(3) = 0.8255.$$

Drawn from simulation results conclusion that a roundabout with distinguished main flow having priority as traffic organization model is the most safe, as the probability of transition to state 0 (collision alert) is the lowest, is even more noticeable for other values of flow parameters.

Assuming that starting times of vessels on main waterway follow normal distribution with mean value 1.2 h and standard deviation 0.52 h and on lateral waterways we have Erlang distribution with mean time between ships departing equal to 1.3 h and 1.4 h and standard deviation 0.65 h and 0.75 h, equivalently for both directions, we obtain results presented below. For a roundabout with distinguished main flow having priority (III scenario) the matrix of transitions' numbers between states is:

$$[n_{ij}]^{III} = \begin{bmatrix} 0 & 0 & 0 & 42 \\ 33 & 0 & 0 & 129 \\ 0 & 146 & 0 & 1192 \\ 9 & 16 & 1338 & 0 \end{bmatrix}, \; i, j = 0, 1, 2, 3, \quad (29)$$

and the matrix of transitions' probabilities takes form:

$$[p_{ij}]^{III} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0.2037 & 0 & 0 & 0.7963 \\ 0 & 0.1091 & 0 & 0.8909 \\ 0.0066 & 0.0117 & 0.9817 & 0 \end{bmatrix}, \quad (30)$$
$$i,\ j = 0, 1, 2, 3.$$

In case of I scenario i.e. when a vessel having another vessel on her own starboard side shall keep out of the way, we get:

$$[n_{ij}]^{I} = \begin{bmatrix} 0 & 0 & 0 & 67 \\ 62 & 0 & 0 & 103 \\ 0 & 149 & 0 & 1134 \\ 5 & 16 & 1283 & 0 \end{bmatrix}, \ i,\ j = 0, 1, 2, 3, \quad (31)$$

and for the matrix of transitions' probabilities:

$$[p_{ij}]^{I} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0.3758 & 0 & 0 & 0.6242 \\ 0 & 0.1161 & 0 & 0.8839 \\ 0.0038 & 0.0123 & 0.9839 & 0 \end{bmatrix}, \quad (32)$$
$$i,\ j = 0, 1, 2, 3.$$

For these parameters, probabilities of ship collision alert, occurrence of high, low or negligible risk of collision, during simulation time, for III scenario are:

$$p(0) = 0.0001,\ p(1) = 0.0004,$$
$$p(2) = 0.0202,\ p(3) = 0.9792$$

and for I scenario, equivalently are:

$$p(0) = 0.0002,\ p(1) = 0.0005,$$
$$p(2) = 0.0166,\ p(3) = 0.9827.$$

4 CONCLUSIONS

ITS involves a large number of research areas, one of them is maritime traffic and its safety. Applying intelligent transportation systems technologies Vessel Traffic Services can improve maritime transport efficiency and safety. This paper introduces the model of basic cellular automaton for the description of maritime traffic flow in restricted area and brief view how it can be useful in maritime transport safety analysis. Detailed analysis of the simulation results for different traffic schemes can be effectively used in evaluation of waterways traffic organization and optimization. Thereby, the simulation model with some further development can be helpful as a tool on the level of safety management or safety-based spatial planning of restricted areas.

Simulation and modeling are tools that can identify, quantify and analyze maritime transportation phenomena and in the ITS context they can influence on development of maritime traffic control systems. Maritime traffic systems incorporate some intelligent systems technology to assist human operators. Therefore further research on dynamic models and parameter identification is still needed.

REFERENCES

ABS Guide for Vessel Maneuverability. 2006. American Bureau of Shipping Incorporated by Act of Legislature of the State of New York 1862.

Blokus-Roszkowska, A., Montewka, J. & Smolarek, L. 2012. Modelling the accident probability in large-scale, maritime transportation system. *Journal of PSRA, Summer Safety and Reliability Seminars* 3(2): 237–244.

Blokus-Roszkowska, A. & Smolarek, L. 2012a. Collision risk estimation for motorways of the sea. *Reliability: Theory & Applications* 2(25): 58–68.

Blokus-Roszkowska, A. & Smolarek, L. 2012b. Influence of traffic schemes on the level of vessels safety. *Journal of KONBiN* 4(24): 5–12.

Blokus-Roszkowska, A. & Smolarek, L. 2013. Application of simulation methods for evaluating the sea waterways traffic organization. *ISRN Applied Mathematics*, doi:10.1155/ 2013/715142.

Chauvin, Ch. & Lardjane, S. 2008. Decision making and strategies in an interaction situation: Collision avoidance at sea. *Transport Research Part F* 11: 59–269.

Chen, R.X., Bai, K.Z. & Liu, M.R. 2006. The CA model for traffic-flow at the grade roundabout crossing. *Chinese Physics* 15(7): 1471–1476.

Doniec, A., Mandiau, R., Piechowiak, S. & Espie, S. (2008). A behavioral multi-agent model for road traffic simulation. *Eng. Appl. Artif. Intel.* 21: 1443–1454.

Fujii, Y. & Tanaka, K. 1971. Traffic capacity. *Journal of Navigation* 24: 543–552.

Jamroz, K. & Krystek, R. 2006. Inteligentne Systemy Transportu—rozwój i struktura. *Transport Miejski i Regionalny* 5 (*in Polish*).

Maerivoet, S. & De Moor, B. 2005. Cellular automata models of road traffic. *Physics Reports* 419: 1–64.

Montewka, J., Hinz T., Kujala, P. & Matusiak, J. 2010. Probability modeling of vessel collisions. *Reliability Engineering and System Safety* 95: 573–589.

Nagel, K. & Schreckenberg, M. 1992. A cellular automaton model for freeway traffic. *Journal de Physique I France* 2(12): 2221–2229.

Perera, L.P., Oliveira, P. & Soares, C.G. 2012. Maritime Traffic Monitoring Based on Vessel Detection, Tracking, State Estimation, and Trajectory Prediction. *IEEE Trans. Intell. Transport. Syst.* 13(3): 1188–1200.

Pietrzykowski, Z. 2011. Maritime Intelligent Transport Systems. *Transport Systems Telematics, Communications in Computer and Information Science* 104: 455–462.

Su, C.M., Chang, K.Y. & Cheng, C.Y. 2012. Fuzzy decision on optimal collision avoidance measures for ships in vessel traffic service. *Journal of Marine Science and Technology* 20(1): 38–48.

Tsou, M.C. & Hsueh, C.K. 2010. The study of ship collision avoidance route planning by ant colony algorithm. *Journal of Marine Science and Technology* 18(5): 746–756.

Wibowo, S. & Deng, H. 2012. Intelligent decision support for effectively evaluating and selecting ships under uncertainty in marine transportation. *Expert Systems with Applications* 39(8): 6911–6920.

Wolfram, S. 1986. *Theory and Application of Cellular Automata*. Singapore: World Scientific.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Modeling of event trees for the rapid scenario development

M.K. Gerigk
Gdańsk University of Technology, Gdańsk, Poland

ABSTRACT: The paper concerns the safety of ships in abnormal/damage conditions. Some conclusions following from the research associated with development of a method for safety assessment of ships in abnormal/damage conditions is presented in the paper. The method called SSAMADC (Ship Safety Assessment Method in Abnormal/Damage Conditions) is a risk-based method and is connected with application of the quantitative risk assessment QRA approach. The method is an alternative method of safety assessment of ships in abnormal/damage conditions in comparison with the method included within the SOLAS 2009 regulations. The aim of the research is to work out a proposal of an alternative method of safety assessment of ships in damaged conditions. There is a lack of such the method for the certain type of ships.

1 INTRODUCTION

The aim of the research is to work out a proposal of an alternative method of safety assessment of ships in damaged conditions. The research has been done because the method included in the SOLAS regulations does not cover certain type of ships.

The key issue in application of the method is to model the event tress for the scenario development under consideration.

There is a market need for good methods enabling the assessment of safety of damaged ships at the design stage, in operation and during the ship salvage. The existing methods for the salvage purposes are mainly based on the expert assessment using the brain storming techniques. The methods based on the requirements included in the SOLAS 2009 regulations (Chapter II-1) are of the prescriptive character and devoted to solve the ship design problems, IMO (2005). This is the reason why it is very difficult to apply such a method for assessing the safety of ships in damage conditions at the design stage, in operation, after the collision at sea and later during the ship salvage procedure.

2 THE PROPOSED METHOD

The proposed method called SSAMADC (Ship Safety Assessment Method in Abnormal/Damage Conditions) is a risk-based method and is connected with application of the quantitative risk assessment QRA approach. The method is an alternative method of safety assessment of ships in abnormal/damage conditions in comparison with the method included within the SOLAS 2009 regulations.

The method combines the ship performance-oriented approach with the risk-based approach, Gerigk (2010). The holistic approach to safety assessment is applied. An influence of design, operational, management-related and human factors on safety is taken into account. Then, the matrix type risk model is applied. This model has a holistic character. Next, it is possible to take into account almost all the possible scenarios of an accident.

The risk model may be defined using the multi-level event tree ETA which general structure is shown in Figure 1.

The accident scenarios may consist of the hazards, intermediate events, additional events and consequences. It is important to define the initial events (hazards). The measure of safety of ships in damage conditions is the risk level. The risk acceptance criteria can be the risk matrix or ALARP concept.

The methodology where the risk-based design and a formalized design methodology were

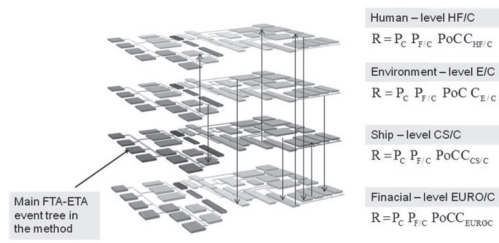


Figure 1. General structure of the multi-level event tree divided into four basic modules: human, environment, ship (property), finance, Gerigk (2010).

integrated together in the design process with the prevention/reduction of risk as a design objective, along the standard design objectives was first introduced by Vassalos, (Arangio 2012, Jasionowski et al. 2006, Mohaghegh 2009, Nowakowski et al. 2009, Skjong et al. 2006, Soares C.G. et al. 2001, Stephans 2012, Stewart et al. 2012, Suddle, 2001, Vassalos 2006).

For the ship performance evaluation the statistics, investigations using the physical models and numerical simulation techniques can be applied. The ship performance evaluation enables to determine the intermediate events, additional events (releases) and consequences and risk of each accident scenario. The aim is to achieve an adequate level of risk by reducing the risk if necessary. Providing a sufficient level of safety based on the risk assessment is the main objective. It is either the design, operational or organizational objective. Then, safety is not a limitation any more, existing in the regulations. It is just the objective. The measure of safety of a ship in damaged conditions is the level of risk.

The proposed method may be used at any ship's life circle, including safety assessment of the ship during a catastrophe. Some elements of the method can be used for safety assessment of different means and systems of seaborne transportation. In the future the method can be useful in elaboration of a new methodology of safety assessment of ships, which bases on the application of risk analysis.

The method is based on the following steps:

- setting the requirements, criteria, limitations, risk acceptance criteria and safety objectives,
- definition of ship and environment,
- hazard identification and scenarios development,
- assessment of ship performance for the data sequence of events,
- risk estimation using the matrix type risk model,
- risk assessment according to the risk acceptance criteria,
- risk control (prevention, reduction),
- selection of designs (operational procedures) that meet the objectives,
- making decisions on safety.

The structure of the method is presented in Figure 2, Gerigk (2010).

The risk and safety assessment of ships in damaged conditions requires modeling of the risk contribution tree. For each hazard a separate event tree may be modeled using the Event Tree Analysis ETA. The basic event tree ETA for the safety assessment of ships in damaged conditions is presented in Figure 3.

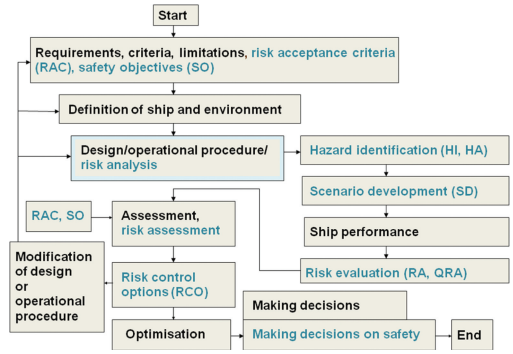


Figure 2. Structure of the method of risk and safety assessment of ships in damaged conditions.

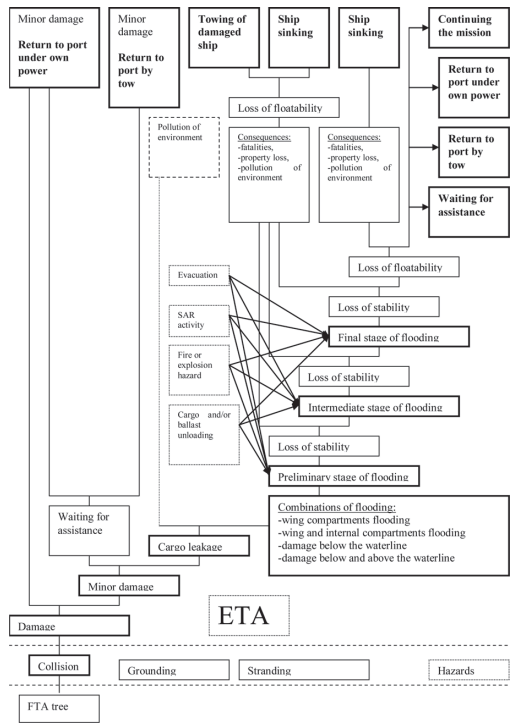


Figure 3. A Basic Event Tree (ETA) for safety assessment of ships in damaged conditions and salvage purposes.

Generally, sixteen safety functions may be defined for each event tree considering a ship safety in damaged conditions, Gerigk (2010).

A location of each function can easily be found in Figure 3. The starting functions are: function 1 (avoiding the hazard), function 2 (hull skin damage (flooding) and function 3 (position and extension of damage). The final functions can be: function

8 (loss of the ship floatability at the final stage of flooding) or function 9 (ship is waiting for assistance), (Abramowicz-Gerigk 2006, Abramowicz et al. 2008, Abramowicz-Gerigk et al. 2013, Gerigk 2004, Gerigk 2006, Gerigk 2008, Gerigk 2010, Gerigk 2012, Perera 2011).

It is important to notice that each event tree may have a dynamical character.

3 THE RISK ESTIMATION USING THE MATRIX TYPE RISK MODEL

The risk associated with the data sequence of events may be estimated according to the well known general formulae, Gerigk (2010):

$$R_i = P_i \times C_i \tag{1}$$

where P_i = probability of occurrence of a given hazard; C_i = consequences following the occurrence of the data hazard and scenario development, in terms of fatalities, injuries, property losses and damage to the environment.

The risk model (1) may concern four different kinds of losses regarding the human fatalities (HF), cargo and ship losses (CS), environment pollution (E) and financial losses ($).

The risk formulae for the risk estimation for a ship in damaged conditions can be presented as follows:

$$R = P_c \, P_{c/f} \, PoC_{dam} \times C \tag{2}$$

where P_c = probability of collision (hazard); $P_{c/f}$ = probability of flooding having the ship hit from given direction at data position with given extent conditional on collision; PoC_{dam} = probability of capsizing in damaged conditions in given time conditional on having flooding when the ship is hit from given direction at data position with given extent conditional on collision; C = consequences regarding the fatalities, property (cargo, ship), environment and finance ($C = C_{HF/C}, C_{CS/C}, C_{E/C}, C_{\$/C}$).

The PoC_{dam} probability of capsizing in damaged conditions in the given time can be calculated according to the following formulae, Gerigk (2010):

$$PoC_{dam} = P_{c/f/ns} \, P_{c/f/ns/tts} \tag{3}$$

where $P_{c/f/ns}$ = probability of not surviving conditional on having flooding when the ship is hit from given direction at data position with given extent conditional on collision; $P_{c/f/ns/tts}$ = probability of given time to sink conditional on not surviving the conditional on having flooding when the ship is hit from given direction at data position with given extent conditional on collision.

The PoC_{dam} probability can be estimated using the following methods, Gerigk (2010):

- binary method;
- method based on definition of the probability of surviving a collision;
- method based on definition of the damage stability;
- method based on definition of the ship performance during the accident.

In the case of the last method the roll function in time domain has been anticipated as a major function enabling the risk assessment, Gerigk (2010).

The risk estimation requires to calculate the conditional probabilities regarding the initial events ZI_i, major events (hazards) ZG_j, intermediate events ZP_k and final events ZK_l which are the consequences.

The basic mathematical formulas are as follows, Gerigk (2010).

First of all the row matrix of initial events is evaluated:

$$P(ZI) = P(ZI_i) = [\, P(ZI_1), P(ZI_2), ..., P(ZI_n)] \quad \text{for } i = 1 \text{ to } n \tag{4}$$

Then the matrix of major events is calculated:

$$MP_{ZG} = P(ZG_j/ZI_i) \quad \text{for } j = 1 \text{ to } m \tag{5}$$

where the $P(ZG_j/ZI_i)$ conditional probabilities belong to the data sequences of events and may be presented as the matrix of conditional probabilities as follows:

$$\begin{bmatrix} P(ZG_1/ZI_1) & P(ZG_2/ZI_1) & ... & P(ZG_m/ZI_1) \\ P(ZG_1/ZI_2) & P(ZG_2/ZI_2) & ... & P(ZG_m/ZI_2) \\ ... & ... & ... & ... \\ P(ZG_1/ZI_n) & P(ZG_2/ZI_n) & ... & P(ZG_m/ZI_n) \end{bmatrix}$$

After that the matrix of intermediate events is calculated:

$$MP_{ZP} = P(ZP_k/ZG_j) \text{ for } k = 1 \text{ to } m1 \tag{6}$$

where the $P(ZP_k/ZG_j)$ conditional probabilities belong to the data sequences of events and may be presented as the matrix of conditional probabilities as follows:

$$\begin{bmatrix} P(ZP_1/ZG_1) & P(ZP_2/ZG_1) & ... & P(ZP_{m1}/ZG_1) \\ P(ZP_1/ZG_2) & P(ZP_2/ZG_2) & ... & P(ZP_{m1}/ZG_2) \\ ... & ... & ... & ... \\ P(ZP_1/ZG_m) & P(ZP_2/ZG_m) & ... & P(ZP_{m1}/ZG_m) \end{bmatrix}$$

Then the matrix of final events is calculated:

$$MP_{ZK} = P(ZK_l/ZP_k) \text{ for } l = 1 \text{ do } m2 \quad (7)$$

where the $P(ZK_l/ZP_k)$ conditional probabilities belong to the data sequences of events and may be presented as the matrix of conditional probabilities as follows:

$$\begin{bmatrix} P(ZK_1/ZP_1) & P(ZK_2/ZP_1) & \ldots & P(ZK_{m2}/ZP_1) \\ P(ZK_1/ZP_2) & P(ZK_2/ZP_2) & \ldots & P(ZK_{m2}/ZP_2) \\ \ldots & \ldots & \ldots & \ldots \\ P(ZK_1/ZP_{m1}) & P(ZK_2/ZP_{m1}) & \ldots & P(ZK_{m2}/ZP_{m1}) \end{bmatrix}$$

Finally, the row matrix for the final events may be estimated as follows:

$$P(ZK) = P(ZI)\, MP_{ZG}\, MP_{ZP}\, MP_{ZK} = P(ZI_i)\, P(ZG_j/ZI_i)\, P(ZP_k/ZG_j)\, P(ZK_l/ZP_k) \quad (8)$$

where i = 1 to n, j = 1 to m, k = 1 to m1 and l = 1 do m2.

Because of the above mathematical model used the entire risk model is called as the matrix type risk model. In the case when the additional events occur the $PoC(C_i)$ probability of occurring the C_i given consequences can be calculated according to the formula worked out by Gerigk, Gerigk (2010). The typical additional events may concern the water on deck, air cushions, cargo leakage, additional heeling moments or passenger behaviour.

4 APPLICATION OF THE METHOD

The ship accidents at sea may lead to the loss of life, loss of properties (ship and cargo) and pollution of environment. The modern approach to safety of seaborne transportation requires to apply the so-called life-circle approach by integrating the design for safety, safe operation and safe salvage methods. Most of the salvage activities have been associated with using the rules of thumb without a support based on the safety assessment process. The effective and safe ship salvage requires to develop the methods, models and tools for the assessment of risk and safety of ships in damaged conditions, Gerigk et al. (2012).

The proposed method of risk and safety assessment of ships in damaged conditions together with the matrix type risk model enables to assess a ship survivability at each stage of flooding including the preliminary, intermediate and final stages of flooding. Such an assessment is necessary to predict any further deterioration of the damage condition. It may be connected with further flooding of compartments and ship listing increase. This assessment also regards predicting how long it would take the ship to capsize or sink. If the ship survives flooding (a ship remains upright (or heeled) and afloat) and is unable to return to port under own power it is necessary to solve the problems associated with the towing when waiting for an assistance. The number of towing points and towing speed in the calm and rough weather conditions should be evaluated. During the towing the risk and safety assessment of the ship should be permanently conducted.

The structure of the procedure for the assessment of safety of ships in damaged conditions during the accident at sea and for the salvage purposes is presented in Figure 4, Gerigk (2010).

The procedure of assessment of safety of damaged ships during the catastrophe at sea should enable as follows:

- assessment of safety of ships in damaged conditions (stages/phases of flooding);
- identification of changes;
- estimation of time of flooding (time for evacuation, time of SAR activity);
- method of ship salvage (RTP, WFA, AS), method of towing.

The key element of the procedure presented in Figure 4 is the decision support system. An idea of this system is based is the approach to safety management. The structure of this approach is presented in Figure 5.

For making the decisions on safety (see Fig. 2) a method of the knowledge representation and efficient reasoning under uncertainties has been applied using the Bayesian Belief Networks (BBN).

The basic structure of the method of knowledge representation and efficient reasoning under

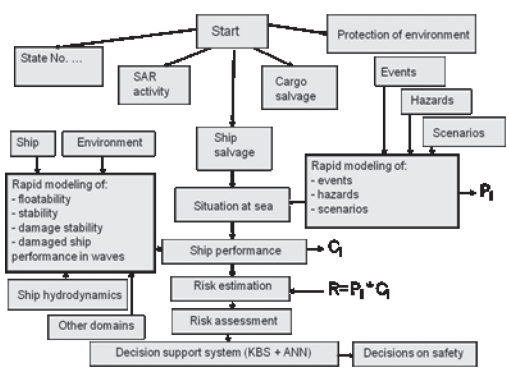


Figure 4. The structure of the procedure for the assessment of safety of ships in damaged conditions during the accident at sea and for the salvage purposes.

uncertainties for the safety assessment of ships in damaged conditions is presented in Figure 6.

An example of the basic structure of this method in the case of collision is presented in Figure 7.

For constructing the safety management network within the decision support system (see Fig. 4) the Hugin Researcher 7.4 has been used.



Figure 5. The structure of the approach to safety management.



Figure 6. The basic structure of the method of knowledge representation and efficient reasoning under uncertainties for the safety assessment of ships in damaged conditions.

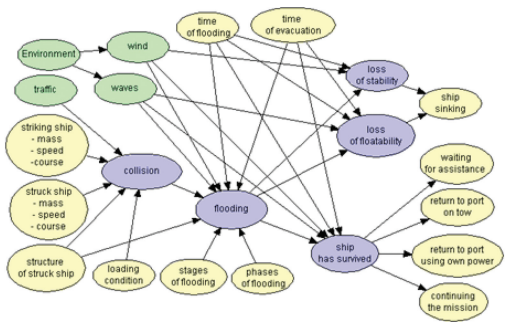


Figure 7. The structure of the method in the case of the collision.

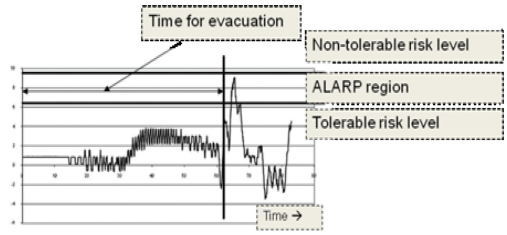


Figure 8. An example of the roll function in time domain and ALARP risk evaluation criteria applied for the assessment of safety of a ship in damaged conditions.

In practice using the proposed concept of a risk-based decision support system for the ship safety assessment in damaged conditions the following major steps are necessary to be done:

- assessment of ship performance,
- risk assessment using the risk acceptance criteria,
- risk management using the risk control options.

An example of application of the ship performance data regarding the ship roll function in time domain and ALARP risk evaluation criteria for assessment of a ship safety in damage conditions is presented in Figure 8. The vertical axis in Figure 8 regards the angle of heel in degrees and the horizontal axis concerns the time in seconds.

5 CONCLUSIONS

The method presented in the paper is based on combining the ship performance-oriented approach and risk-based approach.

The method has the following features:

- no disadvantages which exist in SOLAS;
- holistic approach to safety (design, operation, catastrophe, salvage);
- holistic approach to safety: safety factors (sources of factors: design, operation, management, human factor);
- holistic approach regarding the risk model;
- assessment of safety for all the possible scenarios.

The key issue to apply the method is to have the proper matrix type holistic risk model. The proposed risk model is rather complicated in practice but it seems to be more suitable for the design, operational and salvage purposes than the models published in literature.

The risk model depends on the structure of event tree.

In the case of a risk-based decision support system which is a part of the procedure for the assessment of safety of ships in damaged conditions presented in Figure 4 the decisions of safety should be done performing the following steps:

– assessment of ship performance,
– risk assessment using the risk acceptance criteria,
– risk management using the risk control options.

The current research is associated with further development of the risk models, ship performance procedures and risk acceptance criteria.

ACKNOWLEDGMENTS

The research has been carried out at the Gdansk University of Technology according to support obtained from the Ministry of Science and Higher Education in Warsaw. The author would like to express his sincere gratitude to the above organisations.

REFERENCES

Abramowicz-Gerigk, T., 2006. Determination of Safety Factors for Ship Berthing Operations. Proceedings and Monographs in Engineering, Water and Earth Sciences. In *(ESREL 2006)*. London: Taylor & Francis/ Balkema, pp. 2737–2742.

Abramowicz-Gerigk, T. & Burciu, Z. 2008. The risk analysis of harbour operations. In C.G.S. & J.B. eds. S. Martorell, ed. *(ESREL 2008)*. London: Balkema, pp. 3343–3350.

Abramowicz-Gerigk, T. & Burciu, Z. 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. In & F.L.P. eds. C. Guedes Soares, ed. *(IMAM 2013)*. London: Balkema, pp. 699–704.

Arangio, S. 2012. Reliability based approach for structural design and assessment: performance criteria and indicators in current European codes and guidelines. *International Journal of Lifecycle Performance Engineering*, 1(1), p. 64.

Gerigk, M., 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. *Polish Maritime Research*, 11(1 (39)), pp. 8–13.

Gerigk, M., 2005. Challenges of modern assessment of safety of ships in critical conditions. In *(IMAM 2005)*. London: Taylor & Francis/Balkema, pp. 1529–1536.

Gerigk, M., 2006. A method for assessing hazards, risks and safety of damaged ships at sea. In *(ESREL 2006)*. London: Balkema, pp. 2783–2790.

Gerigk, M., 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. *(ESREL 2008)*, 4, pp. 3303–3310.

Gerigk M. 2010. A complex method for safety assessment of ships in damaged conditions using the risk assessment (D.Sc. thesis), *Monography No. 101, Published by the Gdansk University of Technology (in Polish),* Gdansk 2010.

Gerigk M., Wardynszkiewicz K. 2012. Safety assessment of ships in damaged conditions using a novel concept of a risk-based decision support system. *Proceedings of the 19th International Conference on Hydrodynamics in Ship Design, 4th International Symposium on Ship Manoeuvring*, Iława, Poland, 19–21 September 2012.

Gerigk, M. 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. In *(IMAM 2012)*. London: Balkema, pp. 715–719.

IMO. 2005. Report of the Maritime Safety Committee on Its Eightieth Session, *MSC 80/24/Add.1*, London 2005.

Jasionowski, A. & Vassalos, D. 2006. Conceptualising Risk, *Proceedings of the 9th International Conference on Stability of Ships and Ocean Vehicles STAB 2006*, Rio de Janeiro, 25–29 September 2006.

Mohaghegh, Z. & Mosleh, A. 2009. Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations, *Journal of Safety Science, Vol. 47, 2009,* pp. 1139–1158.

Nowakowski, T. & Werbińka, S., 2009. On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing*, 6(4), pp. 364–378.

Perera L.P. & Soares Guedes C. 2011. Detections of potential collision situations by relative motions of vessels under parameter uncertainties, *Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM), Genova, Italy, 13–16* September 2011.

Skjong, R. & Vanem, E. & Rusas, S. & Olufsen, O. 2006. Holistic and Risk Based Approach to Collision Damage Stability of Passenger Ships, *Proceedings of the 9th International Conference on Stability of Ships and Ocean Vehicles STAB 2006,* Rio de Janeiro, 25–29 September 2006.

Soares, C.G. & Teixeira, A.P., 2001. Risk assessment in maritime transportation. *Reliability engineering and System Safety*, 74, pp. 299–309.

Stephans, R., 2012. System safety for the 21st century: The updated and revised edition of system safety 2000.

Stewart, M. & Melchers, R.E., 1997. *Probabilistic Risk Assessment of Engineering Systems*, London: Chapman & Hall.

Suddle, S., 2001. Safety of construction in intensive use of space. *Proceedings of Congress Risk Analysis*.

Vassalos D. 2006. Passenger Ship Safety: Containing the Risk, *Marine Technology, Vol. 43, No. 4,* October 2006, pp. 203–213.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The influence of screw propellers manufacturing accuracy on conditions of the propulsion system operating

E. Skupień
Institute of Machine Design and Operation, Wroclaw University of Technology, Poland

ABSTRACT: The paper presents an analysis of deviations in diameter D and pitch coefficient P/D and their impact on the determination of efficiency, torque, thrust and power calculated using the exact differential method.

The results of the presented analysis, were applied into the characteristics of propulsion system. On this basis, the operating point has changed in the area. Further analysis allowed to identify, among others, maximum power requirements for obtaining a desired speed under certain navigation conditions.

1 INTRODUCTION

Operating condition on Polish inland waterways significantly differ from conditions on other European waterways. Therefore problems considered in Polish society are often not encountered anywhere else. One of those issues is determinating operating conditions of propulsion system in frequently changing navigation conditions (it is extremely rare not to keep still navigation conditions on specific parts of river). (Kulczyk & Winter, 2003).

Calculating the optimal operating parameters of the inland ship's propulsion system, requires performing many intermediate calculations. At each of the steps, accuracy of the calculations is correlated with the rounding precision, but also with the accuracy of the characteristics and the geometry of the propeller. For this reason, one notes the impact of these errors on the final results. (Eloot & Vantorre, 2011).

Thorough analysis the impact of geometric parameters for further calculations, one can get on the basis of a model tests or theoretical algorithms. Presentation of the hydrodynamic characteristics of the propeller in the form of polynomials, allows to analyze the impact of propeller's workmanship inaccuracy on the operating parameters of the drive system, that is: power, thrust or efficiency.

Measurement errors can be calculated using the total differential method (Hansel, 1968).

$$df(x) = \sum_{i=1}^{n} \frac{\partial f(x)}{\partial x_i} dx_i \tag{1}$$

For indirect measurements, if the measured value is the sum of the values of x_i to x_n:

$$df(x) = \sum_{i=1}^{n} \frac{\partial f(x)}{\partial x_i} dx_i \tag{2}$$

Taking into account all the indirect errors, the result will therefore be the sum of the errors obtained at each stage (Piotrowski, 2002).

Further provided calculations were based on the example of the Ka series ducted propellers.

2 THE IMPACT OF THE ACCURACY OF THE PROPELLER DIAMETER D

Propellers of inland vessels often work in very difficult conditions. This results in a fairly rapid mechanical consumption of propellers (abrasion and deformation). Propellers are also mostly performed in a technology giving low accuracy (welded carbon steel). Most of these results in negligently manufacturing of propellers (Dudziak, 1988).

The accuracy of the propellers manufacturing has an impact on the efficiency of those, obtained thrust, the required torque on the cone bolts and curves of thrust and power on the driving characteristics of the ship (Kulczyk & Winter, 2003; Holtrop & Mennen, 1982).

The efficiency of the propeller, defined by the equation:

$$\eta_0 = \frac{K_T}{K_Q} \frac{J}{2\pi} \tag{3}$$

Can be written indicating dependence:

$$\eta_0 = \frac{K_T\left(\frac{P}{D}, J(D)\right)}{K_Q\left(\frac{P}{D}, J(D)\right)} \frac{J(D)}{2\pi} \tag{4}$$

Calculating the differential of the efficiency assuming as variable a diameter D, relative error equation is obtained:

$$\frac{d\eta_0}{\eta_0} = J\frac{dD}{D}\left(\frac{1}{K_Q}\frac{\partial K_Q}{\partial J} - \frac{1}{K_T}\frac{\partial K_T}{\partial J} - \frac{1}{J}\right) \tag{5}$$

where: $\partial K_Q / \partial J$ and $\partial K_T / \partial J$ are derivatives of torque and thrust coefficients with respect to the feed ratio J.

Relative errors of thrust for constant rotation and torque can be calculated using the equation:

$$T = K_T \cdot \rho \cdot n^2 \cdot D^4 \tag{6}$$

And are:

$$\frac{dT}{T}|_{n=const} = \frac{dD}{D}\left(4 - \frac{J}{K_T}\frac{\partial K_T}{\partial J}\right) \tag{7}$$

$$\frac{dQ}{Q} = \frac{dD}{D}\left(5 - \frac{J}{K_Q}\frac{\partial K_Q}{\partial J}\right) \tag{8}$$

The relative error of power for constant rotation is:

$$\frac{dP_D}{P_D}|_{n=const} = \frac{dD}{D}\left(5 - \frac{J}{K_Q}\frac{\partial K_Q}{\partial J}\right) \tag{9}$$

Assuming constant torque, takes a form:

$$\frac{dP_D}{P_D}|_{Q=const} = \frac{1}{2}\frac{dD}{D}\left(\frac{J}{K_Q}\frac{\partial K_Q}{\partial J} - 5\right) \tag{10}$$

An error of thrust for constant torque is:

$$\frac{dT}{T}|_{Q=const} = J\frac{dD}{D}\left(\frac{1}{K_Q}\frac{\partial K_Q}{\partial J} - \frac{1}{K_T}\frac{\partial K_T}{\partial J} - \frac{1}{J}\right) \tag{11}$$

For these calculations, resulting from the propeller's diameter error, a knowledge of derivatives ∂J and ∂J is required. Presentation of these coefficients as polynomials (for ducted propellers series Ka):

$$K_T = \sum_{s,t}\left[A_{s,t} \cdot J^s \left(\frac{P}{D}\right)^t\right] \tag{12}$$

$$\frac{\partial K_T}{\partial J} = \sum_{s,t}\left[A_{s,t} \cdot t \cdot J^{t-1}\left(\frac{P}{D}\right)^s\right] \tag{13}$$

$$K_Q = \sum_{s,t}\left[B_{s,t} \cdot J^s \left(\frac{P}{D}\right)^t\right] \tag{14}$$

$$\frac{\partial K_Q}{\partial J} = \sum_{s,t}\left[B_{s,t} \cdot t \cdot J^{t-1}\left(\frac{P}{D}\right)^s\right] \tag{15}$$

allows for the calculation of the respective propellers and assumed feed ratio *J*.

For the range of the feed rate J used in practice, an increase in diameter would cause the reduction in efficiency, increasing the thrust, but also torque. In addition, for smaller values of pitch ratio *P*/*D* and *J*, the impact of the error of diameter is smaller.

Increasing the diameter of the propeller causes the risk of overloading the propulsion system (propeller would be to heavy). Therefore, it is safer to allow an error of –5% than +5%.

3 THE IMPACT OF THE ACCURACY OF THE PITCH RATIO P/D

Similar calculations as for the diameter of the propellers, carried out for the pitch ratio will give the following results:

$$\frac{d\eta_0}{\eta_0} = \frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_T}\frac{\partial K_T}{\partial\left(\frac{P}{D}\right)} - \frac{1}{K_Q}\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)}\right) \tag{16}$$

$$\frac{dT}{T}|_{n=const} = \frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_T}\frac{\partial K_T}{\partial\left(\frac{P}{D}\right)}\right) \tag{17}$$

$$\frac{dQ}{Q} = \frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_Q}\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)}\right) \tag{18}$$

$$\frac{dP_D}{P_D}|_{n=const} = \frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_Q}\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)}\right) \tag{19}$$

$$\frac{dP_D}{P_D}|_{Q=const} = -\frac{1}{2}\frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_Q}\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)}\right) \tag{20}$$

$$\frac{dT}{T}\Big|_{Q=const} = \frac{d\left(\frac{P}{D}\right)}{\left(\frac{P}{D}\right)} \cdot \left(\frac{P}{D}\right)\left(\frac{1}{K_T}\frac{\partial K_T}{\partial\left(\frac{P}{D}\right)} - \frac{1}{K_Q}\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)}\right) \tag{21}$$

Increasing the P/D ratio has the same effect as increasing the diameter, but the impact is much smaller. For the torque, there is no unambiguous impact of P/D ratio. The smallest errors are achieved for the lowest P/D ratio.

Derivative $\partial K_Q/\partial(P/D)$ and $\partial K_T/\partial(P/D)$ take the analogous form to the derivatives of diameter:

$$\frac{\partial K_Q}{\partial\left(\frac{P}{D}\right)} = \sum_{s,t}\left[A_{s,t}\cdot s\cdot J^t\left(\frac{P}{D}\right)^{s-1}\right] \tag{22}$$

$$\frac{\partial K_T}{\partial\left(\frac{P}{D}\right)} = \sum_{s,t}\left[B_{s,t}\cdot s\cdot J^t\left(\frac{P}{D}\right)^{s-1}\right] \tag{23}$$

4 ACCURACY CALCULATIONS—SUMMARY

Practice shows that the above-mentioned errors most often take the values: for diameter: $\partial D/D \approx 3\%$, for (P/D) ratio: $(\partial(P/D))/(P/D) \approx 10\%$.

Drawings 1 to 13 show the influence of error of 3% in diameter and 10% in P/D ratio, on efficiency, thrust and torque.

The charts show the calculation for the propeller Ka4-55, with a diameter $D = 1.26$ m, with pitch ratio $P/D = 0.6$; $P/D = 0.778$ (such propeller is

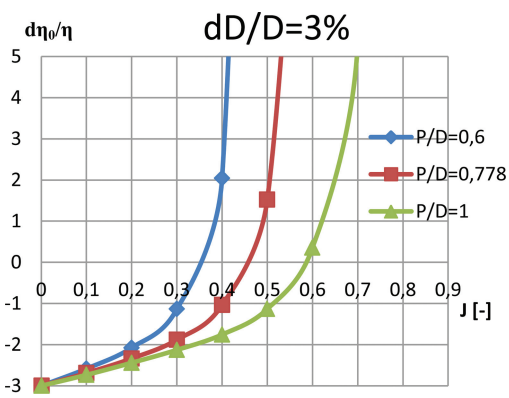


Figure 1. Changes in the efficiency with an error of diameter $\partial D/D = 3\%$, for different pitch ratios of Ka4-55 propeller.

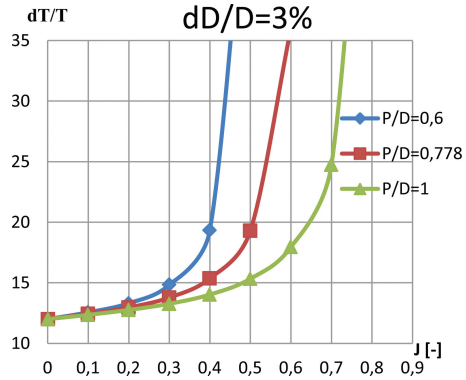


Figure 2. Changes in the thurst with an error of diameter $\partial D/D = 3\%$, for different pitch ratios of Ka4-55 propeller.

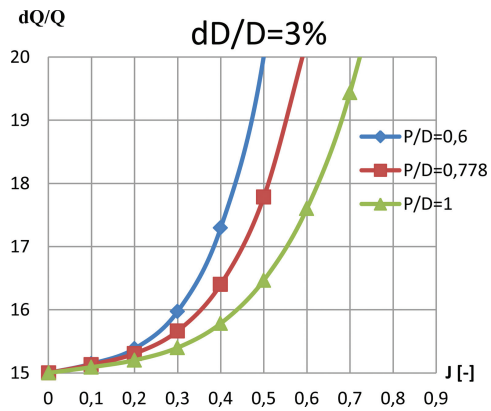


Figure 3. Changes in the torque with an error of diameter $\partial D/D = 3\%$, for different pitch ratios of Ka4-55 propeller.

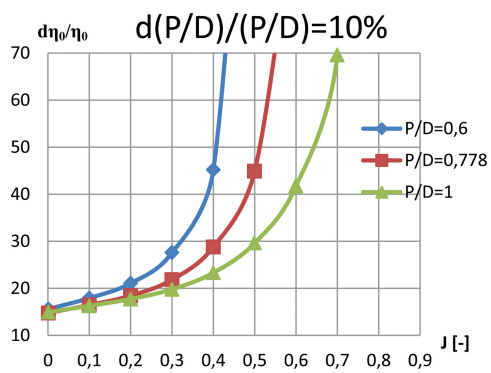


Figure 4. Changes in the efficiency with an error of pitch ratio $\partial(P/D)/(P/D) = 10\%$, for different pitch ratios of Ka4-55 propeller.

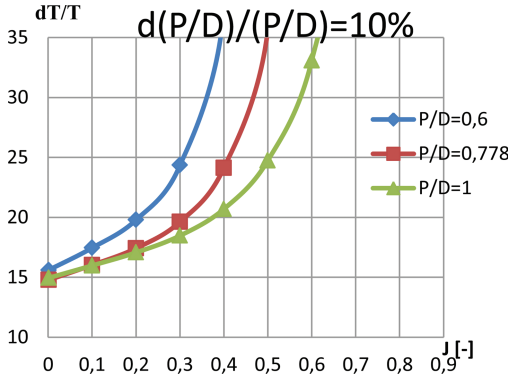


Figure 5. Changes in the thurst with an error of pitch ratio $\partial(P/D)/(P/D)$ = 10%, for different pitch ratios of Ka4-55 propeller.

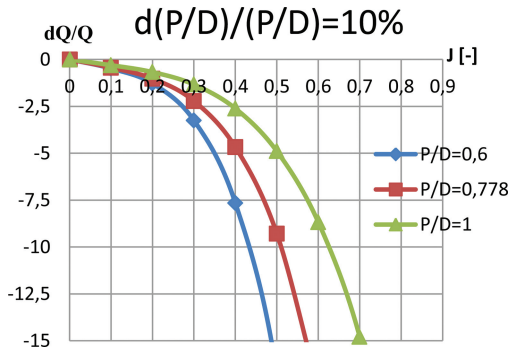


Figure 6. Changes in the torque with an error of pitch ratio $\partial(P/D)/(P/D)$ = 10%, for different pitch ratios of Ka4-55 propeller.

operated on Bison pushers); $P/D = 1$ and $P/D = 1.4$. Different values of pitch ratio illustrate the nature of the changes, along with increases in feed rate. The nature of the changes of errors is similar for all the ducted propellers.

From the graphs above it can be concluded that an increase of the pitch ratio reduces the impact of the accuracy of the propeller on the analyzed parameters for the same value of the feed rate.

5 THE TOTAL VALUE OF ERROR

Knowledge of value of the total error affects the determination of fuel consumption (the accuracy of the determination), but also affects the correct determination of the optimal operating parameters of the propulsion system. Operation the propulsion system outside the optimal operating parameters can lead to overload the system, which in turn can damage it.

The calculations of the effect of errors on the operating parameters of the propulsion system, allow to establish optimum operating conditions of the propulsion system on the ship's propulsion characteristics, not by a point, but as a field.

Each of the analyzed elements affects the operating parameters of the propulsion system. Therefore, their impact should be presented as a sum of errors.

To illustrate, on the characteristics of the thrust T (V) the values of individual errors and their sum was applied.

Figure 7 shows the propulsion characteristics of ship with the Ka4-55 propeller in the nozzle 19A. On the graph curves corresponding to the values of errors resulting from the implementation of the propeller diameter of 3% accuracy were plotted

The following figure double lines mark characteristics of the propulsion system, namely: the nominal speed (double blue line), the nominal torque (double green line) and the needed thrust resulting from the geometry of the vessel and the depth of the waterway (double yellow line). The intersection of these lines represents the theoretical operating point. To obtain the ship speed Vs = 2.95 m/s, the propulsion system must generate thrust TN = 21500 N.

Figure 7 shows extension of the single lines the range of rotation and torque of the system under the assumption of error of 3% of the propeller diameter.

In practice, this means that the operating point extended to the field bounded by the curves taking into account the value of errors. The following situation is possible: the thrust 23500 N (upper point of intersection the needed thrust curve and the

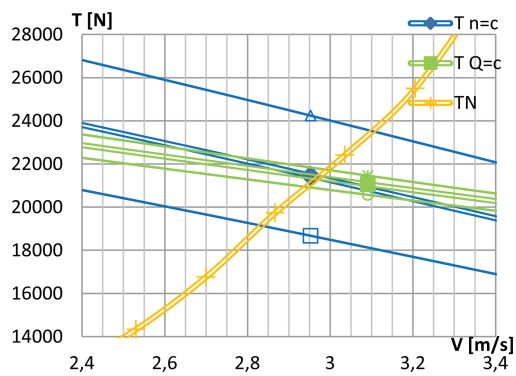


Figure 7. Propulsion characteristics of ship with the Ka4i55 propeller, with the accuracy of propellers diameter $\partial D/D = 3\%$.

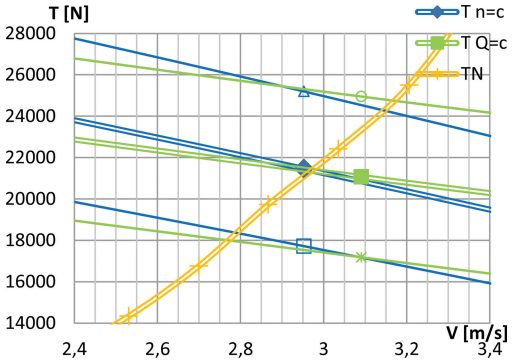


Figure 8. Propulsion characteristics of ship with the Ka4-55 propeller, with the accuracy of pitch ratio $\partial(P/D)/(P/D) = 10\%$.

constant RPM curve) get speed of 2.83 m/s (lower intersection point). It is equally probable, that the thrust 19200 N, gives the ship speed of 3.1 m/s. The situation that occurs depends on the exact value and the direction of errors.

Figure 8 shows the propulsion characteristics of the ship, taking into account the corresponding error of pitch ratio.

As in the previous case, the system may be at the optimal point of work, but also in each of the points lying along the curve of needed thrust, located between the extreme lines of errors arising from the implementation of pitch ratio.

6 CONCLUSION

These values may be questionable. However, to obtain a state where more than 27 kN thrust would not give a greater speed of 2.5 m/s (9 km/h), all the analyzed errors would have to co-exist and would not alleviate.

Going forward, the range of rotation and torque needed to achieve that speed can be determined. Knowing the maximum values of these parameters, corresponding to not overloading operation parameters of the propulsion system, it is possible to exploit the propulsion system to prevent overloading.

REFERENCES

Dudziak J., 1988. Teoria Okrętu. Wydawnictwo Morskie, Gdańsk.

Eloot K., Vantorre M., 2011. Ship behaviour in shallow and confined water: an overview of hydrodynamic effects through EFD, NATO. Research and Technology Organisation (RTO).

Hansel H., 1968. Podstawy rachunku błędów, WNT.

Holtrop J., Mennen G.G.J., 1982. An approximate power prediction method, International Shipbuilding Progress, vol. 29, No. 335.

Kulczyk J., Winter J., 2003. Śródlądowy transport wodny, Oficyna wydawnicza Politechniki Wrocławskiej, Wrocław.

Piotrowski J., 2002. Podstawy miernictwa, WNT.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Contribution to oil data assessment for system condition determination

D. Vališ
University of Defence, Brno, Czech Republic

L. Žák
University of Technology, Brno, Czech Republic

ABSTRACT: The paper deals with application of selected analytical methods for analysing field data from heavy off-road military vehicles. It is the vehicle engine and its oil data which are explored for further utilisation. There is available reasonable set of vehicles and their oil data from in-field-operation. Based on the data we assume it will be possible to determine some changes in the system operation. We apply and will present methods of multi-variate and multi-shape regression analysis to model the data and provide outcomes + estimations for system operation so far and also for system further operation. The novelty is to providing inputs for helping to change e.g. the system maintenance policy, system operation and mission planning.

1 INTRODUCTION

The growing dependability and operation safety requirements for modern equipment together with the increasing complexity and continuous attempts to reduce operation and maintenance costs might be satisfied among others by the consistent use of modern diagnostic systems. The main task of object technical state diagnostics is not only to find out incurred failures, but also to prevent from the failure occurrence with the help of sensible detection and changes localization in the object structure and in its behaviour changes. Many various approaches have been published on system diagnostics and CBM (Condition Based Maintenance).

A tribotechnical system (TTS), friction in it, wear and lubrication, and especially the outcomes of it are the subjects of our major concern. We would like to analyse the outcomes from technical diagnostics of TTS. There exists wide range of data from the TTS which are not analysed further. We find this is a pity. Our main objective is to extract maximum information from the diagnostic of TTS in order to gain tools for optimising: maintenance, cost-benefit processes, operation and mission planning. The authors will apply selected mathematical tools to get some inputs into previously mentioned areas. Regarding the tribotechnical system, the basic information about tribological process, operating and loss variables are provided (Gesellschaft für Tribologie 2002; Czichos & Habig 2003; Koucky & Valis 2011, Valis et al. 2012, 2014).

Owing to the TTS we have got a lot of diagnostic oil data. In view of tribo-diagnostics this data is considered to be the final outcome. This data can tell us a lot about lubricants/life fluids quality itself as well as about system condition. Such data are very valuable. System operation, taking the oil samples and the outcomes themselves, are very fuzzy therefore we further plan using approaches from the fuzzy logic theory in our future research. The procedure and results presented below are based on standard mathematical principles—a regression function and a regression analysis which later will be supported with fuzzy logic. From both presumptions we can expect reasonable costs savings (see e.g. Stodola & Mazal 2012, Stodola et al. 2013). As from the military point of view we would like to determine remaining residual life to be able to perform a mission. Following the regression analysis it is possible among others to assess the operating history of an observed vehicle.

The main goal of the paper is to study and to understand the courses of oil particles generations at the beginning part of the system technical life.

2 OBJECTS OF DIAGNOSTICS AND METHODS

The assumed objects of diagnostics in our case the medium lorry T810 engines have not been ready yet in terms of design to use the ON-LINE system, though in practice similar possibilities for other applications have already existed. It results from the information stated above that we are

still supposed to use OFF-LINE engine diagnostics system when sampling lubrication fluid at certain intervals, and using known and optimised special tribodiagnostic methods (Lippay 1991). In our case we use the results and information from atomic emission spectrometry. Following this analysis we can obtain the information about the presence of the elements of a specific kind and the amount of elements. If the vagueness in classes distribution is not given by a stochastic character of measured characteristics but by the fact that the exact line among states classes does not exists, it will be later on good to use fuzzy set theory and adequate multi-criteria fuzzy logic. However, we cannot identify their real origin—e.g. as a result of fatigue, cutting or sliding.

Therefore in our further research we try to identify where the elements might come from. We base our assumptions on idea to increase the potential for maintenance optimisation inputs and cost benefit analysis inputs. Usable diagnostic approaches might be found e.g. in Klimaszewski & Woch 2012 and Woch 2013.

3 OIL FIELD DATA ASSESSMENT AND MATHEMATICAL MODEL

There is enough statistically important set of field data obtained from the diagnosed objects. It fulfils the basic assumption that we might be capable to solve this problem successfully. Since the data sets are very extensive, we are not going to introduce them here except for a part/example of Ferrum particles representing the sample of T810—it is presented in modified form in Table 1. While Mh is number of motor-hours and ppm is number of particles per milion.

We deal with dozens of samples taken and analysed at different types of observed engines. In certain aspects we consider the engine from an infantry fighting vehicle to be a reference object, because the event of a failure type has occurred in it. All tribodiagnostic processes related to the failure occurrence have been recorded. We assume that we have potential for obtaining inputs for system maintenance optimisation and system residual life estimation.

Table 1. Input data of Fe particles.

Sample/Mh	Fe particles (ppm)	Sample/Mh	Fe particles (ppm)
1/0	4.34	26/233	5.77
2/8	5.11	27/244	5.27
3/11	5.62	28/255	4.35
4/22	4.92	29/259	4.17
5/26	4.58	30/269	3.71
6/35	5.14	31/271	4.98
7/46	4.52	32/283	4.77
8/57	5.28	33/294	4.34
9/64	5.23	34/305	4.73
10/72	5.72	35/316	4.95
11/84	4.62	36/327	1.67
12/95	5.46	37/331	5.54
13/106	4.33	38/341	2.17
14/109	5.05	39/351	1.90
15/119	5.70	40/363	1.94
16/136	5.84	41/374	2.20
17/146	5.10	42/383	4.34
18/153	5.42	43/395	5.48
19/164	5.67	44/402	1.97
20/175	5.14	45/416	2.29
21/179	4.84	46/427	3.73
22/188	5.57	47/438	3.45
23/200	6.22	48/445	4.89
24/211	5.08	49/453	1.80
25/222	7.00	50/464	2.03

3.1 *Utilisation of regression model—theory*

When analysing diagnostic data, the question arises whether the data is described by only one regression function across all measurement interval, or there are areas of a different regression function in the data record. If the data is divided into more areas for which relevant regression functions will be calculated, in most cases the regression functions will have a different functional value at the point where the data is divided. When looking for a suitable regression function, a continuity requirement is often set. We would like to modify the form of our data regression functions so that they could have the same value at the point where the data is divided into single areas. At the beginning let us presume that the system is in two states. The diagnostic data will be therefore divided into two parts/areas and in each of them we will look for the regression functions whose functional value at a dividing point will be the same.

An independent variable is with a view of its random character represented by a random variable X (motohours—Mh), while a dependent variable is represented by a random variable Y (the number of Fe particles). The breakpoint for two parts will be defined by the value x_0. In the first area we are searching for the following regression function:

$y = \varphi_1(x, \boldsymbol{\beta}^1) = E(Y|X = x)$ for the data for which it applies: $x < x_0$.

In the second area we are looking for the regression function as follows:

$y = \varphi_2(x, \boldsymbol{\beta}^2) = E(Y|X = x)$ for the data for which it applies: $x > x_0$

and at the same time we require that the following equation applies:

$$\varphi_1(x_0, \boldsymbol{\beta}^1) = \varphi_2(x_0, \boldsymbol{\beta}^2)$$

We are looking for both regression functions for the whole area of data concurrently. As for our data, the regression functions will be searched for in a linear form and we will use a linear regression model:

$$y = \sum_{j=1}^{m} \beta_j f_j(x),$$

where $f_j(x)$ are known functions not containing $\beta_1, ..., \beta_m$.

This model is based on the assumptions listed below:

1. Values x are non-random so the functions $f_j(x)$ acquire non-random values $f_{ji} = f_j(x_i)$ for $j = 1, ..., m$ a $i = 1, ..., n$.
2. Matrix $F = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{m1} & \cdots & f_{mn} \end{pmatrix}$ of the type (m, n) with the elements f_{ji} is of the rank $m_m \leq n$.
3. Random variable Y_i, where $E(Y_i) = \sum_{j=1} \beta_j f_{ji}$ and $D(Y_i) = \sigma^2 > 0$ for $i = 1, ..., n$.
4. Random variables Y_i are non-correlated and have a regular probability distribution for $i = 1, ..., n$.

In the single areas we have selected the following regression functions:

for the first area: $m = 2, f_1(x) = 1, f_2(x) = x$, the regression function is: $y = \beta_1^1 + \beta_2^1 x$

for the second area: $m = 2, f_1(x) = 1, f_2(x) = x$, the regression function is: $y = \beta_1^2 + \beta_2^2 x$

For the required dependency we select the model which will fit the data and at the same time will be as simple as possible. We are going to do it like this:

1. Gradually we will select the value x_0 and a relevant regression function in the following manner: we are looking for the values $b_1^1, b_2^1, b_1^2, b_2^2$ (the point estimation of the parameters: $\beta_1^1, \beta_2^1, \beta_1^2, \beta_2^2$) so that the function:

$$S = \sum_{x<x_0} (y - (\beta_1^1 + \beta_2^1 x))^2 + \sum_{x>x_0} (y - (\beta_1^2 + \beta_2^2 x))^2$$

could acquire minimum value when:

$$\beta_1^1 + \beta_2^1 x_0 = \beta_1^2 + \beta_2^2 x_0.$$

The minimum is marked as ${}^{x_0}S^*_{\min}$

2. Out of the regression functions we select the one for which the value ${}^{x_0}S^*_{\min}$ is as low as possible. This value will be denoted as $S^*_{\min}$.

The parameters of required points might be obtained by solving the following equation:

$$\left\{ \min_{\beta_1^1, \beta_2^1, \beta_1^2, \beta_2^2} \left\{ \sum_{x<x_0} (y - (\beta_1^1 + \beta_2^1 x))^2 + \cdots + \right\} \right\}$$

$$+ \sum_{x>x_0} (y - (\beta_1^2 + \beta_2^2 x))^2 \Big| \beta_1^1 + \beta_2^1 x_0 = \beta_1^2 + \beta_2^2 x_0 \Bigg\}$$

Limitation: To keep the model simple, in both areas we have chosen linear dependability which is line-shaped. Owing to a large data spread for low values at motohours, we have selected the value x_0 from the value 20.

3.2 *Utilisation of regression model—results*

The lowest value $S^*_{\min}$ we have obtained for $x_0 = 178$ (motohours). $S^*_{\min} = 2817.053$.

The dependency ${}^{x_0}S^*_{\min}$ on the value x_0 is shown in the graph in Figure 1.

For the value $x_0 = 178$ we acquired the following regression coefficients values:

First area: Point estimation of the parameter

$$\beta_1^1 : b_1^1 = 13.039100221$$

$$\beta_2^1 : b_2^1 = 0.0425359370$$

Interval estimations: 95% dependability interval for

$$\beta_1^1 : 12.38572268,\ 13{,}69247777$$

$$\beta_2^1 : 0.033147272,\ 0.051924603$$

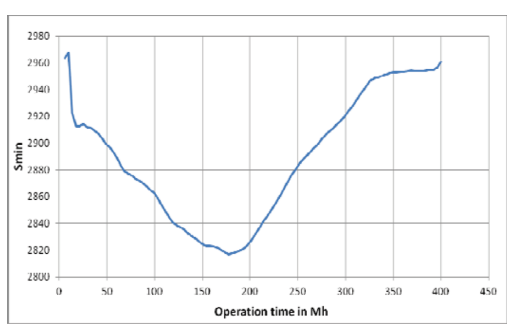


Figure 1. The dependency ${}^{x_0}S^*_{\min}$ on the value x_0.

p-value for the hypothesis H:$\beta_2^1 = 0$:1.50082E-16

Second area: Point estimation of the parameter

$\beta_1^2 : b_1^2 = 19.91494523$

$\beta_2^2 : b_2^2 = 0.003907594$

Interval estimations: 95% dependability interval for

β_1^2 :16.32517339, 23.50471707

β_2^2 : –0.0105137, 0.018328889

p-value for the hypothesis H:$\beta_2^2 = 0$:0.593893926.

As for the values of regression lines, it is important to estimate the coefficient β_2. We are testing the hypothesis H:$\beta_2 = 0$. It results from p-values that in the first area the hypothesis H:$\beta_2^1 = 0$ is rejected at the confidence level of 0.05 (p-value 1.50082E-16). As to the second area the hypothesis H:$\beta_2^2 = 0$ is not rejected at the confidence level 0.05 (p-value 0.593893926). The data in the second area then might be approximated with an invariable without diminishing the mathematical value of determination.

Original intention was to create two regression courses for the two sets of clusters in data. This is presented in Figure 2—for individual vehicle and in Figure 3 for mean value. This expression however does not provide continuous course of the curve which is important for further calculations.

Therefore the "continuous broken function" for the data was constructed. The confidence intervals might be also drawn for both an individual value y (see Fig. 4) and a mean value y (see Fig. 5).

While using the broken function we try to approximate the data by the regression function with more parameters. The value $S^*_{\min}$ then is lower than if all the area is approximated by the regression function of the same type. For two areas divided in $x_0 = 178$ and regression lines we obtained $S^*_{\min} = 2817.053$. If the data is approximated by

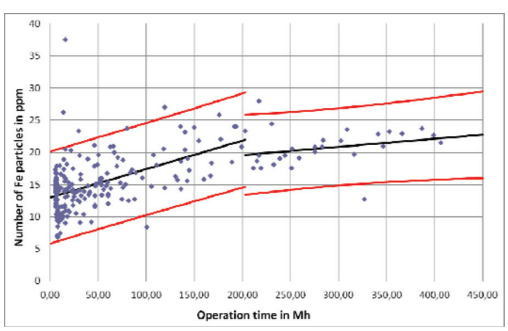


Figure 2. Course of the broken function with 95% confidence interval for individual value.

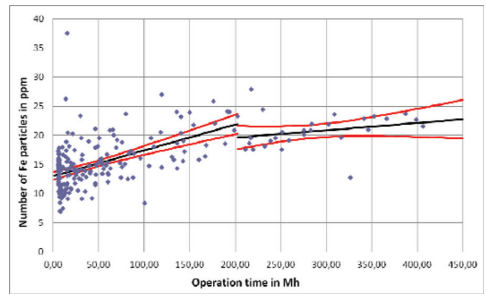


Figure 3. Course of the broken function with 95% confidence interval for individual value.

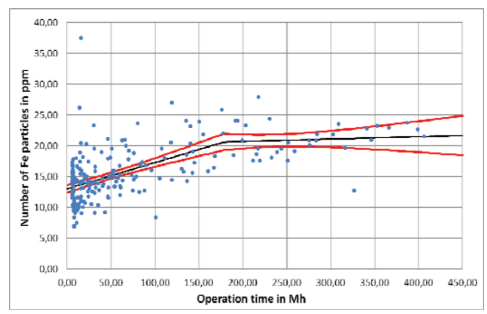


Figure 4. Course of the broken function with 95% confidence interval for individual value.

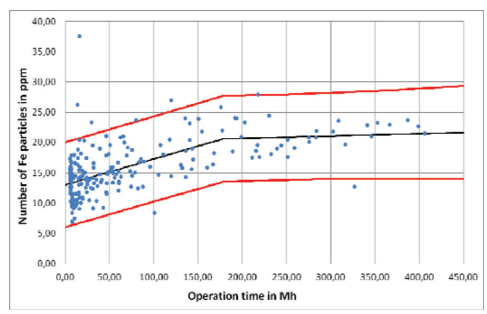


Figure 5. Course of the broken function with 95% confidence interval for mean value.

one line, then $S^*_{\min} = 2974.261342$. When approximating by a second degree polynomial, there is $S^*_{\min} = 2840.857439$, while approximating by a third degree polynomial, there is $S^*_{\min} = 2836.353795$, and with a fourth degree polynomial there is $S^*_{\min} = 2821.54932$. Approximating by a broken function is then more appropriate than using even a fourth degree polynomial. If we do not take into account continuity requirement, the regression function will have a higher degree of freedom and

S^*_{min} will get lower. For two lines we get the value $S^*_{min} = 2795.694467$.

3.3 *Summary*

It is remarkable that the *Fe* particles generation based on oil field data might have the broken form of the course. This co-relation outcome is based on the analysis performed above and will be in later research supported with the fuzzy approach. The fuzzy approach has the chance to capture the course more precisely and may suit better with the coefficient of determination R^2.

The authors hope for having broadened the possibilities of extracting and utilisation of pieces of information from TTS diagnostics- and respective interesting elements indicators. Although the regression analysis and expected utilisation of FIS are common mathematical tools they have never been properly applied for analysis of TTS oil data. Whereas the potential of the TTS oil data is actually big valuable. The authors describe just small portion of the capabilities. Application of FIS will support our idea of describing some data generation course by selected regression forms.

The authors present capabilities of the analysis results which play significant role as inputs e.g. for the system Residual Life Estimation (RLE), maintenance optimisation, mission planning, etc. Some inspirational proposals for further development especially in terms of diagnostics and maintenance optimisation are mentioned e.g. in (Babiarz 2006; Babiarz 2014a,b; Bartlett et al. 2009; Edleston & Bartlett 2012; Jodejko-Pietruczuk et al. 2010; Kierzkowski et al. 2012a,b; Kierzkowski 2010; Klimaszewski & Woch 2012, Kowalski et al. 2011, Nowakowski & Werbińska-Wojciechowska 2009, Quigley & Walls 2007; Rak & Pietrucha 2008; Revie et al. 2011; Stodola & Stodola 2010; Stodola & Stodola 2009a,b; Stodola et al. 2012; Studzinski & Pietrucha-Urbanik 2012; Valis et al. 2010, 2012, 2014; Vintr & Valis 2007, Werbińska-Wojciechowska 2013, Werbińska 2007, Woch 2013, Woch, M. 2014; Zajac et al. 2012). Using the TTS oil data from reference engine it is found that RLE might be determined for the other similar units. This approach will be further extended and developed into more precise RLE approaches.

4 CONCLUSIONS

In this paper we were looking for dependencies among measured values using statistical methods. While have applied two non-typical approaches therefore the comparison of acquired results is reasonable. At the beginning we did not know the exact theoretical background of the possible dependence of *Fe* particles occurrence on operating time.

We were looking for this dependence using suitable approximate methods. The regression analysis and the expected use of Fuzzy Inference System serve as starting methods. When dealing with the regression analysis, it is necessary to choose a regression analysis form in advance. If the regression analysis form cannot be deduced theoretically, it is necessary to select relevant regression functions and then compare them with the measured data. In the case of fuzzy methods we will not have to select the form of an expected function, but need to determine the form and the amount of language values. It follows from the other results of other sets of field data obtained from different vehicle types that when combining properly both methods, we can find out that the dependence of measured data correspond with a real process. When dealing with the assessed data, it is advisable to use the FIS first, and then, following the form of a found dependence, select a relevant regression function. Despite taking a different analytical approach when applying single methods, the results are very similar to each other (see e.g. Figs. 3 and 5). It can be then assumed that the processed dependencies can be used for describing expected development under real operating conditions.

The obtained results will be used for further research, e.g. exact determination of end of the "run-in" period, the optimising of maintenance procedures, mission planning, or the estimation of residual operating units, etc.

ACKNOWLEDGEMENTS

This paper has been prepared with the support of the Ministry of Defence of the Czech republic, Partial Project for Institutional Development, K-202, Department of Combat and Special Vehicles, University of Defence, Brno and the research project no. 3, "Management Support of Small and Middle-Sized Firms Using Mathematical Methods" of Academy Sting, Business College in Brno.

REFERENCES

Babiarz, B. (2006) An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping* 83(4): 230–235.

Babiarz B. (2014) (in prep.) Heat supply system reliability management. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Babiarz B. (2014) (in prep.) Risk assessment in heat supply system. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Bartlett, L.M., Hurdle E.E. & Kelly, E.M. (2009) Intergrated System Fault Diagnostics Utilising Diagraph and Fault Tree-based Approaches. *Reliability Engineering and System Safety* 94(9): 1371–1380.

Czichos, H. & Habig, K-H. (2003) *Tribologie-Handbuch; Reibung und Verschleiß*, 2nd edition. Weisbaden: Vieweg.

Edleston, O.S.S.T. & Bartlett, L.M. (2012) A Tabu search algorithm applied to the staffing roster problem of Leicestershire police force. *Journal of the Operational Research Society* 63(4): 489–496.

Gesellschaft für Tribologie e.V. GfT. (2002) Arbeitsblatt 7: Tribologie—Ver-schleiß, Reibung, Definitionen, Begriffe, Prüfung (GfT, Moers).

Jodejko-Pietruczuk, A., Mlynczak, M. & Zajac, M. (2010) Assessment of economical lifetime of heavy-duty machines, Case study. *Reliability, Risk and Safety: Theory and Applications*. Taylor & Francis Group, London. 1–3, 531–534.

Kierzkowski, A., Kowalski, M., Magott, J. & Nowakowski, T. (2012) Maintenance process optimization for low-cost airlines. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*. 8: 6645–6653.

Kierzkowski, A. & Zajac, M. (2012) Analysis of the reliability discrepancy in container transshipment. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012* 1: 826–831.

Kierzkowski, A. (2010) Reliability models of transportation system of low cost airlines. *Reliability, Risk and Safety: Back to the Future*: 1325–1329.

Klimaszewski, S & Woch, M. (2012) Modified Hagg & Sankey method to estimate the ballistic behaviour of lightweight metal/composite/ceramic armour and a fuselage skin of an aircraft, *Journal of KONES* 19(2): 245–252.

Koucky, M. & Valis, D. (2011) Suitable approach for non-traditional determination of system health and prognostics. Zeszyty Naukowe WSOWL 1(159): 123–134.

Kowalski, M., Magott, J., Nowakowski, T., Werbinska-Wojciechowska, S. (2011) Analysis of transportation system with the use of Petri nets. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 13(1): 48–62.

Lippay, J. (1991) Tribological diagnostics of heavy of road lorries Tatra 815 engines which operate with OA-M6 ADS II oil. Inauguration Thesis, Brno: Military Academy.

Mamdani, E.H. (1977) Applications of fuzzy logic to approximate reasoning using linguistic synthesis, *IEEE Transactions on Computers* 26(12): 1182–1191.

Nowakowski T., Werbińska-Wojciechowska S. (2009) On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing* 6(4): 364–378.

Quigley, J. & Walls, L. (2007) Trading reliability targets within a supply chain using Shapley's values. *Reliability Engineering and System Safety* 92(10): 1448–1457.

Rak, J.R. & Pietrucha, K. (2008) Risk in drinking water quality control. *Przemysl Chemiczny* 87(5): 554–556.

Revie, M., Bedford, T. & Walls, L. (2011) Supporting Reliability Decisions During Defence Procurement Using a Bayes Linear Methodology. *IEEE Transactions on Engineering Management* 58(4): 662–673.

Stodola, P., Mazal, J. (2012) The Trapezoid and S-curve for Real-time Servomotors Control. In *Proceedings of the 15th International Conference on Mechatronics—Mechatronika 2012*. Prague: Czech Technical University in Prague, 165–168.

Stodola, P., Mazal, J., Mokrá, I. & Podhorec, M. (2013) The Real-Time Control Algorithm and Control Curves for Servomotors. *International Journal of Circuits, Systems and Signal Processing*. 7(2): 118–125.

Stodola, J. & Stodola, P. (2010) Mechanical System Wear and Degradation Process Modelling. *Transactions of Famena* 34(4): 19–32.

Stodola, J. & Stodola, P. (2009 a) Operation Reliability and Diagnostics of Mechanical Systems. *Transactions of Famena* 33(1): 47–56.

Stodola, J. & Stodola, P. (2009 b) Tribology's Contribution to Efficient Maintenance of Military Engines. In: *ICMT'09*. Oprox, Brno.

Stodola, P., Jamrichova, Z. & Stodola, J. (2012) Modelling of Erosion Effects on Coating of Military Vehicles Components. *Transactions of Famena* 36(3): 33–44.

Studzinski, A. & Pietrucha-Urbanik, K. (2012) Risk Indicators of Water Network Operation. *Chemical Engineering Transactions* 26: 189–194. DOI: 10.3303/CET1226032.

Sugeno, M. (1985) *Industrial applications of fuzzy control*, Elsevier Science Pub. Co.

Valis, D., Vintr, Z. & Koucky, M. (2010) Contribution to highly reliable items' reliability assessment. *Proc. of the European Safety and Reliability Conference ESREL, Prague, Czech Republic. Reliability, Risk and Safety: Theory and Applications*. Taylor & Francis 1–3: 1321–1326.

Valis, D., Vintr, Z. & Malach, J. (2012) Selected aspects of physical structures vulnerability—state-of-the-art. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 14(3): 189–194.

Valis, D., Koucký, M. & Zak, L. (2012) On approaches for non-direct determination of system deterioration. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 14(1): 33–41.

Valis, D., Zak, L. & Pokora, O. (2014) On approaches for non-direct determination of system deterioration. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 14(1): 33–41.

Vintr, Z. & Valis, D. (2007) Aircraft gun reliability modelling. *Proc. of the European Safety and Reliability Conference ESREL, Stavanger, Norway, Risk, Reliability and Societal Safety.* Proceedings and Monographs in Engineering, Water and Earth Sciences 1–3: 2769–2774.

Werbinska-Wojciechowska, S. (2013) Time resource problem in logistics systems dependability modelling. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 15(4): 427–433.

Werbinska, S. (2007) Interactions between logistic and operational system—an availability model. *Risk, reliability and societal safety. Eds. Terje Aven, Jan Erik Vinnem.* Leiden: Taylor and Francis, 2045–2052.

Woch, M. (2013) Analysis of operating loads on an aircraft's vertical stabilizer on the basis of recorded data, *Chemical Engineering Transactions* 33: 643–648.

Woch, M. (2014) (in prep.) Risk analysis of the point on aging aircraft structure. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Zajac, M. & Kierzkowski, A. (2012) Uncertainty assessment in semi Markov methods for Weibull functions distributions. *Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011*: 1161–1166.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dependability and safety analysis of ERTMS level 3 using analytic estimation

T. Babczyński & J. Magott
Wrocław University of Technology, Wrocław, Poland

ABSTRACT: Dependability and safety in European Rail Traffic Management System (ERTMS) level 3 are influenced by quality of train localisation and GSM-R communication. In ERTMS level 3, traffic is controlled by so called moving block that is associated with the distance between subsequent trains. In order to satisfy strong safety-related railway standards, GNSS (Global Navigation Satellite System) is supported by odometry, e.g. Eddy Current Sensors (ECSs). In the paper, the relationship between probability of emergency train braking as a function of distance between subsequent trains for dependability parameters of GNSS plus ECS train localisation, and GSM-R is studied. Tunnel environment only is considered. An analytic estimations of this relationship has been proposed.

1 INTRODUCTION

Dependability and safety parameters in Europe railway domain are specified in standards (CENELEC, 2000, CENELEC, 2003). According to standard (IEC, 1990): "dependability is the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance". Safety levels are characterized by tolerable hazard rate for Safety Integrity Levels (SIL) (CENELEC, 2003).

European Rail Traffic Management System (ERTMS) is the European standard for train control and command systems, which is intended to unify all European systems and to enhance cross-border interoperability. There are three levels of ERTMS, with level 3 as the highest. In ERTMS level 3, traffic is controlled by so called moving block that is associated with the distance between subsequent trains. Dependability and safety are influenced by quality of localisation of trains (Beugin & Marais, 2012, Lu et al., 2013, Nguyen et al., 2013) and communication (Flammini et al., 2006, Hermanns et al., 2005, Qiu et al., 2014, Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005). Information is exchanged between trains and trackside coordination unit so-called Radio Block Centres (RBCs) via GSM-R (rail GSM communication). A train needs to receive so-called movement authorities from the RBC in order to continuously run at high speed. Data processing on board the train and in the RBCs, and radio communication link are crucial factors for safety and efficient operation. Train localization, speed, and integrity information is prepared on board the train, and reported from train to RBC at regular intervals. Train localization is based on GNSS (Global Navigation Satellite System). GNSS is not sufficient to satisfy the strong safety-related requirements of railway standards (Beugin & Marais, 2012, Lu et al., 2013). Hence, GNSS is supported by odometry (Acharya et al., 2011, GRAIL2, 2012), e.g. Eddy Current Sensors (ECSs) (Nguyen et al., 2013) in order to provide a safe, accurate and continuous train position. The RBC declares the track space behind the train clear which is used in moving block operation mode.

The relationship between probability of train stopping as a function of distance between subsequent trains, for given dependability parameters of GNSS and ECS train localisation, and GSM-R is studied in the paper. Tunnel environment only is considered.

The *problem* investigated in the paper is as follows.

Input:

- Dependability parameters of GNSS plus ECS train position localization in tunnel environment,
- Train speed,
- Emergency braking distance,
- Train length,
- Maximal position localization error,
- Random variable of emergency braking and stopping time,
- Probability of incorrect transmission from train to RBC and from RBC to train,
- Random variable of duration time of correct transmissions from train to RBC and from RBC to train,
- Processing time in RBC.

Output:

– Probability of stopping as a function of distance between subsequent trains.

The above problem with less detailed treatment of train position localization dependability has been studied in the papers (Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005). Our study is based on GSM-R communication and operation parameters from these papers.

Train position localisation service availability for GNSS and ECS unit has been presented in (Nguyen et al., 2013). The results for GNSS localisation service have been obtained using Ergospace software (Ergospace, 2008). Hence, obtained results are approximate only. Our study is based on these data.

Petri nets (Barger et al., 2009, Nguyen et al., 2013, Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005), and statecharts or state machines (Hermanns et al., 2005, Qiu et al., 2014, Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005) are often used in dependability or safety analysis of ERTMS systems. The examples of other modelling languages used in dependability or safety analysis are fault trees and Bayesian networks (Flammini et al., 2006).

In papers (Hermanns et al., 2005, Nguyen et al., 2013, Qiu et al., 2014, Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005), in order to solve dependability or safety problems, simulation experiments are performed or linear equation systems are solved.

The analytical estimation of the probability of stopping as a function of distance between subsequent trains is subject of this paper. This estimation is expressed by simple formula.

Analytic solutions and estimations seems to be valuable research direction in dependability studies of transport systems. This is a complementing approach to Petri net based, or Monte-Carlo simulation. For instance, in paper (Kowalski et al., 2014), exact and approximation methods for dependability assessment of tram system with spare trams and repair under time window constraint have been presented.

Structure of the paper is as follows. Dependability features of GNSS and ECS based train localisation unit (Nguyen et al., 2013) are recalled in Section 2. Communication and operation for ERTMS 3 is given in next section. Analytic estimation of the probability that a train is stopped after emergency braking is presented in Section 4. In this section, train localisation error given in meters is taken into account. An integration of a result given in (Nguyen et al., 2013) and the estimation is given in Section 5. In this section, more dependability aspects of train localisation than in previous section are considered. Finally, there are conclusions.

2 GNSS AND ECS BASED TRAIN POSITION LOCALIZATION

In ERTMS level 3, train position localisation is GNSS based. However, GNSS's do not satisfies safety-related railway requirements. Even GNSS supported by inertial navigation systems do not meet these requirements. Hence, data fusion options of GNSS and other sensors signals is interesting field of studies. In papers (Acharya et al., 2011, Nguyen et al., 2013), integration of GNSS and ECS signals is considered. This section is based on paper (Nguyen et al., 2013).

When analysing dependability of train localisation unit, the following cases can be considered:

Case A—unavailable output of GNSS and EDS signals fusion based component, i.e. localisation service is interrupted.
Case B—untrustworthy position, i.e. the position result has a large estimated confidence interval. Localisation information is delivered, however, it cannot be used safety critical train control.
Case C—estimated position is outside accuracy limits. Localisation service is failed but it is not recognized by the system or by the user.

Train position localisation service availability for single GNSS unit, ECS and GNSS unit, respectively, have been presented in (Beugin & Marais, 2012, Nguyen et al., 2013). The results for GNSS localisation service have been obtained using Ergospace software (Ergospace, 2008). Hence, obtained results are approximate only.

For each case, the following causes (Nguyen et al., 2013) are considered:

Case A—Fusion component failure,
Case B—Missing GNSS during 60 s, Missing ECS & GNSS during 3 s,
Case C—Failed ECS & two consecutive GNSS position errors greater than 50 m, six consecutive GNSS position errors greater than 50 m.

Failure rates for the following hardware components:

GNSS antenna,
GNSS receiver,
ECS device,
fusion component,

have been the input parameters for calculating the probability of service failure.

Failed components are repaired.

Software error in the fusion component has not been taken into account in calculation of dependability.

The research has been done for four environments:

– urban,
– tunnel,

– woody,
– railway cutting.

Now, we recall two interesting results (Nguyen et al., 2013).

In woody environment, the more than six consecutive GNSS position errors greater than 50 m with occurrence probability of $7.59E^{-2}$ is the critical event which leads to the global service failure.

In tunnel environment, the occurrence probability of this factor is reduced and is non significant while the missing GNSS data for more than 60 s with its occurrence probability of $1.53E^{-2}$ is the main cause of the service failure.

In present paper, the results for tunnel environment will be applied.

3 GSM-R COMMUNICATION AND OPERATION FOR ERTMS LEVEL 3

We analyse the same scenario of two trains following one of the other on the same rail, as the authors of the papers (Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005), see Figure 1. The first train automatically checks its integrity and determines its position. The goal of checking the train integrity is e.g. to identify the case when a part of train carriages are lost from the main train. This task, together with the preparing of the *status message*, takes the time of 5 s. Next, the worked up status message is sent through the GSM-R module to the nearest RBC. Due to the possible transmission errors, the message can be incorrect with the probability of 1,88%. The successful transmission takes the exponentially distributed random time with the mean value of 450 ms. Next, the RBC prepares the *authority message* for the succeeding train. This task is 500 ms long and after it the prepared message is sent using the GSM-R module again (with the same error rate and transmission time as in the previous case). The following train waits for the consequent messages. If the message lacks to come for the long time, the situation becomes hazardous and due to this fact the emergency braking procedure is initiated. After the emergency stop the train is immobilized for the exponential random time with mean value of 15 min (900 s).

The deadline used for waiting for the authority message is calculated as the value which ensures the safe stopping of the second train in the case

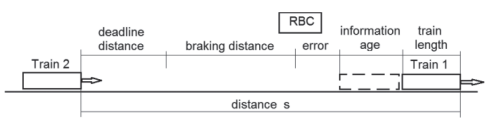


Figure 1. Distances used in eq. (1).

when the first one stops (or lost its integrity) immediately after sending the message that the second train received previously. The deadline is determined from the following equation, (Fig. 1):

$$d = \frac{s - l}{v} - a \tag{1}$$

where s is the initial distance from the head of the first train to the head of the second one, l is the sum of the train length, safety margin, the braking distance and the measured position error, and is assumed as 3000 m, v is the speed of trains—300 km/h (83 m/s), a is the information age assumed as 5 s or 9 s in the future investigations.

4 ANALYTIC ESTIMATION FOR GSM-R COMMUNICATION AND OPERATION

First, analytic estimate from paper (Babczynski & Magott, 2014) will be recalled. The derivation of the estimate in present paper is changed when comparing with the derivation from the above paper. Then an improvement of this estimate will be given.

Position/integrity package is generated by *Train* 1 (Fig. 1) each 5 s. This time will be denoted by p. Let us consider time intervals of length d, where d has been defined in previous section by expression (1). For *Train* 1 this interval is started immediately after sending the last package, while for *Train* 2—after receiving the last package. The number of the packages generated during the interval, without the package which initiates the interval, for *Train* 1 is

$$n = \mathrm{int}(d/p) \tag{2}$$

where int(x) is the integer part of x. If packages are not lost then the number of packages that are sent by *Train* 1 is equal the mean number of packages that are received by *Train* 2.

Property
The mean number of packages that should arrive *Train* 2 in time interval of length d is equal to the mean number of packages that are sent by *Train* 1 in time interval of length d, provided observation interval length is going to infinity.

Let the probability that package transmission from *Train* 1 to the RBC is incorrect be q. In considered example $q = 1.88\%$. Let the probability that package transmission from the RBC to *Train* 2 is incorrect be the same. Package transmission from *Train* 1 to *Train* 2 is incorrect in three cases:

– the package transmission from *Train* 1 to the RBC is incorrect, while the package transmission from the RBC to *Train* 2 is correct,

– the package transmission from *Train* 1 to the RBC is correct, while the package transmission from the RBC to *Train* 2 is incorrect,
– the above both transmissions are incorrect.

Hence, the probability that the package transmission from *Train* 1 to the RBC is incorrect or that the package transmission from the RBC to *Train* 2 is incorrect is equal to:

$$Q = q(1-q) + (1-q)q + q^2 = 2q - q^2 \tag{3}$$

It is the probability of incorrect transmission from *Train* 1 to *Train* 2.

The probability that each of n packages that are sent in time interval d are incorrectly transmitted is $E = Q^n$. It is probability for a train being stopped because of waiting time for the correct package is at least equal to the deadline d.

One is interested in probability of occurrence of the train being stopped event in one year (1 year) period. For one train, the number of package transmissions between *Train* 1 and *Train* 2 in 1 year is

$$k = \frac{1\,\text{year}}{p} \tag{4}$$

Mean number of occurrences of the train being stopped event in the interval is

$$S = Q^n \cdot k \tag{5}$$

Let st be the mean stopping time for one stopping. In our example $st = 900$ s. Mean time of total stopping time in 1 year is

$$T = st \cdot S \tag{6}$$

The estimate of probability that a train is stopped is given by:

$$PS = T/1\,\text{year} \tag{7}$$

Therefore, after transformations the probability estimate that *Train* 2 is stopped is:

$$PS = st \cdot \frac{Q^n}{p} \tag{8}$$

Accuracy of this estimate is illustrated in Figure 2.

Now, an improvement of the estimate will be given.

Let sp_i be a package which is sent from *Train* 1. Then it is processed by the RBC, and finally, the RBC sends packet rp_i to *Train* 2.

Package transmission times from *Train* 1 to RBC and from RBC to *Train* 2 are given by the same

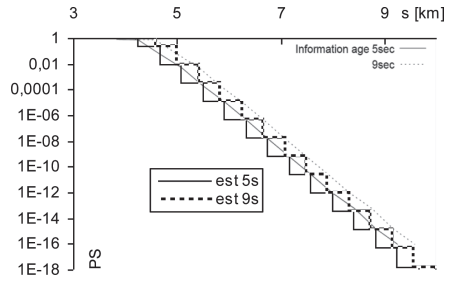


Figure 2. Estimation results (stair shape lines) (Babczynski & Magott, 2014) on the background of the chart from (Trowitzsch & Zimmermann, 2006) (smooth lines).

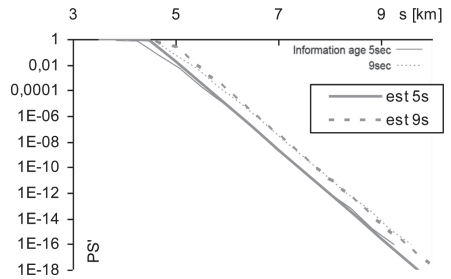


Figure 3. Results of the improved estimate of probability that *Train* 2 is stopped as a function of distance between trains (thicker lines) on the background of the chart from (Trowitzsch & Zimmermann, 2006).

exponential random variable. Hence, transmission time can be much longer than the mean value of the random variable. Let package sp_i, rp_i, respectively, be the one that opens sending, receiving, interval of length d at *Train* 1, *Train* 2, side. Some packages that are sent from *Train* 1 in the sending interval cannot reach *Train* 2 in the receiving interval. Formula of new estimate is adapted to results contained in (Trowitzsch & Zimmermann, 2006). The estimate of mean number of such packages received by *Train* 2 in the receiving interval that have been sent in the sending interval are

$$m = \max\left\{0, \frac{d}{p} - 1\right\} \tag{9}$$

New probability estimate that *Train* 2 is stopped is:

$$PS' = \min\left\{1, st \cdot \frac{Q^m}{p}\right\} \tag{10}$$

Quality of the improved estimate is illustrated by Figure 3.

Accuracy of the estimation is very good for the considered case. However, verification for wider range of parameter values is required.

5 PROBABILITY OF STOPPING AS A FUNCTION OF DISTANCE BETWEEN SUBSEQUENT TRAINS IN TUNNEL

According to approximate results contained in paper (Nguyen et al., 2013), in tunnel environment, Case A and Case B, given in Section 2 are significant factors. For each case, the contribution of them (probability) is as follows (Nguyen et al., 2013):

- Case A—Fusion component failure—$3.42E^{-6}$,
- Case B—Missing GNSS during 60 s—$1.53E^{-2}$, Missing ECS & GNSS during 3 s—$6.63E^{-7}$,
- Case C—Failed ECS & two consecutive GNSS position errors greater than 50 m—0, six consecutive GNSS position errors greater than 50 m—0.

For cases A and B, train localisation service is unavailable at *Train* 1 side.

Train localisation information is unavailable at *Train* 2 side when:

- train localisation service is unavailable at *Train* 1 side,
- the package transmission from *Train* 1 through the RBC to *Train* 2 is incorrect.

Let r be the probability that train localisation service is unavailable at *Train* 1 side. In the considered tunnel environment, $r = 1.53E^{-2}$.

The probability that train localisation information is unavailable at *Train* 2 side is:

$$R = r + (1 - r)Q. \tag{11}$$

Hence, probability estimate that *Train* 2 is stopped is:

$$PS'' = \min\left\{1, st \cdot \frac{R^m}{p}\right\} \tag{12}$$

In Section 3, according to (Zimmermann & Hommel, 2005) it has been supposed that train position localisation error is 20 m. Now, for tunnel environment and GNSS plus ECS localisation unit, it is assumed that maximal value of this error, provided the localisation information is delivered, is 200 m. The other parameters are such as in Sections 3, 4.

The probability estimate of stopping, when dependability of train localisation service and GSM-R are taken into account, as a function of distance between subsequent trains is given by Figure 4.

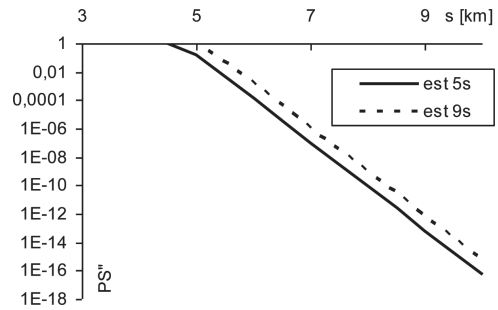


Figure 4. Results of the estimate of probability that *Train* 2 is stopped in a tunnel environment as a function of distance between trains.

6 CONCLUSIONS

New analytic estimation of probability of train stopping as a function of distance between subsequent trains has been given. Computation cost of this estimate is very small. The estimation has been verified against results obtained for GSM-R communication and operation in ERTMS level 3 using simulation approach supported by rare event analysis (Trowitzsch & Zimmermann, 2006, Zimmermann & Hommel, 2005). Standard Monte-Carlo simulation is not sufficient because of computational cost. Accuracy of the estimation is very good for the considered case. However, verification for wider extent of parameter values is required.

Then the estimation has been applied for calculating the probability of train stopping as a function of distance between subsequent trains when dependability of GNSS plus ECS train localisation unit, and GSM-R communication have been taken into account. The studies have been done for tunnel environment. Because of lack of real data, approximate dependability information (Nguyen et al., 2013) has been used. This information (Nguyen et al., 2013) has been obtained using simulation.

The research is stimulated by real life ERTMS level 3. Farther analysis for real life data is planned.

REFERENCES

Acharya, A., Sadhu, S. & Ghoshal, T.K. 2011. Train localization and parting detection using data fusion. Transportation Research Part C-Emerging Technologies, 19, 75–84.

Babczynski, T. & Magott, J. 2014. Dependability and safety analysis of ETCS communication for ERTMS level 3 using performance statecharts and analytic estimation. Advances in Intelligent Systems and Computing. Springer.

Barger, P., Schön, W. & Bouali, M. 2009. A study of railway ERTMS safety with colored Petri nets. Reliability, Risk and Safety: theory and application, 2, 1303–1309.

Beugin, J. & Marais, J. 2012. Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization. Transportation Research Part C-Emerging Technologies, 22, 42–57.

EN50126. 2000. Railway application–The specification and demonstration of dependability, Reliability, Availability, Maintainability and Safety (RAMS). CENELEC. Brussels.

EN50129. 2003. Railway applications-Communication, signalling and processing systems-Safety related electronic systems for signalling. CENELEC. Brussels.

Ergospace. 2008. Ergospace [Online]. Touluse. Available: http://www.ergospace.fr/index_anglais.html [Accessed 28 04 2014].

Flammini, F., Marrone, S., Mazzocca, N. & Vittorini, V. 2006 Modelling structural reliability aspects of ERTMS/ETCS by Fault Trees and Bayesian Networks. Proc. of the European Safety & Reliability Conference, ESREL, 2006.

GRAIL2. 2012. Available: http://grail2.ineco.es/Grail2/html/main.jsp [Accessed 28 04 2014].

Hermanns, H., Jansen, D.N. & Usenko, Y.S. 2005 From StoCharts to MoDeST: a comparative reliability analysis of train radio communications. Proceedings of the 5th international workshop on Software and performance, 2005. ACM, 13–23.

IEC 1990. IEC 60050-191. International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service. International Electrotechnical Commission (IEC) Standard.

Kowalski, M., Magott, J., Nowakowski, T. & Werbinska-Wojciechowska, S. 2014. Exact and approximation methods for dependability assessment of tram systems with time window. European Journal of Operational Research, 235, 671–686.

Lu, D., Grasso Toro, F. & Schnieder, E. 2013 RAMS evaluation of GNSS for railway localisation. Intelligent Rail Transportation (ICIRT), 2013 IEEE International Conference on, 2013. IEEE, 209–214.

Nguyen, T., Beugin, J. & Marais, J. 2013, Dependability evaluation of a GNSS and ECS based localisation unit for railway vehicles. ITS Telecommunications (ITST), 2013 13th International Conference on, 2013. IEEE, 474–479.

Qiu, S., Sallak, M., Schon, W. & Cherfi-Boulanger, Z. 2014. Modeling of ERTMS Level 2 as an SoS and Evaluation of its Dependability Parameters Using Statecharts. Systems Journal, IEEE, PP, 1–13.

Trowitzsch, J. & Zimmermann, A. 2006. Using UML state machines and petri nets for the quantitative investigation of ETCS. Proceedings of the 1st international conference on Performance evaluation methodolgies and tools. Pisa, Italy: ACM.

Zimmermann, A. & Hommel, G. 2005. Towards modeling and evaluation of ETCS real-time communication and operation. *Journal of Systems and Software,* 77, 47–54.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Streamlining architectures for integrated safety analysis using Design Structure Matrices (DSMs)

Kai Höfig & Joe Zhensheng Guo
Siemens AG, Corporate Technology, München, Germany

Amir Kazeminia
TRW Automotive GmbH, Krefeld, Germany

ABSTRACT: A popular trend to handle safety analysis of complex software intensive embedded systems is integrated model-based safety analysis. Well accepted safety engineering approaches like fault trees are shifted to the level of model-driven development by integrating safety models into functional development models. On the one hand this provides benefits for consistency and traceability, on the other hand the selection of appropriate model elements or level of hierarchies for such an integration is a new task to be tackled. Especially for fault tree-based approaches the existence of loops or cyclic dependencies in development models can be problematic since loops cannot be a part of a Boolean model. To prevent such loops in safety analysis models, we show how Design Structure Matrices (DSMs) can be used to cluster architecture elements with loops or with cyclic dependencies. Using this, we assume that small adjustments in the architecture model provide vast improvements when modeling a seamless integrated safety analysis model.

1 INTRODUCTION

Modern safety critical embedded systems tend to increased complexity. To handle this complexity, model-based approaches are introduced in industrial applications and even covered within standards, e.g. ISO26262 for the automotive domain (ISO26262 2009) or DO178C for airborne systems (DO-178C 2012). A popular trend for a safety analysis of such systems is to combine safety analysis models and system development models. Examples for such model-based safety analysis approaches can be found in (Rugina 2005, Fenelon & McDermid 1992, Chen, Johansson, Lnn, Papadopoulos, Sandberg, Trner, & Trngren 2009, Kaiser, Liggesmeyer, & Mäckel 2003). These widely accepted safety engineering approaches shift the task of failure logic modeling to the layer of model-driven development. They integrate or at least relate safety analysis models to elements of functional system development models. This is beneficial for the consistency and also the traceability between safety engineering- and system development models.

Some system modeling approaches such as SysML use ports and connections to model dependencies or a flow of information or goods from one component to another. In such models, loops or cyclic dependencies are unproblematic, but they mislead us to transfer such loops from the development model to the safety analysis model. Even though loops in safety analysis models can be broken up automatically, e.g. for Boolean structures as described in (Domis & Trapp 2008), this leads to confusing and hard to read safety analysis models.

This problem is addressed in this paper by re-clustering components of system development models in a way that do not contain loops. Design Structuring Matrices (DSMs) are used here to minimize the changes in system development models and also to identify such loops. Using this approach, we assume that small changes in the architecture model provide vast improvements when modeling a seamless integrated safety analysis model.

The rest of the paper is structured as follows: first, section 2 summarizes related work. In section 3, an example system is introduced to illustrate the problem of loops for integrated safety analysis models. In section 4, DSMs are used to overcome this problem by re-clustering the component hierarchy. Section 5 summarizes this paper and provides a perspective for future work.

2 RELATED WORK

Fault tree analysis is one of the major applications for Boolean models in safety analysis. Loops in such models lead to events that are caused by itself. For

analysis, they have to be removed from the model in order to solve this illogical dependency. Other models that are used for safety assessment allow loops, for example Markov chains or Petri nets (Reisig 1985, Häggström 2007), but such models are compared to fault trees less intuitive and therefore only used if more advanced logic is required.

Approaches that generate fault trees deal with the problem of loops and how to prevent them. E.g. in (Liggesmeyer & Mäckel 2000), fault trees are generated from electric design plans and a hierarchical abstraction approach is used to prevent the generation of loops. In (Papadopoulos & Maruhn 2001) fault trees are generated for Matlab models and also in (Iverson 1992), fault tree structures are generated. Digraph models are converted and valid loop free fault trees are generated. In (Banach & Bozzano 2006) fault tree structures are generated for large systems that also can contain loops and in (Rae & Lindsay 2004) fault trees are generated over different hierarchy levels and with various cycles in the system development model. In (Papadopoulos & McDermid 1999) failure propagation information is also modeled along with the information flow of components and over different levels of hierarchy. Fault tree information can be extracted from these models. Nevertheless, automatically generated fault trees require precise information about failures and their propagation or are only able to generate fault trees for specific applications.

Other approaches deal with the problem of automatically removing existing loops in fault trees. In (Ciarambino, di Torino, Contini, Demichela, & Piccinini 2002), syntax rules are used to identify and remove loops. In (Domis & Trapp 2008) Boolean structures are analyzed and loops are removed from the safety analysis model. However, these type of approaches require prior recognition by the analyst of the initiation of a loop. To enable automations for fault tree structures that do not require interactions with analysts, the prevention of loops during the design phase is most beneficial. Therefore, in the following sections a methodology is presented that prevent the modeling of loops by restructuring elements of system development models.

3 PROBLEM DESCRIPTION

Boolean safety analysis models that are highly integrated into the architecture models of a safety-critical system easily lead to model loops. Figure 1 shows a SysML Internal Block Diagram (IBD) of a small open-loop example system and the corresponding Boolean safety analysis model. On top of that figure, the model elements marked as *blocks* represent the components of the system. Here, a sensor component evaluates a sensor value and provides the signal to the component *Processing 1*. The component *Processing 2* is interacting with *Processing 1* until a result is calculated that is forwarded to a actuator. A watchdog component monitors the time the processing components requires for calculating a command. If a time line is exceeded, the watchdog sets the actuator in a safe state. This model contains a cyclic dependency. Component *Processing 1* awaits input from *Processing 2* and vice versa. This is unproblematic in this model but easily can mislead to a loop in the corresponding safety analysis model.

In the lower part of figure 1, Component Fault Trees (CFTs) are used as a safety analysis model using Boolean logic (Kaiser, Liggesmeyer, & Mäckel 2003). CFTs are an extension to classic fault trees using additionally elements from the development model, such as components, ports and interconnections. They are integrated into the model of a safety-critical system in order to model the failure logic separately for each component. A failure propagates from one component to another following the ports

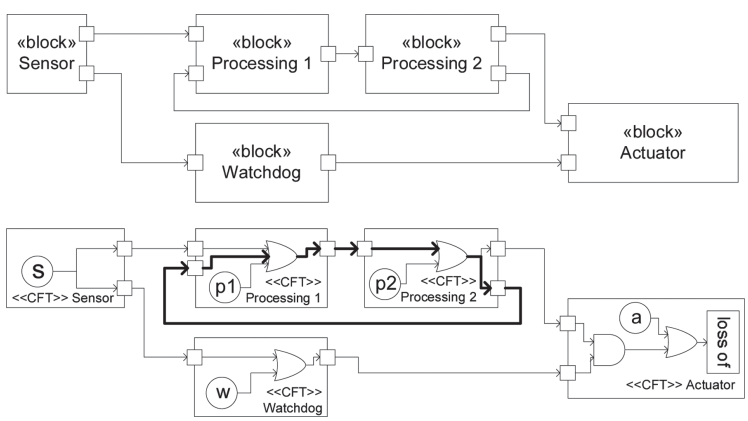


Figure 1. Two views on an example system: interacting blocks and corresponding component integrated fault trees (C^2FTs).

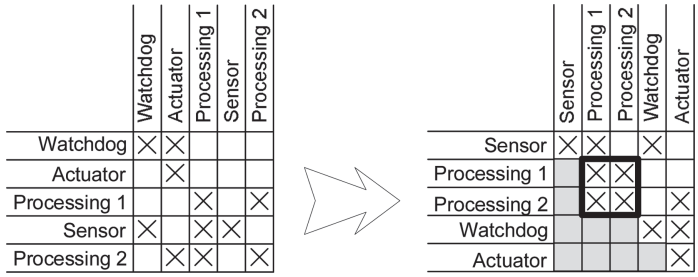


Figure 2. DSM for the example system (left matrix) and DSM after the sequencing algorithm (right matrix).

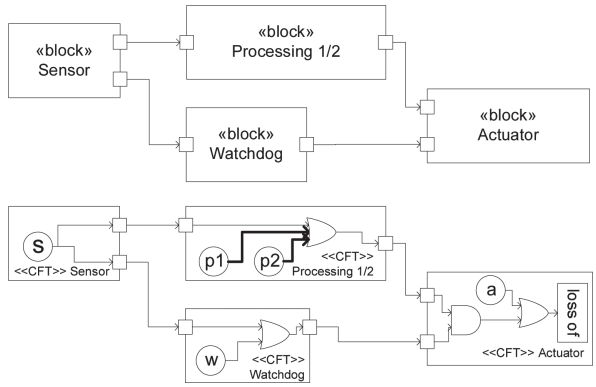


Figure 3. Example system after applying the sequencing algorithm: interacting blocks and corresponding Component Fault Trees (CFTs).

and the connections between the ports. For example, the component *watchdog* gets a signal from the sensor component and provides a signal to the actuator. The command provided to the actuator is either erroneous if the input is erroneous or if the watchdog itself contains an internal error (basic event *W* and *OR*-gate within the watchdog CFT). CFTs can contain multiple failure modes, but in this example only the failure mode *erroneous* is investigated.

If such Boolean structures are part of safety-critical systems, the architecture models can contain loops or cyclic dependencies. Such loops are unproblematic in system development models, but are prohibited in Boolean models. An example for a loop within the development model can be found in figure 1 for *Processing 1* and *Processing 2* as described earlier. If these components are developed by different teams, such a Boolean loop can easily be transferred to the safety analysis model. An example for this loop is marked by the thick black line in the safety analysis model in the lower part of figure 1. The output failure mode modeling the occurrence of an erroneous signal as an output for component *Processing 2* is cyclic. The example system is comparatively small and only contains a single failure mode, but for larger structures, many people involved in a development process and multiple failure modes, such loops can be of various complexity and have to be removed from Boolean safety analysis models such as fault trees.

In the following section, design structuring matrices are used in combination with a sequencing algorithm to prevent such loops or cyclic dependencies in component-based safety analysis models such as component fault trees.

4 USING DSMS FOR INTEGRATED SAFETY ANALYSIS

A Design Structure Matrix (DSM) represents dependencies among various items that can be processes, products, components or organizations (Browning 2001). The corresponding DSM for the example system as illustrated in figure 1 is depicted in figure 2 on the left side. Each component has a row and a column in the DSM. All components depend on themselves and so the diagonal of the matrix is crossed. The rows show provisions, e.g., the row *Sensor* shows that the sensor component sends signals to the components *Watchdog* and *Processing 1*. The columns of the DSM show dependencies, e.g., the column *Actuator* shows that the actuator component receives signals from the *Watchdog* component and the *Processing 2* component.

Using these relations within the DSM, the matrix can be *sequenced* to identify dependency loops as described in (Warfield 1973). This sequencing algorithm helps to identify loops and if found, identify components that can be merged to remove such loops or cyclic dependencies. The result of this algorithm can be seen in figure 2 on the right side. Here, all dependencies are in the right upper part of the matrix. In the left lower part (grey area) is only one dependency between *Processing 1* and *Processing 2*. Without this cross mark, the matrix would be *upper triangular*, what means that there are no loops in the development model. So, if the components *Processing 1* and *Processing 2* are encapsulated within one component, the dependencies between the components of the example system are free of loops and modeling loops in component fault trees is prevented.

Figure 3 shows the system with the encapsulation of the components *Processing 1* and *Processing 2* into one component *Processing 1/2*. As we can see in the CFT model for this encapsulated architecture, all connections between the ports of the model are straightforward and do not form loops. So, it is impossible to erroneously model loops in the safety analysis model even if the components and their component fault trees are modeled by different teams. The DSM can help to identify such loops in the architecture and to identify the corresponding components to be encapsulated for safety analysis.

5 CONCLUSION AND FUTURE WORK

In this paper, a methodology is presented that restructures system development models in order to prevent loops in fault trees using Design Structuring Matrices (DSMs). The assumption is, that small adjustments in the architecture model provide vast improvements when modeling a seamless integrated safety analysis model. Nevertheless, large systems can contain a lot of loops, what would require vast changes of the development model. Also large loops over entire architectures may result in one large component when this methodology is applied. In our future work, the approach needs to be evaluated for larger systems since the current evaluation of the methodology is only based on a small exemplary system. Even if restructuring the system development model is impossible, the DSM approach can help to identify clusters of components where loops can be expected. This can help to improve the process of modeling fault trees and gives hints where development teams for different components need frequent balancing.

REFERENCES

Banach, R. & M. Bozzano (2006). Retrenchment, and generation of fault trees for static, dynamic and cyclic systems. *Proceedings of 25th International Conference, SAFECOMP*, 127–141.

Browning, T. (2001, aug). Applying the design structure matrix to system decomposition and integration problems: a review and new directions. *Engineering Management, IEEE Transactions on 48*(3), 292–306.

Chen, D., R. Johansson, H. Lnn, Y. Papadopoulos, A. Sandberg, F. Trner, & M. Trngren (2009). Modelling Support for Design of Safety-Critical Automotive Embedded Systems. In *Computer Safety, Reliability, and Security*, pp. 72–85.

Ciarambino, I., P. di Torino, S. Contini, M. Demichela, & N. Piccinini (2002). How to avoid the generation of loops in the construction of fault trees. *Reliability and Maintainability Symposium, 2002. Proceedings. Annual,* 178–185.

DO-178C (2012). Software Considerations in Airbone Systems and Equipment Certification Standard. Radio Technincal Commission for Aeronautics.

Domis, D. & M. Trapp (2008). Integrating Safety Analyses and Component-Based Design. In *SAFECOMP*, pp. 58–71.

Fenelon, P. & J. McDermid (1992). Integrated techniques for software safety analysis. *IEE Colloquium on Hazard Analysis*, 2/1–216.

Häggström, O. (2007). *Finite Markov Chains and Algorithmic Applications*. London Mathematical Society, Camebridge University Press.

ISO26262 (2009). ISO/DIS 26262. International Organization for Standardization (ISO), Draft International Standard (DIS).

Iverson, D.L. (1992). Automatic translation of digraph to fault-tree models. *Reliability and Maintainability Symposium, 1992. Proceedings., Annual,* 354–362.

Kaiser, B., P. Liggesmeyer, & O. Mäckel (2003). A new component concept for fault trees. In P.A. Lindsay and A. Cant (Eds.), *Safety Critical Systems and Software 2003, Eigth Australian Workshop on Safety-Related Programmable Systems, (SCS2003), Canberra, ACT, Australia, 9–10 October 2003*, Volume 33 of *CRPIT*, pp. 37–46. Australian Computer Society.

Liggesmeyer, P. & O. Mäckel (2000). Automatic Reliability Analysis of Electronic Designs Using Fault Trees. *Workshop Testmethoden und Zuverlässigkeit von Schaltungen und Systemen 13*.

Papadopoulos, Y. & M. Maruhn (2001). Model-Based Automated Synthesis of Fault Trees from Matlab. Simulink Models. *International Conference on Dependable Systems and Networks*.

Papadopoulos, Y. & J.A. McDermid (1999). Hierarchically Performed Hazard Origin and Propagation Studies. *Computer Safety, Reliability and Security*.

Rae, A. & P. Lindsay (2004). A behaviour-based method for fault tree generation. *Proceedings of the 22nd International System Safety Conference*, 289–298.

Reisig, W. (1985). *Petri Nets: An Introduction*, Volume 4 of *Monographs in Theoretical Computer Science. An EATCS Series*. Springer.

Rugina, A. (2005). System Dependability Evaluation using AADL (Architecture Analysis and Design Language). LAAS-CNRS.

Warfield, J.N. (1973, sept). Binary matrices in system modeling. *Systems, Man and Cybernetics, IEEE Transactions on SMC-3*(5), 441–449.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The Markov reliability and safety model of the railway transportation system

F.J. Restel
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: In this paper, the author's research work is focused on modeling of railway transportation system's reliability and safety. The paper begins with an introduction related to a literature review on railway transportation system functionality, reliability and safety modeling. The set of states can be divided into two subsets: availability set and failure set of states. Defining states in terms of railway transportation system is a complex issue, therefore the state classification into availability an failure is not sufficient. In addition to the technical effects associated with incorrect operation of system components, traffic consequences (traffic disruptions) of events are important, especially in case of railway transportation system. The Markov model was built is described in relation to the parameters above. The paper ends with validation of the model, conclusions of the analysis, dealing with applicability of the model to solve problems for the real system and a summary with prospects for further research.

1 INTRODUCTION

Transport systems are fundamental for the functioning of economy and play important social roles. Because of the far-reaching (social, economic, country defense) effects of disruptions in the operation of these systems they are classified as critical infra-structure systems (Murray & Grubesic 2007).

The task of transport systems is movement of goods and passengers from one place to another. The importance of transport systems increases with rising mobility of the population. Economic development entails the needs to improve transport services. Passengers expect interconnected routes, with minimum travel and waiting times. On the other hand, recipients of goods, in order to effectively compete in the market, engage in optimizing activities which lead to the use of the Just-in-Time and Time Window technologies (Akbalik & Penz 2011, T'kindt 2011), etc. It is clear that a well-functioning transport system should meet the requirements for logistics systems in the form of the 7R formula (Right product, Right quantity, Right quality, Right place, Right time, Right customer, Right price) (Nowakowski 2011). A transport system functioning in a reliable way is therefore characterized by:

- availability of appropriate (planned) products in the transportation offer,
- proper number of executed transportation tasks
- proper quality of execution of transportation tasks (safety of passengers and cargo),
- the right place of destination, according to a timetable (including transportation routes),
- appropriate lead time (punctuality),
- appropriate recipients,
- appropriate price (according to rates established in the plan of the transportation by carriers).

2 LITERATURE REVIEW

2.1 *System models*

An important aspect of railway practice are issues related to determining the state of the infrastructure and linking this state with measures to improve safety (Auer & Schlöpp 2012). In this approach, an alternative to technical maintenance are train speed limits.

Both the choice of when to introduce speed limits and execution of technical maintenance entail costs. An important group of studies are analyses of life cycle costs of vehicles or infrastructure (Marschnig & Veit 2012).

In (Enzi 2012, Hansemann & Marschnig 2012) decision models for finding the time for technical maintenance of infrastructure at minimum total cost have been developed.

Another group of works on railway issues refers to dispatch activities at the time of disruption. One approach is to regulate the speed of trains in order to minimize unscheduled stays (especially felt by the passengers) and reduce energy consumption (Ding 2011). This approach does not propose any structural changes in the executed process, only

changes in the process parameters (e.g., reduction of speeds of trains which are in conflict with a delayed train). Broadly speaking, these are issues related to the reorganization of the traffic after the occurrence of disruptions whose aim is to minimize further propagation of disruptions (Caimi et al. 2012, Törnquist & Persson 2007, Törnquist Krasemann 2012).

Lin (2008) have applied Markov processes to the study of aggregation of trains in a selected portion of the rail network. Wendler (2007) uses a semi-Markov model to determine time intervals between trains of different speeds.

Kroon & Huisman (2011) proposed a model for supporting management of disrupted rail traffic. The model is based on the costs of reorganization of train traffic or cancellation of trains in the context of railroad workers (train drivers and train traffic service). What is more, Acuna-Agost et al. (2011) presents a model for supporting a decision making process while managing disrupted train traffic.

2.2 *Reliability models*

Initially, reliability studies in the rail industry focused on vehicles. Already in 1979 the need to study failures of traction motors in electric vehicles has been indicated (Plewako 1979).

In addition to research on mathematical models, operational data analyses on damage have been carried. These works has been narrowed to statistical analysis and inference made on its basis (Banek et al. 1978, Marciniak 1988, Pustelnik & Świderski 1968, Roman 1972).

Vromans (2005) narrows down the concept of reliability of rail transportation system to punctuality. Only delays are taken into consideration. The author identifies potential causes of disruptions, however, he assumes that temporary disruptions have one common source. The work focuses on max-plus algebra used to evaluation of timetables (Goverde 2007, Goverde 2010), in the context of time reserves.

Chen (2003) has presented a model of rail service reliability and a model of punctuality. The model of rail service reliability consists of three parts:

– reliability of technical objects constituting the system (independence of events occurring in subsystems has been assumed),
– interactions between the rolling stock subsystem and other subsystems,
– intensity of traffic restoration after a break due to an adverse event.

In modeling the reliability of technical systems an important role is played by models based on graphs of states-transitions. The basic mathematical tools used to describe such models are (Lisnianski et al. 2010) Markov processes and Semi-Markov processes (Kierzkowski 2010, Kierzkowski & Zając 2012).

Chandra & Kumar (1997) consider the analysis of reliability and safety of elements of train traffic control devices in terms of safe errors. The study focuses on the analysis of the reliability and safety of the junction with special computing microcomputers, called transputers. For this purpose, a nine-state Markov model has been developed.

Colini et al. (2010) have presented a Markov model of reliability of tram systems. Six possible states of reliability have been adopted for the vehicles.

A frequent subject of research is a separated element of the rail transport system. An example might be the analyses of technical objects included in the infrastructure. Krenželok et al. (2010) have developed a 40-state model of reliability and safety of rail-road transit security devices.

Transit devices, similar to rail traffic control devices work periodically during the transit of a train, and in the rest of the time they are in the so-called stand-by mode. The authors have recognized the problem of determining the time between events, and linking it with real time. In addition to the intensity of damage and repairs, the intensity of damage detection, which is the inverse of the time between inspections, have been included in the model. The first model have been simplified to 21 states.

Dolven et al. (2004) have applied Markov chains for modeling rail track, taking into consideration sudden damage and damage resulting from the technical condition of the track.

2.3 *Safety models*

Schwartz (2010) have presented a method for the identification of barriers on the basis of a fault tree. The method is based on the so-called Swiss Cheese model, in which holes must overlap so that the arrow may go through (so that safety fallibility occurs). The situation of risk, which is the peak event, is modeled by a classic fault tree with AND and OR gates.

In analyzes of risk of adverse events event tree or fault tree may be used for the case of the railway system. In (Albrechtsen & Hokstad 2003) this kind of analysis has been extended to include the risk influencing factors. The issue has been shown on the example of a single-track line, for which the peak event is the collision of two trains coming from the opposite directions. An analysis of the factors affecting the risk shows the relationships and sequences of cause and effect going beyond a simple event tree analysis. In the studies case it

has been shown that the most important factors influencing risk are: human behavior and operating conditions of the system.

The (de Boer et al. 2003a, b, Renpenning 2004) studies raise issues of safety engineering in the design of rail transport systems. The articles relate to issues of implementation of the ERTMS (European Rail Traffic Management System), which in its structure contains also a unified European GSM-Rail. The issue of security in the implementation of ERTMS is all the more important given the lack of operating experience of such a system in conditions corresponding to implementation (for the Dutch railways in 2003). The basis of considerations (de Boer et al. 2003a) is identification of hazards to the case of the implemented system. The authors propose a parallel application of three methods, concluding together in the list of hazards. The first method, namely Design based structured hazard identification, consists in inventorying risks on the basis of possible damage to the system being designed. The second method is the traditional HazOp (Hazard and Operability Analysis). The third method (hazard transfer) consists of the acquisition of already identified threats (or components of similar systems) for the purposes of the studied case. In (de Boer et al. 2003b) the works have been summarized, approximating the components of risk analysis for the rail system (ERTMS) whose design has just been started. In this aspect, the use of the two following approaches is suggested: ALARP and GAMAB. ALARP (the risk must be As Low As Reasonably practicable) aims to demonstrate that everything has been done to achieve a higher level of security than before. The approach called GAMAB (Globalement Au Moins Aussi Bon) is supposed to show that the level of security of a new system is at least equal to an old system. In both approaches the following steps are implemented: hazard identification, casual analysis (tree events with defining of the occurrence frequency), impact analysis (tree of effects), and analysis of losses. Depending on the possibilities of comparing the old system to the new one the next steps may, but need not, concern the GAMAB approach: option analysis and an analysis of the impact on the risk. To assess the safety of the ETCS system, which is a slightly simplified variant of ERTMS, the method of Functional Hazard Assessment has been proposed in (Renpenning et al. 2003).

An important aspect in the safety analysis is determining Safety Integrity Levels. The draft of a European standard (EN50129) uses a simplified SIL table for the case of devices controlling rail, communications, data processing and electronic system traffics which significantly affect the safety of rail transport.

In (Cremonini 2003) a risk assessment has been carried out in the transportation of dangerous goods by using events/vehicle kilometers as a measure of the intensity of event occurrence. According to the adopted approach the frequency of events associated with the transport of dangerous goods is determined as the product of the intensity of occurrence of all events on a homogeneous network segment (events/vehicle kilometers) and intensity of traffic of vehicles carrying dangerous substances on this segment (vehicles/year).

2.4 *Summary of literature review*

The studied models were analyzed in terms of considered essential features for the rail transport system. A collection of these features has been created based on the research on the state of knowledge in scientific publications and knowledge of railway industry experts. Consequently the following features have been focused on:

- intensity of use of the system,
- traffic dependence of trains,
- infrastructure failures,
- rolling stock failures,
- disrupted implementation of the transport process (delays and track changes),
- improper use of the system,
- human factors,
- hazards and safety failures,
- process leading to loss of safety.

The possibility of occurrence of unwanted events and the spread of effects depends on the intensity of use of the system, expressed as operational work (Restel 2012a, b) or transportation work (Bałuch 1980, Potthoff 1964). Performed transportation work directly affects the intensity of the train traffic. The increase in train traffic causes the increases in the number of situations in which trains are interdependent as far as their movement is concerned. This means that in the event of a disruption to a single train, the dependent trains will be disrupted as well. Thus, we can see that these two features are connected with each other.

Disrupted implementation of the transport process is defined as the operation of the train traffic not in accordance with the established timetable while improper use of the system means situations in which there are single errors of the system, but nevertheless the train traffic is conducted. Often, conducting traffic in such a situation takes place without traffic control devices (for account of the traffic orderly and the train driver). The human factor means the possibility of an accident due to the fault of a person.

3 RELIABILITY AND SAFETY MODEL

For the developed model, assumptions associated with the system whose reliability and security can be modeled have been made. This model was developed in its present form for the rail transport system which consists of a railway line between the two junction stations, that is a fragment of the system in which it is possible to move the trains only in two directions. So it is not possible that trains outside the start and end of the line will appear or disappear.

Furthermore, it has been assumed that the lines converging at junction stations located at the interface of the system do not affect each other in terms of disruptions.

3.1 *Defining of states*

Functional model of the rail transportation system can be presented as a process described by a set of S states (Gołąbek et al. 1993, Birolini 2010), which is divided into a definite number of subsets. The most often distinguished subsets are a fault subset and a success subset (Grabski & Jaźwiński 2009, Ważyńska-Fiok & Jaźwiński 1990). Literature research and the study of operational data indicate inadequacy of this approach in the case of the rail transport system. In order to take account of the inventoried essential characteristics of the model, the description of the states in five dimensions has been adopted:

– events related to the success feature of the system,
– correctness of use,
– disruptions of the transportation process,
– traffic dependence of trains.
– type of unwanted event.

Interconnections between train traffic dependence of trains and train traffic intensity are shown in Table 1 The values shown are for illustration only, since the exact values should be determined individually for each railway line.

Table 1. Correlation between train traffic dependence and intensity of system using.

Traffic dependence	Traffic intensity on a single-track line (trains per hour)	Traffic intensity on a double-track line (trains per hour)
Lack of trains	0	0
Independent trains	x < 0,5	x < 1,2
Partially dependent trains	0,5 < x < 1,2	1,2 < x < 6,0
Dependent trains	x > 1,2	x > 6,0

The parameters of the system are partly dependent, which is the reason for the need to assess the states in terms of compatibility of features. The feature type of adverse event is dependent on the feature of the event related to capability. The features correct use, and disruptions of the transportation process depend on the feature movement dependence of trains (which also indicates the intensity of use). The dependence of features describing states does not affect the separate character of the defined states.

Taking account of the events related to the capability of the system in conjunction with the type of adverse events enables us to include fallibility of vehicles, fallibility of infrastructure and human error in the model. Proper use allows the replication of situations in which the system is operated despite of broken train traffic control devices.

By taking into account the correctness of use and disruptions to transportation process we can replicate emergency situations. Along with the movement dependence of trains it is possible to model the process leading to the fallibility of safety. In addition, movement dependence hides information on the intensity of use, which increases with the increase of participation of the trains that are dependent in terms of movement.

In connection with the adopted approach, the so-called super cube model has been developed and successfully used in the description of the safety parameters of the rail transport system (Harms-Ringdahl & Kecklund 2004).

Given the adopted way of defining the states in five dimensions, a list of all the theoretical 288 states have been drafted. Due to the relationships between the features defining the states it has

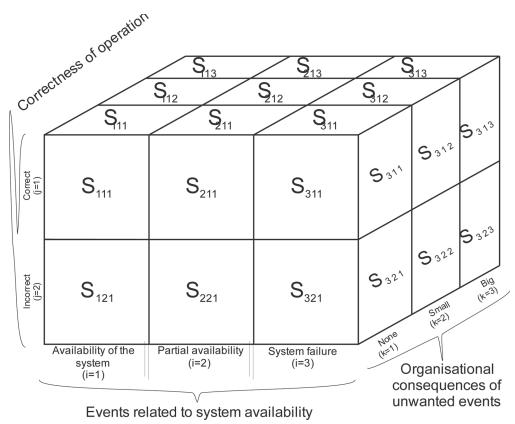


Figure 1. Three of five dimensions of the super cube used for state defining.

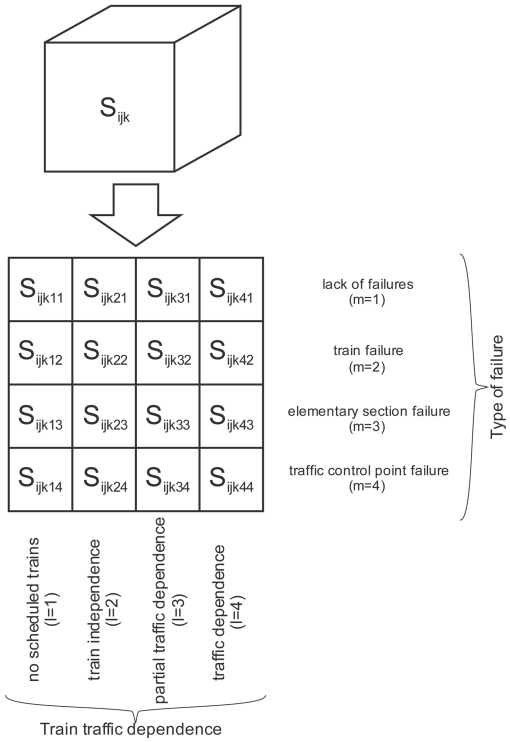


Figure 2. Remaining two dimensions of the state defining super cube.

been necessary to verify whether the features are not mutually exclusive.

In the first step the states with mutually exclusive feature values have been identified. Conflicts between the features leading to the removal of states have been of the following nature:

– lack of traffic and disruptions in traffic,
– successful system and a specific type of adverse event,
– etc.

3.2 *The Markov model*

After the first step of the selection, the operation process of the overall rail transport system has been divided into 83 separable states. These are the states that allow the modeling of each type of the rail transport system. In relation to the specific character of the varieties of the rail transport system, it is possible that some states will prove to be useless in a particular case.

The studies conducted have been based on the rail systems due to their complexity. Therefore, in the second step of the algorithm of the selection of states, these states which characterize the railway transportation systems (excluding metro and tram) have been chosen to the model.

The next step consisted in selecting the states which can be described using the collected operation data. In the last step three major fault states have been merged, thus obtaining:

– preventive maintenance of the entire system,
– accident,
– serious accident.

As a result of these proprietary operational studies the main 44 states have been determined for the model of railway transportation system reliability and safety which is being developed.

Starting from the separability of the states and the assumption that intensities of transitions between the states are independent of time, all the states which had been parallel to each other and had been characterized by transitions to and from the same states have been combined together. The action of combining have been applied to the states of partial faultiness. Intensities of transitions have been summarized after combining the particular states. A simplified model is composed of 29 states and 83 transitions. Finally the model consists of the following states:

– N1—the system is not used, but available,
– N2—the system is correctly used, with independent train traffic, without disruptions,
– N3—the system is correctly used, with partially dependent traffic, without disruptions,
– N4—the system is correctly used, with independent traffic and disruptions,
– N5—the system is correctly used, with partially dependent traffic and disruptions,
– N6—the system is not used and it is partially unavailable, because of maintenance, Train Failures (TF), Elementary Section Failures (ESF) or Traffic Control point Failures (TCF),
– N7—the system is correctly used, with independent traffic and it is partially unavailable, because of maintenance, ESF or TCF,
– N8—the system is correctly used, with independent traffic and it is partially unavailable, because TF,
– N9—the system is correctly used, with partially dependent traffic and it is partially unavailable, because of TF,
– N10—the system is correctly used, with partially dependent traffic and it is partially unavailable, because ESF or TCF,
– N11—the system is correctly used, with independent disrupted traffic and it is partially unavailable, because of maintenance or ESF,
– N12—the system is correctly used, with independent disrupted traffic and it is partially unavailable, because of TF or TCF,

– N13—the system is correctly used, with partially dependent disrupted traffic and it is partially unavailable, because of TF or TCF,
– N14—the system is correctly used, with partially dependent disrupted traffic and it is partially unavailable, because of ESF,
– N15—the system is unavailable because of preventive maintenance,
– N16—the system is unavailable because of an accident,
– N17—the system is unavailable because of serious accident,
– N18 to N29—the same as N2 to N5 and N7 to N14, but the system is incorrect used.

The states were linked with 83 transitions. For presentation the model was split into two layers—correct and incorrect using of the system.

The layer of correct use includes all states in which the system is operated in accordance with assumed procedures. The technical elements of the system are suitable to the extent which allows regulatory operation of the traffic. This means that the system will be in a state of capability even though the elements which are irrelevant to the reliable and safe operation of train traffic may be damaged.

The state of faultiness of the entire system, assigned to this layer, are related to preventive technical maintenance (N15) or accident (N16) due to accidental events (e.g. collision with a wheeled vehicle or being hit). The incident can also be caused by accidental critical damage to a technical element of the system. The state of faultiness due to an accident is a state of safety fallibility.

After a complete system fault, the restoration of capability takes place together with the transition to the state of readiness without train traffic (N1). It has been assumed that the faultiness of the system will disable traffic completely, and thus start-up of the system takes place from the state of no train traffic.

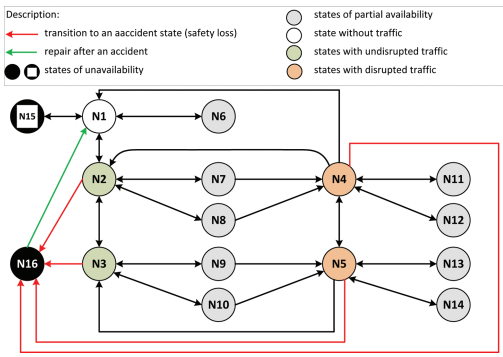


Figure 3. System correct using layer of the model.

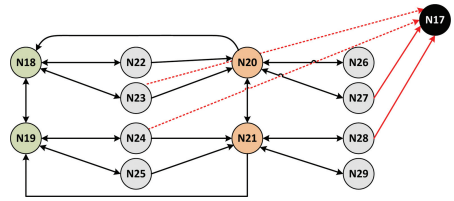


Figure 4. System incorrect using layer of the model.

The transition to a state of faultiness due to preventive technical maintenance (N15) is possible only from the state of traffic expectation, because these repair processes are planned in advance and included in the timetable (i.e., with prior zeroing of train traffic intensity).

It was assumed that the system at the time of partial faultiness (N6–N14 and N22–N29), due to the partial suspension of traffic, cannot significantly change traffic intensity, and therefore at a time of partial faultiness the change in movement dependence of trains must not happen.

Analysis of operating data from polish infrastructure manager has shown that on busy railway lines only 6% of adverse events occur before the end of the previous event. In the case of the less busy lines this phenomenon is less likely. On the lines under consideration no situation in which such impermanent damage occurred simultaneously in one minimum cross-section of faultiness has been noted. For this reason, it has been assumed that at one moment only one damage causing partial faultiness to the system can occur. The transition to a state of partial faultiness as a result of other damage is possible indirectly by one of the states of capability.

The occurrence of an incident as an accidental event is only possible from the states in which the system is capable and used for the execution of transportation tasks (N2–N5). This assumption is also based on the non-simultaneous occurrence of events. Therefore, the system cannot change the state from operating train traffic at partial faultiness to the state of faultiness (accident).

Disrupted traffic can occur only when traffic was previously conducted in the system and an adverse event occurred causing partial faultiness of the system. On the other hand, partial faultiness, as an adverse event does not necessarily disrupt train traffic.

As improper use of the system has been identified as a prerequisite of a major accident, major accidents have not been considered in this layer.

The second layer which consists of a model of reliability and safety of the rail transport system is a layer of improper use. It has been assumed that in this layer there are no states of capability and partial capability in anticipation of the transportation

tasks because the system cannot be improperly used when there is no train traffic (when it is not used).

The state of complete faultiness as a result of a serious accident (loss of security) has been assigned to this layer because improper use must take place to trigger the occurrence of the accident with catastrophic consequences. This has been identified in the chapter on an accident formation model. In the context of this layer the state of complete faultiness due to a serious accident is an absorbing state. However, when taking into account the transitions between the states of two layers it will not be an absorbing state, which is illustrated below. The transition to the state of complete faultiness of the system due to a serious accident is possible from four states:

– N23—partial faultiness of the system caused by damage/train error (in a situation of unhindered traffic, movement independent trains),
– N24—partial faultiness of the system caused by damage/train error (in a situation of unhindered traffic, partially movement dependent trains),
– N27—partial faultiness of the system caused by damage/train error (in a situation of disrupted traffic, movement independent trains); or partial faultiness of the system caused by damage/signal box error (in a situation of disrupted traffic, movement independent trains),
– N28—partial faultiness of the system caused by damage/train error (in a situation of disrupted traffic, partially movement dependent trains); or partial faultiness of the system caused by damage/signal box error (in a situation of disrupted traffic, partially movement dependent trains).

Determination of transitions to the state of a serious accident has been based on the assumption of necessary prior occurrence of a human error (a train driver's or traffic orderly's). States belonging to the layers of improper use of the system constitute a set of safety risk states. In contrast, the states of partial faultiness in this layer constitute states of a direct threat to safety (this applies to the states taking into account human errors).

Putting together the layers of correct and incorrect use results in complementing the model with transitions between these layers. It has been assumed that as a result of human decisions, it is possible to continue using the system, despite some technical or organizational constraints, which causes the transition from the state of partial faultiness of the layer of proper use to the corresponding state of partial faultiness of the layer of improper use. These transitions are the only path of changing the layer from proper to improper use.

Disappearance of the threat, or return to the layer of correct use is possible after restarting the system, that is through the state N1. The renewal of the system after a serious accident takes a similar form.

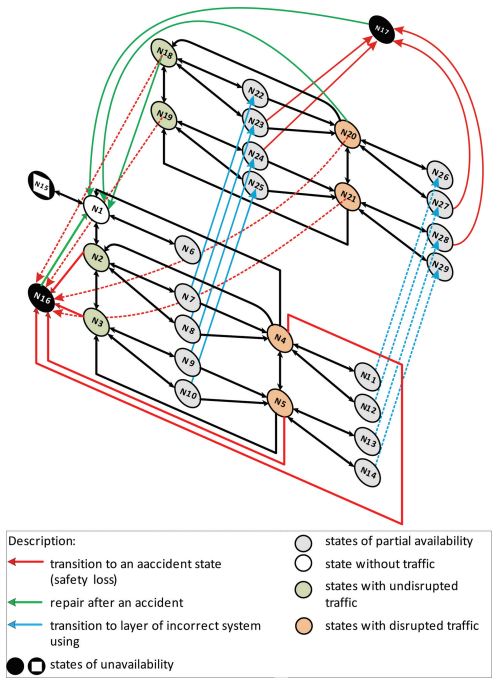


Figure 5. Complete Markov reliability and safety model.

Another path to return to proper use is through the loss of safety as a result of a random accident.

The developed model of has been mathematically described by a linear differential equation system with constant coefficients. It is therefore assumed that the probability of transitions between states is described by exponential distributions, and, consequently, the intensities of transitions between the states are independent of time. The system of forty-four Chapman-Kolmogorov differential equations have been prepared.

Simplifications related to merging of states have been introduced in the model to the process of verification.

3.3 *Model validation*

After the reduction of the number of states for the purposes of validation, a simplified model for the GRIF computing environment have been introduced. The said computing environment is used for calculation of Markov processes.

The verification of the model has been carried out with the use of three pre-estimated sets of intensities of transitions between the states. Using the GRIF computing environment stationary probability values of residing in the states have been determined for a simplified model. Stationarity have been obtained after 2–15 days.

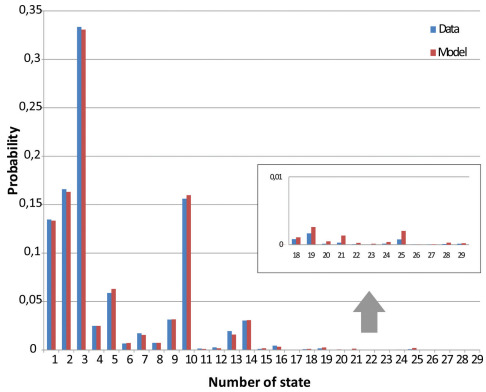


Figure 6. Comparing of empirical data with results from the proposed model.

For a real railway line, called in the paper A–B, state probabilities have been determined based on infrastructure manager's data from the year 2011. Then empirical values have been put together with the results of the model, which was parameterized by data for the same railway line, but previous operation interval (years 2009–2010). The results were shown in Figure 6.

After determining the probabilities and residence times in states on the basis of empirical data and after performing the calculations for the model, the values obtained have been put together and the test of the model compliance with reality have been conducted. The Chi squared test at the statistical significance $\alpha = 0.05$ has been chosen. The critical quantile for the distribution takes the value of 41.337 for the studied case. For line A-B it has been stated (comparing the model with data from 2011) that for the given statistical significance there is no basis to reject the null hypothesis of compatibility of the model with reality.

4 SUMMARY

The studies of the state of art have shown the lack of models of reliability and safety of the rail transportation system taking into account functional features. In particular, the need for considering the following factors has been identified: reliability of infrastructure and rolling stock subsystem, intensity of system using (traffic dependence of trains), the impact of the human factor in conjunction with the functioning of the system, disruptions in train traffic, the exposure of the system to situations of emergency and safety unreliability. Therefore, the following objective of the work has been formulated. Such conclusions have been drawn from both the research on literature sources, operation tests of the system as well as observation of the practice of conducting rail traffic and system management.

A concept of the system has been developed based on which faultiness states have been defined and the concept of partial faultiness of the rail transport system has been introduced. Barriers which have not yet been systematically taken into account and which prevent the occurrence of railway accidents have been identified.

The developed way of defining the states has made it possible to take into account the identified, significant functional, reliability and safety qualities. The formulated model based on graph of states and transitions has been mathematically described with the use of the system of 44 linear differential equations, assuming the independence of intensities of transitions between the states. With the use of the mathematical model the probabilities of occurrence of the above-defined states are calculated. The verification of the model shows a good representation of reality. This has been proven by the Chi squared test at the statistical significance $\alpha = 0.05$.

REFERENCES

Acuna-Agost, R. et al. 2011. SAPI: Statistical Analysis of Propagation of Incidents. A new approach for rescheduling trains after disruptions. *European Journal of Operational Research Vol. 215*. ELSEVIER.

Akbalik, A. & Penz, B. 2011. Comparison of just-in-time and time window delivery policies for a single-item capacitated lot sizing problem. *International Journal of Production Research Volume 49/no. 9*. Taylor & Francis.

Albrechtsen, E. & Hokstad, P. 2003. An analysis of barriers in train traffic using risk influencing factors. *Safety and Reliability*. Lisse: Swets & Zeitlinger.

Auer, F. & Schlöpp, A. 2012. Substance determination of permanent-way components (in German). *ZEV Rail 9/2012*. Siemens Verlag.

Banek, A. et al. 1978. Determination of durability and reliability of traction network (in Polish). *Prace Centralnego Ośrodka Badań i Rozwoju Techniki Kolejnictwa—zeszyt 71*. Warszawa: Wydawnictwa Komunikacji i Łączności.

Bałuch, H. 1980. Operational durability and reliability of railway superstructure (in Polish). Warszawa: Wydawnictwa Komunikacji i Łączności.

Birolini, A. 2010. Reliability Engineering—Theory and Practice. Springer.

Caimi, G. et al. 2012. A model predictive control approach for discrete-time rescheduling in complex central railway station areas. *Computers & Operations Research Vol 39.* ELSEVIER.

Chandra, V. & Kumar, V. 1997. Reliability and safety analysis of fault tolerant and fail safe node for use in a railway signalling system. *Reliability Engineering and System Safety Vol. 57*. ELSEVIER.

Chen, H.K. 2003. New models for measuring the reliability performance of train service. *Safety and Reliability*. Lisse: Swets & Zeitlinger.

Colini, A. et al. 2010. A practical Markovian model of the availability and reliability of mass transport service with non-exponential repair times. *Reliability, Risk and Safety: Theory and Applications*. London: Taylor & Francis.
Cremonini, M.G. 2003. Industrial areas and transportation networks risk assessment. *Safety and Reliability*. Lisse: Swets & Zeitlinger.
de Boer, J. et al. 2003. Design based safety engineering applied to railway systems part I. *Safety and Reliability*. Lisse: Swets & Zeitlinger.
de Boer, J. et al. 2003. Design based safety engineering applied to railway systems, part II. *Safety and Reliability*. Lisse: Swets & Zeitlinger.
Ding, Y. 2011. Simulation model and algorithm for train speed regulation in disturbed operating condition. *ZEV Rail 10|2011*. Siemens Verlag.
Dolven, O.F. et al. 2004. Statistical Modelling and Analysis of Failure and Inspection Data for a Railway Line. *Proceedings of the European Safety and Reliability Conference, ESREL 2004.*
Enzi, M. 2012. Right time to reinvest superstructure considering the aspect of Life Cycle Costs (in German). *ZEV Rail 3|2012*. Siemens Verlag.
European Standard: EN50129.
Gołąbek, A. et al. 1993. Reliability of road busses (in Polish). Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.
Goverde, R. 2007. Railway timetable stability analysis using max-plus system theory. *Transportation Research Part B Vol. 41*. ELSEVIER.
Goverde, R. 2010. A delay propagation algorithm for large scale railway traffic networks. *Transportation Research Part C Vol. 18*. ELSEVIER.
Grabski, F. & Jaźwiński, J. 2009. Functions of random arguments—reliability, safety and logistics issues (in Polish). Warszawa: Wydawnictwa Komunikacji i Łączności.
Hansemann, F. & Marschnig, S. 2012. Der Gleisprophet—ein Impuls zur Nachhaltigkeit. *ZEV Rail 9|2012*. Siemens Verlag.
Harms-Ringdahl, L. & Kecklund L. 2004. Safety Functions in Railways—a Structural Analysis of Safety Rules. *Probabilistic Safety Assessment and Management—Proceedings of ESREL 2004*. Springer.
Kierzkowski, A. 2010. Reliability models of transportation system of low cost airlines. *Reliability, Risk and Safety: Back to the Future.*
Kierzkowski, A. & Zając, M. 2012. Uncertainty assessment in semi Markov methods for Weibull functions distributions. Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011.
Krenželok, T. et al. 2010. Reliability and safety of railway signalling and interlocking devices. *Reliability, Risk and Safety: Theory and Applications*. London: Tylor & Francis Group.
Kroon, L. & Huisman, D. 2011. Algorithmic Support for Railway Disruption Management. *Transitions Towards Sustainable Mobility Part 3*. Springer-Verlag.
Lin, B.-L. et al. 2008. Train aggregation in a railway subsystem by Markov approach. *International Journal of Modern Physics C Vol. 19 No. 3*. World Scientific Publishing Company.
Lisnianski A. et al. 2010. Multi-state System Reliability Analysis and Optimization for Engineers and Industrial Managers. Springer-Verlag.
Marciniak, J. 1988. Operational unreliability of electric traction machines and causes research (in Polish). *VII Konferencja Naukowa Pojazdy Szynowe, Rydzyna 1988.*
Marschnig, S. & Veit, P. 2012. Life Cycle Management in the Reality (in Polish). *ZEV Rail 9|2012*. Siemens Verlag.
Murray, T. & Grubesic, T.H. 2007. Critical Infrastructure—Reliability and Vulnerability. Springer.
Nowakowski, T. 2011. Reliability of logistics systems (in Polish). Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.
Plewako, S. 1979. Influence of traction motors maintenance on durability and reliability of railway vehicles (in Polish). *III Konferencja Naukowa Pojazdy Szynowe*. Poznań.
Potthoff, G. 1964. Traffic science—part 3 (in German). Berlin: Transpress.
Pustelnik, I. & Świderski, Z. 1968. Statistical analysis of rail failures on Polish railways in the years 1963–1965 (in Polish). *Prace Centralnego Ośrodka Badań i Rozwoju Techniki Kolejnictwa—zeszyt 29*. Warszawa: Wydawnictwa Komunikacji i Łączności.
Renpenning, F. et al. 2003. Application of functional hazard assessment in railway signalling. *Safety and Reliability*. Lisse: Swets & Zeitlinger.
Renpenning, F. 2004. Reliability Prediction in Railway Signalling. *Proceedings of the European Safety and Reliability Conference, ESREL 2004*.
Restel, F.J. 2012a. Measures of reliability and safety of rail transportation system. *Advances in safety, reliability and risk management.* CRC Press/Balkema.
Restel, F.J. 2012b. The model of transportation process disruptions on a railway line (in Polish). *XX Międzynarodowa Konferencja Naukowa Pojazdy Szynowe 2012*.
Roman Z. 1972. Traction network failure analysis for Polish railways (in Polish). *Prace Centralnego Ośrodka Badań i Rozwoju Techniki Kolejnictwa—zeszyt 45*. Warszawa: Wydawnictwa Komunikacji i Łączności.
Schwartz, S. 2010. Identification of safety barriers at a level crossing (in German). *ZEV Rail 1-2|2010*. Siemens Verlag.
T'kindt, V. 2011. Multicriteria models for just-in-time scheduling. *International Journal of Production Research Volume 49|no. 11.* Taylor & Francis.
Törnquist, J. & Persson, J.A. 2007. N-tracked railway traffic re-scheduling during disturbances. *Transportation Research Part B Vol. 41*. ELSEVIER.
Törnquist Krasemann, J. 2012. Design of an effective algorithm for fast response to the re-scheduling of railway traffic during disturbances. *Transportation Research Part C Vol. 20*. ELSEVIER.
Vromans, M. 2005. Reliability of Railway Systems. *TRAIL Thesis series T2005|7*. The Netherlands TRAIL Research School 2005.
Ważyńska-Fiok, K. & Jaźwiński, J. 1990. Reliability of technical systems (in Polish). Warszawa: Państwowe Wydawnictwo Naukowe.
Wendler, E. 2007. The scheduled waiting time on railway lines. *Transportation Research Part B Vol. 41*. ELSEVIER.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability analysis of rail teleinformation system

M. Siergiejczyk
Warsaw University of Technology, Warsaw, Poland

ABSTRACT: The paper presents the issues related to the modeling of the reliability of rail teleinformation system. This Rail ICT system is intended to modernize the technical and technological solutions in dedicated networks (communication networks, mobility, dispatcher, etc), functioning outside the railway public operating telephone network. It is presented the architecture of railway communication system and described the functions of the respective subsystems. Analyzing the functional structure and method for transmitting information in the railway technology communication system it is proposed a method for calculating the rate of system reliability. To evaluate the reliability of rail ICT system as a recoverable system it is proposed the rate of readiness.

1 INTRODUCTION

Centralised rail traffic control and management poses a considerable challenge to telecommunications infrastructure in terms of data transfer, reliability, performance and data transmission services.

Technical condition of individual system components and their maintenance processes have key influence on rail dispatcher communication system. System reliability is a good indicator of maintenance performance. By design, planned downtimes for central offices do not exceed two hours over forty years. Longer down periods are permitted for small subscriber groups or inter-office connections. Another popular indicator of reliability of ICT systems is probability of failure during a year. Mean failure time i.e. mean time to repair is also essential to evaluate ICT system reliability. An indicator connecting Mean Time To Repair (MTTR) and Mean Cycle Between Failures (MTBF) is the availability rate Kg (Jajszczyk A. 2006).

Attempt to evaluate operational reliability of Rail ICT system was presented in this paper. It is a modern, digital ICT system facilitating modernisation of technical and technological solutions in closed loop networks (shunting team radio, dispatch communications etc.) operating outside the main Polish Railways telephone network (Siergiejczyk M. and others 2001). The rationale behind closed networks using separate cables and transmission channels, including digital ones, is beyond all rail traffic safety, efficient traffic management, infrastructure maintenance as well as redundancy to provide alternative functional channels in case of failure.

The aim of the article is to assess the reliability of rail communications system of new generation that is currently being implemented to operate on Polish railways.

The correct operation of the communication system has a direct impact on the safety of railway traffic. At the stage of implementation of the exploitation there are no information on reliability properties of the railway dispatch communication system during exploitation, therefore there is a need to assess the reliability on the basis of forecasting methods. Knowledge of reliability indicators will allow for implementation of appropriate operational strategies allow for the maintenance of these systems in the states of functional and task ability.

In the area of rail transport issues of assessment of reliability are fairly well described in terms of traffic control systems, rail automation (Lewiński A, Perzyński T. 2010), ETCS systems and rail infrastructure (Flammini F. 2012). There are also publications related to the work of the dispatcher in rail transport, and specifically with the analysis of the reliability of the operator (Human Reliability Analysis) (Belmonte F, Boulanger J.-L., Schön W. 2008). In contrast, there are no publications that relate to the assessment of the reliability of a wired system of railway dispatch communication.

2 RAIL ICT SYSTEM

Rail ICT System (RICTS) is digital ICT system facilitating modernisation of technical and technological solutions in closed loop networks and thus in traffic communication. Logical architecture of the digital dispatch communication system has been illustrated on Figure 1.

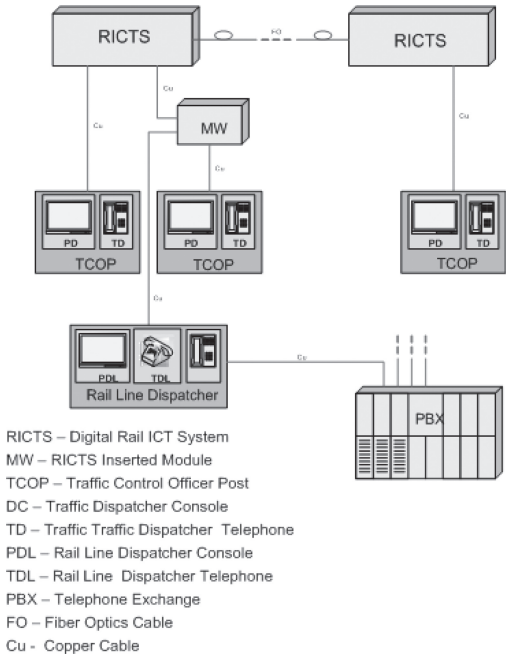


Figure 1. Architecture of rail teleinformation system (RICTS).

In its default configuration (integrated rail communication equipment for closed networks) it consists of:

– Digital server equipped with transmission and commutation modules allowing to make connections with mobile object,
– Computer equipment required for the operator to use the system i.e. LCD display, keyboard, hands-free headset with auto switching (optional) or manual switching, but note by default equipment are in "receiver" mode.
– Operator workstation (traffic controller) am integral part of the telecommunications server, which is a dedicated terminal for communication between traffic controller (dispatcher) and all connected points. That workstation features a keyboard, microtelephone, hands-free headset and readable display (min. 4 lines 40 characters each, or graphical)—optional extra.
– Operator workstation voice recorder,
– Power supply,
– Acoustic amplifiers controlled by the system, power output 100 W or 200 W (depending on ordered specification) controlling road side units,
– User terminals.

The system is built from modules, hence its configuration may be changed to suit individual user preference. Majority of system components features processors enabling distributed control. Hardware specification of the system is based on VLSI technology (very large scale integration). The modules are built using multi-layer laminates with electronic components embedded in the substrate.

Duplication or repetition of elements in electronic equipment provides alternative functional channels in case of failure thus increase reliability of:

– control unit,
– switching network,
– group processors, operating in "non-spinning reserve" arrangement, where at each given moment one can take over the function of central component.

Continuity is also assured through splitting cable harnesses and using protection fibres for rerouting traffic in case of failure.

All components are diagnosed in real time by system software. It signals failure or anomalies instantly, automatically reconfigures the system and eliminates failed component by switching to the reserve components without disconnecting traffic. The software also allows to manually initiate internal system tests. Thanks to that many reliability enhancing features improving service availability it does not go below 99.999% per annum.

System software was designed to provide all functionalities which are engaged by reconfiguring the data base. It offers flexibility to accommodate different applications, network characteristics, services, functions and interfaces.

The Rail ICT system creates a network assuring communication between traffic controllers (or other authorised personnel) and all stations located within perimeter of the railway station, dispatcher and stations track-side along the railway route. The RICTS facilitates data transmission required to assure and maintain safety and control rail traffic.

3 EVALUATION OF DIGITAL RICTS SERVER RELIABILITY

Those assumptions were made based on reliability guidelines for telecommunications lines described among other in (Kwestarz, Krygier 1999, Siergiejczyk 2000, Siergiejczyk 2009) and reliability analysis of computer and microprocessor systems (Military Handbook 1979, Siergiejczyk M., Rosinski A. 2011, Verma & Ajit & Karanki 2010). It is assumed that the stochastic process $\{X(t): t > 0\}$ describing operating principle of the system is the Markov process. The following states were defined:

S_{PZ},—system staying in state of full ability,

S_{ZB1}—one (processor A) processor is in state of full ability and the other (processor B) undergoes repair,
S_{ZB2}—one (processor B) processor is in state of full ability and the other (processor A) undergoes repair,
S_B—both processors' failure.

It was also assumed that the combinational circuit upon processor failure is in state of full ability and that uptime of combinational circuit is not independent of processor uptime. Figure 2 illustrates relationships within the system, derived based on functional analysis.

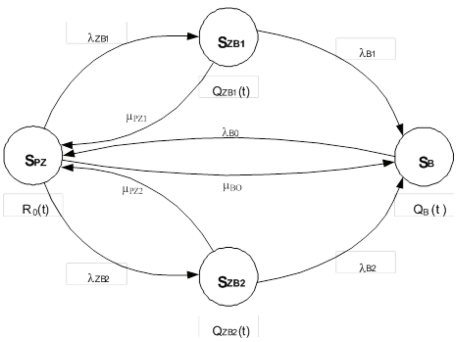


Figure 2. Relationships in the system.

Denotations in figures:
$R_O(t)$—probability of system staying in state of full ability S_{PZ},
$Q_{ZB1}(t)$—probability of event, where one (processor A) processor is in state of full ability and the other (processor B) undergoes repair,
$Q_{ZB2}(t)$—probability of event, where one (processor B) processor is in state of full ability and the other (processor A) undergoes repair,
$Q_B(t)$—probability of both processors' failure,
λ_{ZB1}—transition rate from state of full ability S_{PZ} to one (processor A) processor is in state of full ability and the other (processor B) undergoes repair,
λ_{ZB2}—transition rate from state of full ability S_{PZ} to one (processor B) processor is in state of full ability and the other (processor B) undergoes repair,
μ_{PZ1}—repair rate of failed processor B and transition to state of full ability S_{PZ},
μ_{PZ2}—repair rate of failed processor A and transition to state of full ability S_{PZ},
λ_{B0}—transition rate from state of full ability S_{PZ} to state of reached operational capability S_B after failure of combinational circuit,
μ_{B0}—repair rate after failures of combinational circuit and both processors and transition from state of reached operational capability S_B to state of full ability S_{PZ},
λ_{B1}—transition rate from state of partial ability where S_{B1} one (processor A) processor is in state of full ability and the other (processor B) undergoes repair to of reached operational capability S_B after failure of processor A,
λ_{B2}—transition rate from state of partial ability where S_{B2} one (processor B) processor is in state of full ability and the other (processor A) undergoes repair to of reached operational capability S_B after failure of processor B,

The system illustrated in Figure 1 may be described by the following Chapman–Kolmogorov equations:

$$\begin{aligned}
R_0'(t) &= -\lambda_{ZB1}\cdot R_0(t) + \mu_{PZ1}\cdot Q_{ZB1}(t) - \lambda_{ZB2}\cdot R_0(t) \\
&\quad + \mu_{PZ2}\cdot Q_{ZB2}(t) - \lambda_{B0}\cdot R_0(t) + \mu_{B0}\cdot Q_B(t) \\
Q_{ZB1}'(t) &= \lambda_{ZB1}\cdot R_0(t) - \mu_{PZ1}\cdot Q_{ZB1}(t) - \lambda_{B1}\cdot Q_{ZB1}(t \\
Q_{ZB2}'(t) &= \lambda_{ZB2}\cdot R_0(t) - \mu_{PZ2}\cdot Q_{ZB2}(t) \\
&\quad - \lambda_{B2}\cdot Q_{ZB2}(t) \\
Q_B'(t) &= \lambda_{B1}\cdot Q_{ZB1}(t) + \lambda_{B2}\cdot Q_{ZB2}(t) + \lambda_{B0}\cdot R_0(t) \\
&\quad - \mu_{B0}\cdot Q_B(t)
\end{aligned} \tag{1}$$

Given the initial conditions:

$$\begin{aligned}
R_0(0) &= 1 \\
Q_{ZB}(0) &= Q_B(0) = 0
\end{aligned} \tag{2}$$

Laplace transform yields the following system of linear equations:

$$\begin{aligned}
s\cdot R_0^*(s) - 1 &= -\lambda_{ZB1}\cdot R_0^*(s) + \mu_{PZ1}\cdot Q_{ZB1}^*(s) \\
&\quad - \lambda_{ZB2}\cdot R_0^*(s) + \mu_{PZ2}\cdot Q_{ZB2}^*(s) \\
&\quad - \lambda_{B0}\cdot R_0^*(s) + \mu_{B0}\cdot Q_B^*(s) \\
s\cdot Q_{ZB1}^*(s) &= \lambda_{ZB1}\cdot R_0^*(s) - \mu_{PZ1}\cdot Q_{ZB1}^*(s) \\
&\quad - \lambda_{B1}\cdot Q_{ZB1}^*(s) \\
s\cdot Q_{ZB2}^*(s) &= \lambda_{ZB2}\cdot R_0^*(s) - \mu_{PZ2}\cdot Q_{ZB2}^*(s) \\
&\quad - \lambda_{B2}\cdot Q_{ZB2}^*(s) \\
s\cdot Q_B^*(s) &= \lambda_{B1}\cdot Q_{ZB1}^*(s) + \lambda_{B2}\cdot Q_{ZB2}^*(s) \\
&\quad + \lambda_{B0}\cdot R_0^*(s) - \mu_{B0}\cdot Q_B^*(s)
\end{aligned} \tag{3}$$

By rearranging we get:

$$R_0^*(s) = \frac{-b_1\cdot b_2\cdot b_3}{\begin{aligned} &b_1\cdot b_2\cdot \lambda_{B0}\cdot \mu_{B0} - a\cdot b_1\cdot b_2\cdot b_3 \\ &+ b_2\cdot b_3\cdot \lambda_{ZB1}\cdot \mu_{PZ1} + b_1\cdot b_3\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ &+ b_2\cdot \mu_{B0}\cdot \lambda_{B1}\cdot \lambda_{ZB1} + b_1\cdot \mu_{B0}\cdot \lambda_{B2}\cdot \lambda_{ZB2}\end{aligned}}$$

$$Q_{ZB1}^*(s) = \frac{-b_2\cdot b_3\cdot \lambda_{ZB1}}{\begin{aligned} &b_1\cdot b_2\cdot \lambda_{B0}\cdot \mu_{B0} - a\cdot b_1\cdot b_2\cdot b_3 \\ &+ b_2\cdot b_3\cdot \lambda_{ZB1}\cdot \mu_{PZ1} + b_1\cdot b_3\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ &+ b_2\cdot \mu_{B0}\cdot \lambda_{B1}\cdot \lambda_{ZB1} + b_1\cdot \mu_{B0}\cdot \lambda_{B2}\cdot \lambda_{ZB2}\end{aligned}}$$

$$Q_{ZB2}^*(s) = \frac{-b_1\cdot b_3\cdot \lambda_{ZB2}}{\begin{aligned} &b_1\cdot b_2\cdot \lambda_{B0}\cdot \mu_{B0} - a\cdot b_1\cdot b_2\cdot b_3 \\ &+ b_2\cdot b_3\cdot \lambda_{ZB1}\cdot \mu_{PZ1} + b_1\cdot b_3\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ &+ b_2\cdot \mu_{B0}\cdot \lambda_{B1}\cdot \lambda_{ZB1} + b_1\cdot \mu_{B0}\cdot \lambda_{B2}\cdot \lambda_{ZB2}\end{aligned}}$$

$$Q_B^*(s) = \frac{-b_1\cdot b_2\cdot \lambda_{B0} - b_2\cdot \lambda_{B1}\cdot \lambda_{ZB1} - b_1\cdot \lambda_{B2}\cdot \lambda_{ZB2}}{\begin{aligned} &b_1\cdot b_2\cdot \lambda_{B0}\cdot \mu_{B0} - a\cdot b_1\cdot b_2\cdot b_3 \\ &+ b_2\cdot b_3\cdot \lambda_{ZB1}\cdot \mu_{PZ1} + b_1\cdot b_3\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ &+ b_2\cdot \mu_{B0}\cdot \lambda_{B1}\cdot \lambda_{ZB1} + b_1\cdot \mu_{B0}\cdot \lambda_{B2}\cdot \lambda_{ZB2}\end{aligned}} \tag{4}$$

where:

$$a = s + \lambda_{ZB1} + \lambda_{ZB2} + \lambda_{B0}$$

$$b_1 = s + \mu_{PZ1} + \lambda_{B1}$$

$$b_2 = s + \mu_{PZ2} + \lambda_{B2}$$

$$b_3 = s + \mu_{B0}$$

Solving above equations in time domain is a next step of the analysis which has not been included in this paper.

4 MODELLING OF PROCESS RAIL ICT MAINTENANCE

Computer simulation and computer-aided analysis facilitate to relatively quickly determine the influence of change in reliability-exploitation parameters of individual components on reliability of the entire system. Using computer aided allows to perform the calculation of the value of probability of system staying in state of full ability R_0. That procedure is illustrated with below example.

The following quantities were defined for the system:

– test duration—1 year (in [h]):

$$t = 8760 \ [h]$$

– transition rate from state of full ability SPZ to one (processor A) processor is in state of full ability and the other (processor B) undergoes repair:

$$\lambda_{ZB1} = 0{,}000000006$$

– transition rate from state of full ability SPZ to one (processor B) processor is in state of full ability and the other (processor B) undergoes repair,:

$$\lambda_{ZB2} = 0{,}000000006$$

– transition rate from state of partial ability where S_{ZB1} one (processor A) processor is in state of full ability and the other (processor B) undergoes repair to of reached operational capability SB after failure of processor A λ_{B1}:

$$\lambda_{B1} = 0{,}000000006$$

– transition rate from state of partial ability where S_{ZB2} one (processor B) processor is in state of full ability and the other (processor A) undergoes repair to of reached operational capability SB after failure of processor B λ_{B2}:

$$\lambda_{B2} = 0{,}000000006$$

– transition rate from state of full ability SPZ to state of reached operational capability SB after failure of combinational circuit λ_{B0}:

$$\lambda_{B0} = 0{,}000000001$$

– repair rate of failed processor B and transition to state of full ability SPZ:

$$\mu_{PZ1} = \frac{1}{24}$$

– repair rate of failed processor A and transition to state of full ability SPZ,:

$$\mu_{PZ2} = \frac{1}{24}$$

After using the inverse Laplace transform for equation (4) and given transition rate from state of reached operational capability to state of full ability is

$$\mu_{BO} = \frac{1}{0{,}5}$$

obtained is: $R_O = 0{,}9999997115$

After using the inverse Laplace transform for equation (4) and given transition rate from state of reached operational capability to state of full ability is

$$\mu_{BO} = \frac{1}{6}$$

obtained is: $R_O = 0{,}999999706$

5 CONCLUSION

Results suggest that proposed evaluation method for determining utilisation of rail transport telematics system support train driving is valid and viable. Furthermore reliability parameters of individual digital rail ICT system components is rather high (high availability rates). Availability rate of the entire system depends on availability rates of switching systems and does not deviate considerably from availability guidelines for digital switching systems.

Practical application of deliberations presented hereinbefore enables to determine the impact of transition rate from the state of the impendency over safety to the state of full ability μ_{PZ1} i, transition rate from the state of unreliability of safety to the state of the impendency over safety μ_{PZ2} and transition rate from the state of unreliability of safety to the state of full ability μ_{PZ} on probability

of system staying in the state of full ability. Rates μ_{PZ1}, μ_{PZ2} and μ_{PZ} should be read as inverse times t_{PZ1}, t_{PZ2} and t_{PZ} which determine the time taken to restore system elements to the state of full ability.

REFERENCES

Belmonte F, Boulanger J.-L., Schön W. 2008. *Dispatcher Reliability Analysis: SPICA-RAIL Experiments. Author manuscript, published in "COMPRAIL"*, Toledo: Espagne.

Chołda P., Jajszczyk A. 2003. Assessment of availability in telecommunication network. *Telecommunication Review and Telecommunication News*. No. 2-3/2003. Publication by Sigma NOT Warsaw (in Polish).

Flammini F. (Book Editor). 2012. *Railway Safety, Reliability, and Security: Technologies and Systems Engineering. Copyright.* (www.igi-global.com/book/railway-safety-reliability-security/).

Jajszczyk A. 2006. *Bases of the telecommuting.* Publisher WKiŁ. Warsaw (in Polish).

Kołowrocki K., Soszyńska-Budny J. 2011. *Reliability and safety of complex technical systems and processes*. Springer-Verlag, London.

Kwestarz W., Krygier J. 1999. Reliability requirements for telecommunication lines. *Proceedings of the National Telecommunication Symposium,* Warsaw, Poland (in Polish).

Lewiński A, Perzyński T. 2010. The Reliability and Safety of Railway Control Systems Based on New Information Technologies. *Transport Systems Telematics. Communications in Computer and Information Science* 104. Springer Berlin Heidelberg.

Military Handbook:217 C 1979. *Reliability prediction of electronic equipment*. USA Department of Defense.

Military Handbook:470 A 1997. *Designing and developing maintainable products and systems.* Volume I. Department of Defense.

Siergiejczyk M. and others 2000. Technical and exploitation requirements for integrated devices of the railway telecommunication networks. *Railway Institute Research work. CNTK JBR Typescript.* Warsaw (in Polish).

Siergiejczyk M. 2009. Operational Availability of Railway Dispatch Communication System. *Dependability of Computer Systems.* IEEE Computer Society Press. Los Alamitos, Washington, Tokyo.

Siergiejczyk M., Rosinski A. 2011. Reliability analysis of electronic protection systems using optical links. In W. Zamojski & J. Kacprzyk & J. Mazurkiewicz & J. Sugier & T. Walkowiak (eds) *Dependable Computer Systems*: 193–203, given as the monographic publishing series—"Advances in intelligent and soft computing", Vol. 97. Berlin Heidelberg: Springer-Verlag.

Verma A.K., Ajit S., Karanki D.R. 2010. *Reliability and safety engineering*. London: Springer.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Premises of evaluation of the technical object suitability with including the quality of its maintenance and operation, and their initial conditions

R. Grądzki
Bialystok University of Technology, Faculty of Mechanical Engineering, Bialystok, Poland

P. Lindstedt
Air Force Institute of Technology, Warsaw, Poland

K. Golak
Bialystok University of Technology, Faculty of Mechanical Engineering, Bialystok, Poland

ABSTRACT: In this article, results of exploitation research of three various technical objects (engines of public transport buses) for different initial conditions are presented. Gathered data is presented in three sets (1—concerning object, 2—concerning driving conditions, 3—concerning driver, where sets 2 and 3 are the object environment) in form of conventional points (experts numerical assessments). Relation between point information of object and point information of environment was described by coupled equations of state (describing relations between operation condition and technical condition including initial conditions for each exploitation period). Such approach allows to determine parameters of technical condition a_T and operation condition a_R and subsequently, from the course of a_T parameter, set of parametrical damage $m_T(t)$ and from course of parameter a_R—set of momentary damage $a_R(t)$. Hence for each moment of exploitation data on technical and operation conditions of each object (bus engine) is available. This data allows to optimally control exploitation and service of particular objects as set of objects and its elements.

1 INTRODUCTION

Gradual damage of technical object (decrease in its exploitation properties and mechanical wear) occurs during the process of its exploitation. This damage consists on deregulation, wear and increase of unreliability. Hence the importance of permanent observation for changes of operation condition changes, technical condition changes and reliability changes during service and use of the object (Ashby 1963, Szczepaniak 1999).

In this article, work on new method of exploitation analysis of object aptitude is presented, based on assumption that every information (diagnostic signals, use signals, use condition signals) is expressed (presented) in form of points (numerical expert assessment).

Diagnostic signals in form of points were used for the first time in diagnostics of ship-based helicopter SH-2G (USA) (Szawłowski 2005). In this method aptitude was analyzed only by summing all the points. Next, obtained value is compared to threshold set by manufacturer (USA). Based on relation between sum of the points and allowed number of points, the machine is qualified for further exploitation or renovation.

The new method of using exploitation data presented in this article is based on transforming every signal, symptom and expert assessments to standard point form and (which is innovatory) using them to determine parameters of regulation and technical condition from model in form of coupled interaction equations of state (including initial conditions) [Cempel 2006] and subsequently from its courses—set of damages that are base for determining reliability characteristics [Bukowski 2003, Lindstedt 2006, Lindstedt & Sudakowski 2006].

Presented practical method of exploitation analysis of object aptitude (operation condition, wear, reliability) might be, and partially is, applied to process of servicing technical objects. Such data allows to decide on object further destination.

2 DIAGNOSTIC RESEARCH OF TECHNICAL OBJECT AND ITS ENVIRONMENT

The analyzed objects were three various MAN buses exploited in Municipal Transport Company of the City of Bialystok. The aim of the research was to obtain diagnostic signals D_k concerning condition of objects (data from diagnostician)

and data on their environment (expert information from driver).

Analysis was undertaken for each week of a year, thus obtaining database for twelve months.

Obtained determined (measurable), probabilistic and heuristic data was divided into two subgroups:

- signals concerning technical condition D_k
- signals concerning environment condition U.

All measured signals were presented in Table 1. These signals are of varying physical nature and thus were in each case transformed to point value.

Table 1. Expert point weights for assessment of condition of engine, driver (Table 3) and diagnostician.

Signal	Signal name	Ep	N	N + 5%	N + 10%	N + 15%	N + 20%
D_{M1}	Average fuel consumption without heating [l/100 km]	15	15	30	45	60	75
D_{M2}	Average fuel consumption with heating [l/100 km]	15	15	30	45	60	75
D_{M3}	Fogging value during engine blowout [1/m]	10	10	20	30	40	50
D_{M4}	Fogging value during engine operation [1/m]	10	10	20	30	40	50
D_{M5}	Peak value of noise level [dB]	5	5	10	15	20	25
D_{M6}	Average value of noise level [dB]	5	5	10	15	20	25

Signal	Signal name	Ep	<1%	1–10%	10–20%	20–30%	>30%
D_{M7}	Braking force value for front axis—left wheel [kN]	–	–	–	–	–	–
D_{M8}	Braking force value for front axis—right wheel [kN]	–	–	–	–	–	–
D_{M9}	Percentage difference between D_{M7} and DM8 [%]	15	15	30	45	60	75
D_{M10}	Braking force value for rear axis—left wheel [kN]	–	–	–	–	–	–
D_{M11}	Braking force value for rear axis—right wheel [kN]	–	–	–	–	–	–
D_{M12}	Percentage difference between D_{M10} and DM11 [%]	15	15	30	45	60	75
D_{M13}	Braking force value for middle axis—left wheel [kN]	–	–	–	–	–	–
D_{M14}	Braking force value for middle axis—right wheel [kN]	–	–	–	–	–	–
D_{M15}	Percentage difference between DM13 and D_{M14} [%]	10	10	20	30	40	50

Signal	Signal name	Ep	0–2	2–5	>5
D_{E1}	Clatters	8	8	16	24
D_{E2}	Spontaneous engine stalls (on neutral gear)	4	4	8	12
D_{E3}	Engine stalls (during operation)	12	12	24	36

Signal	Signal name	Ep	<500 k	500 k–1 mln	>1 mln
D_{E4}	Bus mileage	4	4	8	12

Signal	Signal name	Ep	<5 lat	5–12 lat	>12 lat
U_{K1}	Driver's tenure [years]	3	3	6	9

Signal	Signal name	Ep	<140 h	140–180 h	>180 h
U_{K2}	Number of work hours in month [h]	6	6	12	18

Signal	Signal name	Ep	<10	10–15	>15
U_{K3}	Driving fluency (braking, accelerating)	9	9	18	27

Signal	Signal name	Ep	<15	15–30	>30
U_{D1}	Number of stops	4	4	8	12

Signal	Signal name	Ep	<10 km	10–15 km	>15 km
U_{D2}	Route length	2	2	4	6

(*Continued*)

Table 1. (*Continued*)

Signal	Signal name	Ep	Good surface	Medium surface	Poor surface
U_{D3}	Surface and formation	6	6	12	18

Signal	Signal name	Ep	<–10 °C	–10–10 °C	10–20 °C	20–30 °C	>30 °C
U_{P1}	Environment temperature	1	3	2	1	2	3

Signal	Signal name	Ep	<28,4 km/h	28,4–61,56 km/h	>61,56 km/h
U_{P2}	Wind	1	1	2	3

Signal	Signal name	Ep	<994,66 hPa	996,66–1020 hPa	>1020 hPa
U_{P3}	Atmospheric pressure	1	1	2	3

Signal	Signal name	Ep	No rainfall	No significant rainfall	Little rainfall	Rainfall	Little snow	Snow
U_{P4}	Rainfall	1	1	2	3	4	5	6

E_p—experts points of weight (importance of problem).

Table 2. Combination of diagnostic and environment signals in physical form.

Month	D_{M1}	D_{M2}	D_{M3}	D_{M4}	D_{M5}	D_{M6}	D_{M7}	D_{M8}	D_{M9}	D_{M10}	D_{M11}	D_{M12}	D_{E1}	D_{E2}	D_{E3}	D_{E4}
Operation signals																
1	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	0	0	0	215582
2	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	0	1	0	217982
3	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	0	0	0	220102
4	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	0	0	2	222669
5	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	1	0	0	225125
6	35,7	35,7	0,37	0,02	95	92	12	13,2	9	15,8	14,7	6	0	3	0	227358
7	33,7	33,7	0,45	0,03	94	90	11,4	12	5	12,5	12,3	1	0	0	0	229758
8	33,7	33,7	0,45	0,03	94	90	11,4	12	5	12,5	12,3	1	0	0	0	232273
9	33,7	33,7	0,45	0,03	94	90	11,4	12	5	12,5	12,3	1	0	0	0	234571
10	35,1	35,1	0,42	0,03	91,9	91	8,8	12,6	29	11,9	13,3	10	3	3	0	236699
11	35,1	35,1	0,42	0,03	91,9	91	8,8	12,6	29	11,9	14,7	10	0	0	0	239047
12	35,1	35,1	0,42	0,03	91,9	91	8,8	12,6	29	11,9	14,7	10	0	0	0	241392

Month	U_{K1}	U_{K2}	U_{K3}	U_{D1}	U_{D2}	U_{D3}	U_{P1}	U_{P2}	U_{P3}	U_{P4}
Environment signals										
1	4	125	5	33	15	2	–0,8	15,2	995,7	No significant rainfall
2	24	164	5	21	9,4	1	–5,8	16,2	1002,2	Little rainfall
3	24	160	5	21	9,4	1	7,7	19,4	999,3	No significant rainfall
4	10	179	5	21	9,4	1	14,9	16,3	987,2	No significant rainfall
5	10	146	5	40	16,9	2	20,9	14,9	997,0	No significant rainfall
6	16	187	6	40	16,9	2	22,1	16,4	992,2	Little rainfall
7	16	110	6	40	16,9	2	26,6	13,7	995,8	No significant rainfall
8	16	144	4	40	16,9	2	23,8	14,6	996,7	No significant rainfall
9	16	170	4	40	16,9	2	20,2	16,4	995,7	No rainfall
10	4	144	4	29	14,6	2	11,8	16,0	994,0	No significant rainfall
11	4	154	7	29	14,6	2	6,9	15,8	995,7	No rainfall
12	4	185	7	29	14,6	2	–2,3	16,3	994,5	No significant rainfall

Table 3. Combination of diagnostic and environment signals in point form.

Month	D_{M1P}	D_{M2P}	D_{M3P}	D_{M4P}	D_{M5P}	D_{M6P}	D_{M9P}	D_{M12P}	D_{E1P}	D_{E2P}	D_{E3P}	D_{E4P}
1	15	15	10	10	5	5	30	30	0	0	0	4
2	15	15	10	10	5	5	30	30	0	4	0	4
3	15	15	10	10	5	5	30	30	0	0	0	4
4	15	15	10	10	5	5	30	30	0	0	12	4
5	15	15	10	10	5	5	30	30	8	0	0	4
6	15	15	10	10	5	5	30	30	0	8	0	4
7	15	15	10	10	5	5	30	15	0	0	0	4
8	15	15	10	10	5	5	30	15	0	0	0	4
9	15	15	10	10	5	5	30	15	0	0	0	4
10	15	15	10	10	5	5	60	30	16	8	0	4
11	15	15	10	10	5	5	60	30	0	0	0	4
12	15	15	10	10	5	5	60	30	0	0	0	4

Month	U_{K1P}	U_{K2P}	U_{K3P}	U_{D1P}	U_{D2P}	U_{D3P}	U_{P1P}	U_{P2P}	U_{P3P}	U_{P4P}
1	3,00	6,00	9,00	12,00	4,00	12,00	2,03	1,00	1,55	2,32
2	9,00	12,00	9,00	12,00	2,00	6,00	2,25	1,07	1,61	2,89
3	9,00	12,00	9,00	12,00	2,00	6,00	1,58	1,13	1,77	2,06
4	6,00	12,00	9,00	12,00	2,00	6,00	1,43	1,03	1,17	2,10
5	6,00	12,00	9,00	12,00	6,00	12,00	1,65	1,00	1,71	2,26
6	9,00	18,00	9,00	12,00	6,00	12,00	1,80	1,00	1,33	2,73
7	9,00	6,00	9,00	12,00	6,00	12,00	2,35	1,00	1,52	1,94
8	9,00	12,00	9,00	12,00	6,00	12,00	1,97	1,03	1,65	1,97
9	9,00	12,00	9,00	12,00	6,00	12,00	1,47	1,03	1,70	1,40
10	3,00	12,00	9,00	12,00	4,00	12,00	1,29	1,06	1,45	1,55
11	3,00	12,00	9,00	12,00	4,00	12,00	1,77	1,00	1,57	1,33
12	3,00	18,00	9,00	12,00	4,00	12,00	2,03	1,06	1,55	2,03

In order to obtain knowledge from specialists (experts) for expressing data in form of points, detailed questionnaires were developed in cooperation with users—bus drivers.

Research was undertaken on group of 20 experts, whose tenure as drivers was at least 5 years. Summarizing tables with importance of information D_i and U_i expressed in expert point weights for assessment of engine and its environment condition obtained from driver and diagnostician were presented in Table 1.

Based on Table 1, each situation, phenomenon and exploitation facts might be expressed using proper point value.

Values of signals $U_{P1} \div U_{P3}$ in Table 2 were taken as average values from whole month, whereas values of signal U_{P4} were most frequently occurring. In Table 3 total number of points were obtained by daily change of observed signals to point values which were subsequently, at the end of the month, summed and divided by number of days in the month.

Based on data from Table 2. and including experts weight (Table 3 and 4) point forms of signals were obtained—Table 3 (data for other two buses was filled analogically).

3 ALGORITHM OF DETERMINING PARAMETERS OF TECHNICAL AND OPERATION CONDITION OF TECHNICAL OBJECT

Object (engine) in its environment is described by coupled state equations including initial conditions describing relations between technical condition and operation condition (Cempel 2006, Lindstedt 2006, 2009, Söderström & Stoica 1997). It should be noticed that, in these equations diagnostic signals D_k are environment for operation signals U and operation signals U are environment for diagnostic signals D_k.

$$\frac{dU}{dt} = a_R U + b_{R1} D_k + b_{R0} \tag{1}$$

$$\frac{dD_k}{dt} = a_T D_k + b_{T1} U + b_{T0} \tag{2}$$

Equation (1) and (2) might be written as follows:

$$\frac{\Delta U}{\Delta \theta} = a_R U + a_R \hat{a}_{R1} D_k + a_R \hat{a}_{R0} \tag{3}$$

Table 4. Procedure of calculating technical condition and regulation parameters for bus no. 301.

Month	Operation time θ	θ	D_k	U	Δθ	ΔDK	ΔU	D_k*U	∑D_k*U	U^2	∑U^2	D_k^2	∑D_k^2	$\hat{a}_{T0}$	$\hat{a}_{T1}$	$\hat{a}_{R0}$	$\hat{a}_{R1}$	a_T	a_R	Δa_T	Δa_R
1	213429	2200	54,28	22,98	2200	54,28	22,98	1247,35	1055,65	528,08	528,08	2946,32	2946,32								
2	215582	2153	50,16	21,05	4353	104,44	44,03	1055,65	2188,84	442,92	971,00	2516,00	5462,32	17,67	0,70	7,37	0,13	290,29	291,32		
3	217982	2400	50,32	22,52	6753	154,76	66,55	1133,20	2188,84	507,16	1478,16	2532,00	7994,32	6,39	1,38	3,26	0,25	260,83	255,80	–29,46	–35,53
4	220102	2120	50,16	22,39	8873	204,92	88,93	1122,93	3311,78	501,18	1979,35	2516,00	10510,32	3,39	1,63	1,75	0,31	256,18	253,59	–4,64	–2,20
5	222669	2567	51,58	21,30	11440	256,49	110,24	1098,80	4410,57	453,89	2433,24	2660,00	13170,32	2,69	1,79	0,84	0,33	242,69	245,52	–13,49	–8,07
6	225125	2456	50,79	24,43	13896	307,29	134,67	1240,79	5651,36	596,73	3029,97	2580,00	15750,32	0,90	1,86	1,06	0,36	227,79	222,57	–14,91	–22,96
7	227358	2233	50,79	28,70	16129	358,08	163,36	1457,60	7108,96	823,49	3853,46	2580,00	18330,32	–0,32	1,85	1,31	0,38	214,53	204,52	–13,25	–18,04
8	229758	2400	42,91	23,12	18529	400,99	186,48	992,06	8101,02	534,59	4388,05	1841,00	20171,32	0,03	1,85	0,74	0,40	252,77	245,30	38,23	40,77
9	232273	2515	42,91	25,33	21044	443,89	211,81	1086,75	9187,78	641,52	5029,56	1841,00	22012,32	–0,38	1,83	0,83	0,42	237,42	228,76	–15,34	–16,54
10	234571	2298	42,91	25,26	23342	486,80	237,07	1083,73	10271,51	637,96	5667,52	1841,00	23853,32	–0,29	1,81	0,68	0,43	235,85	228,93	–1,57	0,17
11	236699	2128	74,40	23,35	25470	561,21	260,42	1737,47	12008,98	545,30	6212,82	5536,00	29389,32	2,68	1,92	–0,65	0,41	180,62	192,10	–55,23	–36,83
12	239047	2348	72,22	23,37	27818	633,43	283,79	1687,97	13696,95	546,25	6759,07	5216,00	34605,32	2,09	2,02	–0,44	0,40	187,41	197,77	6,79	5,67
13	241392	2345	72,22	27,01	30163	705,65	310,81	1951,05	15648,00	729,79	7488,86	5216,00	39821,32	1,22	2,09	–0,11	0,39	180,27	186,33	–7,14	–11,44

$$\frac{\Delta U}{\Delta \theta} = a_R(U + \hat{a}_{R1}D_k + \hat{a}_{R0}) \tag{4}$$

$$\frac{\Delta D_k}{\Delta \theta} = a_T D_k + a_T \hat{a}_{T1} U + a_T \hat{a}_{T0} \tag{5}$$

$$\frac{\Delta D_k}{\Delta \theta} = a_T(D_k + \hat{a}_{T1}U + \hat{a}_{T0}) \tag{6}$$

where: U—operation signal (signal of use); D_k—bus diagnostic signal; a_R—operation condition parameter, dependent mostly on object operation U and influence of diagnostic signals D_k on this operation; b_{R1}, b_{R0}—parameters of influence of diagnostic signals and initial conditions on operation condition; a_T—object technical condition parameter, dependent mostly on diagnostic signals and signals coming from environment; b_{T1}, b_{T0}—parameters of influence of signals of regulation and initial conditions on technical condition of the bus.

According to rules of statistical identification $\dot{D}_k = 0$ (Söderström & Stoica 1997) from equations (2, 5, 6) we obtain::

$$\hat{a}_{T1} = \frac{n\sum_{i=1}^{n} Dk_i U_i - \sum_{i=1}^{n} Dk_i \sum_{i=1}^{n} U_i}{n\sum_{i=1}^{n} U_i^2 - \sum_{i=1}^{n} U_i \sum_{i=1}^{n} U_i} \tag{7}$$

$$\hat{a}_{T0} = \frac{\sum_{i=1}^{n} Dk_i \sum_{i=1}^{n} U_i^2 - \sum_{i=1}^{n} Dk_i U_i \sum_{i=1}^{n} U_i}{n\sum_{i=1}^{n} U_i^2 - \sum_{i=1}^{n} U_i \sum_{i=1}^{n} U_i} \tag{8}$$

and ultimately sought parameter of technical condition a_T:

$$a_T = \frac{\Delta D_k}{\frac{\Delta \Theta}{resurs}(D_k + \hat{a}_{T1}U + \hat{a}_{T0})} \tag{9}$$

Parameter a_T characterizes object technical condition and depends on diagnostic signals (D_k) and signals coming from driver's and environment influence as well as initial conditions $\hat{a}_{T0}$.

According to rules of statistical identification $\dot{U} = 0$ (Söderström & Stoica 1997) from equation (1, 3, 4) we obtain:

$$\hat{a}_{R1} = \frac{n\sum_{i=1}^{n} Dk_i U_i - \sum_{i=1}^{n} Dk_i \sum_{i=1}^{n} U_i}{n\sum_{i=1}^{n} Dk_i^2 - \sum_{i=1}^{n} Dk_i \sum_{i=1}^{n} Dk_i} \tag{10}$$

$$\hat{a}_{R0} = \frac{\sum_{i=1}^{n} U_i \sum_{i=1}^{n} Dk_i^2 - \sum_{i=1}^{n} Dk_i U_i \sum_{i=1}^{n} Dk_i}{n\sum_{i=1}^{n} Dk_i^2 - \sum_{i=1}^{n} Dk_i \sum_{i=1}^{n} Dk_i} \tag{11}$$

and ultimately sought parameter of operation condition a_R:

$$a_R = \frac{\Delta U}{\frac{\Delta \Theta}{resurs}(U + \hat{a}_{R1} D_k + \hat{a}_{R0})} \tag{12}$$

Parameter a_R characterizes object operation condition and depends on operation (utility) signals coming from driver action and environment U, diagnostic signals D_k and initial conditions $\hat{a}_{R0}$.

Signals D_k and U in homogenous point form (Table 6) were transformed to resultant diagnostic signal (D_k) and environment (U).

$$D_k = \sqrt{\begin{array}{l} D_{M1P}^2 + D_{M2P}^2 + D_{M3P}^2 + D_{M4P}^2 + D_{M5P}^2 \\ + D_{M6P}^2 + D_{M9P}^2 + D_{M12P}^2 + D_{I5P}^2 + D_{IEP}^2 \\ + D_{2EP}^2 + D_{3EP}^2 + D_{4EP}^2 \end{array}} \tag{13}$$

$$U = \sqrt{\begin{array}{l} U_{K1P}^2 + U_{K2P}^2 + U_{K3P}^2 + U_{D1P}^2 + U_{D2P}^2 + U_{D3P}^2 \\ + U_{P1P}^2 + U_{P2P}^2 + U_{P3P}^2 + U_{P4P}^2 \end{array}} \tag{14}$$

Using data from Table 3 and equations 1÷12, increases in technical condition described by parameter a_T and operation (regulation) condition described by parameter a_R are calculated.

Subsequently Σa_T describing level of object wear and Σa_R describing resource of proper operation possibility are determined.

In Table 4, row 1 data was implemented from previous year thus allowing determination of parameters a_T and a_R starting from February (row 2).

Results of courses of normalized parameters a_T and a_R changes for bus no. 301 were presented on Figure 1, for bus no. 303 on Figure 3 and for bus no. 304 on Figure 5, whereas courses of sums of these parameters were presented on Figure 2, Figure 4 and Figure 6 respectively.

On the base of data from Table 5 and charts 1, 3, 5 the following might be noted: the best technical and regulation condition is that of bus no. 301. Values of sum of a_R and a_T are the least, thus statement can be made that wear of bus no. 301 is the least and regulation potential was used to the least extent.

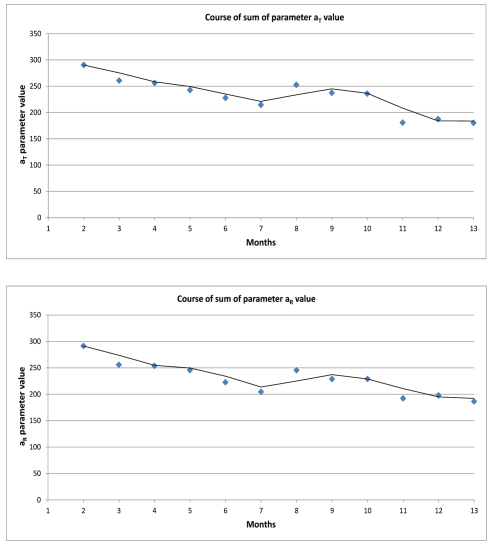


Figure 1. Changes of normalized parameter of technical condition and regulation for bus no. 301.

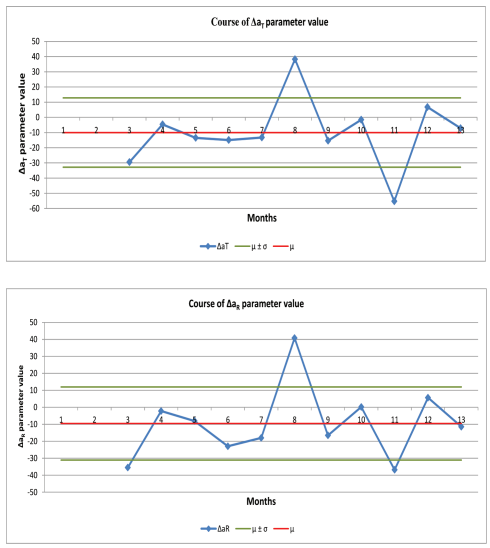
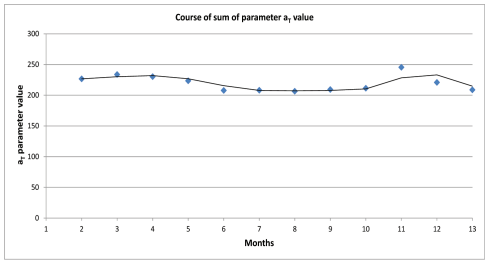


Figure 2. Course of value of technical condition and regulation parameter increase for bus no. 301.

Obtained results were confirmed by discerning analysis of analytical assessments of aptitude of aforementioned buses by direct method realized by experts (diagnosticians—drivers).

Excess of increases values of technical condition and operation condition from the value of standard deviation might be observed in Figures 2, 4, 6.



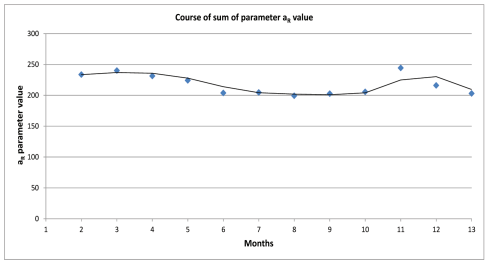
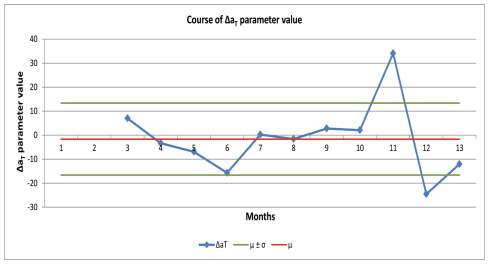


Figure 3. Changes of normalized parameter of technical condition and regulation for bus no. 303.



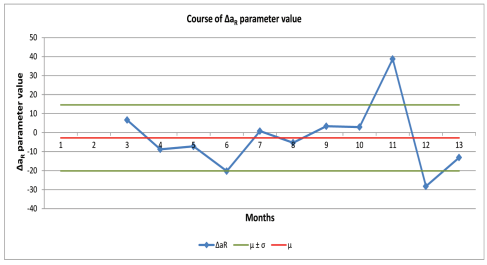
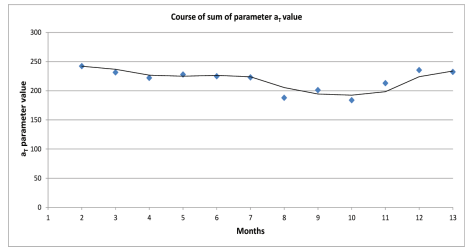


Figure 4. Course of value of technical condition and regulation parameter increase for bus no. 303.

It means that in case when increase of technical condition is greater than deviation value, parametrical damage occurred, whereas in case of operation parameter exceeding deviation value, momentary damage occurred (Table 5).

Parametrical and momentary damage do not disqualify object from further exploitation, but



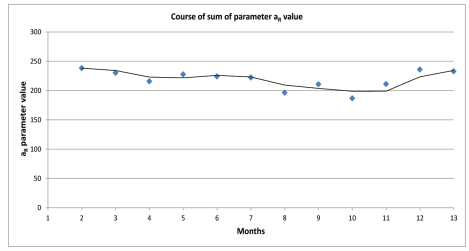
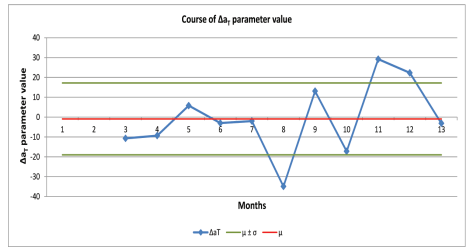


Figure 5. Changes of normalized parameter of technical condition and regulation for bus no. 304.



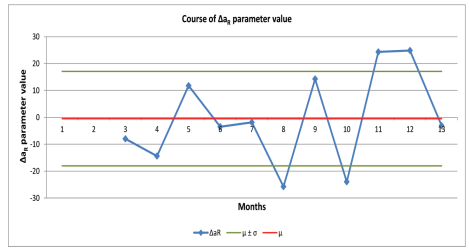


Figure 6. Course of value of technical condition and regulation parameter increase for bus no. 304.

Table 5. Summary table.

	Bus no. 301	Bus no. 303	Bus no. 304
Sum of a_T	180,272	208,792	232,173
Parametrical damage $m_T(t)$			
Sum of a_R	186,323	202,933	232,884
Momentary damage $m_R(t)$			

may be the base for determining reliability characteristics before the occurrence of dangerous catastrophic damage.

4 SUMMARY

Exploitation research activity is realized during object exploitation in order to determine its current and future operation, technical and reliability condition. In complex and advanced technical objects several research methods are used simultaneously based on data in various form (determined, probabilistic and heuristic signals).

The basis of innovatory method of using varying diagnostic data (in form of points) are presented. Each change of signal (depending on its value and moment of occurrence) corresponds with number of points predetermined by the experts. So far in such method of aptitude analysis, all the points were summed and subsequently a range was determined in which is the object, its condition and level of exploitation (Bukowski 2003, Söderström & Stoica 1997). Proposed method is based on using signals in form of points to determine parameters of regulation and technical condition (equations 3, 4) from coupled state equations (Cempel 2006, Lindstedt 2006, 2009) and subsequently reliability and safety of the object during exploitation. The described method may prove to be very useful due to unequivocal presentation of object global exploitation condition using parameters a_R, a_T and thus allows to predict how the object should be used and when the object should be serviced (repaired, overhauled).

ACKNOWLEDGEMENTS

Rafał Grądzki was supported by the Bialystok University of Technology under the research project No. W/WM/9/2013.

Karol Golak was supported by the Bialystok University of Technology under the research project No. W/WM/7/2013.

REFERENCES

Ashby R.W.: Wstęp do cybernetyki (Introduction to Cybernetics), PWN, Warszawa 1963.

Bukowski L.: Prognozowanie niezawodności i bezpieczeństwa systemów zautomatyzowanych, Materiały XXXI Szkoły Niezawodności, Szczyrk 2003. (Prediction of Reliability and Safety for Automated Systems. Proceedings of the 21st School of Reliability, Szczyrk, 2003).

Cempel C.: Teoria i inżynieria systemów (Theory and Engineering Practice of Systems), Wyd. Naukowe Instytutu Technologii Eksploatacyjnej PIB, Poznań 2006.

Günther H.: Diagnozowanie silników wysokprężnych (Diagnostics of Diesel Engines), Wyd. Komunikacji i Łączności, Warszawa 2006.

Lindstedt P.: The Method of complex worthiness assessment of an engineering object in the process of its use and service, Solid State Phenomena Vol. 144 (2009) pp 45–52.

Lindstedt P.: Reliability and its relation to regulation and diagnostics in the machinery exploitation systems, Journal of KONBiN Vol. 1, No 2/2006.

Lindstedt P., Sudakowski T: The effect of pilot's work quality on technical condition of propeller engine bearing. Journal of Vibroenginering Vol 8 No 2 2006.

Söderström T., Stoica P.: Identyfikacja systemów (Identification of Systems), PWN, Warszawa 1997.

Szawłowski S.: Przegląd kontrolny ASPA w systemie obsługiwania śmigłowca pokładowego SH-2G (Maintenance Inspection ASPA in the System of Service Operations to the Board Helicopter SH-2G), AIRD-IAG Warszawa 27–28. 10.2005.

Szczepaniak C.: Podstawy modelowania sytemu człowiek—pojazd—otoczenie (Fundamentals for Modelling of the Human—Vehicle—Environment Systems), PWN, Warszawa 1999.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Bivariate reliability analysis of driving profiles in automobile fleets

T. Köttermann, M. Grabert & S. Kempe
Daimler AG, Stuttgart, Baden-Wurttemberg, Germany

S. Bracke
University of Wuppertal, Wuppertal, North Rhine-Westphalia, Germany

ABSTRACT: Common reliability models in the automotive industry rarely take into account the wide variety of real world customer driving profiles. The only explanatory variable very often is the lifespan variable mileage, although it alone does not give further information about the specific driving profile that caused the damage. This paper demonstrates that a vehicle's reliability can highly differ, depending on its driving profile and that many practical applications of reliability models in the automotive industry, like failure predictions, are influenced by this fact. In order to take various driving profiles into account, a bivariate approach, using the two most common explanatory variables in automotive data, i.e. time in service and mileage, is presented. It is demonstrated in case studies that this extension of reliability models to the bivariate case already offers a substantial increase in performance compared to univariate models for many reliability related questions.

1 INTRODUCTION

In practice, reliability analyses in the automotive industry are done for various purposes. First of all field data analysis is used to evaluate the potential of an emerging failure mode, to estimate the number of expected failures within a defined timespan or to get a risk estimate for single vehicles, to concentrate campaigns to the group of vehicles under the highest risk. Further manufacturers (OEMs) are often interested in information about the general failure behavior of a component, e.g. its Weibull shape parameter. This information helps, in combination with further reliability analyses of testing results, to evaluate the reliability of components during the development. The performance of all these applications highly depends on the failure model's ability to explain the actual damage process that leads to a failure. In many years of working in the automotive industry, we noticed in a lot of cases that this damage process is more complex than common univariate reliability models are able to explain. This observation is reflected in false failure prediction and significantly changing results of reliability analyses over time. The main reason for this circumstance is, that one single variable rarely includes all the necessary information, to fully describe the complexity of a failure mode. In common univariate reliability analyses, these single variables are mostly either mileage or time in service. The true stress that a component is experiencing is the result of its individual usage. We define a set of variables to describe a vehicles usage as a driving profile. These profiles give information additionally to the absolute mileage of a vehicle. This paper describes a method to include these profiles into analyses and describe their effect on the component's reliability. The first and easiest step to achieve this goal is an extension to the bivariate case, so overall two variables are included to describe the vehicle's usage. The advantage of this approach lies in a minimal extension of complexity, yet significantly increased model performance, regarding a wide set of practical applications. This paper introduces a method to allow for the influence of a covariate on the failure behavior and illustrates its effectiveness by performance comparisons in form of case studies.

2 DRIVING PROFILES

Driving profiles give further details about the way a vehicle is used in addition to its absolute mileage. We are interested in using this information for reliability analyses to improve their performance. On the most detailed level every vehicle has an individual driving profile. The set of variables which could be used for its description is large because of a wide range of customers who are using their vehicles differently. Due to global activities of today's OEMs and the increasing diversity in the vehicles' concepts and their technology, the variety continues

to increase. Some of the most relevant aspects are given by these three following categories:

- The drivers behavior
  - Sportive driving
  - Fuel efficient driving
- The driving conditions
  - Quality of the roads
  - Traffic conditions, e.g. frequent traffic jams
  - Climate
- Main purpose of the vehicle
  - Private usage
  - Commuter traffic
  - Professional usage, e.g. Taxi vehicles

Thus in general driving profiles are complex there are two reasons why only reduced profiles are often used to work with in reliability models. First of all most automotive OEM's possibilities are limited by the available data. In the case of customer data analysis, they are facing the situation of very big samples but only limited information about each vehicle. Further an obvious assumption is that only a part of the information is relevant regarding a component's failure behavior. Some of the possible variables can be excluded from the start on, due to no expected influence on the failure mode.

We consider a bivariate solution, using mileage and time in service in this paper. The time in service can be expected to be available for the whole fleet, due to the usually known day of registration. In addition information about mileage is at least available for every failed vehicle and a portion of the failure free vehicles over the time of warranty. Although the reduction to only two variables seems to be very strict, it will be shown that the increase in the model's performance in different applications, compared to a common univariate approach, is still remarkable.

In the following, two explaining variables to analyze a failure behavior are considered, i.e. mileage at the failure's appearance and the timespan between the vehicle's registration and the day of failure. It is convenient to define one of these variables as the variable in which the lifetime is measured and the other one as a covariate. In the automotive industry it is common to measure the lifetime in mileage. This idea will be followed and the time in service is taken as covariate into account. Obviously time in service and mileage depend on each other. Vehicles which reached a high mileage tend to have a longer time in service and vice versa. That means that the covariate is time dependent. This problem can be simplified by one assumption which is regularly used analyzing automotive data as by Krivtsov & Frankstein (2006), Lawless et al. (1995) or Lawless et al. (2009):

$$\frac{mileage}{time} = a = const. \tag{1}$$

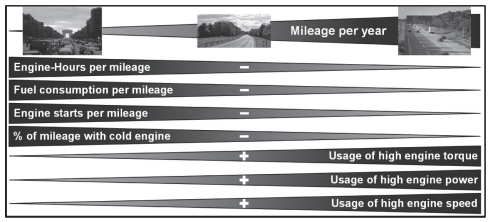


Figure 1. Correlation of the mileage accumulation rate to other driving profile variables.

where a = mileage accumulation rate. Within the warranty period, a can be treated as being constant. Besides the mentioned papers above, our practical experience strongly supports a mostly constant α.

It is worth mentioning that the mileage accumulation rate is actually able to add partially information about various other possible profile variables, due to the fact that it correlates to some specific driving patterns. A high value of a has the tendency to be observed for vehicles which are rather using highways, while a low value of a usually indicates that this vehicle is frequently used in city traffic. Driving mostly on highways or in the city, leads to specific usage characteristics regarding fuel consumption, engine starts or engine speed. Figure 1 indicates if a is positively or negatively correlated to these and several other variables that could be included into a reliability analysis but are mostly not available. This means that the use of a can lead to more informative models, even if it is not assumed that the time in service of a vehicle has a direct influence on the failure mode.

3 RELATED LITERATURE TO THIS WORK

The literature offers several methods and models to analyze survival data under the circumstance of different usage conditions. Cox (1972) introduced the Proportional Hazards Model (PHM) to allow for the influence of covariates. This approach is one of the most widely used, particularly in survival analysis. Bendell et al. (1991) discuss the application of this model especially in the context of reliability data. Case studies involving the PHM in the area of reliability were done by Kumar et al. (1992), Bendell et al. (1986) and Jardine et al. (1989). Alternatives to the PHM can be found in Oakes (1995), Kordonsky & Gertsbakh (1997) and Duchesne (1999) which follow the idea of multiple times scales to take more than one explanatory variable into account. Another possibility arises if there is some knowledge about the physical-failure mechanism. This approach is usually used with acceler-

ated testing data to estimate the failure distribution of customers in the field. This task is highly related to general influence of the specific usage on the failure behavior. Meeker et al. (1998) and Nelson (2001) discuss several examples of possible acceleration models and Escobar & Meeker (2006) describe in detail the general use of acceleration test models and necessary conditions to make them work well. The works by Hong & Meeker (2010 & 2013) refer particularly to predicting field-failures when use-rate information is available. Very similar to this work, Hong & Meeker evaluate their model by its prediction performance. All the mentioned references have in common that need assumptions about the usage's influence, some more and some less. This paper offers a rather assumption free approach to deal with the situation that reliability experts have no knowledge about the covariate's influence. It is fair to say that in many reliability analyses in automotive practice, reliability experts and engineers do not know a suitable model for the covariates' influence in advance. This circumstance is even gaining in importance, due to the increasing amount of new technologies in the automotive industry. Out of this reason it is desirable to use non-parametric methods, to allow for unspecified influences by a covariate.

4 BIVARIATE NON-PARAMETRIC APPROACH

Let us assume that a vehicle's usage can be primarily measured by its mileage in kilometer. In addition the influence of a vehicle's driving profile, i.e. a vehicle's mileage accumulation rate *a,* as defined above, is allowed. An estimate for alpha can be done by data of any visit in a workshop where the day of service and the vehicle's mileage were documented due to the assumption of *a* being time independent.

The main goal of this research, besides the bivariate approach itself, was to get a picture of the potential of taking a second usage variable into account in the context of various practical applications. To achieve that, we assumed that information about mileage and time in service is available for every vehicle. Therefore data of one production year that lies several years in the past was used. In this way an estimation of the mileage accumulation rate was available for most vehicles. Vehicles which had only a documented visit within their first three months of service or had no documented visit in a workshop at all were excluded from the dataset. In this case over 90% of the fleet was used for the analysis.

We assumed that vehicles with comparable driving profiles have a similar failure behavior. Vehicles with significantly different profiles might have different failure behaviors. The basic idea is to form clusters of vehicles with similar driving profiles and analyze the clusters' failure behaviors separately. Another way to describe the basic idea is that some amount of data is traded for a greater homogeneity. The failure probabilities can be estimated by any non-parametric univariate method, after suitable clusters were formed. A common approach is given by Kaplan & Meier (1958) in form of the Product Limit Estimator (PLE). The PLE was designed to estimate a survival probability in dependence of a lifetime variable for censored data. For this approach the PLE was slightly adapted. Equation 2 estimates the cumulative distribution function of the failure probability for a given cluster *g*:

$$F(t_j)_g = 1 - \prod_{j=1}^{kg} \left[1 - \left(\frac{\delta_{j,g}}{n_{j,g}} \right) \right] \tag{2}$$

where g is the index representing the clusters of vehicles with a similar driving profile, j is the index representing the mileage intervals within a cluster, t_j is the upper mileage of interval j, k_g is the number of mileage intervals of cluster g, $\delta_{j,g}$ is the number of failures in interval j of cluster g, $n_{j,g}$ is the number of vehicles that reached or passed interval j in cluster g. A detailed description of the PLE is given in Kaplan & Meier (1958).

It is worth pointing out that the PLE generally works better as the number of observed vehicles and the number of observed failures increase. Especially the number of observed failures is of great importance and therefore at least a minimum of failures which has to be defined by the reliability experts is needed. This means in every formed cluster this minimum of failures has to be observed. At the same time the clusters should be as homogeneous as possible regarding the mileage accumulation rate, to minimize the differences of the vehicles' failure behaviors to each other. In this trade-off situation, where bigger clusters tend to increase the PLE's performance but also decrease the clusters homogeneity and vice versa, an optimal way of forming the clusters has to be chosen. This optimum might change for various sets of data, which leads to several possible approaches to assign every single vehicle to a cluster that might be optimal. Table 1 describes three possibilities in detail. The proposed algorithm's suitability may depend on the distribution of a, the total number of vehicles and the number of observed failures.

Method 1 guarantees every cluster to have almost the same number of. The number of clusters can be raised until one of them has only a minimum of failures to achieve a well working PLE. This way

Table 1. Overview of possible approaches to cluster the vehicles regarding the mileage accumulation rate *a*.

Method	Description/steps
1) Quantiles Q_p over all vehicles	• Sort all vehicles by their mileage accumulation rate • Calculate p^* for the desired number of groups G by: $p^* = 100/G'$ • Assign every vehicle to one of the G quantiles Q_{p^*}
2) Intervals of a with a const. width	• Define a plausible range for a from a_{min} to a_{max} • Calculate an interval width w^* for the desired number of clusters G by: $w^* = (a_{max} - a_{min})/G'$ • Assign vehicle i regarding their value a_i to the interval in which a_i lies
3) Quantiles $Q_{p^*,\delta}$ over failed vehicles	• Sort failed vehicles by their mileage accumulation rate • Calculate p^* for the desired number of groups G by: $p^* = 100/G'$ • Assign every failed vehicle to the G quantiles $Q_{p^*,\delta}$ • Calculate a value $a_{p,}\delta$ which separates two groups by: $a_{p,}\delta = a_{jF} - (a_{jF} - a_{j-1,\,L})/2$, where $a_{j,F}$ is the a of the first vehicle in quantile j of the failed vehicles and $a_{j-1,\,L}$ is the a of the last vehicle in quantile $j-1$ of the failed vehicles • Assign every non-failed vehicle i to the group so that: $a_{j-1,}\delta \le a_i \le a_{j,}\delta$

a maximal number of clusters can be used and a useful estimation of the failure behavior of each cluster is guaranteed. A disadvantage should be mentioned. This method leads to a different variation of the mileage accumulation rate in every cluster, due to a usually lognormal distributed alpha. Clusters around the median of alpha are the most homogeneous while especially the last group with the highest values of α has also the highest variation. That is caused by the lognormal distribution which is skewed to the right.

Method 2 leads to clusters with a similar homogeneity but the constant width forms clusters with a high number of vehicles around the median and less crowded clusters for very high or low values of α. In order to still reach a desired minimal number of failures in each cluster, the width has to be increased which leads to fewer clusters and therefore the overall homogeneity is not necessarily better, compared to method 1. By using method 3 all the clusters are formed in a way to have the same amount of failures. By using the minimum in every cluster, the number of clusters is maximized. Again the disadvantage is that the clusters' widths regarding alpha might differ.

In the following, method 1 was used, forming quantiles regarding *a,* for the whole fleet of vehicles. The decision to cluster the data by method 1 was made because it was the target to use the non-parametric estimates in further practical applications directly, which is only possible if a PLE for every group can be calculated.

In the end the real data was divided into 25 clusters following method 1, which corresponds to $Q_{0.04}$, i.e. 4% quantiles. In addition a synthetic dataset was generated and analyzed using only 5 groups, i.e. $Q_{0.20}$, to use it in this publication. The main reason for an additional synthetic data set was to illustrate some systematic effects which can be observed for univariate analyses given an influence by a driving profile. In both cases, the data results from a production timespan of one calendar year and was observed at the end of that year, leading to a maximum time in service of one year. The majority of the fleet was less than a year in service at the day of the analysis, therefore this is meant to be an example of an early field data analysis with rather high failure probabilities.

5 BIVARIATE AND UNIVARIATE ANALYSES IN COMPARISON

Before the influence of the mileage accumulation rate on the failure behavior is described, some further steps are explained, which were done after calculating a PLE. These steps are necessary to perform failure predictions and the following procedure has proven itself in practice. In Figure 2 the univariate PLE is drawn in a Weibull Probability Plot (WPP) as small circles. The exact values had to be censored for this paper. Please note the logarithmic scaling of the WPP where $\ln(t)$ is used on the abscissa and $\ln(-\ln(1 - F(t)))$ is used on the ordinate. In addition to the PLE itself, a 90% confidence interval is given as dashed line and towards the last values of the estimator, a Weibull extrapolation was added. It is a common method in automotive practice, to use a combination of the PLE or any other non-parametric estimator and a fitted Weibull distribution for extrapolation. The extrapolation was achieved by manually selecting values of the PLE and fitting a Weibull distribution for these values by using a Maximum Likelihood Estimate (MLE). One reason why a manual selection of values is purposeful is that often the shape

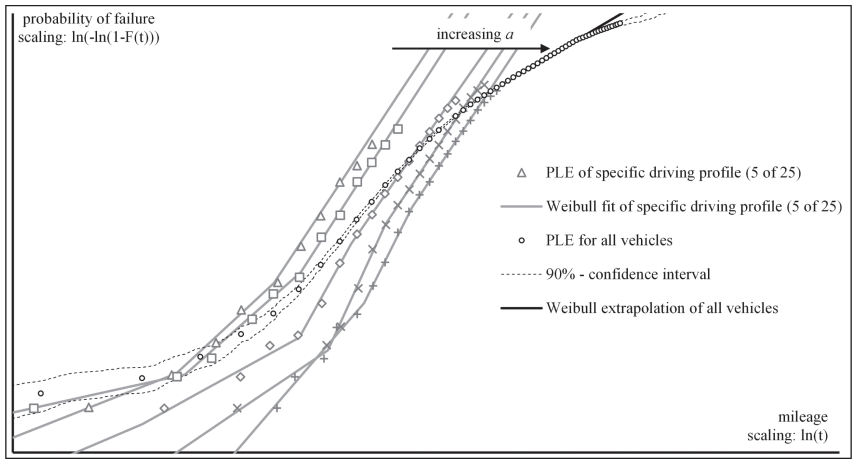


Figure 2. Selected PLE and corresponding mixed Weibull distributions of real data-analysis, plotted in censored WPP.

of the Weibull distribution is changing over mileage or time in service and therefore a fit, using the complete PLE is inaccurate. This makes it convenient to use the PLE itself for all kinds of failure prediction until the last value of the PLE and use for predictions beyond the observable mileage a Weibull extrapolation. This is done under the assumption that the failure behavior is following the slope of the last observations. A Weibull distribution is a straight line, plotted in the WPP, so those values at the end of the PLE are used, which seem to follow the shape of a straight line. In comparison to the univariate PLE, 5 out of the 25 PLE are plotted.

For each of these PLE, a Weibull interpolation was fitted due to lager intervals of the PLE step function in comparison to the univariate PLE. The reason for that is obvious because by splitting the data into 25 disjoint clusters, fewer failures are taken into account for each PLE, leading to lager intervals. Also the last fitted Weibull distribution per cluster was used to extrapolate the failure behavior for further failure predictions. As can be seen in Figure 2, up to three different shape parameters for Weibull distributions are used for the inter- and extrapolation of each PLE, so the changing failure behavior can be taken into account for prediction purposes.

It can be observed that the PLE is consistently moving from the left of the diagram to the right with an increase of the mileage accumulation rate. Please note that the observation was the same for all of the 25 clusters. Some of the PLE intersect at lower mileage where the PLE is less robust. However there was no intersection observed at higher mileage. The shift to the right implies that each driven kilometer of a vehicle tends to be all the more stressful to the analyzed component, the lower the mileage accumulation rate is. Another interesting observation is that the shift seems to be parallel and therefore the mileage accumulation rate apparently does not influence the shape of the failure behavior itself but is an indicator for the intensity of the stress.

The most important fact is revealed by the comparison to the univariate PLE. It does not show a constant shape in terms of a Weibull distribution towards higher mileage, whereas each profile cluster tends to do so. The shape parameter seems to decrease with increasing mileage which leads to an intersection with all the clustered PLE. The explanation is a change in the data structure over mileage and the influence of a on the failure behavior. At low mileage the univariate PLE is taking data of every driving profile according to its weight within the fleet into account. This changes with increasing mileage because at some point those profiles with a low mileage accumulation rate reach their maximum mileage, given the time in service that they had to accumulate mileage. In Figure 2 it can be seen that the mileage of the last observation of each clustered PLE increases with the mileage accumulation rate. This is a case of systematical censoring of high risk vehicles in terms of mileage. The univariate PLE consequently decreases to a failure probability which corresponds to the remaining structure of the data. As mentioned, the PLE is an estimator which considers censoring but assumes random censoring whereas the data is subject to the effect of a specific censoring, due to the influence of the failure behavior. If the data was randomly censored regarding mileage or

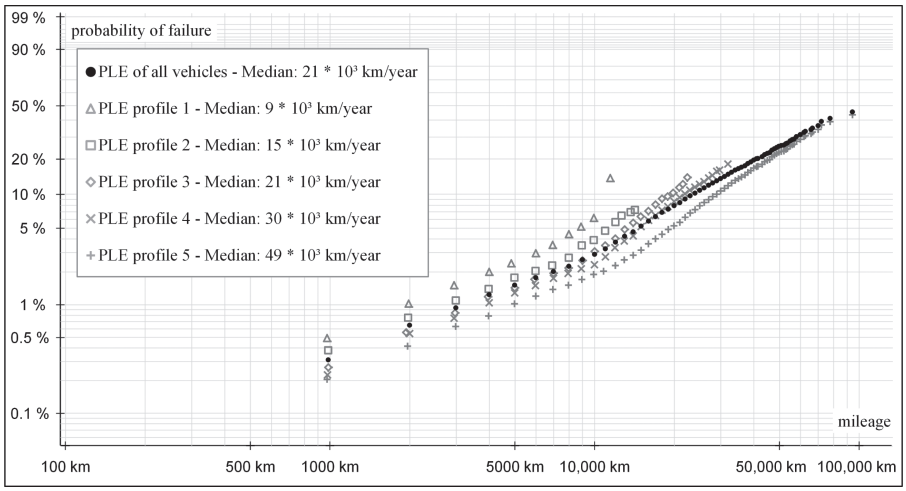


Figure 3. PLE of synthetic data plotted in WPP.

if there was no influence given by a, the standard approach by Kaplan and Meier would estimate the failure probability correctly.

To underline this statement, the assumed influence of the mileage accumulation rate, i.e. a parallel shift to the right for higher values of a, was simulated into the synthetic data set. This data was afterwards analyzed, following the same approach as on the real dataset. Out of simplicity the number of separated clusters was reduced to 5. Figure 3 shows the 5 clustered PLE in comparison to one univariate PLE. The comparison shows quite similar results to the real data set therefore only a few additional remarks are made. The univariate PLE appears to give back an average of the failure probability of the 5 clusters whereas the clusters indicate the underlying variation within the fleet. This average decreases from the point on, when profiles, which tend to have higher failure probabilities, are censored and this censoring is not considered. Hence the failure probability of the univariate PLE does not increase at the same rate anymore and adjusts to the failure behavior of the remaining vehicles. The result is a lower value for beta in comparison to the clustered PLE which all show a similar slope in comparison to each other. This is even more apparent in the synthetic data set but the underlying effect can be assumed to be the same as within the real data.

6 PERFORMANCE COMPARISON TO A UNIVARIATE METHOD

When it comes to measuring the performance of a reliability model, there is no standard approach to be used. One way to handle it is to compare competing models in practical applications, for which the models are going to be used for. This is a very pragmatic method to measure the models performance, but it makes it even more relevant for a reliability expert's daily tasks. The fundamental goal is to find the model which describes the process that leads to a failure as accurately as possible. The model which does it the best should consequently be the model that leads to the better failure prediction. This was done on the real data set by a prediction of the three month timespan following the first year which was analyzed. Only data available at the beginning of these 3 months was used. To illustrate the models' performances, an individual hazard for this prediction interval was estimated for every vehicle that had not failed so far using both models. Afterwards the accumulation of these hazards was compared to the sum of actual observed failures at the end of the three months. The cumulative hazard is a predictor of the total number of failures to expect. Hence if the model's prediction is close to every vehicle's actual hazard, the total number of failures within a fleet should be similar to the fleet's cumulative hazard. Figure 4 shows the results of this comparison. Again it was necessary to partially censor the results. The graphs were generated by sorting the vehicles according to their individual estimated hazard over the prediction interval. The estimation resulting from the bivariate approach is clearly closer to the number of failures in the field while the standard approach underestimates the number of failures by 25%. This can in fact be explained by the continuous decrease of the slope of the univariate PLE towards the last observations. Especially vehicles with a low mileage accumulation are

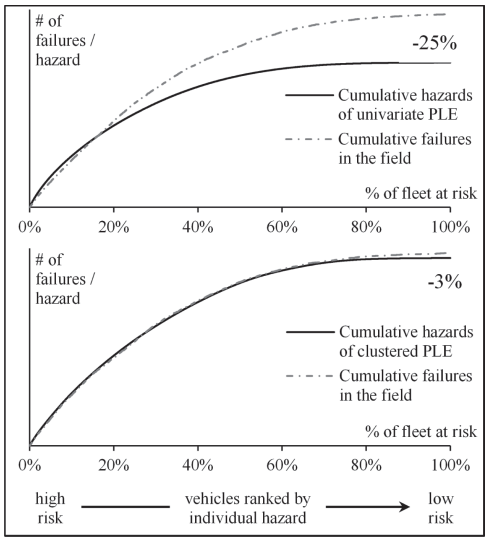


Figure 4. Short term prediction performance on real data.

subject to a systematic underestimation which even starts to increase when these vehicles are no longer part of the PLE due to their censoring. Before the censoring begins, the underestimation is mostly compensated by an overestimation of vehicles with higher mileage accumulation. That is the reason why the univariate PLE's prediction for the total number of failures is still close to number of failures occurred in the field for about the first 20% of the fleet and is below afterwards.

Table 2 shows the results based only on the synthetic data. Only the total number of expected failures and the total number of observed failures are given. In addition to the three month prediction interval, a prediction for two full years of service was added. First of all, the results show that the degree of underestimation increases with the degree of extrapolation. This is an intuitive result that can be inferred from the WPP in Figure 3, where even the vehicles of profile five are exposed to underestimation from some point on, due to the extrapolation of the univariate PLE with a lower slope.

A second performance comparison deals with the situation that an OEM wants to start a campaign in form of a customer satisfaction and cost efficiency by avoiding failures which would otherwise have occurred within the next three months. In case of the univariate, as well as the clustered PLE, the vehicles were selected according to their individual hazard to fail in those three months.

Both models succeed in sorting high-risk vehicles to the top of the selection, as can be seen in the decreasing rate of avoided failures in the field with

Table 2. Failure prediction results on synthetic data.

	3 month period		2 years of service	
Prediction model	# of failures	Deviation in %	# of failures	Deviation in %
Field (simulated)	950	–	34,560	–
Estimation by univariate PLE	828	–12.8	22,984	–33.5
Estimation by clustered PLE	965	+1.6	34,991	+1.2

Table 3. Results of theoretical recalls on synthetic data.

	Univariate PLE	Clustered PLE
# of vehicles for the recall	# of avoided failures	# of avoided failures
5000	176 (3.52%)	186 (3.72%)
10,000	290 (2.90%)	294 (2.94%)
25,000	541 (2.16%)	542 (2.17%)
50,000	776 (1.55%)	797 (1.59%)

an increase of the recall size. The absolute success rate in this performance measurement mostly depends on the timespan that is considered and on the failure probability itself and is thereby no suitable indicator of how well a model works. The reason for both models being similar successful is that the univariate PLE is still able to rank the vehicles well regarding their risk. This is because the effect of the mileage accumulation rate does not outweigh the fact that vehicles with a high a simply drive more total mileage in these three months. The results would be different analyzing a stronger effect by a covariate. Further it can be assumed that the difference between a vehicle's true hazard and the hazard estimated by the univariate PLE is higher in comparison to the clustered PLE. In case of preventive maintenance programs this would be a crucial factor for the program's effectiveness.

7 CONCLUSIONS

This paper highlights several aspects about the connection between the usage of a vehicle, i.e. its driving profile and its reliability. The analyses are limited to automotive data and several specific circumstances of the data were considered which may not be transferred to other industries completely. Nonetheless it can be assumed that with

some adjustments the presented method will lead to similar results in other industries as well. For the case of automotive data it was illustrated that the mileage accumulation rate can have a significant impact on a vehicle's reliability. Also it was shown that this impact leads to related problems if a given influence of driving profiles is ignored. One of the most relevant consequences is a false failure prediction caused by a misleading extrapolation. The data shows a systematic underestimation in case of an increase in the failure probability for decreasing mileage accumulation. Naturally a decreasing failure probability for a decreasing mileage accumulation rate would analogical lead to an overestimation. By using the approach described in this paper which takes the driving profile into account, it was shown that the quality of failure predictions is increased substantially. Further the reliability expert is given a more detailed image of the failure behavior. Consequently this approach can be a valuable input for hypothesis generation to understand the physical process in detail which leads to the failure. In order to measure a general potential of including additional data into the analysis, one assumption was made which does not hold in most of the cases in reliability practice. The analyses were done with data where all necessary information about failed vehicles, as well as not failed vehicles, was available. In practice this data mostly has to be additionally estimated before going into the actual reliability analysis. However the approach can be extended to meet the requirements of this kind of incomplete data by estimating missing information under consideration of the formed clusters. Also the given method allows for several extensions to increase its performance and allow for its applicability with fewer observed failures compared to this example. The authors see great potential in a combination of this approach and the use of parametric models. This way the advantage of analyzing with as less as necessary pre-assumptions can be combined with a parametric model derived from the non-parametric analysis. Parametric models are easier to handle in most applications like failure predictions and also allow for optimization methods like maximum likelihood. Another important improvement would be the possibility to take several covariates into account. In section 3 several approaches were mentioned which already offer this possibility. However some of these methods might demand for some adjustments and extensions to handle the specific structure of automotive data as described by Lawless et al. (1992). This initial approach motivates further research by the illustrated potential and highlighted the importance of extending reliability models, so that all available information is taken into account.

REFERENCES

Bendell, A., Walley, M., Wightman, D.W., & Wood, L.M., 1986. Proportional hazards modelling in reliability analysis-An application to brake discs on high speed trains. *Quality and reliability engineering international*, 2(1), 45–52.

Bendell, A., Wightman, D.W., & Walker, E.V., 1991. Applying proportional hazards modelling in reliability. *Reliability Engineering & System Safety*, 34(1), 35–53.

Cox, D.R., 1972. Regression models and life tables. JR stat soc B, 34(2), 187–220.

Duchesne, T., 1999. Multiple time scales in survival analysis. University of Waterloo.

Escobar, L.A., & Meeker, W.Q., 2006. A review of accelerated test models. *Statistical Science*, 21(4), 552–577.

Hong, Y., & Meeker, W.Q., 2010. Field-failure and warranty prediction based on auxiliary use-rate information. *Technometrics*, 52(2), 148–159.

Hong, Y., & Meeker, W.Q., 2013. Field-failure predictions based on failure-time data with dynamic covariate information. *Technometrics,* 55(2), 135–149.

Jardine, A.K.S., Ralston, P., Reid, N., & Stafford, J., 1989. Proportional hazards analysis of diesel engine failure data. *Quality and Reliability Engineering International*, 5(3), 207–216.

Kaplan, E.L., & Meier, P., 1958. Nonparametric estimation from incomplete observations. *Journal of the American Statistical Association*, 53(282), 457–481.

Kordonsky, K.B., & Gertsbakh, I., 1997. Multiple time scales and the lifetime coefficient of variation: engineering applications. *Lifetime Data Analysis*, 3(2), 139–156.

Krivtsov, V., & Frankstein, M., 2006. Automotive component reliability: should it be measured in time or mileage?. In Reliability and Maintainability Symposium, RAMS'06. Annual, pp. 601–603, IEEE.

Kumar, D., Klefsjö, B., & Kumar, U., 1992. Reliability analysis of power transmission cables of electric mine loaders using the proportional hazards model. *Reliability Engineering & System Safety*, 37(3), 217–222.

Lawless, J.F., Kalbfleisch, J.D., & Blumenthal, S., 1992. Some issues in the collection and analysis of field reliability data. In Survival analysis: State of the art, pp. 141–152. Springer Netherlands.

Lawless, J., Hu, J., & Cao, J., 1995. Methods for the estimation of failure distributions and rates from automobile warranty data. *Lifetime Data Analysis*, 1(3), 227–240.

Lawless, J.F., Crowder, M.J., & Lee, K.A., 2009. Analysis of reliability and warranty claims in products with age and usage scales. *Technometrics*, 51(1), 14–24.

Meeker, W.Q., Escobar, L.A., & Lu, C.J., 1998. Accelerated degradation tests: modeling and analysis. *Technometrics,* 40(2), 89–99.

Nelson, W., 2001. Prediction of field reliability of units, each under differing dynamic stresses, from accelerated test data. In Handbook of statistics, Vol 20. N. Balakrishnan and C.R. Rao, eds. Elsevier

Oakes, D., 1995. Multiple scales in survival analysis. *Lifetime Data Analysis*, 1(1), 7–18.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Attempt to apply the theory of reliability to assessment of signalised lane operation

K. Ostrowski
Cracow University of Technology, Poland

ABSTRACT: The paper offers an analysis of the reliability of traffic conditions measures renewable in time at an actual signalised intersection located in Krakow. The left turn lane selected for the empirical studies is notoriously congested during morning and afternoon peaks. The author designed density and reliability functions for a selected measure of traffic conditions, i.e. the proper operation of the lane between 2400 hours until the occurrence of the state of failure. The results of the analyses may be used to complement traffic signals design methodology in congestion conditions, and in modern traffic information systems.

1 INTRODUCTION

City streets and intersections have limited capacity. Capacity is not a constant but a variable whose value varies in line with deterministic factors (lane and roadway width, slope, structure of traffic by vehicle type, speed limits) and random factors (human behaviour, weather conditions). Often in the densely built-up areas of the city it is impossible to increase street or intersection capacity by changing the number of lanes or their width. Growing car ownership means that many of the streets and intersections in the cities are congested. At the same time the development of road infrastructure cannot not keep pace with the growth in car ownership and therefore traffic management methods and tools preventing congestion or minimising its effects are being looked for. In this regard, what is important is the way in which traffic information is communicated to drivers. Currently information conveyance levels are inadequate, with information often quickly becoming outdated as the situation on the road changes instantaneously, depending as it does on the number of vehicles entering the intersection or on weather conditions. In cities, traffic information is communicated mainly through the media, including the radio or websites, such as www.targeo.pl. Out of town, some roads have systems with variable displays informing about trip time needed to pass through sensitive road sections [Saleh 2009]. At present, the information is fed based on historical data for several days or months, or derived from GPS, in which case it is updated, e.g. every two minutes. These systems however often provide information which is too general, and not infrequently unreliable. There is a lack of methods that would enable the provision of real-time traffic information, along with meaningful interpretation of service levels from the viewpoint of drivers and road managers alike [Ostrowski 2010]. There is also a lack of reliable methods to predict short-term traffic condition such as 15 or 30 minutes in advance.

Often commuters encounter intersections which operate near capacity limits and do not know when they will experience unacceptable traffic conditions. There are days where they drive through such intersections without major disruption and days on which they do not accept adverse traffic conditions, which can be expressed by means of a variety of measures including delays, queues, stops etc. [Chodur 2004]. For each driver the ability to estimate the likelihood of favourable traffic conditions at the time of departure and select the best route is extremely important in terms of minimizing trip time. The aim of this paper is to show the application of elements of reliability theory to the description of the functioning of a lane with a left turn at a signalised intersection in Krakow over several successive working days in favourable weather conditions. The analysis will cover 24-hour periods and record moments in time in which there were adverse traffic conditions from the viewpoint of drivers. Lane's functioning is associated with the level and quality of service and is renewable in time. The concept of renewal in this case is directly related to theoretical renewal, when a renewed object reveals the same reliability as directly before the overload.

2 REVIEW OF PERTINENT LITERATURE

The concept of an object's reliability relates to objects which are either renewable or non-renewable in time [Słowiński 1999]. An object's reliability

means the probability that the object will be usable (efficient) during a given period (t_i, t_{i+1}). In reality, we encounter object with finite durability (e.g. light bulb, battery) or objects whose correct operation in time entails periodic renewals, i.e. repair (e.g. car, washing machine) until they reach durability and disrepair. Figure 1 presents sample of simple theoretical renewal process [Słowiński 1999].

The specificity of the operation of such objects as an intersection in conditions of congestion differs considerably from the operation of e.g. steel or reinforced concrete structures in terms of the effects of overload because once a queue of vehicles has dissipated, the intersection resumes normal operation in conditions of lesser traffic.

The concept of an object's renewal may refer to either theoretical renewal, in which case the object enjoys the same reliability as it did prior to the failure or to practical renewal when the object can resume operation after a prior loss of its operability [Migdalski 1982].

With respect to signalised intersections and the quality of service the picture is similar [Faragó 2006]. The proper operation of traffic signals usually occurs during periods when demand flows are below capacity ($Q < C$). These periods typically are between-peak spans of time or traffic peaks at under-loaded intersections. Research into the reliability of technical objects which are non-renewable in time has been conducted for many years, and its results are used in the planning of repairs, replacement of worn parts in order to reduce machine downtime and ensure continuity of production as well as to ensure the safety of operation and supply [Kołowrocki 2013]. Noteworthy are both theoretical works [Nowakowski 2009] which seek to use new theoretical methods e.g. in processes such as maintenance of technical [Jodejko-Pietruczuk 2014] and transport systems [Kowalski 2011] as well as works of a practical nature in many areas of science and operation [Babiarz 2006 and 2014]. Recently researchers have undertaken work on the reliability of complex technical objects [Cambridge Systematics 2005], such as intersection or road sections mainly to analyse travel time on road sections [Brilon 2007, Park 2007, Lam 2008, Adachi 2009, Mehran 2011, Taylor 2013] and in network of streets with signalised intersections [Lo 2006, Lam 2010]. A small number of publications relates to the analysis of functional reliability of renewable traffic conditions at entries to intersections in various traffic [Chen 2008] and weather conditions [Lam 2008, Ostrowski 2010, Tracz 2012]. Studies generally are limited to the analysis of headways between vehicles [Hung 2003, Chodur 2011, Kumar 2014] and capacity and measures of traffic conditions [Akçelik 1999, Gartner 2004, Chodur 2006 and 2011, Teply 2008, HCM 2010]. This article complements knowledge in the research field relating to the use of signalised intersections. Knowledge of the operational reliability of intersections and road sections can be used to keep drivers informed about the state of congestion and travel time (ITS equipment, variable message signs [Saleh 2009, Konior 2012]).

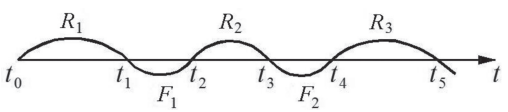


Figure 1. Renewal process (R_i—time periods of proper lane functioning, F_i—failure periods).

3 DESCRIPTION OF THE RESEARCH SITE

The study was conducted on a specially selected congested intersection in Krakow, on a lane carrying left-bound traffic (Fig. 2). The intersection is located along a dual carriageway named Powstańców Wielkopolskich, whisking traffic from the south of Krakow to its north (towards Krakow's Third Ring Road). The left turn under analysis is located on the side leading to the town of Skawina and takes traffic towards the city centre, i.e. towards ul. Limanowskiego. During peak hours the lane sustains long queues of vehicles and drivers wait a long time until exit from the intersection, incurring significant loss of time. During off-peak hours the intersection and the lane function adequately in good traffic conditions. The intersection is controlled by accommodative traffic lights, adapting their parameters to existing traffic needs.

The green signal allocated to the lane is very short relative to the length of the cycle. During the

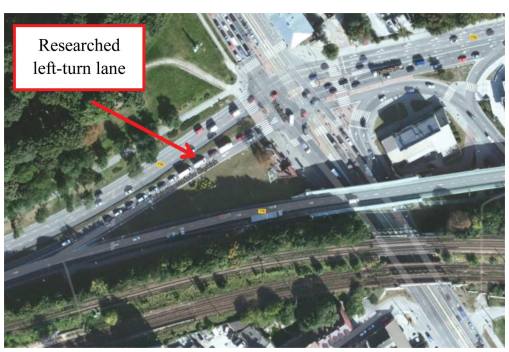


Figure 2. Location of the research site i.e. of a lane with left-bound traffic at the entry to the intersection of Powstańców Śląskich and Wielicka streets [www.google.pl].

green signal lasting an average of 10 s, an average of 130 vehicles exits the intersection in one hour peak traffic. Other vehicles (residual queue) are forced to wait in a queue at a red signal, whose average length is 140 s. According to www.targeo.pl (Fig. 3) the adverse functioning of the lane is well reflected in the colours describing the speed of a moving vehicle at the exit from the intersection.

3.1 *Capacity and traffic conditions at the intersection*

The author has conducted numerous empirical studies into capacity and traffic conditions on the lane, including surveys of drivers' feelings about the quality of the traffic conditions. In analytical methods for signalised intersections [Chodur 2004, Teply 2008, HCM 2010], the assessment of traffic conditions relies on the concept of service levels, which define the best (LOS I) and the worst traffic conditions (LOS IV). These qualitative measures result from analysis of quantitative measures of traffic conditions, i.e. delay. The methods give boundary values of delay for LOS IV, beyond which traffic conditions are considered to be unacceptable. In the Polish method [Chodur 2004] LOS IV is reached once the average delay exceeds to 80 s/P.

Field research into delay and queue (residual and maximum) length variability conducted in major cities shows that drivers are often forced to accept much worse traffic conditions, and consequently become accustomed to inconvenience. Polish studies also corroborate German research [Brilon 2008] in which service level F is divided into four sub-levels that can be used in the design of intersections in states of traffic saturation in major cities. Figure 4 shows the results of a survey of drivers who travel frequently through the given intersection. The results are combined with empirical research into variability of the delay of approaching and queued vehicles until they exit

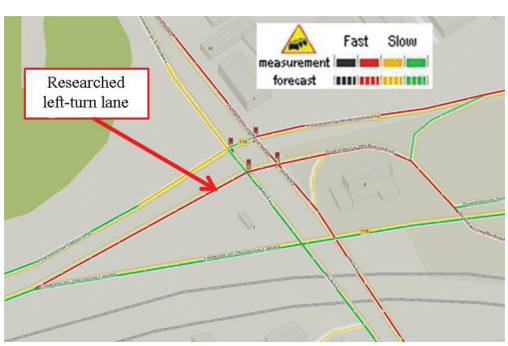


Figure 3. Congestion at the intersection during the morning hours of a working day [www.targeo.pl].

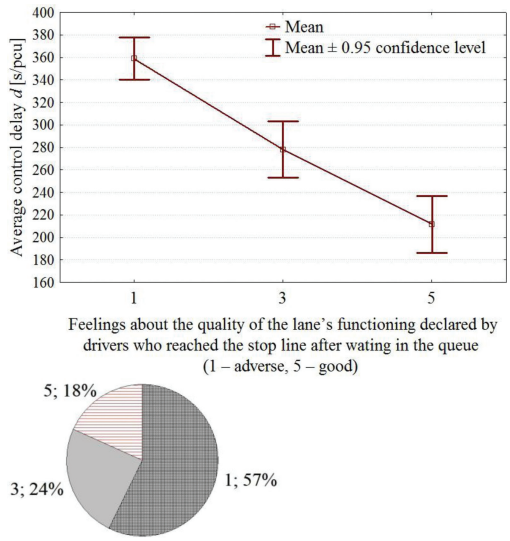


Figure 4. Survey results and average delay on the lane.

the intersection. Analyses conducted on the lane indicate that many drivers (approx. 18%) consider traffic conditions to be adequate when the average delay is approximately 210 seconds. 24% of the respondents deem traffic conditions to be average when the average delay is 280 seconds. The result is surprising if we apply the values obtained to the boundary average delay used in the analytical methods. It should be noted that the result refers to a single lane and may be different for other intersections located in other parts of the city, and for other control parameters.

The above description of the operation of the lane shows the average delay values at which drivers perceive the traffic conditions on the lane to be unreliable. Road managers may have a slightly different perception on the functioning of this lane. At the design stage, it may be difficult, for numerous reasons, to design satisfactory traffic conditions on the lane. The intersection carried and continues to carry a very large volume of traffic, approaching and sometimes exceeding its capacity. Hence, the selection of control parameters at the design stage is extremely difficult, and the accommodative signals used in congestion bring little relief. Hence, the road manager can use three approaches, in which the terms and conditions he considers as unreliable arise when:

Option (1): demand flow exceeds capacity and short residual queue develop, evidencing traffic overload. This option if highly favourable for drivers because the road manager does not accept the formation of queues and drivers experience small delays.

Option (2): average delays exceed the boundary value of 80 [s/pcu] [Chodur 2004] or another higher value—Figure 4. This option is rather unfavorable for vehicle drivers, because the road manager allows some congestion and considerable delays.
Option (3): queue exceeds the critical length in terms of the functioning of the road network and traffic safety. On the entry to intersection the queue must not extend further than the place at which vehicle routes fork into those which go to the overpass and those that lead to the intersection. The option is unfavorable for drivers, as the road manager ignores the significant level of delay.

Based on the above analysis, the paper presents reliability functions for the operation of the lane until two critical states are reached, i.e. when the average delay is 280 seconds and 360 seconds (Fig. 4), and the length of residual queues amounts to 7 and 10 vehicles (option 2).

4 EMPIRICAL RESEARCH AND STATISTICAL ANALYSES

The study into lane reliability consisted in recording the time needed by the residual queue to reach the assumed critical value of 7 and 10 vehicles and persist for at least 2 consecutive signal cycles. After the critical length of residual queues is exceeded, drivers consider traffic conditions, including the length of delay, to be unreliable. Control parameters (duration of the red and green signals) did not change significantly during the morning and afternoon peaks under analysis, and therefore their impact on traffic conditions was negligible. The study at the intersection was conducted over 100 working days in similar weather conditions, for dry surface between 500 to 2000 hours. Weather conditions' adverse effect of on throughput and traffic conditions was shown in a paper titled [Tracz & Ostrowski 2012].

Drawing on the variable values of the proper functioning of lane t_p obtained during the study period i.e. over 100 working days the author built empirical distributions, to which he fitted the following theoretical distributions: normal, log-normal, Gumbel, gamma, and Weibull. In the analysis the author used the Kolmogorov-Smirnov compatibility test ($\alpha = 0.05$), and Chi-square, which revealed two theoretical distributions that best describe the variability of the test measure, i.e. gamma and Weibull distributions (Figs. 5 and 6). These distributions are commonly used in reliability theory analysis [Rao 1992, Gertsbakh 2005].

Below are time periods density functions of the lane's proper operation t_p until the occurrence of a failure (Chapter 4), shown separately for the morning and the afternoon.

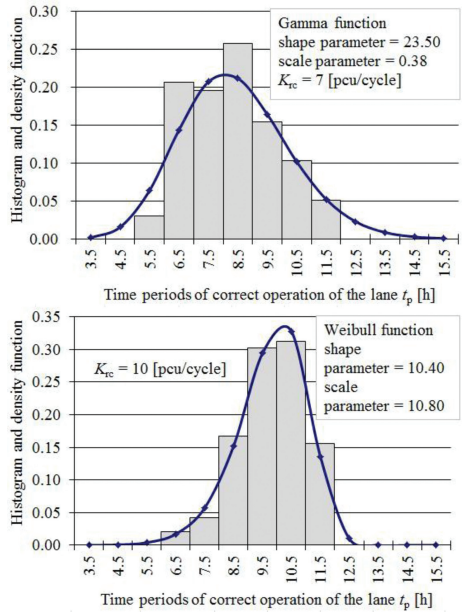


Figure 5. Density functions of the time periods of proper lane functioning until the occurrence of a failure at critical remaining queues of 7 and 10 vehicles in the morning (until 1200 hours; from 2400 to 1200 hours).

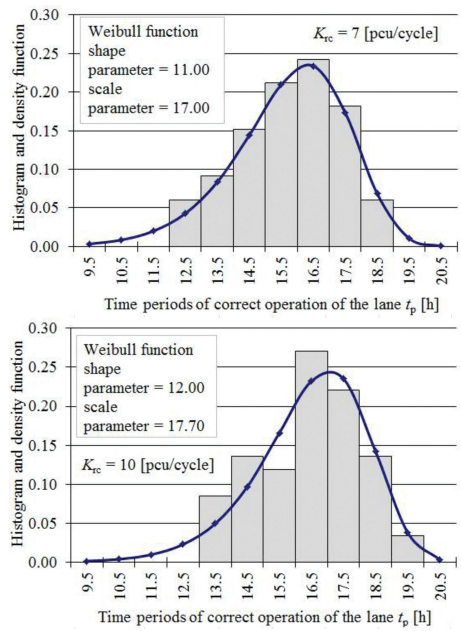


Figure 6. Density functions of the time periods of proper lane functioning until the occurrence of a failure at critical remaining queues of 7 and 10 vehicles in the afternoon (after 1200 hours).

Next, drawing on a set of determined theoretical density functions $f(t_p)$ describing the variability of the traffic conditions measure t_p one can determine reliability functions $R(t_p)$, failure function $F(t_p)$ and the renewal intensity function $\lambda_{int}(t_p)$ for its/the measure's value. In reliability theory, the proper construction and interpretation of the above reliability characteristics requires that the term "failure" be defined in relation to the unit of the analysed measure which is variable in time. In the case of time periods t_p "failure" is the case when time periods t_p of the proper functioning of the lane until occurrence of the critical length of the residual queue K_{rc} are greater then t_{pcr}. If $t_p \leq t_{pcr}$, it can be concluded that service will be reliable.

Pertinent literature [Słowiński 1999, Gertsbakh 2005] offers general formulas and ready-made procedures that can apply to both the assessment of reliability of a non-renewable object, and an object which is renewable in time. The following are reliability characteristics of measure t_p assuming that $t_p > 0$.

$$R(t_p) = P(t_{pcr} \geq t_p), \quad (1)$$

$$F(t_p) = 1 - R(t_p) \quad (2)$$

5 RELIABILITY MODELS OF LANE OPERATION

In reliability analyses of lane group operation it is key to determine boundary traffic conditions at which a transition from reliability to failure occurs. Reliability status covers the period of time in which the intersection operates without problems, i.e. when traffic intensity Q is less than capacity C (usually between peak periods or in night-time conditions). During traffic peak periods entries to intersections can also function reliably when traffic intensity is low and delays are accepted by all drivers. Where traffic intensity Q is close to or exceeds capacity C the conditions at entries to the intersection are characterized by failure and long and unacceptable queues and delays. On the lane in question unreliability occurred both in morning and afternoon peaks (Table 1).

The following graphs show the reliability functions of the proper operation time periods of the lane t_p until the occurrence of critical lengths of residual queues totalling 7 and 10 vehicles. Critical residual queues are associated with critical values of average delay, whose values are shown in Chapter 4.

The analyses show that in the morning drivers who do not accept significant delays and long queues should pass through the intersection as early as possible. The probability that they will then find reliable (acceptable) traffic conditions on the lane is the highest. Comparison of the operation of the lane at a previously assumed reliability level of 0.9 between the two K_{rc} clearly indicates that the boundary value of time t_{pcr} is 5.5 (until 530 hours) for a curve describing failure at $K_{rc} = 7$ [pcu/cycle] and 7.75 (until 745 hours) for $K_{rc} = 10$ [pcu/cycle]. The analysis shows a significant discrepancy in the course of the reliability curves of time periods of correct operation of the lane t_p in the morning between the two cases of K_{rc} under analysis. These differences arise from the variability of demand flow on the lane. In the morning, when most people commute to work, demand flow is less distributed over time compared to the afternoon peak. Figure 5 clearly indicates a greater range of variability at $K_{rc} = 7$ [pcu/cycle] and a shift in modal values.

Krakow's afternoon peak takes much longer than the morning peak, hence the reliability curves run closer to each other (Fig. 8), and the dispersal of results is similar in both cases of Krc. At the assumed reliability level of 0.9, the difference in the boundary value of time t_{pcr} is much smaller than in the morning peak and stands at 0.75 (45 mins). Thus, the probability of encountering worse traffic conditions than those at $K_{rc} = 7$ [pcu/cycle] is much higher. Figure 8 shows that in the afternoon e.g.

Table 1. Number of working days when the lane operated under conditions of failure (out of a total of 100 days).

	When failure is characterised by queue K_{rc}= 7 [pcu/cycle]	When failure is characterised by queue K_{rc}= 10 [pcu/cycle]
Morning peaks	86 days	50 days
Afternoon peaks	79 days	32 days

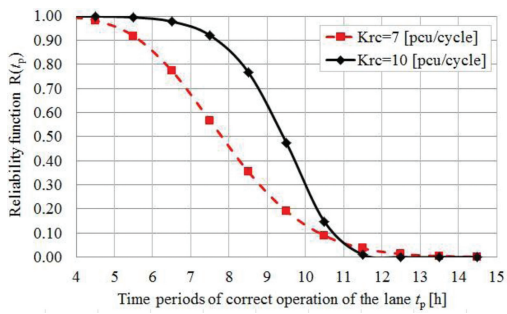


Figure 7. Reliability functions of time periods of correct operation of the lane t_p until occurrence of failure in the morning (until 1200 hours; from 2400 to 1200 hours).

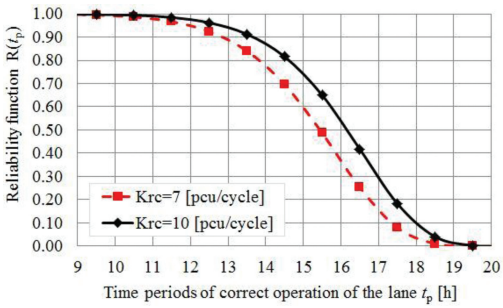


Figure 8. Reliability functions of time periods of correct operation of the lane t_p until occurrence of failure in the afternoon (after 1200 hours).

until 1500 hours drivers enjoy reliable (acceptable) traffic conditions on the lane, and a probability of 60% of drivers in the group accepting queue lengths no longer than K_{rc} = 7 [pcu/cycle] and delays no greater than d = 280 [s/pcu]. For less demanding drivers accepting a longer queue and greater delay (K_{rc} = 10 [pcu/cycle] and d = 360 [s/pcu]) the probability of encountering reliable (acceptable) traffic conditions will stand at 75%.

6 CONCLUSIONS

The analyses performed in the paper lead to the following conclusions:

- Lane operation is renewable in time. It may be assessed by both drivers who mainly consider the quality of traffic conditions and by road managers who are also interested in the impact of adverse traffic conditions on the operation of the adjacent road network;
- The author's surveys of drivers conducted to enquire about the quality of traffic conditions indicate that level IV of service [Chodur 2004] may be further subdivided. Bearing that in mind more extensive research would be needed to determine drivers' acceptance of adverse weather conditions in major cities. In the paper the author uses selected surveys to determine the beginning of two states of failure defined by means of average delay and related lengths of residual queues (K_{rc} = 7 [pcu/cycle] and K_{rc} = 10 [pcu/cycle]);
- The time periods of correct operation of the lane t_p until the occurrence of failure is highly important to drivers and helps them plan their daily commute routes;
- Reliability curves relating to values of time periods of correct operation of the lane t_p help determine the probability of the occurrence of lane service which is reliable (acceptable) to drivers;
- The introduction of several classes of service quality (e.g. by means of K_{rc}) allows describing drivers' expectations of the quality of traffic conditions at the intersection. This approach allows dividing drivers on account of the level of overload acceptance;
- If road managers define and determine service quality classes (e.g. by means of K_{rc}) determining the beginning of the occurrence of failure for lane groups at signalised intersections, this will allow them to control intersections in overload states;
- The introduction of critical lengths of residual queues K_{rc} (service quality classes) allows modelling of congestion duration.

REFERENCES

Adachi, T. & Fujikawa, K. & Asakura, Y. 2009. Empirical Studies on Travel Time Reliability for Expressway with Alternative Routes. *16th ITS World Congress*. Stockholm, Sweden.

Akçelik, R. & Besley M. & Roper, R. 1999. Fundamental Relationships for Traffic Flows at Signalised Intersections. Research Report ARR 340. ARRB Transport Research Ltd, Vermont South, Australia.

Babiarz B. 2014. Heat supply system reliability management. *European Safety and Reliability Conference ESREL*. Wroclaw. Poland.

Babiarz B. 2006: An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping, Volume 83, No 4/2006*: 230–235. Elsevier.

Babiarz B. 2014: (in prep.) Risk assessment in heat supply system. Article accepted for *European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September*. Wroclaw. Poland.

Brilon, W. & Estel, A. 2008. Forschung Straβenbau und Straβenverkehrstechnik. *Helf 999, Ruhr—Universität Bochum*. Germany.

Brilon, W. & Geistefeldt, J. & Zurlinden H. 2007. Implementing the Concept of Reliability for Highway Capacity Analysis. *Transportation Research Record. 2027*:1–8.

Cambridge Systematics, Inc. 2005. Traffic Congestion and Reliability: Trends and Advanced Strategies for Congestion Mitigation, *U.S. Department of Transportation, Federal Highway Administration*, Final report.

Chen, X.M. & Shao, C.F. & Xiong, Z.H. 2008. Reliability of signalized intersection capacity under mixed traffic. China *Journal of Highway and Transport, 21(4)*: 99–104.

Chodur, J. & Ostrowski, K. 2006. Assessment of traffic performance at signalized intersections, *The Archives of Transport, vol. 18: 5–24.* Warsaw. Poland.

Chodur, J. & Ostrowski, K. & Tracz, M. 2011. Impact of saturation flow changes on performance of traffic lanes at signalized intersections. *Proceedings of the 6th International Symposium on Highway Capacity and Quality of Service, Procedia—Social and Behavioral Sciences, Elsevier Vol 16*: 600–611. Stockholm, Sweden.

Chodur, J. & Tracz, M. & Gaca, S. & Gondek, S. & Kieć, M. & Ostrowski, K. 2004. Manual for capacity analyses of at-grade intersections. *General Directorate of National Roads and Motorways*. Warsaw. Poland.

Faragó, A. 2006. Towards the Integration of Reliability and Traffic Engineering. *Communications in Computing*: 28–34.

Gartner, N.H. & Wagner, P. 2004. Analysis of Traffic Flow Characteristics on Signalized Arterials. *Transportation Research Record No. 1883, J. of the Transportation Research Board*: 94–100.

Gertsbakh, I. 2005. Reliability theory with applications to preventive maintenance, *Springer*: New York.

Highway Capacity Manual. 2010. *Transportation Research Board*. Washington D.C. USA.

Hung, W.T. & Tian, F. & Tong, H.Y. 2003. Discharge Headway at Signalized Intersections in Hong Kong. *Journal of Advanced Transportation, Vol. 37*:105–117.

Jodejko-Pietruczuk, A. & Werbińska—Wojciechowska, S. 2014. Block inspection policy for non—series technical objects. *Proc. Of the ESREL 2013 Conference, Amsterdam, Leiden: CRC Press/Balkena*: 889–898.

Kołowrocki K. 2013. On safety of critical infrastructures. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, Vol. 4, No 1*: 51–72.

Konior, W. & Mitas, A.W. 2012. Vehicle in motion parameter measurement pre-selection system. *Polish Academy of Science. Committee of Transport Design*. *The Archives of Transport, Vol. XXIV:* 43–61.

Kowalski, M. & Magott, J. & Nowakowski, T. & Werbińska-Wojciechowska, S. 2011. Analysis of transportation system with the use of Petri nets. *Maintenance and reliability Vol 1*: 49–62.

Kumar, R. & Parida, P. & Saleh, W. 2014. Effect of type of lead vehicle on following headway behaviour in mixed traffic. *World Journal of Science, Technology and Sustainable Development, 11(1)*: 28–43.

Lam, W.H.K. & Chan, K.S. & Li, Z.C. & Bell, M.G.H. 2010. A risk-averse user equilibrium model forroute choice problem in signal-controlled networks. *Journal of Advanced Transportation 44*: 219–230.

Lam, W.H.K. & Shao, H. & Sumalee, A. 2008. Modeling impacts of adverse weather conditions on aroad network with uncertainties in demand and supply. *Transportation Research Part B 42*: 890–910.

Lo, H.K. 2006. A reliability framework for traffic signal control. *Intelligent Transportation Systems, IEEE Transactions on, 7(2):* 250–260.

Mehran, B. & Nakamura, H. 2011. Application of Travel Time Reliability for Performance Oriented Operational Planning of Expressways, *Journal of Japan Society of Civil Engineers, Ser.D3, Vol. 67, No. 3:* 283–299.

Migdalski, J. 1982. Poradnik niezawodności. Podstawy matematyczne. *WEMA*. Warsaw. Poland.

Nowakowski, T. & Werbińska-Wojciechowska, S. 2009. On problems of multicomponent system maintenance modelling, *International Journal of Automation & Computing, Vol 9 No 4*: 364–378.

Ostrowski, K. 2010. Reliability of signalized intersection operation at variable saturation flows (in polish). *Ph. D. Thesis*. *Cracow University of Technology*. Poland.

Park, M. & Kim, S. & Park, C. & Chon, K. 2007. Transportation network design considering travel time reliability. In *Intelligent Transportation Systems Conference, ITSC. IEEE*: 496–502.

Rao, S.S. 1992. Reliability based design. *Purdue University*. USA.

Saleh, W. & Walker, C. & Pai, C. 2009. Variable Message Signs: Are they effective TDM measures?. *Travel Demand Management and Road User Pricing: Success, Failure and Feasibility*: 135–150. Ashgate Publishing.

Słowiński, B. 1999. Podstawy badań i oceny niezawodności obiektów technicznych. *Koszalin*. Poland.

Taylor, M.A.P. 2013. Travel through time: the story of research on travel time reliability. *Transportmetrica B: Transport Dynamics, Vol 1, Issue 3*: 174–194.

Teply, S. 2008. Canadian capacity guide for signalized intersections. *The Institute of Transportation Engineers*. Canada.

Tracz, M. & Ostrowski, K. 2012. Impact of capacity variability in different weather conditions on reliability of signalised intersections, *Proceedings of the 5th International Symposium on Transportation Network Reliability*: 901–916, Hong Kong.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability-exploitation analysis of power supply in transport telematics system

A. Rosiński
Warsaw University of Technology, Warsaw, Poland

ABSTRACT: Issues concerning reliability-maintenance of power-supply for transport telematics systems were presented in this paper. Relationships graph was presented, and then Chapman–Kolmogorov system of equations was derived to describe it. Drawing on those equations, relationships for calculating function of probability of system staying in state of full ability S_{PZ}, state of the impendency over safety S_{ZB1} and S_{ZB2} as well as state of unreliability of safety S_B were derived.

1 INTRODUCTION

The term "telematics" comes from the French (fr. *télématique*). In the literature it began to appear at the beginning of the seventies of the twentieth century. It is a combination of two French words: telecommunications (fr. *télécommunications*) and informatics (fr. *informatique*). In the English vocabulary it began to be used only in the late seventies of the twentieth century, however, it was not widely used. It was not until the start of the European Union EU programs for the development of telematics in various fields, caused that the term began to be used more frequently. This period falls in the nineties. Today, the term "telematics" describes a field of science that integrates telecommunications and IT solutions.

The term is used where such a combination may be beneficial compared with dedicated solutions (including synergies achieved). It can highlight several areas in which it operates:

– transport telematics,
– medical telematics,
– environment telematics,
– telematics urban,
– financial telematics,
– library telematics,
– operational telematics,
– industries telematics,
– home telematics,
– post telematics.

Among these areas of telematics applications, one of the largest and fastest-growing (both in Poland and in Europe and in the world) is the transport. Issues relating to transport telematics appeared in Polish publications in the mid-nineties of 20th century. Transport telematics was consequently defined as a field of knowledge and technical activity integrating IT with telecommunications, in applications addressed to transport systems' needs [Kasprzyk 2012, Laskowski & Łubkowki 2013, Siergiejczyk & Paś & Rosiński 2012, Sumila 2012].

Transport telematics systems work in different exploitation conditions [Duer & Zajkowski & Duer & Paś 2012, Dyduch & Paś & Rosiński 2011, Paś & Duer 2012]. As the elements of critical infrastructure they should maintain their suitability [Bajda & Wrażeń & Laskowski 2011]. One of the main problems is to ensure the continuity of supply of transport telematics systems So far it has been provided the reliability analysis of the system structures [Rosinski & Dabrowski 2013, Siergiejczyk & Rosinski 2011, Siergiejczyk & Rosinski 2011], however, it is also important to analyze the power supply relations in the system. Therefore, such an important role play the analyze of this issue.

The reliability theory in respect of general considerations has had sound footing for many years [Będkowski & Dąbrowski 2006, Epstein & Weissman 2008, Verma & Ajit & Karanki 2010]. The scope of the operation of power systems can provide the following publications [Keyhani & Marwali 2011, Soliman & Mantawy 2012]. Issues related to the reliability in power supply systems are presented in the books [Billinton & Allan 1996, Sozański 1990]. The use of the reserve power sources are presented in publications [Wiatr & Miegoń 2008, Wiatr 2009].

2 ANALYSIS OF POWER SUPPLY MAINTENANCE

In order for transport telematics systems to function properly, they require that each device

constituting the system is powered correctly. Power cut off leads to full or partial system failure. Hence, usually two power supplies are used. First one is the basic supply. If it fails, the reserve power supply starts running to keep the device powered up.

Structural sketch of the power supply system, comprising the two independent energy sources, addressed to transport telematics system is shown in Figure 1.

Figure 2 illustrates relationships within the transport telematics system, based on the exploitation-reliability analysis of dedicated power supply systems.

The state of full ability S_{PZ} is a state in which the properly functioning both power sources (both primary and reserve). State of the impendency over safety S_{ZB1} is a state in which the basic power supply is unsuitable. State of the impendency over safety S_{ZB2} is a state in which the reserve power supply is unsuitable. State of unreliability of safety S_B is a state in which the two power sources are unsuitable.

If the system is in state of full ability S_{PZ} and there occur the damage of the basic power supply that takes the system to the state the impendency over safety S_{ZB1} with intensity λ_{ZB1}. If the system is in the state the impendency over safety S_{ZB1} it is possible to come back to state of full ability S_{PZ} under condit6ion of providing the action to restore the state of full ability of the basic power supply.

When the system is in the state of the impendency over safety S_{ZB1} and additionally there occur damage to the reserve power supply, the system is a transition to state of unreliability of safety S_B with intensity λ_{B1}. Backlinks transition from the state of unreliability of safety S_B to the state of the impendency over safety S_{ZB1} is possible only if there are taken actions of bringing back the state of full ability of the reserve power supply.

If the system is in state of full ability S_{PZ} and there occur the damage of the reserve power supply that takes the system to the state the impendency over safety S_{ZB2} with intensity λ_{ZB2}. If the system is in the state the impendency over safety S_{ZB2} it is possible to come back to state of full ability S_{PZ} under condit6ion of providing the action to restore the state of full ability of the reserve power supply.

When the system is in the state of the impendency over safety S_{ZB2} and additionally there occur damage to the basic power supply, the system is a transition to state of unreliability of safety S_B with intensity λ_{B2}. Backlinks transition from the state of unreliability of safety S_B to the state of the impendency over safety S_{ZB2} is possible only if there are taken actions of bringing back the state of full ability of the basic power supply.

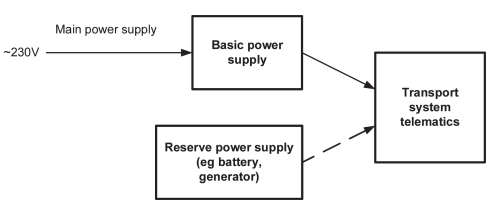


Figure 1. Basic and reserve power supply.

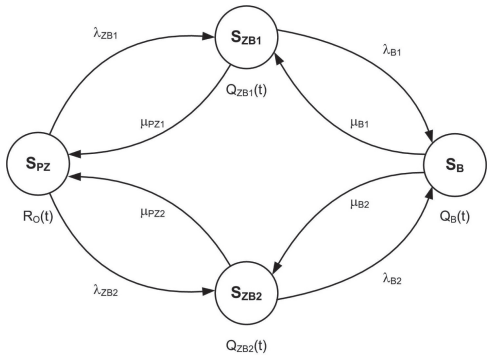


Figure 2. Relationships in the power supply system.
Denotations in figures:
$R_O(t)$—the function of probability of system staying in state of full ability S_{PZ},
$Q_{ZB1}(t)$—the function of probability of system staying in state of the impendency over safety S_{ZB1},
Q_{ZB2}(t)—the function of probability of system staying in state of the impendency over safety S_{ZB2},
$Q_B(t)$—the function of probability of system staying in state of unreliability of safety S_B,
λ_{ZB1}—transition rate from the state of full ability S_{PZ} into the state of the impendency over safety S_{ZB1},
λ_{ZB2}—transition rate from the state of full ability S_{PZ} into the state of the impendency over safety S_{ZB2},
μ_{PZ1}—transition rate from the state of the impendency over safety S_{ZB1} into the state of full ability S_{PZ},
μ_{PZ2}—transition rate from the state of the impendency over safety S_{ZB2} into the state of full ability S_{PZ},
λ_{B1}—transition rate from the state of the impendency over safety S_{ZB1} into the state of unreliability of safety S_B,
λ_{B2}—transition rate from the state of the impendency over safety S_{ZB2} into the state of unreliability of safety S_B,
μ_{B1}—transition rate from the state of unreliability of safety S_B into the state of the impendency over safety S_{ZB1},
μ_{B2}—transition rate from the state of unreliability of safety S_B into the state of the impendency over safety S_{ZB2}.

The system illustrated in Figure 2 may be described by the following Chapman–Kolmogorov equations:

$$\begin{aligned}
R_0'(t) &= -\lambda_{ZB1}\cdot R_0(t) + \mu_{PZ1}\cdot Q_{ZB1}(t) \\
&\quad -\lambda_{ZB2}\cdot R_0(t) + \mu_{PZ2}\cdot Q_{ZB2}(t) \\
Q_{ZB1}'(t) &= \lambda_{ZB1}\cdot R_0(t) - \mu_{PZ1}\cdot Q_{ZB1}(t) \\
&\quad -\lambda_{B1}\cdot Q_{ZB1}(t) + \mu_{B1}\cdot Q_B(t) \\
Q_{ZB2}'(t) &= \lambda_{ZB2}\cdot R_0(t) - \mu_{PZ2}\cdot Q_{ZB2}(t) \\
&\quad -\lambda_{B2}\cdot Q_{ZB2}(t) + \mu_{B2}\cdot Q_B(t) \\
Q_B'(t) &= \lambda_{B1}\cdot Q_{ZB1}(t) + \lambda_{B2}\cdot Q_{ZB2}(t) \\
&\quad -\mu_{B1}\cdot Q_B(t) - \mu_{B2}\cdot Q_B(t)
\end{aligned} \tag{1}$$

Given the initial conditions:

$$\begin{aligned}
&R_0(0) = 1 \\
&Q_{ZB1}(0) = Q_{ZB2}(0) = Q_B(0) = 0
\end{aligned} \tag{2}$$

Laplace transform yields the following system of linear equations:

$$\begin{aligned}
s\cdot R_0^*(s) - 1 &= -\lambda_{ZB1}\cdot R_0^*(s) + \mu_{PZ1}\cdot Q_{ZB1}^*(s) \\
&\quad -\lambda_{ZB2}\cdot R_0^*(s) + \mu_{PZ2}\cdot Q_{ZB2}^*(s) \\
s\cdot Q_{ZB1}^*(s) &= \lambda_{ZB1}\cdot R_0^*(s) - \mu_{PZ1}\cdot Q_{ZB1}^*(s) \\
&\quad -\lambda_{B1}\cdot Q_{ZB1}^*(s) + \mu_{B1}\cdot Q_B^*(s) \\
s\cdot Q_{ZB2}^*(s) &= \lambda_{ZB2}\cdot R_0^*(s) - \mu_{PZ2}\cdot Q_{ZB2}^*(s) \\
&\quad -\lambda_{B2}\cdot Q_{ZB2}^*(s) + \mu_{B2}\cdot Q_B^*(s) \\
s\cdot Q_B^*(s) &= \lambda_{B1}\cdot Q_{ZB1}^*(s) + \lambda_{B2}\cdot Q_{ZB2}^*(s) \\
&\quad -\mu_{B1}\cdot Q_B^*(s) - \mu_{B2}\cdot Q_B^*(s)
\end{aligned} \tag{3}$$

Probabilities of system staying in a distinguished functional states in symbolic (Laplace) terms have the following form:

$$\begin{aligned}
&R_0^*(s) \\
&= -\frac{\begin{array}{l} b_1\cdot b_2\cdot s + b_1\cdot b_2\cdot \mu_{B1} + b_1\cdot b_2\cdot \mu_{B2} \\ -b_2\cdot \lambda_{B1}\cdot \mu_{B1} - b_1\cdot \lambda_{B2}\cdot \mu_{B2} \end{array}}{\begin{array}{l} a\cdot b_2\cdot \lambda_{B1}\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B2} \\ -a\cdot b_1\cdot b_2\cdot s + a\cdot b_1\cdot \lambda_{B2}\cdot \mu_{B2} + b_2\cdot s\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot s\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B1}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B2}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} - \lambda_{B1}\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ +\lambda_{B1}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ2} + \lambda_{B2}\cdot \mu_{B1}\cdot \mu_{PZ1}\cdot \lambda_{ZB2} \\ -\lambda_{B2}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \end{array}}
\end{aligned}$$

$$\begin{aligned}
&Q_{ZB1}^*(s) \\
&= -\frac{\begin{array}{l} b_2\cdot s\cdot \lambda_{ZB1} + b_2\cdot \mu_{B1}\cdot \lambda_{ZB1} + b_2\cdot \mu_{B2}\cdot \lambda_{ZB1} \\ +\lambda_{B2}\cdot \mu_{B1}\cdot \lambda_{ZB2} - \lambda_{B2}\cdot \mu_{B2}\cdot \lambda_{ZB1} \end{array}}{\begin{array}{l} a\cdot b_2\cdot \lambda_{B1}\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B2} \\ -a\cdot b_1\cdot b_2\cdot s + a\cdot b_1\cdot \lambda_{B2}\cdot \mu_{B2} + b_2\cdot s\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot s\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B1}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B2}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} - \lambda_{B1}\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ +\lambda_{B1}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ2} + \lambda_{B2}\cdot \mu_{B1}\cdot \mu_{PZ1}\cdot \lambda_{ZB2} \\ -\lambda_{B2}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \end{array}}
\end{aligned}$$

$$\begin{aligned}
&Q_{ZB2}^*(s) \\
&= -\frac{\begin{array}{l} b_1\cdot s\cdot \lambda_{ZB2} + b_1\cdot \mu_{B1}\cdot \lambda_{ZB2} + b_1\cdot \mu_{B2}\cdot \lambda_{ZB2} \\ +\lambda_{B1}\cdot \mu_{B2}\cdot \lambda_{ZB1} - \lambda_{B1}\cdot \mu_{B1}\cdot \lambda_{ZB2} \end{array}}{\begin{array}{l} a\cdot b_2\cdot \lambda_{B1}\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B2} \\ -a\cdot b_1\cdot b_2\cdot s + a\cdot b_1\cdot \lambda_{B2}\cdot \mu_{B2} + b_2\cdot s\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot s\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B1}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B2}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} - \lambda_{B1}\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ +\lambda_{B1}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ2} + \lambda_{B2}\cdot \mu_{B1}\cdot \mu_{PZ1}\cdot \lambda_{ZB2} \\ -\lambda_{B2}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \end{array}}
\end{aligned}$$

$$\begin{aligned}
&Q_B^*(s) \\
&= -\frac{b_2\cdot \lambda_{B1}\cdot \lambda_{ZB1} + b_1\cdot \lambda_{B2}\cdot \lambda_{ZB2}}{\begin{array}{l} a\cdot b_2\cdot \lambda_{B1}\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B1} - a\cdot b_1\cdot b_2\cdot \mu_{B2} \\ -a\cdot b_1\cdot b_2\cdot s + a\cdot b_1\cdot \lambda_{B2}\cdot \mu_{B2} + b_2\cdot s\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot s\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B1}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} + b_2\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \\ +b_1\cdot \mu_{B2}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} - \lambda_{B1}\cdot \mu_{B1}\cdot \lambda_{ZB2}\cdot \mu_{PZ2} \\ +\lambda_{B1}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ2} + \lambda_{B2}\cdot \mu_{B1}\cdot \mu_{PZ1}\cdot \lambda_{ZB2} \\ -\lambda_{B2}\cdot \mu_{B2}\cdot \lambda_{ZB1}\cdot \mu_{PZ1} \end{array}}
\end{aligned} \tag{4}$$

where:

$$\begin{aligned}
a &= s + \lambda_{ZB1} + \lambda_{ZB2} \\
b_1 &= s + \mu_{PZ1} + \lambda_{B1} \\
b_2 &= s + \mu_{PZ2} + \lambda_{B2}
\end{aligned}$$

Solution to the above set of equations in the time domain is the next step in the analysis and is not discussed here.

3 MODELLING OF PROCESS OF POWER SUPPLY MAINTENANCE

Computer simulation and computer-aided analysis facilitate to relatively quickly determine the influence of change in reliability-exploitation parameters of individual components on reliability of the entire system. Of course, the reliability structure of both the entire system and its components has to be known beforehand.

Using computer aided allows to perform the calculation of the value of probability of system staying in state of full operational capability R_O. That procedure is illustrated with below example.

Example

The following quantities were defined for the system:

– test duration—1 year (values of this parameter is given in [h]):

$$t = 8760 \ \left[\mathrm{h}\right]$$

– reliability of basic power supply:

$$R_{ZB1}(t) = 0{,}949$$

– reliability of reserve power supply:

$$R_{ZB2}(t) = 0{,}991$$

– transition rate from the state of the impendency over safety S_{ZB1} into the state of unreliability of safety S_B (failure of reserve power supply):

$$\lambda_{B1} = 0{,}000001$$

– transition rate from the state of the impendency over safety S_{ZB2} into the state of unreliability of safety S_B (failure of basic power supply):

$$\lambda_{B2} = 0{,}000006$$

– transition rate from the state of unreliability of safety S_B into the state of the impendency over safety S_{ZB1}:

$$\mu_{B1} = 0{,}1$$

– transition rate from the state of unreliability of safety S_B into the state of the impendency over safety S_{ZB2}:

$$\mu_{B2} = 0{,}1$$

Knowing the value of reliability $R_{ZB1}(t)$, transition rate from the state of full ability into the state of the impendency over safety S_{ZB1} may be estimated. Provided the up time is described by exponential distribution, the following relationship can be used:

$$R_{ZB1}(t) = e^{-\lambda_{ZB1} t} \text{ for } t \geq 0$$

thus

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t}$$

For $t = 8760 \ \left[\mathrm{h}\right]$ and $R_{ZB1}(t) = 0{,}949$ we obtain:

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t} = -\frac{\ln 0{,}949}{8760} = 0{,}000006\left[\frac{1}{\mathrm{h}}\right]$$

Knowing the value of reliability $R_{ZB2}(t)$, transition rate from the state of full ability into the state of the impendency over safety S_{ZB2} may be estimated. Provided the up time is described by exponential distribution, the following relationship can be used:

$$R_{ZB2}(t) = e^{-\lambda_{ZB2} t} \text{ for } t \geq 0$$

thus

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t}$$

For $t = 8760 \ \left[\mathrm{h}\right]$ and $R_{ZB2}(t) = 0{,}991$ we obtain:

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t} = -\frac{\ln 0{,}991}{8760} = 0{,}000001\left[\frac{1}{\mathrm{h}}\right]$$

For the above input values according to equation (4) is obtained:

$$R_0^*(s) = \frac{\begin{aligned} &3{,}50003 \cdot 10^{11} \cdot s + 3 \cdot 10^{11} \cdot \mu_{PZ1} \\ &+ 5 \cdot 10^{10} \cdot \mu_{PZ2} + 5 \cdot 10^{17} \cdot s^2 \cdot \mu_{PZ1} \\ &+ 5 \cdot 10^{17} \cdot s^2 \cdot \mu_{PZ2} + 1{,}000035 \cdot 10^{17} \cdot s^2 \\ &+ 5 \cdot 10^{17} \cdot s^3 + 1{,}00003 \cdot 10^{17} \cdot s \cdot \mu_{PZ1} \\ &+ 1{,}000005 \cdot 10^{17} \cdot s \cdot \mu_{PZ2} \\ &+ 1 \cdot 10^{17} \cdot \mu_{PZ1} \cdot \mu_{PZ2} \\ &+ 5 \cdot 10^{17} \cdot s \cdot \mu_{PZ1} \cdot \mu_{PZ2} \end{aligned}}{\begin{aligned} &2{,}450021 \cdot 10^6 \cdot s + 1{,}000035 \cdot 10^{17} \cdot s^2 \cdot \mu_{PZ1} \\ &+ 1{,}000035 \cdot 10^{17} \cdot s^2 \cdot \mu_{PZ2} + 5 \cdot 10^{17} \cdot s^3 \cdot \mu_{PZ1} \\ &+ 5 \cdot 10^{17} \cdot s^3 \cdot \mu_{PZ2} + 1{,}0500275 \cdot 10^{12} \cdot s^2 \\ &+ 1{,}00007 \cdot 10^{17} \cdot s^3 + 5 \cdot 10^{17} \cdot s^4 \\ &+ 4{,}00003 \cdot 10^{11} \cdot s \cdot \mu_{PZ1} \\ &+ 6{,}50003 \cdot 10^{11} \cdot s \cdot \mu_{PZ2} \\ &+ 1 \cdot 10^{17} \cdot s \cdot \mu_{PZ1} \cdot \mu_{PZ2} \\ &+ 5 \cdot 10^{17} \cdot s^2 \cdot \mu_{PZ1} \cdot \mu_{PZ2} \end{aligned}}$$

Assuming $\mu_{PZ1} = 0{,}1$, $\mu_{PZ2} = 0{,}2$ and using the Laplace'a transformation we receive:

$$R_0(t) = 0{,}0000024805093 \cdot e^{-0{,}199229397513 \cdot t} + 0{,}0000599964 \cdot e^{-0{,}100006 \cdot t} + 0{,}0000025192406 \cdot e^{-0{,}200778602 \cdot t} + 0{,}99993500384977$$

Finally, we obtain:

$$R_O = 0{,}999935004$$

Using equation (4) it is possible to determine the effect of the impact of values of the transition rate from the state of the impendency over safety to the state of full ability μ_{PZ1} and μ_{PZ2} on the value of the probability of the system staying in the state of full operational capability R_O. Intensity μ_{PZ1} and μ_{PZ2} should be understood as the inverse of time t_{PZ1} and t_{PZ2} that determine the recovery time to the state of full operational capability.

4 SUMMARY

The article presents a schematic exploitation-reliability analysis of two source supply system used in transport telematics systems. There are given basic types of power supply systems and then presented the exploitation-reliability analysis of the whole system. It was assumed the four functional states (state of full ability S_{PZ}, states of the impendency over safety S_{ZB1} and $S_{ZB2,}$ state of unreliability of safety S_B) and defined basic transitions between them. This allowed for the determination of the set of equations describing the power supply system. The obtained relations allow to determine the influence of particular intensities rates on values of assigned probabilities. Further research is expected to carry out analysis aimed the rationalization of the intensity of restoring the states of full abilities of the respective tracks of power supply.

REFERENCES

Bajda A., Wrażeń M. Laskowski D., 2011. Diagnostics the quality of data transfer in the management of crisis situation. *Electrical Review*, 87(9A): 72–78.

Będkowski L., Dąbrowski T., 2006. *Basics of maintenance, vol. II Basic of operational reliability*. Warsaw: Military Academy of Technology.

Billinton R., Allan R.N., 1996. *Reliability evaluation of power systems*. New York: Plenum Press.

Duer S., Zajkowski K., Duer R., Paś J., 2012. Designing of an effective structure of system for the maintenance of a technical object with the using information from an artificial neural network. *Neural Computing & Applications* DOI: 10.1007/s00521-012-1016-0.

Dyduch J., Paś J., Rosiński A., 2011. *Basics of maintaining electronic transport systems.* Radom: Publishing House of Radom University of Technology, 2011.

Epstein B., Weissman I., 2008. *Mathematical models for systems reliability*. CRC Press/Taylor & Francis Group.

Kasprzyk Z., 2012. Delivering payment services through manual toll collection system. In J. Mikulski (eds) *Telematics in the transport environment*: 60–68, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Keyhani A., Marwali M., 2011. *Smart power grids*. Springer-Verlag.

Laskowski D., Łubkowki P., 2013. The end-to-end rate adaptation application for real-time video monitoring. In *Advances in Intelligent Systems and Computing*: 295–305. Springer International Publishing AG.

Paś J., Duer S., 2012. Determination of the impact indicators of electromagnetic interferences on computer information systems. *Neural Computing & Applications*. DOI:10.1007/s00521-012-1165-1.

Rosinski A., Dabrowski T., 2013. Modelling reliability of uninterruptible power supply units. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* Vol.15, No. 4, 2013: 409–413.

Siergiejczyk M., Paś J., Rosiński A., 2012. Application of closed circuit television for highway telematics. In J. Mikulski (eds) *Telematics in the transport environment*: 159–165, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M., Rosinski A., 2011. Reliability analysis of electronic protection systems using optical links. In W. Zamojski & J. Kacprzyk & J. Mazurkiewicz & J. Sugier & T. Walkowiak (eds) *Dependable Computer Systems*: 193–203, given as the monographic publishing series—"Advances in intelligent and soft computing", Vol. 97. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M., Rosinski A., 2011. Reliability analysis of power supply systems for devices used in transport telematic systems. In J. Mikulski (eds) *Modern Transport Telematics*: 314–319, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 239. Berlin Heidelberg: Springer-Verlag.

Soliman S. A., Mantawy A. H., 2012. *Modern optimization techniques with applications in electric power systems*. Springer Science+Business Media.

Sozański J., 1990. *Reliability and operating quality of electric power system*. Warsaw: WNT.

Sumila M., 2012. Selected aspects of message transmission management in its systems. In J. Mikulski (eds) *Telematics in the transport environment*: 141–147, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Verma A.K., Ajit S., Karanki D.R., 2010. *Reliability and safety engineering*. London: Springer.

Wiatr J., Miegoń M., 2008. *UPS power supplies and accumulator batteries in emergency power systems*. Warsaw: MEDIUM Publishing House.

Wiatr J., 2009. *Generating sets in building emergency power systems*. Warsaw: MEDIUM Publishing House.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability-maintenance analysis of highway emergency communication systems

M. Siergiejczyk, J. Chmiel & A. Rosiński
Warsaw University of Technology, Warsaw, Poland

ABSTRACT: Transport telematics is defined as a field of knowledge and technical activity integrating IT with telecommunications, intended to support transport systems. The assistance comes in form of integrated sensor, telecommunications, IT and information systems complemented by telematics-enabled apps (services). An example of a telematic system is the highway emergency response system. Reliability-maintenance analysis of highway emergency communication systems was presented in this paper. The influence of time required for the system to regain its state of full ability on system's availability rate was at the centre of this analysis. In real terms, it will make possible to rationalise the process of periodic inspections.

1 INTRODUCTION

Transport telematics is defined as a field of knowledge and technical activity integrating IT with telecommunications, intended to support transport systems (Siergiejczyk 2009, Wydro 2005). The assistance comes in form of integrated sensor, telecommunications (Bajda & Wrażeń & Laskowski 2011, Laskowski & Łubkowki 2013) IT and information systems complemented by telematics-enabled apps (services) (Chowdhury & Sadek 2003, Klein 2001).

As of late, highway telematic systems have been subject of multiple papers (Kasprzyk 2012, Siergiejczyk & Paś & Rosiński 2012, Sumila 2012). There are multiple reasons behind that. It has been widely acknowledged that development of road transport, especially Polish highway network is a top priority. Traffic density on trunk roads has reached volumes so high that without high efforts aimed at building and expanding the highway network, the country could potentially face a much higher congestion. No wonder then, highway transport issues should be close to hearts of researchers.

Thus far the authors have analysed their structures in terms of reliability analysis covering both intra-system relationships as well as power supply related issues (Rosinski & Dabrowski 2013, Siergiejczyk & Rosinski 2011) and information transmission (Siergiejczyk & Rosinski 2011, Siergiejczyk 2012, Siergiejczyk 2008).

Highway emergency response system enables users to report from their current position any breakdowns, collisions etc. to the highway control centre managing that road section. The roads where the system was deployed are significantly safer.

2 HIGHWAY EMERGENCY RESPONSE SYSTEM ARCHITECTURE

The key component of a highway emergency response system is alarm indicator column. It enables either unidirectional or bidirectional communication between the person calling for help and the control centre. Unidirectional communication entails sending a request (by pressing the call help button on alarm indicator column) for help to the control centre. Bidirectional communication is possible when (also by pressing the same call help button on the column) request for help is sent to the control centre followed by voice conversation between the centre and stranded person. By pressing the call help button, the user is automatically sending identification data of the alarm indicator column it used to the control centre. Hence exact location of the accident scene or emergency and consequently the person calling for help is immediately known. Rational measures can be therefore undertaken by road rescue and/or technical services.

Figure 1 shows schematically the general architecture of emergency response network. The information is transmitted between control centre and alarm indicator columns via fibre optic cable. The rationale for using that technology is its resilience to environmental electromagnetic interference (Duer & Zajkowski & Duer & Paś 2012, Paś & Duer 2012) and high data transfer speeds. The

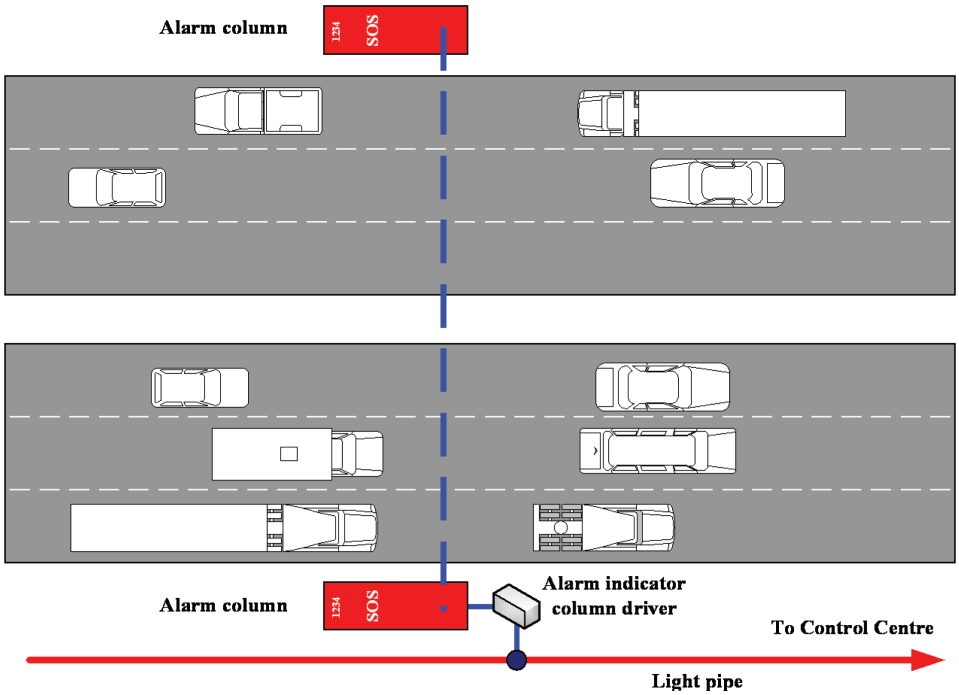


Figure 1. Architecture of emergency response network.

cable runs adjacent to the motorway buried in the ground.

Fibre optics emergency response system consists of the following elements:

- control centre—manages user requests received via alarm indicator columns and informs road rescue and/or technical services about the need to attend to a accident scene or other emergency.
- optoelectronic interface—Central Access Point (CAP) which enables two-way transmission over fibre optic cable.
- network of passive photocouplers—they are connected with optical fibre for purposes of emergency response system. They allow to connect together alarm indicator columns located in particular part of the network using only one fibre.
- optoelectronic interface i.e. Field Optical Box (FOB) assign to each alarm indicator column and to the master column. FOBs and the master column are connected using a short, copper multi-couple cable, thus facilitating maintenance and repairs/replacement (restoring the state of full ability) in case of any damage caused by ongoing traffic.
- alarm indicator columns (master and secondary)—located road-side along the highway thus creating branches leading to the control centre. Master alarm indicator columns consist of electronic setup (audio frequency amplifier, input, acoustical system with microprocessor, modem and interface), microphone, speaker, emergency button.

3 ANALYSIS OF HIGHWAY EMERGENCY COMMUNICATION SYSTEMS MAINTENANCE

In telecommunications network (including emergency response networks) readiness i.e. the network's capability to establish and maintain connection between active users over given time under specific operating conditions, is determined by readiness of its constituting elements and the network's reliability structure (Siergiejczyk 2012, Verma & Ajit & Karanki 2010).

Overview of emergency response network structure is displayed in Figure 2. It includes a control centre, two optical fibre lines and alarm indicator columns.

Relationships between structure elements, from reliability and maintenance perspective (Będkowski & Dąbrowski 2006, Dyduch & Paś & Rosiński 2011), were determined by analysing the highway emergency response system operation and are presented in Figure 3.

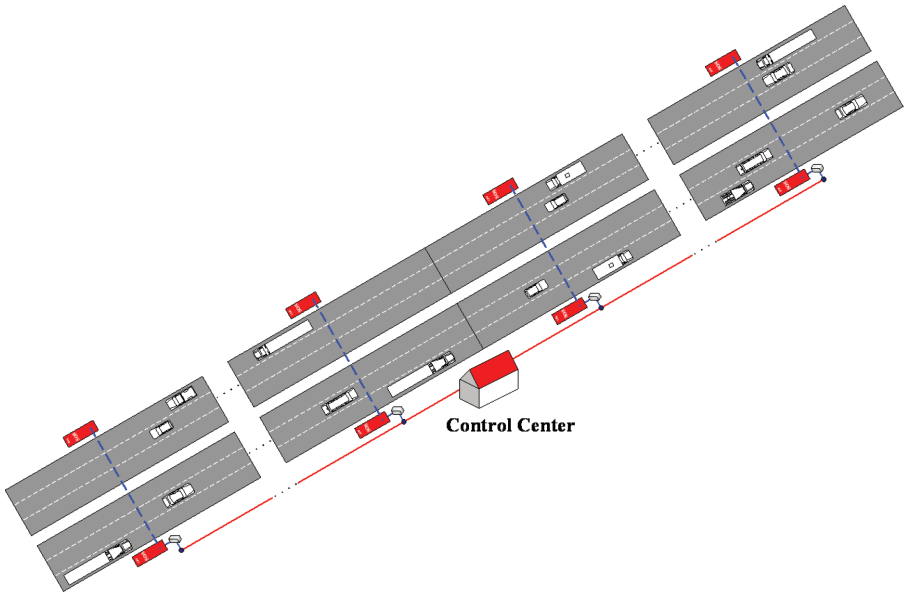


Figure 2. Highway emergency response system.

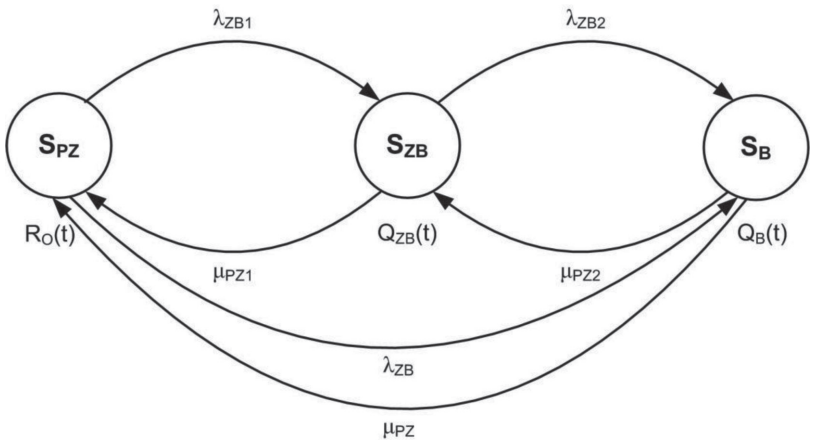


Figure 3. Relationships in the highway emergency communication system.

Denotations in figures:

$R_O(t)$—the function of probability of system staying in state of full ability S_{PZ},
$Q_{ZB}(t)$—the function of probability of system staying in state of the impendency over safety S_{ZB},
$Q_B(t)$—the function of probability of system staying in state of unreliability of safety S_B,
λ_{ZB1}—transition rate from the state of full ability S_{PZ} into the state of the impendency over safety S_{ZB},
μ_{PZ1}—transition rate from the state of the impendency over safety S_{ZB} into the state of full ability S_{PZ},
λ_{ZB2}—transition rate from the state of the impendency over safety S_{ZB} into the state of unreliability of safety S_B,
μ_{ZB1}—transition rate from the state of unreliability of safety S_B into the state of the impendency over safety S_{ZB},
λ_{ZB}—transition rate from the state of the full ability S_{PZ} into the state of unreliability of safety S_B,

μ_{PZ}—transition rate from the state of unreliability of safety S_B into the state of the full ability S_{PZ}.

Should highway emergency response system be in state of full ability S_{PZ} and one optical fibre line fails the system goes into state of the impendency over safety S_{ZB} at a rate λ_{ZB1}. A system in state of the impendency over safety S_{ZB} could go into state of full ability S_{PZ} provided adequate measures to restore the optical fibre line to be fully operational are undertaken.

Should highway emergency response system be in state of the impendency over safety S_{ZB} and second optical fibre line fails the system goes into state of unreliability of safety S_B at a rate λ_{ZB2}. A system in state of unreliability of safety S_B could go into state of the impendency over safety S_{ZB} provided adequate measures to restore the second optical fibre line to be fully operational are undertaken.

Should highway emergency response system be in state of full ability S_{PZ} and the control centre fails the system goes into state of unreliability of safety S_B at a rate λ_{ZB}. A system in state of unreliability of safety S_B could go into state of full ability S_{PZ} provided adequate measures to restore the control centre to be fully operational are undertaken.

The system illustrated in Figure 3 may be described by the following Chapman–Kolmogorov equations:

$$\begin{aligned}
R_0'(t) &= -\lambda_{ZB1}\cdot R_0(t) + \mu_{PZ1}\cdot Q_{ZB}(t)\\
&\quad -\lambda_{ZB}\cdot R_0(t) + \mu_{PZ}\cdot Q_B(t)\\
Q_{ZB}'(t) &= \lambda_{ZB1}\cdot R_0(t) - \mu_{PZ1}\cdot Q_{ZB}(t)\\
&\quad -\lambda_{ZB2}\cdot Q_{ZB}(t) + \mu_{PZ2}\cdot Q_B(t)\\
Q_B'(t) &= \lambda_{ZB2}\cdot Q_{ZB}(t) - \mu_{PZ2}\cdot Q_B(t)\\
&\quad +\lambda_{ZB}\cdot R_0(t) - \mu_{PZ}\cdot Q_B(t)
\end{aligned} \tag{1}$$

Given the initial conditions:

$$\begin{aligned}
R_0(0) &= 1\\
Q_{ZB}(0) &= Q_B(0) = 0
\end{aligned} \tag{2}$$

Laplace transform yields the following system of linear equations:

$$\begin{aligned}
s\cdot R_0^*(s) - 1 &= -\lambda_{ZB1}\cdot R_0^*(s) + \mu_{PZ1}\cdot Q_{ZB}^*(s)\\
&\quad -\lambda_{ZB}\cdot R_0^*(s) + \mu_{PZ}\cdot Q_B^*(s)\\
s\cdot Q_{ZB}^*(s) &= \lambda_{ZB1}\cdot R_0^*(s) - \mu_{PZ1}\cdot Q_{ZB}^*(s)\\
&\quad -\lambda_{ZB2}\cdot Q_{ZB}^*(s) + \mu_{PZ2}\cdot Q_B^*(s)\\
s\cdot Q_B^*(s) &= \lambda_{ZB2}\cdot Q_{ZB}^*(s) - \mu_{PZ2}\cdot Q_B^*(s)\\
&\quad +\lambda_{ZB}\cdot R_0^*(s) - \mu_{PZ}\cdot Q_B^*(s)
\end{aligned} \tag{3}$$

Probability of system staying in specific state denoted symbolically (Laplace) reads as follows:

$$\begin{aligned}
R_0^*(s) &= \frac{\begin{array}{l}s^2 + s\cdot\mu_{PZ} + s\cdot\mu_{PZ1} + s\cdot\lambda_{ZB2} + s\cdot\mu_{PZ2}\\ +\mu_{PZ}\cdot\mu_{PZ1} + \mu_{PZ}\cdot\lambda_{ZB2} + \mu_{PZ1}\cdot\mu_{PZ2}\end{array}}{\begin{array}{l}s^2\cdot\lambda_{ZB} + s^2\cdot\mu_{PZ} + s^2\cdot\lambda_{ZB1} + s^2\cdot\lambda_{PZ1}\\ + s^2\cdot\lambda_{ZB2} + s^2\cdot\mu_{PZ2} + s^3 + s\cdot\lambda_{ZB}\cdot\mu_{PZ1}\\ + s\cdot\mu_{PZ}\cdot\lambda_{ZB1} + s\cdot\mu_{PZ}\cdot\mu_{PZ1} + s\cdot\lambda_{ZB}\\ \cdot\lambda_{ZB2} + s\cdot\lambda_{ZB}\cdot\mu_{PZ2} + s\cdot\mu_{PZ}\cdot\lambda_{ZB2}\\ + s\cdot\lambda_{ZB1}\cdot\lambda_{ZB2} + s\cdot\lambda_{ZB1}\cdot\mu_{PZ2}\\ + s\cdot\mu_{PZ1}\cdot\mu_{PZ2}\end{array}}\\
Q_{ZB}^*(s) &= \frac{\begin{array}{l}s\cdot\lambda_{ZB1} + \mu_{PZ}\cdot\lambda_{ZB1} + \lambda_{ZB}\cdot\mu_{PZ2} + \lambda_{ZB1}\cdot\mu_{PZ2}\end{array}}{\begin{array}{l}s^2\cdot\lambda_{ZB} + s^2\cdot\mu_{PZ} + s^2\cdot\lambda_{ZB1} + s^2\cdot\mu_{PZ1}\\ + s^2\cdot\lambda_{ZB2} + s^2\cdot\mu_{PZ2} + s^3 + s\cdot\lambda_{ZB}\\ \cdot\mu_{PZ1} + s\cdot\mu_{PZ}\cdot\lambda_{ZB1} + s\cdot\mu_{PZ}\cdot\mu_{PZ1}\\ + s\cdot\lambda_{ZB}\cdot\lambda_{ZB2} + s\cdot\lambda_{ZB}\cdot\mu_{PZ2} + s\cdot\mu_{PZ}\\ \cdot\lambda_{ZB2} + s\cdot\lambda_{ZB1}\cdot\lambda_{ZB2} + s\cdot\lambda_{ZB1}\cdot\mu_{PZ2}\\ + s\cdot\mu_{PZ1}\cdot\mu_{PZ2}\end{array}}\\
Q_B^*(s) &= \frac{\begin{array}{l}s\cdot\lambda_{ZB} + \lambda_{ZB}\cdot\mu_{PZ1} + \lambda_{ZB}\cdot\lambda_{ZB2} + \lambda_{ZB1}\cdot\lambda_{ZB2}\end{array}}{\begin{array}{l}s^2\cdot\lambda_{ZB} + s^2\cdot\mu_{PZ} + s^2\cdot\lambda_{ZB1} + s^2\cdot\mu_{PZ1}\\ + s^2\cdot\lambda_{ZB2} + s^2\cdot\mu_{PZ2} + s^3 + s\cdot\lambda_{ZB}\cdot\mu_{PZ1}\\ + s\cdot\mu_{PZ}\cdot\lambda_{ZB1} + s\cdot\mu_{PZ}\cdot\mu_{PZ1} + s\cdot\lambda_{ZB}\\ \cdot\lambda_{ZB2} + s\cdot\lambda_{ZB}\cdot\mu_{PZ2} + s\cdot\mu_{PZ}\cdot\lambda_{ZB2}\\ + s\cdot\lambda_{ZB1}\cdot\lambda_{ZB2} + s\cdot\lambda_{ZB1}\cdot\mu_{PZ2}\\ + s\cdot\mu_{PZ1}\cdot\mu_{PZ2}\end{array}}
\end{aligned} \tag{4}$$

Solving above equations in time domain is a next step of the analysis which has not been included in this paper.

4 MODELLING OF PROCESS OF HIGHWAY EMERGENCY RESPONSE MAINTENANCE

Computer simulation and computer-aided analysis facilitate to relatively quickly determine the influence of change in reliability-exploitation parameters of individual components on reliability of the entire system. Of course, the reliability structure of both the entire system and its components has to be known beforehand.

Using computer aided allows to perform the calculation of the value of probability of system staying in state of full ability R_O. That procedure is illustrated with below example.

Example

The following quantities were defined for the system:

– test duration—1 year (values of this parameter is given in [h]):

$$t = 8760 \ [h]$$

– reliability of first optical fibre line:

$$R_{ZB1}(t) = 0{,}99$$

– reliability of second optical fibre line:

$$R_{ZB2}(t) = 0{,}999$$

– reliability of control centre:

$$R_{ZB}(t) = 0{,}9999$$

– transition rate from the state of the impendency over safety into the state of full ability:

$$\mu_{PZ1} = 0{,}1\left[\frac{1}{h}\right]$$

– transition rate from the state of unreliability of safety into the state of full ability:

$$\mu_{PZ2} = 0{,}1\left[\frac{1}{h}\right]$$

– transition rate from the state of the unreliability of safety into the state of full ability:

$$\mu_{PZ} = 0{,}05\left[\frac{1}{h}\right]$$

Provided the value of reliability $R_{ZB1}(t)$ is known, transition rate from the state of full ability into the state of the impendency over safety may be estimated. Provided the up time is described by exponential distribution, the following relationship can be used:

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t}$$

thus

$$R_{ZB1}(t) = e^{-\lambda_{ZB1}t} \quad \text{for} \quad t \geq 0$$

For $t = 8760 \ [h]$ and $R_{ZB1}(t) = 0{,}99$ we obtain:

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t} = -\frac{\ln 0{,}99}{8760} = 1{,}147298 \cdot 10^{-6}\left[\frac{1}{h}\right]$$

Provided the value of reliability $R_{ZB2}(t)$ is known, transition rate from the state of the impendency over safety into the state of unreliability of safety may be estimated. The following relationships are true for exponential distribution:

$$R_{ZB2}(t) = e^{-\lambda_{ZB2}t} \quad \text{for} \quad t \geq 0$$

thus

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t}$$

For $t = 8760 \ [h]$ and $R_{ZB2}(t) = 0{,}999$ we obtain:

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t} = -\frac{\ln 0{,}999}{8760} = 1{,}142124 \cdot 10^{-7}\left[\frac{1}{h}\right]$$

Provided the value of reliability $R_{ZB}(t)$ is known, transition rate from the state of full ability into the state of unreliability of safety may be estimated. The following relationships are true for exponential distribution:

$$R_{ZB}(t) = e^{-\lambda_{ZB}t} \quad \text{for} \quad t \geq 0$$

thus

$$\lambda_{ZB} = -\frac{\ln R_{ZB}(t)}{t}$$

For $t = 8760[h]$ and $R_{ZB}(t) = 0{,}9999$ we obtain:

$$\lambda_{ZB} = -\frac{\ln R_{ZB}(t)}{t} = -\frac{\ln 0{,}9999}{8760} = 1{,}141609 \cdot 10^{-8}\left[\frac{1}{h}\right]$$

For above input values using equation (4) we get:

$$R_0 = 0{,}9999883749$$
$$Q_{ZB} = 0{,}0000115489$$
$$Q_B = 7{,}6115 \cdot 10^{-8}$$

Practical application of deliberations presented hereinbefore enables to determine the impact of transition rate from the state of the impendency over safety to the state of full ability μ_{PZ1} i, transition rate from the state of unreliability of safety to the state of the impendency over safety μ_{PZ2} and transition rate from the state of unreliability of safety to the state of full ability μ_{PZ} on probability of system staying in the state of full ability. Rates $\mu_{PZ1,}$ μ_{PZ2} and μ_{PZ} should be read as inverse times $t_{PZ1,}$ t_{PZ2} and t_{PZ} which determine the time taken to restore system elements to the state of full ability.

5 SUMMARY

Reliability-maintenance analysis of highway emergency communication systems was presented in

this paper. Assuming three states (state of full ability R_0, state of the impendency over safety Q_{ZB} and state of unreliability of safety Q_B) and transitions, relationships for determining probability of the system staying in particular state were derived. The relationships obtained make possible to ascertain impact of transition rate on the aforementioned probabilities.

In order to determine the availability rate of emergency response network, transition rate between defined system states has to be known. Numerical values of those parameters could be estimated based on reliability prediction methods. This is justified for newly built systems. Operational tests or empirical data from system elements testing can be the other way to obtain those numerical values. This pertains among other to estimating parameters of fibre optic telecommunications networks.

REFERENCES

Bajda A., Wrażeń M. Laskowski D. 2011. Diagnostics the quality of data transfer in the management of crisis situation. *Electrical Review* 87(9 A): 72–78.

Będkowski L., Dąbrowski T. 2006. *Basics of maintenance, vol. II Basic of operational reliability*. Warsaw: Military Academy of Technology.

Chowdhury M.A., Sadek A. 2003. *Fundamentals of Intelligent Transportation Systems Planning*. Boston, London: Artech House ITS Library.

Duer S., Zajkowski K., Duer R., Paś J. 2012. Designing of an effective structure of system for the maintenance of a "technical object with the using information from an artificial neural network. *Neural Computing & Applications* DOI: 10.1007/s00521-012-1016-0.

Dyduch J., Paś J., Rosiński A. 2011. *Basics of maintaining electronic transport systems.* Radom: Publishing House of Radom University of Technology, 2011.

Kasprzyk Z. 2012. Delivering payment services through manual toll collection system. In J. Mikulski (eds) *Telematics in the transport environment*: 60–68, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Klein L.A. 2001. *Sensor Technologies and date requirements if ITS.* Artech House, ITS Library.

Laskowski D., Łubkowki P. 2013. The end-to-end rate adaptation application for real-time video monitoring. In *Advances in Intelligent Systems and Computing*: 295–305. Springer International Publishing AG.

Paś J., Duer S. 2012. Determination of the impact indicators of electromagnetic interferences on computer information systems. *Neural Computing & Applications*. DOI:10.1007/s00521-012-1165-1.

Rosinski A., Dabrowski T. 2013. Modelling reliability of uninterruptible power supply units. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* Vol. 15, No. 4, 2013: 409–413.

Siergiejczyk M., Paś J., Rosiński A. 2012. Application of closed circuit television for highway telematics. In J. Mikulski (eds) *Telematics in the transport environment*: 159–165, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M., Rosinski A. 2011. Reliability analysis of electronic protection systems using optical links. In W. Zamojski & J. Kacprzyk & J. Mazurkiewicz & J. Sugier & T. Walkowiak (eds) *Dependable Computer Systems*: 193–203, given as the monographic publishing series—"Advances in intelligent and soft computing", Vol. 97. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M., Rosinski A. 2011. Reliability analysis of power supply systems for devices used in transport telematic systems. In J. Mikulski (eds) *Modern Transport Telematics*: 314–319, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 239. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M. 2012. Assessing Transport Telematic Systems in Terms of Data Services Quality. In J. Mikulski (eds) *Telematics in the transport environment*: 356–363, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Siergiejczyk M. 2008. Maintaining readiness of telecommunications network using a management system. In Proc. XXXVI Winter School of Reliability. Radom: Publishing House of the Institute of Maintenance Technology.

Siergiejczyk M. 2009. *Maintenance Effectiveness of Transport Telematics Systems*. Warsaw: Scientific Works of the Warsaw University of Technology.

Sumila M. 2012. Selected aspects of message transmission management in its systems. In J. Mikulski (eds) *Telematics in the transport environment*: 141–147, given as the monographic publishing series—"Communications in Computer and Information Science", Vol. 329. Berlin Heidelberg: Springer-Verlag.

Verma A.K., Ajit S., Karanki D.R. 2010. *Reliability and safety engineering*. London: Springer.

Wydro K. 2005. Telematics—significance and definition of the term. Telecommunication and IT. Warsaw: Publishing House of National Institute of Telecommunications.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Hierarchical random models in road transport safety

J. Wachnicka & K. Jamroz
Gdańsk University of Technology, Gdańsk, Poland

L. Smolarek
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: In this paper multilevel approach to the issue of road safety level on the road network of European regions, classified as NUTS 2 in statistical databases of the EU, has been presented. The risk calculated as the number of death casualties in road accidents per 100,000 inhabitants of a given region has Poisson distribution. Therefore, generalized Poisson model has been assumed in the modelling process. Multilevel stochastic analysis was performed for the studied factor. Then a model was created that took into account the impact of different characteristics available on different level of aggregation, which may be helpful in the actions aimed at improvement of road safety in respective regions.

1 INTRODUCTION

In 1771 the first accident involving motor vehicle, a steam powered one, was reported. Since then several hundred million accidents have occurred, in which over 60 million people have died. Despite the activities being carried out with an aim to improve safety, over 1.2 m people die on roads each year, and even up to 50 million are injured. This is then a global issue of an epidemiologic nature. Scientists in Western Europe and United States for quite a long time have been searching for the cause of this situation. The issue is complex enough to be addressed by scientists from different fields: economy, mathematics, transport or medicine. However, so far they have focused on researches covering data for respective countries, without going deeper into differences between respective regions of a given country. Most frequently analysed were the figures of changes in number of casualties over time, by means of time series (Commandeur et al. 2012). In researches aimed at finding factors that could influence fatality on roads national product per capita (Van Beeck et al. 1991) and transport activity (Jamroz 2011) have been indicated. Unfortunately, transport activity is unavailable in regional databases. Therefore, the scientists often point to population density as a good substitute index, which may replace transport activity (Fridstrøm 1995). Literature studies showed that the researchers focus either on national characteristics or on regional characteristics alone, and do not combine both. In this paper the combination of national and regional characteristics in one model has been presented.

2 MULTILEVEL MODEL— METHODOLOGY OF THE APPROACH

Analyses of road safety at levels below the national level have usually compared selected rates of road safety (such as the road fatality rate in relation to demography). Fatality is calculated as follows:

$$\mathrm{FATALR_{ij}} = \frac{\mathrm{FATAL_{ij}}}{\mathrm{POP_{ij}}} \tag{1}$$

where:
$FATALR_{ij}$—traffic fatality rate in an i-th region in j-th year
$FATAL_{ij}$—number of fatalities of an i-th region in j-th year
POP_{ij}—number of population of an i-th region in j-th

In order to create model that combines national and regional characteristics, data concerning the number of death casualties in a given region have been collected as well as additional characteristics that describe regions and countries. The reason for this approach was the fact that there were characteristics available on national level that could effectively differentiate safety levels in the regions of respective countries, though unfortunately they were unavailable on regional level of aggregation. On the other hand, respective regions of a given country differ among each other in terms of population density or road network concentration and these elements are worth considering in the model. Since significant dispersion of fatality rate has been observed, it was decided to model demographic index of fatalities on roads (FATALR) calculated

as the number of killed per 100,000 inhabitants. The assumption was that the model should have the following formula:

$$FATALR = \alpha \cdot MODEL_{NATIONAL}^{\beta_1} \cdot MODEL_{REGION}^{\beta_2} \cdot NPPCMODEL_{NATIONAL}^{\beta_3} \quad (2)$$

where:
FATALR—demographic rate of fatalities in road accidents in a given region [fat./100 thou. inhab.]
$MODEL_{NATIONAL}$—model for national data
$MODEL_{REGION}$—model for regional data
$NPPC_{NATIONAL}$—model describing changes of average national product per capita
α, β_1,β_2,β_3—estimated parameters

FATALR estimation is based on the assumption that this parameter has Poisson distribution. National model was created on the basis of data from 11 European countries, whereas in the case of regional model in this paper the focus has been on German. Histogram of FATALR value in regions of Germany in the analysed period of 1999–2008 presented on Figure 1 shows that there are no grounds for rejecting the hypothesis of Poisson distribution, frequently assumed in the analyses of safety level (Firth 1995). In further analyses, according to this assumption, FATALR index will be alternatively referred to as λ.

2.1 *National model*

Taking into account the assumptions, λ parameter has been evaluated with 95% probability for the set of data from comparable countries. Then the set of independent variables, available only on national level of aggregation, which characterize the country, used for development of descriptive models for evaluated λ parameters ($MODEL_{NATIONAL}$), has been created. In this paper the impact of such factors were analysed as: corruption index—COR (the higher the value, the better a country is perceived, i.e. as less corrupted), percentage of passenger cars older than 10 years—OLD in the total fleet of the country, calculated as average from 10 years. Model was developed in previous article (Wachnicka & Smolarek 2013) and has a shape of linear model:

$$\lambda = 15.920 - 1.308 \cdot COR + 0.093 \cdot OLD\ ,\ R^2 = 0,87 \quad (3)$$

where:
λ—demographic rate of fatalities in road accidents in a given country [fat./100 thou. inhab.]
COR—country corruption index [–]
OLD—percentage of passenger cars older than 10 years [%]
R^2—coefficient of determination

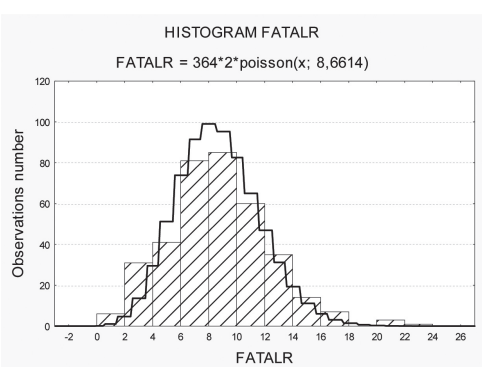


Figure 1. Histograms of analysed FATALR indices in the regions of Germany.

2.2 *Model for trend of national product per capita variation in time*

Global national and local regional models are the ones, in which the majority of independent variables are characterized by slight variability in time. The only variable dynamically changing in time, and at the same time occurring in almost all models, is national product per capita. Analysis of variations of average national product per capita NPPC over time proved that analysed country is characterized by linear type of NPPC change trend in time.

$$NPPC_{NATIONAL} = -1159,17 + 0,59 \cdot year,\ R^2 = 0,98 \quad (4)$$

2.3 *Regional model*

The next step was development of model describing the impact of regional characteristics in Germany on FATALR values in these regions. For this purpose, separated base of regional data was created the attempts were made to develop a model of impact of respective variables on modelled dependent variable. Cluster analysis allowed specification of classes of correlated variables. In individual models the impact of respective classes have been taken into account through selection of their representatives.

$$MODEL_{REGION} = Z \cdot (\ln NPPC)^{-0,54} \cdot \frac{1}{\sqrt{DPOP}} \cdot \exp(-0,369 \cdot MRV),\ R^2 = 0,74 \quad (5)$$

where:
lnNPPC—logarythm of national product per capita in each region [–]

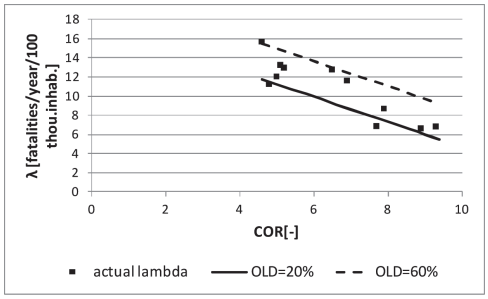


Figure 2. Illustration of linear model that takes into account corruption index and the percentage of cars older than 10 years old in the total fleet.

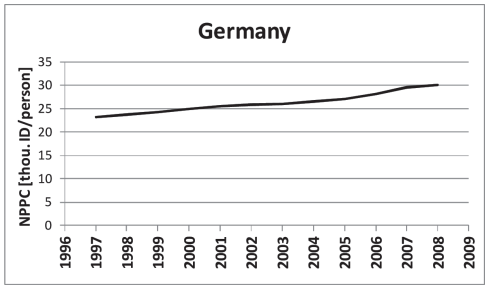


Figure 3. Graph of dependence of NPPC changes in Germany in the analysed years.

lnDPOP—logarythm of population density in each region [–]
MRV—motorisation vehicle rate [vehicle/person]

As shown in Figures 4 and 5, although theoretically quite good fit of the model to real data—$R^2 = 0.74$ much data is above or below the model functions. This may be due, inter alia, that the developed model only depends on three variables: the NPPC, DPOP and MRV.

There are probably characteristics not included in this model, because they are not available in databases. The individual NUTS 2 regions may vary among other such characteristic contacts as part of transit traffic, network routes, the type of land use (more agricultural or more industrial for example) and the age structure of the drivers in the region. Therefore, the model developed is burdened with some kind of uncertainty. That's why it is possible to perform stochastic process on developed function coefficients.

Because the most important factor in the developed model proved to be NPPC, it was decided to just the coefficient of this variable is treated as a random variable.

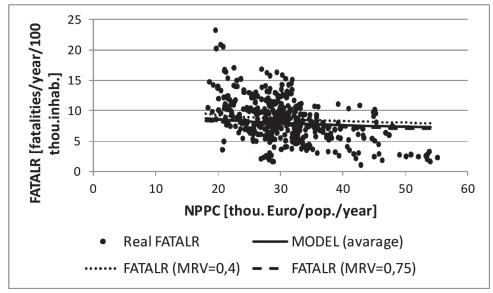


Figure 4. Graph of prepared regional FATALR model in relation to national product per capita and against the actual data—motorisation vehicle rate MRV from the model assumed as minimum, average and maximum value from data set.

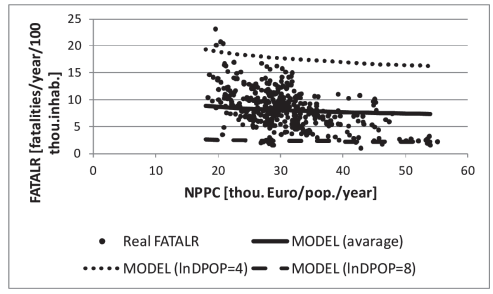


Figure 5. Graph of prepared regional FATALR model in relation to national product per capita and against the actual data—population density DPOP from the model assumed as minimum, average and maximum value from data set.

2.4 *Aggregated model*

After preparation of partial models, the model comprising all partial models has been created and it has the following formula:

$$FATALR = 0{,}7 \cdot MODEL_{NATIONAL}^{2{,}285} \cdot MODEL_{REGION}^{1{,}054} \cdot NPPC_{NATIONAL}^{-1{,}506}, R^2 = 0{,}88 \quad (6)$$

3 RANDOM MODEL

There are several alternative ways of analyzing hierarchical data, traditional statistical techniques is the first one. The problem with traditional statistical techniques is that it discards all within-group information (takes the average of the individual level variables), (Chow 1984).

Another way to analyze hierarchical data would be through a random-coefficients model. This model assumes that each group has a different

regression model with its own coefficients. Because groups are sampled, the model assumes that the regression coefficients are also randomly sampled from a population of group coefficients. The problem with using a random-coefficients model in order to analyze hierarchical data is that is still not possible to incorporate higher order variables, (De Leeuw 1985).

3.1 *Data analysis*

Based on the data shown in Figure 6 the data are divided into homogeneous groups, statistical description of which is given in Table 1. This analysis shows the results of fitting a normal distribution to the data.

The estimated parameters of the fitted distribution are shown above, Table 1.

The Table 2 shows the results of several tests run to determine whether data can be adequately modeled by a normal distribution. The Shapiro-Wilk test is based upon comparing the quantiles of the fitted normal distribution to the quantiles of the data. The standardized skewness test looks for lack of symmetry in the data. The standardized kurtosis test looks for distributional shape which is either flatter or more peaked than the normal distribution. Since the smallest P-value amongst the tests performed for each data seat is greater than or equal to 0,05, we can not reject the idea that it comes from a normal distribution with 95% confidence.

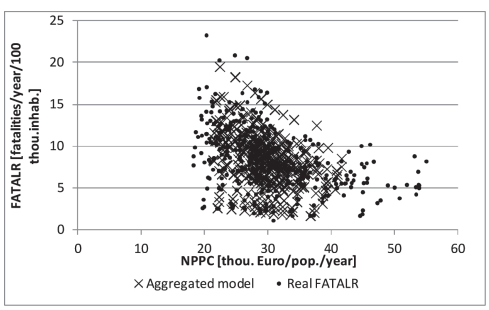


Figure 6. Graph of aggregated FATALR model in relation to national product per capita and against the actual data.

3.2 *The doubly truncated normal probability*

The doubly truncated normal probability density function (pdf) is normally distributed on the interval from a to b; and takes on a value of 0 elsewhere, (Lee 1979). Since a valid pdf must integrate to 1 over its range, the doubly truncated normal pdf must be normalized, Figure 7, and is given by formula

$$\phi_T(t;\mu,\sigma,a,b) \equiv \begin{cases} \dfrac{\phi(t;\mu,\sigma)}{\Phi(b;\mu,\sigma)-\Phi(a;\mu,\sigma)} & a<t<b \\ 0 & elsewhere \end{cases}. \quad (7)$$

A truncated normal pdf is when we have $b=\infty$ or $a=-\infty$. In such cases,

Table 1. Fitted normal distributions parameters to each group.

Data	Mean	Standard deviation
d1520	13,7033	4,49095
d2025	10,6829	3,50678
d2530	8,48976	3,18291
d3035	8,26568	3,00758
d3540	6,59454	2,0081
d4045	5,69156	2,87799
d4550	5,84994	2,78894
d5055	2,37173	0,510187

Table 2. Tests for normality.

	Shapiro-Wilk W		Skewness Z-score		Kurtosis Z-score	
Data	Statistic	P-Value	Statistic	P-Value	Statistic	P-Value
d1520	0,884336	0,1146	1,21344	0,224962	Insufficient data	
d2025	0,95908	0,0801	1,69493	0,09009	1,17488	0,240041
d2530	0,973983	0,1544	0,145033	0,88468	0,121449	0,90333
d3035	0,950495	0,0515	1,3092	0,190466	–1,05747	0,290297
d3540	0,951859	0,1492	0,255812	0,798092	0,714878	0,474682
d4045	0,959896	0,5695	0,401755	0,687861	Insufficient data	
d4550	0,96418	0,8045	0,112227	0,910638	Insufficient data	
d5055	0,969501	0,8773	0,0133125	0,989373	Insufficient data	

$$\phi_T(t;\mu,\sigma,a,\infty)\equiv\begin{cases}\dfrac{\phi(t;\mu,\sigma)}{1-\Phi(a;\mu,\sigma)} & a<t\\ 0 & elsewhere\end{cases}. \quad (8)$$

$$\phi_T(t;\mu,\sigma,-\infty,b)=\begin{cases}\dfrac{\phi(t;\mu,\sigma)}{\Phi(b;\mu,\sigma)} & t<b\\ 0 & elsewhere\end{cases}. \quad (9)$$

The mean of a doubly truncated normal pdf (7) is

$$E(Y;\mu,\sigma,a,b)=\mu+\sigma\lambda$$

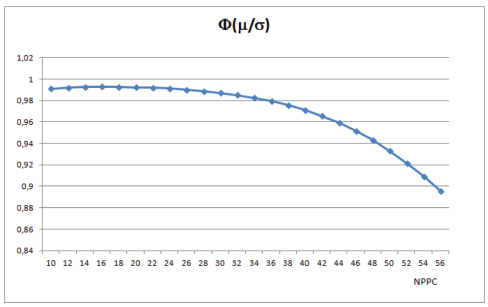


Figure 7. Normalized constant as a function of NPPC.

where $\lambda\equiv\phi_a-\phi_b/\Phi_b-\Phi_a$.

For lower and upper truncation (8,9) this formula becomes

$$\lambda\equiv\frac{\phi_a}{1-\Phi_a},\qquad \lambda\equiv\frac{-\phi_b}{\Phi_b}.$$

Using the model and logarithmic transformation we have linear model according to data transformation.

Let us now consider the regional model where coefficient Z is random variable with a truncated normal distribution with mean μ and standard deviation $\sigma>0$.

Probability density function of random variable Z is given by formula:

$$f(t)=\frac{1}{\sigma\cdot\Phi_{N(0,1)}\left(\dfrac{\mu}{\sigma}\right)\cdot\sqrt{2\pi}}e^{-\frac{(t-\mu)^2}{2\sigma^2}} \quad (10)$$

where

$$\Phi_{N(0,1)}(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{t^2}{2}}dt,$$

we use only FATALR ≥ 0 it means that for $\forall\ t<0$ the probability of FATALR is zero, Figure A, B.

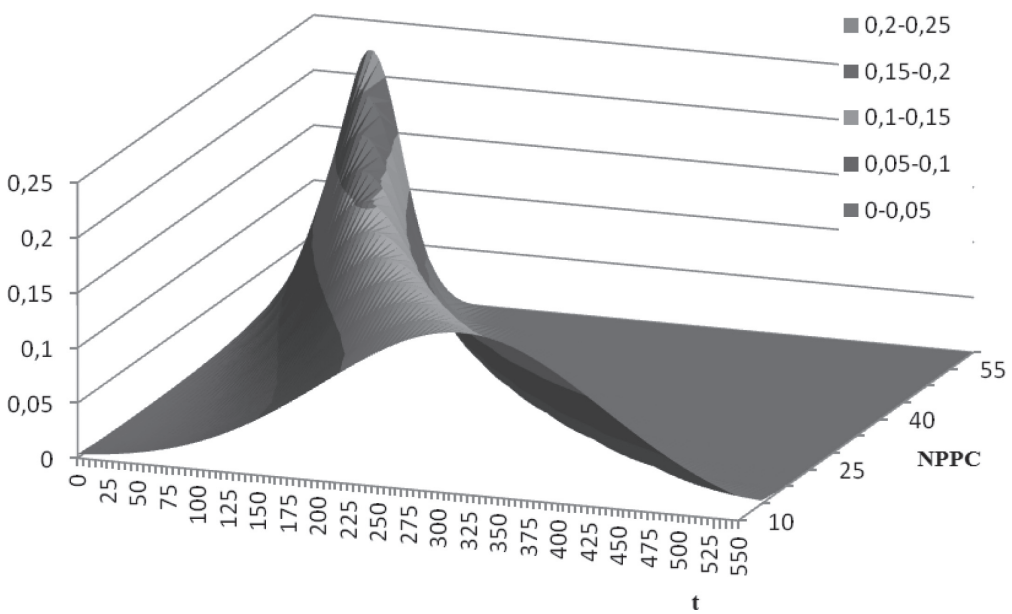


Figure 8. Probability density function (10) of the main model parameter as a function of independent variable NPPC.

The general regression modeling approach takes the standard perspective in much of statistical modeling of focusing directly on the mean responses and how they change over time (Phoebus 1986).

However, the modeling approach acknowledges the separate sources of variation we have discussed earlier.

Such models helps in controlling for unobserved heterogeneity when this heterogeneity is constant over time and correlated with independent variables, (Phoebus 1986, Wooldridge 2013).

4 CONCLUSION

The conducted heuristic statistical analysis, the results of which were presented in previous sections, indicates usefulness of employing local characteristics for evaluation of road transport safety. Due to varying availability of registered data, both at national and regional level, the cluster analysis was necessary in order to single out classes of "correlated" variables of which each one could be used in the model as representative of specified group of effects (impacts). Division into impact groups was conducted both at the level of countries and regions. All variables present in the models are significant. NPPC variable has the biggest impact.

In a multilevel modeling we want to investigate the relations between variables with different domains. The multilevel characteristics of the data also have implications for statistical modeling and analysis. In the paper we analyzed these statistical aspects of the problem. Random coefficient regression models are more appropriate than fixed coefficient models for multilevel analysis in our problem consideration.

There are two common assumptions made about the individual specific effect, the random effects assumption and the fixed effects assumption. The random effects assumption (made in a random effects model) is that the individual specific effects are uncorrelated with the independent variables. The fixed effect assumption is that the individual specific effect is correlated with the independent variables. If the random effects assumption holds, the random effects model is more efficient than the fixed effects model (Phoebus 1986, Wooldridge 2013).

REFERENCES

Chow, G.C., 1984. Random and changing coefficient models. In Z. Griliches & M.D. Intriligator (Eds.), *Handbook of econometrics (Vol. 2)*. Amsterdam, The Netherlands: North Holland Publishing.

Commandeur, J.J.F., et al. 2012. On statistical inference in time series analysis of the evolution of road safety. *Accident; analysis and prevention*, pp. 1–11.

De Leeuw, J., 1985. Path models with random coefficients. Leiden, The Netherlands: Department of Data Theory FSWIRUL.

Firth, D., 1991. Generalized linear models. In: Hinkley V, Reid N, Snell EJ, editors. *Statistical theory and modelling: in honour of Sir David Cox, FRS*. London: Chapman and Hall, p. 66–93.

Fridstrøm, L. et al., 1995. Measuring the contribution of randomness, exposure, weather, and daylight to the variation in road accident counts. *Accident; analysis and prevention*, vol. 27, no. 1, pp. 1–20.

Jamroz, K., 2012. The impact of road network structure and mobility on the national traffic fatality rate. *Energy Efficient Transportation Networks, International Scientific Conference,* Paris.

Lee, L.F., 1979. On the first and second moments of the truncated multi-normal distribution and a simple estimator. *Economics Letters 3*, 165–169.

Phoebus, J., 1986. DHRYMES Chapter 27 Limited Dependend Variables, *Handbook of Econometrics, Volume III, Edited by 2*. Griliches and M.D. Intriligutorc Elsevier Science Publishers BV, Columbia University.

Van Beeck, A.E. et al., 1991. Determinants of Traffic Accident Mortality in the Netherlands: A Geographical Analysis. *International Journal of Epidemiology*, vol. 20, no. 3, pp. 698–706.

Wachnicka, J. & Smolarek, L., 2013. Model Of Multilevel Stochastic Analysis Of Road Safety On Regional Level. *Reliability: Theory & Applications, Vol. 8 No. 9*, June, str. 39–48 ISSN 1932-2321.

Wooldridge, Jeffrey M., 2013. Random Effects Estimation. *Introductory Econometrics: A Modern Approach (Fifth international ed.*). Mason, OH: South-Western, pp. 474–478.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, *ISBN 978-1-138-02681-0*

Overall regional risk analysis of four Norwegian municipalities

R. Flage & Ø. Amundrud
University of Stavanger, Norway

H.S. Wiencke
Proactima, Norway

ABSTRACT: Norwegian municipalities are required by legislation to perform overall risk and vulnerability analyses covering the municipality as geographical area, as provider of public services and as a driving force in the area of societal safety and emergency preparedness. Cooperation between municipalities in this area is encouraged, if appropriate, including common risk and vulnerability analyses. This paper reports on the execution of an overall regional risk and vulnerability analysis covering four Norwegian municipalities. Selected issues are highlighted and discussed, including the structure of the hazard/threat identification, the representation of uncertainty and the presentation of the total risk picture.

1 INTRODUCTION

Since 2010 Norwegian municipalities are required by legislation to perform overall Risk and Vulnerability analyses (RVAs) (in Norwegian: "helhetlig risiko- og sårbarhetsanalyse") covering the municipality as geographical area, as provider of public services and as a driving force in the area of societal safety and emergency preparedness. The Norwegian Directorate for Civil Protection (NDCP 2012a) defines an overall RVA of a municipality as: "A systematic review of the municipality's geographic area and activities, with the aim of:

- Mapping risk and vulnerability, including adverse events that are of such a nature or extent that it involves municipal management in the assessment of preventive measures as well as in emergency preparedness and crisis management, and adverse events affecting several sectors.
- Revealing inter-sectorial vulnerabilities and interdependencies.
- Avoiding risk and vulnerability where possible.
- Reducing risk and vulnerability through preventive and mitigating measures.
- Dealing with any residual risk through emergency preparedness."

The requirement to perform such analyses applies to individual municipalities; however, cooperation between municipalities in the area of societal safety and emergency preparedness is encouraged, if appropriate, including common RVAs.

This paper reports on the execution of an overall *regional* RVA covering four Norwegian municipalities in the Stavanger region. The paper mainly covers the planning and performance of the analysis; the subsequent decision-making and risk treatment will only be briefly commented upon. In addition to reporting on the risk analysis process, selected issues are highlighted and discussed, including the structure of the hazard/threat identification, the representation of uncertainty and the presentation of the total risk picture.

As will be described in Section 2, there exist some guidelines on how to perform an overall (municipal) RVA. However, no updated, complete and application-specific authoritative guidelines have currently been published. The purpose and contribution of the present paper is to describe and discuss one possible approach to such an analysis. The presented method may be viewed as a practical implementation of theoretical risk frameworks that have been developed during the last decades, where more weight is put on uncertainty descriptions instead of calculated probabilities and expected values based on historical data, see for example (Aven & Renn 2010, Aven 2012, Aven 2013, Haimes 2009).

The remainder of the present paper is organized as follows: Section 2 reviews Norwegian legislative requirements relating to overall RVAs, as well as associated guidelines that apply. Section 3 gives a brief description of the Stavanger region, and Section 4 describes the risk analysis process that was carried out. Section 5 discusses some selected issues related to the analysis process, and Section 6 concludes.

2 LEGISLATIVE REQUIREMENTS GUIDELINES

The legislative requirements relating to overall RVAs for Norwegian municipalities can be found in the Civil Protection Act (2010) and the associated Regulations (2011). The regulations require municipalities to perform such an analysis, to use it as a basis for their work on societal safety and emergency preparedness, to update it in step with revisions of municipal plans, and to use it as a basis for developing an emergency preparedness plan. The RVA should take an all-risks approach and cover the municipality as geographical area, as provider of public services and as a driving force in the area of societal safety and emergency preparedness. The analysis is intended to be kept at a general level, taking a "bird's-view" perspective on the municipal risk factors; deferring more detailed analyses to the sectorial and individual company/organisational level. The analysis shall as a minimum cover: a) existing and future risk and vulnerability factors in the municipality; b) risk and vulnerability outside the geographical area of the municipality that could have implications for the municipality; c) how different risk and vulnerability factors can influence each other; d) specific challenges related to critical societal functions and loss of critical infrastructure; e) the municipality's ability to maintain its activity when exposed to an undesirable event and the ability to resume its activities after the event has occurred; and, f) the need for population alerting and evacuation.

The municipalities are required to use the analysis to develop long-term goals, strategies, priorities and plans for following up its work relating to societal safety and emergency preparedness. Scenarios for municipal emergency preparedness exercises should also be selected from the analysis. Collaboration between neighbouring municipalities is encouraged in the regulations, for example in terms of a common RVA process.

A guideline document to the Regulations on municipal duties relating to emergency preparedness has been published by the Norwegian Directorate for Civil Protection (NDCP 2012a). It provides detailed recommendations on inter alia how to perform and use the RVA. As for the execution of the risk analysis, the guideline refers the Norwegian standard NS 5814 (2008) containing general requirements to risk assessments, as well as to the guideline on municipal RVAs (NDCP 1994).

3 THE STAVANGER REGION

The Stavanger region here refers to the region made up by the municipalities Randaberg, Sandnes, Sola and Stavanger. Figure 1 shows a map of the region, as well as a map showing where in Norway the region is situated.

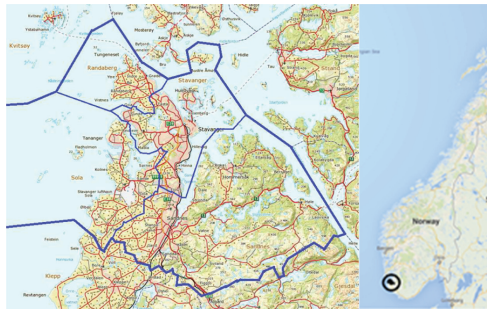


Figure 1. Map of the Stavanger region (Source: The Norwegian Mapping Authority).

The RVA includes a textual description of the individual municipalities with regard to geographical and sociotechnical factors. The region has a total population of 234.000 inhabitants (as of 1.1.2013) spread over a total area of 1150 km^2 (including territorial waters). There are significant differences between the municipalities in terms of size and population; however, the region to a large extent represents one combined labour and housing market; distances are small and the commuter rate is high. Many of the challenges that the municipalities face go across municipal borders, also in the area of societal safety and emergency preparedness. The municipalities have for several years collaborated both informally and the last few years also formally on issues and challenges related to this area.

4 THE RISK ANALYSIS PROCESS

This section describes the risk analysis process that was carried out, and follows the steps of the risk analysis process described by Aven (2009).

4.1 *Problem definition, information gathering and organisation*

4.1.1 *Problem definition*

The four municipalities had formulated a mandate for the RVA, describing inter alia the purpose, objectives, prerequisites, scope and follow-up of the analysis. The objectives of the analysis were:

- Map risk and vulnerability in the region.
- Identify risk reducing measures, both preventive and consequence reducing.
- Provide input to the development of long-term goals, strategies, priorities and plans for following up work relating to societal safety and emergency preparedness.
- Provide input to overall municipal and inter-municipal emergency planning.

- Form the basis for preparing municipal-specific RVAs.
- Uncover the need for further detailed analyses.

As mentioned in Section 1, the analysis covers the municipalities as geographical areas, as providers of services and as a driving force in the area of societal safety and emergency preparedness.

The analysis was conducted prior to corresponding municipality-specific RVAs in the municipalities. Whereas the regional analysis were to include hazards/threats affecting two or more of the municipalities simultaneously, as well as hazards/threats common to two or more of the municipalities, the municipality-specific analyses were to include hazards/threats specific to a single municipality. It was decided that the analysis should deal with the municipalities in normal operation in any season; i.e. conditions occurring during security-political crises and war were not to be included in the analysis as such scenarios are treated at the national level.

4.1.2 *Information sources*

The information gathering for the analysis took the form of review of written sources and information received from meeting participants/experts in analysis meetings. The written sources consisted of unrestricted sources in the public domain (national risk assessment, county RVA, openly available statistics, webpages, etc.). Analysis meetings were organised around critical societal functions, cf. Section 4.3. Three full-day and six half-day analysis meetings were conducted.

All existing sectorial and area RVAs were requested from the municipalities. Furthermore, all actors, public and private, who were invited to participate in the analysis process, were requested to provide their own RVAs or other relevant information. In addition, system descriptions, plans and more overall risk assessments (county, national, global) were used both to identify hazards/threats as well as to support the detailed analysis of these.

4.1.3 *Organisation*

There were mainly three actors involved in the analysis work: i) the municipalities' working group (emergency preparedness managers and advisors; responsible for political and administrative anchoring of the process, project planning and coordination, internal and external information activities regarding the analysis, and contributing to the hazard/threat identification and more detailed risk analysis); ii) consultancy company project group (responsible for the professional content of the analysis, including hazard/threat identification and detailed risk analysis; facilitation and documentation of the analysis meetings; as well as documentation of the analysis); and, iii) participants in the analysis meetings (about 100 representatives from public and private sector contributing to hazard/threat identification and more detailed risk analysis during dedicated meetings).

4.2 *Selection of analysis method*

4.2.1 *Analysis method*

Municipal RVAs in Norway are typically performed using a method best covered by the label coarse risk analysis, which is described by Aven (2009) as a qualitative risk analysis method that can be carried out with relatively modest effort. This is consistent with the recommended method in the existing guideline on municipal RVAs (NDCP 1994).

The RVA reported on in the present paper was performed using a semi-quantitative coarse risk analysis method with extended uncertainty assessment. Semi-quantitative here refers to the use of quantitative expressions for the consequence and probability assignments for individual adverse events, but no combination or aggregation of these into an overall risk index, as would typically be done in a full quantitative risk analysis. Extended uncertainty assessment refers to an assessment of uncertainty that extends beyond the quantitative consequence and probability assignments, in our case performed by qualitatively assessing the strength of knowledge of these quantitative assignments; as explained in the following sub-section.

4.2.2 *Components used to characterise risk*

In a coarse risk analysis, risk is typically characterised by assigning the probability and (expected) consequences of each identified event. The regional RVA for the Stavanger region used the following components to characterise risk:

- The consequences given occurrence of an adverse event; specifically: i) expected consequences given occurrence; and ii) potential for significant deviation between the expected consequences and actual consequences.
- The probability that the event will occur.
- The strength of knowledge underlying the consequence and probability assignments.
- Manageability of the risk related to the event, i.e. to what extent the municipalities can reduce the risk by introducing measures.

The consequence analysis followed a similar structure as that used in the Norwegian national risk picture methodology, where consequences are assessed for five so-called *societal values* (NDCP 2010): 1) life and health; 2) nature and environment; 3) economy; 4) social stability; and 5) ability to govern/territorial control.

For each societal value a set of *consequence types* has been defined (NDCP 2010), and each of these is associated with a set of *observable quantities*

Table 1. Probability categories; and consequence categories for "Life and health—Deaths".

Category	Probability	Consequences (fatalities)
5	> 10%	> 50
4	1%–10%	15–50
3	0,1%–1%	5–15
2	0,01%–0,1%	3–5
1	< 0,01%	1–2

characterising the consequences. For example, the societal value "Life and health" is broken down into the consequence types "Death", "Injuries and illnesses" and "Physical strains". Furthermore, the consequence type "Death" is associated with the observable quantities "Number of fatalities" and "Time of death"; the latter categorised as either "Within 1 year" or "Within 20 years" (to account for immediate deaths and reduced life expectancy, respectively).

This structure was adopted in the consequence analysis part of the RVA for the Stavanger region; with some modifications: Societal value 5 in the above list was not considered as it largely relates to situations outside the scope of the analysis, i.e. security-political crises and war (cf. Section 4.1.1). Moreover, a new societal value called "Cultural values" was added. Finally, a new consequence type was added to the societal value "Life and health", namely "Psychological injuries". The last modification was made as a result of the experience gained after the 22 July 2011 terrorist attacks in Norway, where municipalities all over the country were tasked with the long-term psychological follow-up of people affected by the attacks. This was an example of how a municipality could be affected by an event occurring outside the geographical area of the municipality; cf. point b) in Section 2. Table 1 shows, as an example, the consequence categories defined for the observable quantity "Number of fatalities" related to the consequence type "Deaths".

Table 1 also shows the probability categories used. Subjective probabilities were used to describe the uncertainty related to the occurrence of events; hence the probabilities express the degree of belief that the events will occur. They are conditional on the background knowledge that their assignment is based on, including data, expert opinions and assumptions. Accordingly they are sometimes also referred to as knowledge-based probabilities. These probabilities are used to describe uncertainty (about the occurrence of events) and are hence not themselves uncertain. However, because the probabilities are conditional on a particular background knowledge, such as the assumptions made in the analysis (which in reality may turn out not to be fulfilled), there may be "uncertainties hidden in the background knowledge" (Aven 2009). Furthermore, the consequence characterisation in a coarse risk analysis is based on the specification of a single consequence per event (and per consequence type). However, there will for a given event usually be a number of possible consequences of varying severity. In an attempt to compensate for these methodological shortcomings, the probability and consequence assessment in the regional RVA was supplemented by an "extended uncertainty analysis", by highlighting: i) the strength of the knowledge base for the assigned probabilities and (expected) consequences; and, ii) potential for significant deviation between the expected result and the actual result.

The deviation potential was assessed according to the analyst's judgement using a binary classification ("Yes" or "No"). Both strength of knowledge and manageability were categorised according to qualitative criteria. The strength of knowledge underlying the assigned probabilities and (expected) consequences was assessed by categorising the probability/consequence assignment for each event according to the classification scheme of Flage & Aven (2009). Weak knowledge is characterised by situations where: the assumptions made represent strong simplifications; or, data are not available or are unreliable; or, there is lack of agreement/consensus among experts; or, the phenomena involved are not well understood. Strong knowledge is characterised by fulfilling all of the following conditions: the assumptions made are seen as very reasonable; much reliable data are available; there is broad agreement/consensus among experts; and, the phenomena involved are well understood. Moderate knowledge is characterized by conditions between those characterising weak and strong knowledge.

Manageability was categorised as follows: high—the municipalities can control/reduce the risk level (with mitigating measures, by avoiding the activity, etc.); moderate—the municipalities can influence the risk level to some extent; and, low—the municipalities cannot influence the risk level.

4.3 *Identification of initiating events (hazards/threats)*

A coarse risk analysis is commonly performed by dividing the analysis object into sub-elements and then performing a risk analysis for each of these (Aven 2009). In the present analysis both geographical areas and public services provided by the municipalities can be considered main analysis objects; cf. the analysis scope described in Section 4.1.1. However, the Civil Protection Act (2010) also imposes a general emergency

preparedness duty on the municipalities, implying an inter-sectorial responsibility intended to make the municipalities assess and plan societal safety and emergency preparedness in a more overall and integrated perspective, not limited to those areas of responsibilities imposed on the municipalities through other legislation (NDCP 2012a).

As mentioned in Section 2, the overall RVA is required to address specific challenges related to critical societal functions and loss of critical infrastructure. Critical infrastructure is defined by NDCP (2012a) as "those constructions and systems that are essential for maintaining the society's critical functions which again cover the society's basic needs and people's sense of security". Furthermore, NDCP (2012b) has presented a set of *critical societal functions* and associated *basic capabilities*, as well as a set of *critical input factors*:

- Critical societal function: Societal function whose loss threatens the basic needs (food, water, heat, safety/security, etc.) of the society and the population.
- Basic capability: The functional ability that society must be able to maintain almost regardless of the stresses to which it is subjected; capability is often defined as a combination of competence and capacity.
- Critical input factor: The external deliveries public and private actors depend on to produce and deliver in order to maintain the basic needs of the society and the population.

The critical societal functions and input factors are reproduced in Table 2.

Table 2. Critical societal functions and critical input factors (NDCP 2012b).

Critical societal functions	Critical input factors
1. Maintain necessary food supply	A. Electronic communication services
2. Maintain necessary (drinking) water supply	B. Electricity supply
3. Maintain the population's need for heat	C. Water supply
4. Maintain national crisis management	D. Wastewater treatment
5. Maintain control and crisis management	E. Fuel supply
6. Maintain democratic state of justice	F. Goods and personnel transport
7. Maintain safety/ security of life and health	G. Satellite-based services
8. Maintain law and order	H. Meteorological services
9. Maintain financial stability	
10. Maintain basic security of stored information	
11. Protect cultural values of national significance	
12. Protect the nature and environment	

In the RVA for the Stavanger region, a critical societal function called "Maintain value creation" was added, as a significant percentage of the Norwegian value creation is generated by companies with headquarters in the Stavanger region. To each of the critical societal functions there is as mentioned above associated one or more basic capabilities; for example, the critical societal function "3. Maintain the population's need for heat" is associated with the two basic capabilities "3.1 Ability to provide the population with sufficient energy to heat homes" and "3.2 Ability to provide necessary temporary shelter". Critical infrastructures can be derived from the critical input factors, e.g. electricity networks from the critical input factor "Electricity supply".

The RVA process for the Stavanger region included a survey of critical elements related to critical societal functions, associated basic capabilities, and critical input factors/infrastructures in the region. The hazard/threat identification was structured around these functions, capabilities and input factors in two ways: Firstly, the analysis meetings (cf. Section 4.1.2) were put together in an attempt to cover the totality of functions, capabilities and inputs. Secondly, the final overall hazards/threats reported as initiating events in the risk picture were to a large extent formulated in terms of loss of such functions, capabilities and inputs. This is further described and discussed in Section 5.1.

The hazards/threats/adverse events identification process related to the analysis meetings was carried out in three steps: 1) Before analysis meeting: brainstorming using online questionnaire sent to meeting participants by e-mail. 2) During analysis meeting: structured review and identification based on the principle of dividing the analysis object into sub-parts. 3) During and/or after analysis meeting: review of and identification based on checklist.

4.4 *Cause and consequence analysis*

As a result of the hazard/threat identification process described in the previous section, a large number of adverse events were identified. Many of these events would lead to loss of the

same critical societal function or input factor. For example, a total of 18 events were identified that would lead to loss of the critical input factor 'Electricity supply' (e.g., national deficit of power, breakdown of critical power line, extreme weather, etc.). In order to achieve a manageable number of events and an appropriate level of analysis for further assessment and presentation of risk, these 'sub-events' were aggregated to one main event "Failure of power supply (prolonged)". This is the event that the municipalities need to handle; the sub-event (cause) "Breakdown of critical power line" per se needs to be handled by the infrastructure owner, i.e. the power company. The sub-events were then listed as causes to the main event. This provided an appropriate focus and level of detail considering the purpose of the RVA (cf. Section 4.1.1).

Existing barriers, both preventive and consequence reducing, were identified as a part of this process along with suggestion of new risk reducing measures.

4.5 *Risk picture*

The term "risk picture" is used frequently by Norwegian authorities and professionals working with risk analysis and management. The NORSOK Z-013 standard uses the following definition: "Risk picture: synthesis of the risk assessment, with the intention to provide useful and understandable information to relevant decision makers". Among other things, uncertainty factors along with prerequisites and assumptions should be clearly and explicitly documented (NORSOK 2010).

Table 3. Extract of the events list. The right column shows the corresponding societal function/input.

Event	Societal function/input factor
1. Failure of food supply	Maintain necessary food supply
2. Distribution of hazardous food	
3. Failure of drinking water supply (prolonged)	Maintain necessary (drinking) water supply
4. Distribution of contaminated drinking water	
5. Contaminated drinking water, food, air, etc. due to radioactive fallout	
6. Failure of power supply (prolonged)	Maintain the population's need for heat/electricity supply
…	…

The risk picture for the regional RVA was established based on the identification of initiating events (hazards/threats) and the cause and consequence analysis (cf. Section 4.3, 4.4). From an initial number of several hundred adverse events, the filtering, merging and aggregation process described in Section 4.4 resulted in 51 events in the final risk picture.

For each event, the following factors were covered and presented in tabular form: Causes, probability of event, expected consequence of event, potential for significant deviation between the expected consequences and actual consequences, strength-of-knowledge base for the probability and consequence assignments, description of knowledge base (statistics, historical records, previous risk assessments, etc.), barriers and mitigating measures (both existing and suggestions for new), and manageability.

The 51 events were presented in risk matrices as a combination of probability and consequence. In addition, uncertainty and strength-of-knowledge factors were indicated the following way: i) events where there is potential for significant deviation between the expected and actual consequences were indicated with an arrow, and ii) events where the strength-of-knowledge was assigned 'Weak' according to the classification scheme in Section 4.2.2 were highlighted with a grey background.

Different risk matrices were created for the different consequence types. Figure 2 shows an example for the consequence type Life and health—Deaths.

In addition to the risk matrices, a textual description was given of the principal risk factors related to each societal value, both existing and future. Interdependencies and vulnerabilities related to critical infrastructures which became apparent in the analysis were also highlighted.

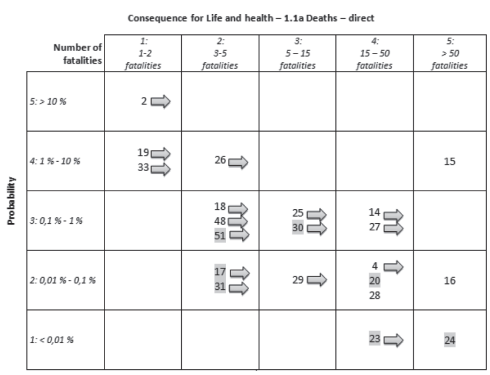


Figure 2. Risk matrix for Life and health: Deaths within 1 year.

4.6 *Compare alternatives, identification and assessment of measures*

A number of risk reducing measures were identified during the analysis process. These were structured according to whether the measure already existed or were suggested during the analysis process, and according to the level responsible for follow-up (i.e., nation or county level, regional, municipality, company/organisation—inter-municipal, municipal or private, or individual level—households/inhabitants).

Based on the analysis and the responsibilities that rest with the local authorities, 12 scenarios/events were suggested as dimensioning for the regional and municipal emergency preparedness. These events were ranging from major accidents (including terrorism and criminal acts); extreme weather and natural disasters; breakdown in critical infrastructures; and, emission of hazardous substances. The events were chosen based on the following criteria: i) events where the expected consequences are severe; ii) events where the potential for deviation from the expected consequences is considered significant or the strength of knowledge is considered weak; and, iii) events which trigger the regional and municipal top executives in the risk treatment decisions.

4.7 *Management review and judgment. Decision*

This step of the process is beyond the scope of the present paper. According to the Regulations (2011), the overall RVA shall be anchored in the municipality council, which is hence to be considered the decision-maker in this context (the decision authority possibly being delegated to other municipal political bodies or to the municipal administration). In addition to internal information activities within each municipality, the mayors and city managers of the four municipalities attended two joint project information meetings, respectively during the analysis work and after finalisation of the analysis. There were also two project information meetings for relevant actors and contributors to the analysis, respectively before and after the analysis work.

We only mention briefly two decisions that have been made based on recommendations from the analysis: Firstly, the municipalities have decided to follow up the RVA with an emergency preparedness analysis, based on the RVA results. This is inspired by the practice in the oil & gas industry (NORSOK 2010). Secondly, the municipalities have decided to establish a regional emergency preparedness council, comprising representatives from the municipality, other public actors, as well as owners of critical infrastructure. A regional council will be able to coordinate work in the area of societal safety and emergency preparedness across municipal borders.

5 DISCUSSION

In this section we discuss some selected aspects of the chosen approach to the RVA. These are methodological aspects that we consider have a transfer value to other risk analyses, in particular municipal RVAs, but also other risk analyses performed according to a semi-quantitative methodology.

5.1 *Structure of the hazard/threat identification*

The core steps taken to establish a risk picture in the regional RVA are broadly speaking the same as those taken to establish the Norwegian national risk picture (NDCP 2010); which to a large extent is based on the Dutch national risk assessment, see Veland et al. (2013) for a comparison: 1) define societal values; 2) identify hazards/threats; 3) perform risk analysis; and, 4) establish risk matrix.

A main challenge related to the hazard/threat identification is achieving some sense of completeness, i.e. identifying all relevant events. An alternative to the chosen process would be to focus on specific event types and scenarios, as done in the Norwegian national risk picture (NDCP 2013).

In the national risk picture the events are structured according to type of phenomenon: There is a phenomenological distinction between intentional and non-intentional events, and for non-intentional events we can further distinguish between natural hazards and major accidents. These three are referred to in the national risk picture as "Main categories" of hazards/threats. To each main category is associated several risk areas, e.g. "Dangerous substances" to the main category "Major accidents"; and to each risk area is associated one or more "Scenarios", e.g. "Fire at oil terminal in a city" to the risk area "Dangerous substances".

As described in Section 4.3, the hazard/threat identification in the regional RVA followed a different approach, structured around critical societal functions, associated basic capabilities, and critical inputs. The reasoning behind such an approach is that in order to safeguard societal values, certain societal functions and inputs need to be in place. Adverse events can threaten the societal values either directly or indirectly through loss of critical inputs (infrastructure) and/or critical societal functions.

For example, a car accident could threaten the societal value "Life and health" directly. Emergency services are dimensioned to handle such an event and will under normal circumstances not be challenged on the ability to handle it. However, if an event occurs (or several events simultaneously) that either "block" or "overload" the hospital, then the society value "Life and health" is also threatened indirectly through loss of the societal function

"Maintain safety/security of life and health". The selected approach involves a form of "backwards risk analysis", or risk analysis starting from the consequences, see e.g. (Aven 2009), which means that we first select the consequences that we are most concerned about, and then find events that could lead to these consequences. This of course means that not all events that could lead to consequences in terms of the societal values are included; instead, focus is placed on certain types of events that will challenge the emergency preparedness.

The chosen approach means that what enters as initiating events in the National risk picture (risk areas/scenarios), and are thus implicitly placed in the middle of a bow-tie diagram, may instead enter as causes in the regional RVA.

5.2 *Representation of uncertainty*

The risk analysis approach adopted with respect to uncertainty representation may be labelled as a predictive Bayesian approach (Aven 2012), where knowledge-based/subjective probabilities are used to express uncertainty directly about observable quantities. Frequentist probabilities were not introduced; however, the interpretation of subjective probabilities was explained such as to relate the way these were defined to long-run frequencies along the lines of the urn standard by Lindley (2006). For example, the probability category 1% – 10% (cf. Table 1 in Section 4.2.2) was explained as follows: The uncertainty related to (or degree of belief in) the event occurring is considered comparable with the uncertainty related to (or degree of belief in) drawing a coloured ball from an urn containing a total of 100 balls of which between 1 and 10 are coloured; an event that would occur on average between each 10 and 100 years if a ball is drawn (with replication) once each year in the long run.

To motivate the consequence deviation potential part of the extended uncertainty assessment (cf. Section 4.2.2), consider as an example the event "Bus Accident". The expected consequences of such an event could perhaps be a few injuries; however, the consequences could also be a large number of fatalities. If the risk analysis only reports the probability and expected consequence of this event, its consequence potential is not reflected. On the other hand, if the probability of the rather broadly defined event "Bus Accident" is linked to some sort of "worst case" scenario, there will be a mismatch between probability and consequence. One solution could be to split the single event into two events, for example "Bus Accident" and "Bus accident with multiple fatalities". This is still a simplification, as the consequences of a bus accident could be one injury, two injuries, three injuries, etc.; one fatality, two fatalities, three fatalities, etc.; or a combination of these. However, there will always be a need for a trade-off between level of detail and effort. In the regional RVA for the Stavanger region, the event "Contamination of drinking water" was split into the two events, due to a significant difference in consequence potential between these: i) distribution of contaminated drinking water; and, ii) contaminated drinking water, food, air, etc. due to radioactive fallout.

As for the strength-of-knowledge assessment, returning to the event "Bus accident" it may be assumed in the risk analysis that the bus is carrying half the number of permitted passengers at the time of the accident, and that everyone on board are using seatbelts; while in reality the bus is carrying upwards of or above the permitted number of passengers, of which only a small fraction are using seatbelts when the accident occurs.

In the regional RVA for the Stavanger several events where flagged with a 'Weak' strength-of-knowledge, due to lack of relevant data or lack of knowledge of the underlying phenomena, for example; violent acts/terror attack in the city; and, extreme weather/natural disaster.

6 CONCLUSIONS

This paper reports on the execution of an overall RVA covering four Norwegian municipalities. Selected issues are highlighted and discussed, including the structure of the hazard/threat identification, the representation of uncertainty and the presentation of the total risk picture. These are methodological aspects that we consider have a transfer value to other risk analyses, in particular municipal RVAs, but also other risk analyses performed according to a semi-quantitative methodology.

ACKNOWLEDGEMENTS

The authors would like to thank the municipalities of Randaberg, Sandnes, Sola and Stavanger for their valuable collaboration.

REFERENCES

Aven, T., 2009. Risk analysis: assessing uncertainties beyond expected values and probabilities. Chichester, England, Wiley.

Aven, T., 2012. *Foundations of risk analysis*, 2nd Edition. Chichester, Wiley.

Aven, T., 2013. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety,* 115: 136–145.

Aven, T. & Renn, O., 2010. *Risk management and governance: concepts, guidelines and applications*. Berlin, Springer-Verlag.

Civil Protection Act., 2010. Law on municipal duties relating to emergency preparedness, civil protection measures and the Civil Defence [Translation from Norwegian]. LOV-2010-06-25-45.

Flage, R. & Aven, T., 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability and Risk Analysis: Theory & Applications,* 2(13): 9–18.

Haimes, Y.Y., 2009. *Risk Modeling, Assessment, and* Management, 3rd Edition. New York, Wiley.

Lindley, D.V., 2006. *Understanding uncertainty*. Hoboken, N.J., Wiley.

NDCP, 1994. *Guideline on municipal risk and vulnerability analyses* [Translation from Norwegian]. Norwegian Directorate for Civil Protection.

NDCP, 2010. *National risk picture—process and method* [Translation from Norwegian]. Norwegian Directorate for Civil Protection.

NDCP, 2012a. *Guideline to Regulations on municipal duties relating to emergency preparedness* [Translation from Norwegian]. Norwegian Directorate for Civil Protection.

NDCP, 2012b. *Security in critical infrastructures and critical societal functions* [Translation from Norwegian]. Norwegian Directorate for Civil Protection.

NDCP, 2013. *National risk picture 2013* [Translation from Norwegian]. Norwegian Directorate for Civil Protection.

NORSOK, 2010. Z-013, Risk assessment and emergency preparedness analysis, 3rd edition, Standard Norge

NS 5814, 2008. Requirements to risk assessments. Standard Norge.

PSA, 2013. Principles for barrier management in the petroleum industry. Petroleum Safety Authority Norway.

Regulations, 2011. *Regulations on municipal duties relating to emergency preparedness* [Translation from Norwegian]. FOR-2011-08-22-894.

Veland, H., Amundrud, Ø., & Aven, T., 2013. Foundational issues in relation to national risk assesssment methodologies. *Journal of Risk and Reliability,* 227(3): 348–358.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Modeling reliability of complex port transportation system

K. Kołowrocki & J. Soszyńska-Budny
Department of Mathematics, Maritime University, Gdynia, Poland

ABSTRACT: Modelling and prediction of the operation and reliability of technical systems related to their operation processes are presented. The emphasis is on multistate systems composed of ageing components and changing their reliability structures and their components reliability parameters during their operation processes that are called the complex systems. The integrated general model of complex systems' reliability, linking their reliability models and their operation processes models and considering variable at different operation states their reliability structures and their components reliability parameters is constructed. This theoretical tool is applied to modelling and prediction of the operation processes and reliability characteristics of the port grain transportation system composed of three multistate non-homogeneous series-parallel subsystems linked in series, changing its reliability structure and its components reliability parameters at variable operation conditions.

1 INTRODUCTION

Most real technical systems are very complex and it is difficult to analyze their reliability. Large numbers of multistate components and subsystems and their operating complexity cause that the identification, evaluation and prediction of their reliability are complicated. The complexity of the systems' operation processes and their influence on changing in time the systems' structures and their components' reliability parameters are very often met in real practice. Thus, the practical importance of an approach linking the multistate system reliability models (Hue 1985, Hue & Yang 1995a,b) and the system operation processes models (Kołowrocki & Soszyńska-Budny 2011, Kołowrocki 2006, 2008, 2014, Kołowrocki & Soszyńska 2006, 2010, Soszyńska 2007) into an integrated general model in reliability assessment of real technical systems is evident.

2 COMPLEX SYSTEM OPERATION PROCESS MODELLING

2.1 *Theoretical backgrounds*

We assume that the system during its operation process is taking v, $v \in N$, different operation states $z_1, z_2, ..., z_v$. Further, we define the system operation process $Z(t)$, $t \in <0,+\infty)$, with discrete operation states from the set $\{z_1, z_2, ..., z_v\}$. Moreover, we assume that the system operation process $Z(t)$ is a semi-Markov process (Grabski 2002, Glynn & Haas 2006, Ferreira & Pacheco 2007, Limnios & Oprisan 2001, Mercier 2008) with the conditional sojourn times θ_{bl} at the operation states z_b when its next operation state is z_l, $b, l = 1,2, ..., v$, $b \neq l$. Under these assumptions, the system operation process may be described by:

- the vector $[p_b(0)]_{1\times v}$ of the initial probabilities $p_b(0) = P(Z(0) = z_b)$, $b = 1,2, ..., v$, of the system operation process $Z(t)$ staying at particular operation states at the moment $t = 0$;
- the matrix $[p_{bl}]_{v\times v}$ of probabilities p_{bl}, $b, l = 1,2, ..., v$, $b \neq l$, of the system operation process $Z(t)$ transitions between the operation states z_b and z_l;
- the matrix $[H_{bl}(t)]_{v\times v}$ of conditional distribution functions $H_{bl}(t) = P(\theta_{bl} < t)$, $t \geq 0$, $b, l = 1,2, ..., v$, $b \neq l$, of the system operation process $Z(t)$ conditional sojourn times θ_{bl} at the operation states.

As the mean values $E[\theta_{bl}]$ of the conditional sojourn times θ_{bl} are given by

$$M_{bl} = E[\theta_{bl}] = \int_0^\infty t dH_{bl}(t), b,l = 1,2, ..., v, b \neq l, \qquad (1)$$

then from the formula for total probability, it follows that the unconditional distribution functions of the sojourn times θ_b, $b = 1,2, ..., v$, of the system operation process $Z(t)$ at the operation states z_b, $b = 1,2, ..., v$, are given by (Grabski 2002, Kołowrocki & Soszyńska-Budny 2011)

$$H_b(t) = \sum_{l=1}^{v} p_{bl} H_{bl}(t), \; t \geq 0, \; b = 1,2, ..., v.$$

Hence, the mean values $E[\theta_b]$ of the system operation process $Z(t)$ unconditional sojourn times θ_b, $b = 1,2, ..., v$, at the operation states are given by

$$M_b = E[\theta_b] = \sum_{l=1}^{v} p_{bl} M_{bl}, \; b = 1,2, ..., v, \tag{2}$$

where M_{bl} are defined by the formula (1).

The limit values of the system operation process $Z(t)$ transient probabilities at the particular operation states $p_b(t) = P(Z(t) = z_b)$, $t \in <0, +\infty)$, $b = 1,2, ..., v$, are given by Grabski 2002, Kołowrocki & Soszyńska-Budny 2011, Kołowrocki 2006, Soszyńska 2007)

$$p_b = \lim_{t \to \infty} p_b(t) = \frac{\pi_b M_b}{\sum_{l=1}^{v} \pi_l M_l}, \quad b = 1,2, ..., v, \tag{3}$$

where M_b, $b = 1,2, ..., v$, are given by (2), while the steady probabilities π_b of the vector $[\pi_b]_{1xv}$ satisfy the system of equations

$$\begin{cases} [\pi_b] = [\pi_b][p_{bl}] \\ \sum_{l=1}^{v} \pi_l = 1. \end{cases} \tag{4}$$

Other interesting characteristics of the system operation process $Z(t)$ possible to obtain are its total sojourn times $\hat{\theta}_b$ at the particular operation states z_b, $b = 1,2, ..., v$, during the fixed system opetation time. It is well known (Grabski 2002) that the system operation process total sojourn times $\hat{\theta}_b$ at the particular operation states z_b, for sufficiently large operation time θ, have approximately normal distributions with the expected value given by

$$\hat{M}_b = E[\hat{\theta}_b] = p_b \theta, \; b = 1,2, ..., v, \tag{5}$$

where p_b are given by (3).

2.2 *Example*

We consider the port grain transportation system, presented in Figure 1, assigned to handle the clearing of exported and imported grain.

The port grain transportation system function is loading railway trucks with grain. The railway truck loading is performed in the following successive grain transportation system steps:

- gravitational passing of grain from the storage placed on the 8th elevator floor through 45 hall to horizontal conveyors placed in the elevator basement,

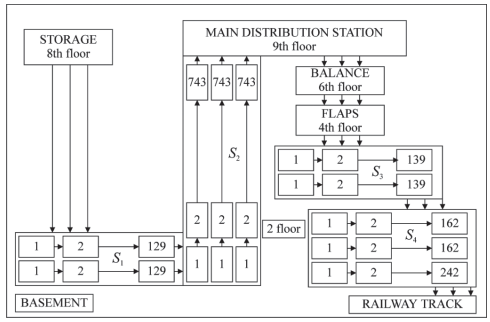


Figure 1. The scheme of the port grain transportation system structure at the operation state z_1.

- transport of grain through horizontal conveyors to vertical bucket elevators transporting grain to the main distribution station placed on the 9th floor,
- gravitational dumping of grain through the main distribution station to the balance placed on the 6th floor,
- dumping weighed grain through the complex of flaps placed on the 4th floor to horizontal conveyors placed on the 2nd floor,
- dumping of grain from horizontal conveyors to worm conveyors,
- dumping of grain from worm conveyors to railway trucks.

In loading the railway trucks with grain the following presented in Figures 1 and 2 transportation subsystems take part:

S_1—horizontal conveyors of the first type,
S_2—vertical bucket elevators,
S_3—horizontal conveyors of the second type,
S_4—worm conveyors,

the main distribution station and the balance.

The main distribution station is the system of dumping channels in the form of a steel box composed of dividing walls, which direct the grain from bucket conveyors to the balance. Its executive elements are composed of three steel sleeves and pneumatic elements in the form of three servomotors. The electronic balance weighs the dumped grain with electronic indicators. Its executive elements during loading and unloading with grain are flaps, which are opened and closed by five pneumatic servomotors. In further analysis, we omit these two subsystems and will deal with the reliability of the subsystems S_1, S_2, S_3 and S_4 only.

The transportation subsystems S_1, S_2, S_3 and S_4 have steel covers and they are provided with drives in the form of electrical engines with gears. In their reliability analysis we omit their drives as they are different types mechanisms. We also omit their

covers as they have a high reliability and, practically, do not fail.

Taking into account the operation process of the considered transportation system, described by its operators, we distinguish its following $\nu = 3$ operation states:

z_1—the system operation with the largest efficiency when all components of the subsystems S_1, S_2, S_3 and S_4 are used (Fig. 1),

z_2—the system operation with less efficiency system when the first conveyor of subsystem S_1, the first and second elevators of subsystem S_2, the first conveyor of subsystem S_3 and the first and second conveyors of subsystem S_4 are used (Fig. 3),

z_3—the system operation with least efficiency when only the first conveyor of subsystem S_1, the first elevator of subsystem S_2, the first conveyor of subsystem S_3 and the first conveyor of subsystem S_4 are used (Fig. 4).

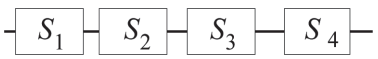


Figure 2. The general scheme of the port grain transportation system reliability structure.

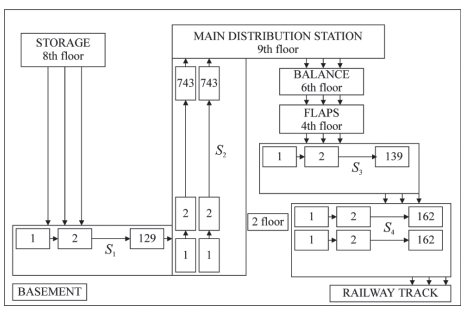


Figure 3. The scheme of the port grain transportation system structure at the operation state z_2.

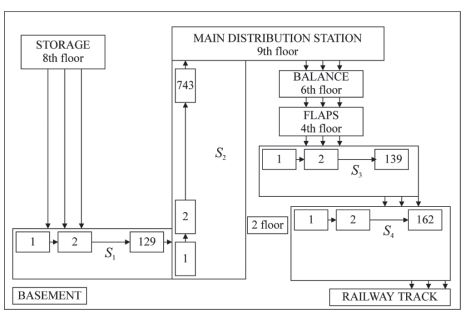


Figure 4. The scheme of the port grain transportation system structure at the operation state z_3.

At all system operation states, subsystems S_1, S_2, S_3 and S_4 become either non-homogeneous series-parallel systems or non-homogeneous series systems.

This way, the changes of the grain transportation system reliability structure at different operation states are defined. Its components reliability parameters at different operation states will be defined in this example continuation in Section 3.

Considering the system operators opinion, we assume the matrix of the probabilities of transitions between the states are given by

$$[p_{bl}]_{3x3} = \begin{bmatrix} 0 & \frac{1}{3} & \frac{2}{3} \\ \frac{4}{9} & 0 & \frac{5}{9} \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} \tag{6}$$

Moreover, we assume the following matrix of the conditional distribution functions of the system sojourn times θ_{bl}, $b, l = 1, 2, 3$,

$$[H_{bl}(t)]_{3x3} = \begin{bmatrix} 0 & 1-e^{-5t} & 1-e^{-10t} \\ 1-e^{-40t} & 0 & 1-e^{-50t} \\ 1-e^{-10t} & 1-e^{-20t} & 0 \end{bmatrix}.$$

Further, using (5), we fix the conditional mean values $M_{bl} = E[\theta_{bl}]$, $b,l = 1,2,3,4$, of the exemplary system sojourn times at the particular operation states as follows:

$$M_{12} = 0.20, \quad M_{13} = 0.10, \; M_{21} = 0.025, \\ M_{23} = 0.020, \; M_{31} = 0.10, \; M_{32} = 0.05. \tag{7}$$

This way, the exemplary system operation process is defined and we may find its main characteristics. Namely, applying (2), (6) and (7), the unconditional mean sojourn times at the particular operation states are given by:

$$M_1 = 0.133, \; M_2 = 0.022, \; M_3 = 0.067. \tag{8}$$

Further, according to (4), the system of equations after considering (6), we find the steady probabilities

$$\pi_1 \cong 0.279, \; \pi_2 \cong 0.344, \; \pi_3 \cong 0.377. \tag{9}$$

After considering the result (8) and (9), according to (3), the limit values of the exemplary system operation process transient probabilities $p_b(t)$ at the operation states z_b are given by

$$p_1 \cong 0.530, \; p_2 \cong 0.109, \; p_3 \cong 0.361. \tag{10}$$

Hence, the expected values of the total sojourn times $\hat{\theta}_b$, $b=1,2,3,4$, of the exemplary system operation process at the particular operation states z_b, $b=1,2,3,4$, during the fixed operation time $\theta=1$ year = 365 days, after applying (5), amount (in days):

$$\hat{M}_1 \cong 193.4,\ \hat{M}_2 \cong 39.8,\ \hat{M}_3 \cong 131.8. \tag{11}$$

3 COMPLEX SYSTEM RELIABILITY MODELLING

3.1 *Theoretical backgrounds*

We assume that the changes of the operation states of the system operation process $Z(t)$ have an influence on the system multistate components E_i, $i=1,2,...,n$, reliability and the system reliability structure as well. Consequently, we denote the system multistate component E_i, $i=1,2,...,n$, conditional lifetime in the reliability state subset $\{u,u+1,...,z\}$ while the system is at the operation state z_b, $b=1,2,...,v$, by $T_i^{(b)}(u)$ and its conditional reliability function by the vector

$$[R_i(t,\cdot)]^{(b)} = [1,[R_i(t,1)]^{(b)},...,[R_i(t,z)]^{(b)}],$$

with the coordinates defined by

$$[R_i(t,u)]^{(b)} = P(T_i^{(b)}(u) > t \,|\, Z(t) = z_b)$$

For $t \in <0,\infty)$, $u=1,2,...,z$, $b=1,2,...,v$.

The reliability function $[R_i(t,u)]^{(b)}$ is the conditional probability that the component E_i lifetime $T_i^{(b)}(u)$ in the reliability state subset $\{u,u+1,...,z\}$ is greater than t, while the system operation process $Z(t)$ is at the operation state z_b.

Similarly, we denote the system conditional lifetime in the reliability state subset $\{u,u+1,...,z\}$ while the system is at the operation state z_b, $b=1,2,...,v$, by $T^{(b)}(u)$ and the conditional reliability function of the system by the vector

$$[\boldsymbol{R}(t,\cdot)]^{(b)} = [1,\ [\boldsymbol{R}(t,1)]^{(b)},...,[\boldsymbol{R}(t,z)]^{(b)}],$$

with the coordinates defined by

$$[\boldsymbol{R}(t,u)]^{(b)} = P(T^{(b)}(u) > t \,|\, Z(t) = z_b) \tag{12}$$

For $t \in <0,\infty)$, $u=1,2,...,z$, $b=1,2,...,\nu$.

The reliability function $[\boldsymbol{R}(t,u)]^{(b)}$ is the conditional probability that the system lifetime $T^{(b)}(u)$ in the reliability state subset $\{u,u+1,...,z\}$ is greater than t, while the system operation process $Z(t)$ is at the operation state z_b.

Further, we denote the system unconditional lifetime in the reliability state subset $\{u,u+1,...,z\}$ by $T(u)$ and the unconditional reliability function of the system by the vector

$$\boldsymbol{R}(t,\cdot) = [1,\ \boldsymbol{R}(t,1),...,\ \boldsymbol{R}(t,z)],$$

with the coordinates defined by

$$\boldsymbol{R}(t,u) = P(T(u) > t) \tag{13}$$

For $t \in <0,\infty)$, $u=1,2,...,z$.

In the case when the system operation time θ is large enough, the coordinates of the unconditional reliability function of the system defined by (13) are given by

$$\boldsymbol{R}(t,u) \cong \sum_{b=1}^{v} p_b [\boldsymbol{R}(t,u)]^{(b)} \ for\ t \geq 0,\ u=1,2,...,z, \tag{14}$$

where $[\boldsymbol{R}(t,u)]^{(b)}$ $u=1,2,...,z$, $b=1,2,...,\nu$, are the coordinates of the system conditional reliability functions defined by (12) and p_b, $b=1,2,...,\nu$, are the system operation process limit transient probabilities given by (3).

Thus, the mean value $\mu(u)=E[T(u)]$ of the system unconditional lifetime $T(u)$ in the reliability state subset $\{u,u+1,...,z\}$ is given by (Kołowrocki & Soszyńska-Budny 2011)

$$\mu(u) \cong \sum_{b=1}^{\nu} p_b \mu_b(u),\ u=1,2,...,z, \tag{15}$$

where $M_b(u)=E[T^{(b)}(u)]$ are the mean values of the system conditional lifetimes $T^{(b)}(u)$ in the reliability state subset $\{u,u+1,...,z\}$ at the operation state z_b, $b=1,2,...,\nu$, given by

$$\mu_b(u) = \int_0^{\infty} [\boldsymbol{R}(t,u)]^{(b)} dt,\ u=1,2,...,z, \tag{16}$$

$[\boldsymbol{R}(t,u)]^{(b)}$, $u=1,2,...,z$, $b=1,2,...,\nu$, are defined by (12) and p_b are given by (3). Since the relationships between the system unconditional lifetimes $\overline{T}(u)$ in the particular reliability states and the system unconditional lifetimes $T(u)$ in the reliability state subsets can be expressed by

$$\overline{T}(u) = T(u) - T(u+1),\ u=0,1,...,z-1,$$
$$\overline{T}(z) = T(z),$$

then we get the following formulae for the mean values of the unconditional lifetimes of the system in particular reliability states

$$\overline{\mu}(u) = \mu(u) - \mu(u+1),\ u=0,1,...,z-1,$$
$$\overline{\mu}(z) = \mu(z), \tag{17}$$

where $\mu(u)$, $u = 0,1, ..., z$, are given by (15).

Moreover, if $s(t)$ is the system reliability state at he moment t, $t \in <0,\infty)$, and r, $r \in \{1,2, ..., z\}$, is the system critical reliability state, then the system risk function

$$\boldsymbol{r}(t) = P(s(t) < r \mid s(0) = z) = P(T(r) \leq t),\ t \in <0, \infty),$$

defined as the probability that the system is in the subset of states worse than the critical state r, $r \in \{1, ..., z\}$ while it was in the state z at the moment $t = 0$ is given by (Kołowrocki & Soszyńska-Budny 2011)

$$\boldsymbol{r}(t) = 1 - \boldsymbol{R}(t,r),\ t \in <0,\infty), \tag{18}$$

where $\boldsymbol{R}(t,r)$ is the coordinate of the system unconditional reliability function given by (14) for $u = r$ and if τ is the moment when the system risk function exceeds a permitted level δ, then

$$\tau = \boldsymbol{r}^{-1}(\delta), \tag{19}$$

where $\boldsymbol{r}^{-1}(t)$, if it exists, is the inverse function of the risk function $\boldsymbol{r}(t)$ given by (18).

3.2 *Example—continuation*

Taking into account the efficiency of the considered in Section 2 port grain transportation system we distinguish the following three reliability states of the systems and its components:

state 2—the state ensuring the largest efficiency of the system and its conveyors,
state 1—the state ensuring less efficiency of the system caused by throwing grain off the system conveyors,
state 0—the state involving failure of the system.

The considered here transportation system analysis of its varying in time operation process is analyzed in this paper Section 2.2. In Section 2.2, it is assumed that the system reliability structure and its subsystems and components reliability depend on its changing in time operation states. Considering the assumptions and agreements of these sections, we assume that its subsystems S_υ, $\upsilon = 1,2,3,4$, are composed of three-state, i.e. z = 3, components $E_{ij}^{(\upsilon)}$, $\upsilon = 1,2,3,4$, having the conditional reliability functions given by the vector

$$[R_{ij}^{(\upsilon)}(t,\cdot)]^{(b)} = [1,[R_{ij}^{(\upsilon)}(t,1)]^{(b)},[R_{ij}^{(\upsilon)}(t,2)]^{(b)}],$$
$$b = 1,2,3,$$

with the exponential co-ordinates

$$[R_{ij}^{(\upsilon)}(t,1)]^{(b)} = \exp[-[\lambda_{ij}^{(\upsilon)}(1)]^{(b)}t],$$
$$[R_{ij}^{(\upsilon)}(t,2)]^{(b)} = \exp[-[\lambda_{ij}^{(\upsilon)}(2)]^{(b)}t],$$

different at various operation states z_b, $b = 1,2,3$, and with the intensities of departure from the reliability state subsets $\{1,2\}$, $\{2\}$, respectively

$$[\lambda_{ij}^{(\upsilon)}(1)]^{(b)}, [\lambda_{ij}^{(\upsilon)}(2)]^{(b)},\ b = 1,2,3.$$

The influence of the system operation states changing on the changes of the system reliability structure and its components reliability functions is as follows.

At the system operation state z_1, the system is a series system with the structure showed in Figure 2, composed of four series-parallel subsystems S_1, S_2, S_3 and S_4 illustrated respectively in Figure 1.

The subsystem S_1 with the structure showed in Figure 1, consists of two identical belt conveyors forming series subsystems ($k^{(1)} = 2$) each composed of 129 components ($l_1^{(1)} = 129$, $l_2^{(1)} = 129$) with the exponential reliability functions. In both series subsystems of the subsystem S_1 there are respectively:

– 1 belt marked by $E_{ij}^{(1)}$, $i = 1,2$, $j = 1$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(1)} = \exp[-0.0125t],$$
$$[R_{ij}^{(1)}(t,2)]^{(1)} = \exp[-0.0150t],\ t \geq 0,\ i = 1,2,\ j = 1;$$

– 2 drums marked by $E_{ij}^{(1)}$, $i = 1,2$, $j = 2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(1)} = \exp[-0.0015t],$$
$$[R_{ij}^{(1)}(t,2)]^{(1)} = \exp[-0.0020t],\ t \geq 0,\ i = 1,2,\ j = 2,3;$$

– 117 channeled rollers marked by $E_{ij}^{(1)}$, $i = 1,2$, $j = 4,5, ..., 120$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(1)} = \exp[-0.005t],$$
$$[R_{ij}^{(1)}(t,2)]^{(1)} = \exp[-0.010t],\ t \geq 0,$$
$$i = 1,2,\ j = 4,5, ..., 120;$$

– 9 supporting rollers marked by $E_{ij}^{(1)}$, $i = 1,2$, $j = 121,122, ..., 129$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(1)} = \exp[-0.004t],$$
$$[R_{ij}^{(1)}(t,2)]^{(1)} = \exp[-0.008t],\ t \geq 0,$$
$$i = 1,2,\ j = 121,122, ..., 129.$$

Thus, at the operation state z_1, the subsystem S_1 is a three-state series-parallel system with its structure shape parameters $k^{(1)} = 2$, $l_1^{(1)} = 129$, $l_2^{(1)} = 129$, and

according to Proposition 9.1 given in [24], its conditional reliability function is given by

$$[\boldsymbol{R}^{(1)}(t,\cdot)]^{(1)} = [1,[\boldsymbol{R}^{(1)}(t,1)]^{(1)},[\boldsymbol{R}^{(1)}(t,2)]^{(1)}],\ t \geq 0, \tag{20}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(1)}(t,1)]^{(1)} &= 2\exp[-0.6365t] - \exp[-1.2730t],\\ [\boldsymbol{R}^{(1)}(t,2)]^{(1)} &= 2\exp[-1.2610t] - \exp[-2.5220t].\end{aligned} \tag{21}$$

The subsystem S_2 with the structure showed in Figure 1, consists of three identical bucket elevators forming series subsystems ($k^{(1)} = 3$) each composed of 743 components ($l_1^{(1)} = 743$, $l_2^{(1)} = 743$, $l_3^{(1)} = 743$) with the exponential reliability functions. In each series subsystems of the subsystem S_2 there are respectively:

– 1 belt marked by $E_{ij}^{(2)}$, $i = 1,2,3$, $j = 1$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(1)} = \exp[-0.025t],$$
$$[R_{ij}^{(2)}(t,2)]^{(1)} = \exp[-0.030t],\ t \geq 0,\ i = 1,2,3,\ j = 1;$$

– 2 drums marked by $E_{ij}^{(2)}$, $i = 1,2,3$, $j = 2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(1)} = \exp[-0.0015t],$$
$$[R_{ij}^{(2)}(t,2)]^{(1)} = \exp[-0.0020t],\ t \geq 0,\ i = 1,2,3,\ j = 2,3;$$

– 740 buckets marked by $E_{ij}^{(2)}$, $i = 1,2,3$, $j = 4,5, ..., 743$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(1)} = \exp[-0.030t],$$
$$[R_{ij}^{(2)}(t,2)]^{(1)} = \exp[-0.035t],\ t \geq 0,$$
$$i = 1,2,3,\ j = 4,5, ..., 743.$$

Thus, at the operation state z_1, the subsystem S_2 is a three-state series-parallel system with its structure shape parameters $k^{(1)} = 3$, $l_1^{(1)} = 743$, $l_2^{(1)} = 743$, $l_3^{(1)} = 743$, and according to Proposition 9.1 given in [24], its conditional reliability function is given by

$$[\boldsymbol{R}^{(2)}(t,\cdot)]^{(1)} = [1,[\boldsymbol{R}^{(2)}(t,1)]^{(1)},[\boldsymbol{R}^{(2)}(t,2)]^{(1)}],\ t \geq 0, \tag{22}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(2)}(t,1)]^{(1)} &= 3\exp[-22.2280t] - 3\exp[-44.4560t]\\ &\quad + \exp[-66.6840t],\\ [\boldsymbol{R}^{(2)}(t,2)]^{(1)} &= 3\exp[-25.9340t] - 3\exp[-51.8680t]\\ &\quad + \exp[-77.8020t],\end{aligned} \tag{23}$$

The subsystem S_3 with the structure showed in Figure 1, consists of two identical belt conveyors forming series subsystems ($k^{(1)} = 2$) each composed of 139 components ($l_1^{(1)} = 139$, $l_2^{(1)} = 139$) with the exponential reliability functions. In both series subsystems of the subsystem S_3 there are respectively:

– 1 belt marked by $E_{ij}^{(3)}$, $i = 1,2$, $j = 1$, with a reliability function co-ordinates

$$[\boldsymbol{R}_{ij}^{(3)}(t,1)]^{(1)} = \exp[-0.0125t],$$
$$[\boldsymbol{R}_{ij}^{(3)}(t,2)]^{(1)} = \exp[-0.0150t],\ t \geq 0,\ i = 1,2,\ j = 1;$$

– 2 drums marked by $E_{ij}^{(3)}$, $i = 1,2$, $j = 2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(1)} = \exp[-0.0015t],$$
$$[R_{ij}^{(3)}(t,2)]^{(3)} = \exp[-0.0020t],\ t \geq 0,\ i = 1,2,\ j = 2,3;$$

– 117 channeled rollers marked by $E_{ij}^{(3)}$, $i = 1,2$, $j = 4,5, ..., 120$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(1)} = \exp[-0.005t],$$
$$[R_{ij}^{(3)}(t,2)]^{(1)} = \exp[-0.010t],\ t \geq 0,$$
$$i = 1,2,\ j = 4,5, ..., 120;$$

– 19 supporting rollers marked by $E_{ij}^{(1)}$, $i = 1,2$, $j = 121,122, ..., 139$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(1)} = \exp[-0.004t],$$
$$[R_{ij}^{(3)}(t,2)]^{(1)} = \exp[-0.008t],\ t \geq 0,$$
$$i = 1,2,\ j = 121,122, ..., 139.$$

Thus, at the operation state z_1, the subsystem S_3 is a three-state series-parallel system with its structure shape parameters $k^{(1)} = 2$, $l_1^{(1)} = 139$, $l_2^{(1)} = 139$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(3)}(t,\cdot)]^{(1)} = [1,[\boldsymbol{R}^{(3)}(t,1)]^{(1)},[\boldsymbol{R}^{(3)}(t,2)]^{(1)}],\ t \geq 0, \tag{24}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(3)}(t,1)]^{(1)} &= 2\exp[-0.6765t] - \exp[-1.3530t],\\ [\boldsymbol{R}^{(3)}(t,2)]^{(1)} &= 2\exp[-1.3410t] - \exp[-2.6820t].\end{aligned} \tag{25}$$

The subsystem S_4 with the structure showed in Figure 3, consists of three chain conveyors forming series subsystems ($k^{(1)} = 3$), each composed of a wheel driving the belt, a reversible driving wheel and 160, 160 and 240 links respectively. Thus, two

conveyors have 162 components and the remaining one has 242 components ($l_1^{(1)} = 162$, $l_2^{(1)} = 162$, $l_3^{(1)} = 242$) what means that the subsystem is a non-homogeneous non-regular three-state series-parallel system with the exponential reliability functions. In two series subsystems of the subsystem S_4 there are respectively:

– 2 two driving wheels marked by $E_{ij}^{(4)}$, $i = 1,2$, $j = 2$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(1)} = \exp[-0.005t],$$
$$[R_{ij}^{(4)}(t,2)]^{(1)} = \exp[-0.006t],\ t \geq 0,\ i = 1,2,\ j = 2;$$

– 160 links marked by $E_{ij}^{(4)}$, $i = 1,2$, $j = 3,4, ..., 162$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(1)} = \exp[-0.012t],$$
$$[R_{ij}^{(4)}(t,2)]^{(1)} = \exp[-0.014t], t \geq 0,$$
$$i = 1,2, j = 3,4, ..., 162.$$

In the third series subsystems of the subsystem S_4 there are respectively:

– 2 two driving wheels marked by $E_{ij}^{(4)}$, $i = 3$, $j = 2$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(1)} = \exp[-0.022t],$$
$$[R_{ij}^{(4)}(t,2)]^{(1)} = \exp[-0.024t],\ t \geq 0,\ i = 3,\ j = 2;$$

– 240 links marked by $E_{ij}^{(4)}$, $i = 3$, $j = 3,4, ..., 242$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(1)} = \exp[-0.034t],$$
$$[R_{ij}^{(4)}(t,2)]^{(1)} = \exp[-0.040t],\ t \geq 0,$$
$$i = 3, j = 3,4, ..., 242.$$

Thus, at the operation state z_1, the subsystem S_4 is a three-state series-parallel system with its structure shape parameters $k^{(1)} = 3$, $l_1^{(1)} = 162$, $l_2^{(1)} = 162$, $l_3^{(1)} = 242$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(4)}(t,\cdot)]^{(1)} = [1,[\boldsymbol{R}^{(4)}(t,1)]^{(1)},[\boldsymbol{R}^{(4)}(t,2)]^{(1)}],\ t \geq 0, \tag{26}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(4)}(t,1)]^{(1)} &= 2\exp[-1.930t] - 2\exp[-10.134t] \\ &\quad - \exp[-3.860t] + \exp[-12.064t] \\ &\quad + \exp[-8.204t], \\ [\boldsymbol{R}^{(4)}(t,2)]^{(1)} &= 2\exp[-2.252t] - 2\exp[-11.900t] \\ &\quad - \exp[-4.504t] + \exp[-14.152t] \\ &\quad + \exp[-9.648t].\end{aligned} \tag{27}$$

Considering that the system at the operation state z_1 is a three-state series system composed of subsystems S_1, S_2, S_3 and S_4, after applying the formulae appearing after Definition 3.4 given in (Kołowrocki 2014) and the results (20)-(21), (22)-(23), (24)-(25) and (26)-(27), its conditional reliability function is given by

$$[\boldsymbol{R}(t,\cdot)]^{(1)} = [1,[\boldsymbol{R}(t,1)]^{(1)},[\boldsymbol{R}(t,2)]^{(1)}],\ t \geq 0, \tag{28}$$

where

$$\begin{aligned}[R(t,1)]^{(1)} &= 24\exp[-25.4710t] - 24\exp[-47.6990t] \\ &\quad + 8\exp[-69.9270t] - 12\exp[-26.1075t] \\ &\quad + 12\exp[-48.3355t] - 4\exp[-70.5635t] \\ &\quad - 12\exp[-26.1475t] + 12\exp[-48.3755t] \\ &\quad - 4\exp[-70.6035t] + 6\exp[-26.7840t] \\ &\quad - 6\exp[-49.0120t] + 2\exp[-71.2400t] \\ &\quad - 24\exp[-33.6750t] + 24\exp[-55.9030t] \\ &\quad - 8\exp[-78.1310t] + 12\exp[-34.3115t] \\ &\quad - 12\exp[-56.5395t] + 4\exp[-78.7675t] \\ &\quad + 12\exp[-34.3515t] - 12\exp[-56.5795t] \\ &\quad + 4\exp[-78.8075t] - 6\exp[-34.9880t] \\ &\quad + 6\exp[-57.2160t] - 2\exp[-79.4440t] \\ &\quad - 12\exp[-27.4010t] + 12\exp[-49.6290t] \\ &\quad - 4\exp[-71.8570t] + 6\exp[-28.0375t] \\ &\quad - 6\exp[-50.2655t] + 2\exp[-72.4935t] \\ &\quad + 6\exp[-28.0775t] - 6\exp[-50.3055t] \\ &\quad + 2\exp[-72.5335t] - 3\exp[-28.7140t] \\ &\quad + 3\exp[-50.9420t] - \exp[-73.1700t] \\ &\quad + 12\exp[-35.6050t] - 12\exp[-57.8330t] \\ &\quad + 4\exp[-80.0610t] - 6\exp[-36.2415t] \\ &\quad + 6\exp[-58.4695t] - 2\exp[-80.9750t] \\ &\quad - 6\exp[-36.2815t] + 6\exp[-58.5095t] \\ &\quad - 2\exp[80.7375t] + 3\exp[-36.9180t] \\ &\quad - 3\exp[-59.1460t] + \exp[-81.3740t] \\ &\quad + 12\exp[-31.7450t] - 6\exp[-32.4215t] \\ &\quad - 12\exp[-53.9730t] + 6\exp[-54.6495t] \\ &\quad + 4\exp[-76.2010t] - 2\exp[-76.8775t] \\ &\quad - 6\exp[-32.3815t] + 3\exp[-33.0580t] \\ &\quad + 6\exp[-54.6095t] - 3\exp[-55.2860t] \\ &\quad - 2\exp[-76.8375t] + \exp[-77.5140t],\end{aligned}$$

$$\begin{aligned}[R(t,2)]^{(1)} &= 24\exp[-30.7880t] - 24\exp[-56.7220t] \\ &\quad + 8\exp[-82.6560t] - 12\exp[-32.0490t] \\ &\quad + 12\exp[-57.9830t] - 4\exp[-83.9170t] \\ &\quad - 12\exp[-32.1290t] + 12\exp[-58.0630t] \\ &\quad - 4\exp[-83.9970t] + 6\exp[-33.3900t] \\ &\quad - 6\exp[-59.3240t] + 2\exp[-86.1690t] \\ &\quad - 24\exp[-40.4360t] + 24\exp[-66.3700t] \\ &\quad - 8\exp[-92.3040t] + 12\exp[-41.6970t] \\ &\quad - 12\exp[-67.6310t] + 4\exp[-93.5650t] \\ &\quad + 12\exp[-41.7770t] - 12\exp[-67.7110t] \\ &\quad + 4\exp[-93.6450t] - 6\exp[-43.0380t] \\ &\quad + 6\exp[-68.9720t] - 2\exp[-94.9060t] \\ &\quad - 12\exp[-33.0400t] + 12\exp[-58.9740t]\end{aligned}$$

$$
\begin{aligned}
&- 4\exp[-84.9080t] + 6\exp[-34.3010t] \\
&- 6\exp[-60.2350t] + 2\exp[-85.2580t] \\
&+ 6\exp[-34.3810t] - 6\exp[-60.3150t] \\
&+ 2\exp[-86.2490t] - 3\exp[-35.6420t] \\
&+ 3\exp[-61.5760t] - \exp[-87.5100t] \\
&+ 12\exp[-42.6880t] - 12\exp[-68.6220t] \\
&+ 4\exp[-94.5560t] - 6\exp[-43.9490t] \\
&+ 6\exp[-69.8830t] - 2\exp[-95.8170t] \\
&- 6\exp[-44.0290t] + 6\exp[-69.9630t] \\
&- 2\exp[-95.8970t] + 3\exp[-45.2900t] \\
&- 3\exp[-71.2240t] + \exp[-97.1580t] \\
&+ 12\exp[-38.1840t] - 6\exp[-39.5250t] \\
&- 12\exp[-64.1180t] + 6\exp[-65.4590t] \\
&+ 4\exp[-90.0520t] - 2\exp[-91.3930t] \\
&- 6\exp[-39.4450t] + 3\exp[-40.7860t] \\
&+ 6\exp[-65.3790t] - 3\exp[-66.7200t] \\
&- 2\exp[-91.3130t] + \exp[-92.6540t], \qquad (29)
\end{aligned}
$$

The expected values and standard deviations of the system conditional lifetimes in the reliability state subsets {1,2}, {2} at the operation state z_1, calculated from the results given by (29), according to (16), respectively are:

$$
\begin{aligned}
\mu_1(1) &= \int_0^\infty [\mathrm{R}(t,1)]^{(1)}\,dt \cong 0.0813 \text{ month}, \\
\mu_1(2) &= \int_0^\infty [\mathrm{R}(t,2)]^{(1)}\,dt \cong 0.0691 \text{ month}. \qquad (30)
\end{aligned}
$$

At the system operation state z_2, the system is a series system with the structure showed in Figure 2, composed of four subsystems S_1, S_2, S_3 and S_4 illustrated respectively in Figure 3.

The subsystem S_1 with the structure showed in Figure 3, consists of one belt conveyor forming a series systems ($k^{(2)} = 1$) composed of 129 components ($l_1^{(2)} = 129$) with the exponential reliability functions. In the series system of the subsystem S_1 there are respectively:

– 1 belt marked by $E_{ij}^{(1)}$, $i = 1$, $j = 1$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(1)}(t,1)]^{(2)} = \exp[-0.0110t], \\
&[R_{ij}^{(1)}(t,2)]^{(2)} = \exp[-0.0120t],\ t \geq 0,\ i = 1,\ j = 1;
\end{aligned}
$$

– 2 drums marked by $E_{ij}^{(1)}$ $i = 1$, $j = 2,3$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(1)}(t,1)]^{(2)} = \exp[-0.0010t], \\
&[R_{ij}^{(1)}(t,2)]^{(2)} = \exp[-0.0012t],\ t \geq 0,\ i = 1,21,\ j = 2,3;
\end{aligned}
$$

– 117 channeled rollers marked by $E_{ij}^{(1)}$, $i = 1$, $j = 4,5, ..., 120$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(1)}(t,1)]^{(2)} = \exp[-0.003t], \\
&[R_{ij}^{(1)}(t,2)]^{(2)} = \exp[-0.006t],\ t \geq 0, \\
&i = 1,\ j = 4,5, ..., 120;
\end{aligned}
$$

– 9 supporting rollers marked by $E_{ij}^{(1)}$, $i = 1$, $j = 121,122, ..., 129$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(1)}(t,1)]^{(2)} = \exp[-0.002t], \\
&[R_{ij}^{(1)}(t,2)]^{(2)} = \exp[-0.003t],\ t \geq 0, \\
&i = 1,\ j = 121,122, ..., 129.
\end{aligned}
$$

Thus, at the operation state z_2, the subsystem S_1 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(2)} = 1$, $l_1^{(2)} = 129$, and according to the formulae appearing after according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$
[\boldsymbol{R}^{(1)}(t,\cdot)]^{(2)} = [1,[\boldsymbol{R}^{(1)}(t,1)]^{(2)},[\boldsymbol{R}^{(1)}(t,2)]^{(2)},\ t \geq 0, \qquad (31)
$$

where

$$
\begin{aligned}
&[\boldsymbol{R}^{(1)}(t,1)]^{(2)} = \exp[-0.3710t], \\
&[\boldsymbol{R}^{(1)}(t,2)]^{(2)} = \exp[-0.7434t]. \qquad (32)
\end{aligned}
$$

The subsystem S_2 with the structure showed in Figure 3, consists of two identical bucket elevators forming series subsystems ($k^{(2)} = 2$) each composed of 743 components ($l_1^{(2)} = 743$, $l_2^{(2)} = 743$) with the exponential reliability functions. In each series subsystems of the subsystem S_2 there are respectively:

– 1 belt marked by $E_{ij}^{(2)}$, $i = 1,2$, $j = 1$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(2)}(t,1)]^{(2)} = \exp[-0.020t], \\
&[R_{ij}^{(2)}(t,2)]^{(2)} = \exp[-0.024t],\ t \geq 0,\ i = 1,2,\ j = 1;
\end{aligned}
$$

– 2 drums marked by $E_{ij}^{(2)}$ $i = 1,2$, $j = 2,3$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(2)}(t,1)]^{(2)} = \exp[-0.0012t], \\
&[R_{ij}^{(2)}(t,2)]^{(2)} = \exp[-0.0014t],\ t \geq 0,\ i = 1,2,\ j = 2,3;
\end{aligned}
$$

– 740 buckets marked by $E_{ij}^{(2)}$ $i = 1,2$, $j = 4,5, ..., 743$, with a reliability function co-ordinates

$$
\begin{aligned}
&[R_{ij}^{(2)}(t,1)]^{(2)} = \exp[-0.022t], \\
&[R_{ij}^{(2)}(t,2)]^{(2)} = \exp[-0.025t],\ t \geq 0, \\
&i = 1,2,\ j = 4,5, ..., 743.
\end{aligned}
$$

Thus, at the operation state z_2, the subsystem S_2 is a three-state series-parallel system with its

structure shape parameters $k^{(2)}=2$, $l_1^{(2)}=743$, $l_2^{(2)}=743$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(2)}(t,\cdot)]^{(2)}=[1,[\boldsymbol{R}^{(2)}(t,1)]^{(2)},[\boldsymbol{R}^{(2)}(t,2)]^{(2)}], \tag{33}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(2)}(t,1)]^{(2)}&=2\exp[-16.324t]-\exp[-32.648t],\\ [\boldsymbol{R}^{(2)}(t,2)]^{(2)}&=2\exp[-18.552t]-\exp[-37.104t].\end{aligned} \tag{34}$$

The subsystem S_3 with the structure showed in Figure 3, consists of one belt conveyors forming a series system ($k^{(1)}=1$) composed of 139 components ($l_1^{(2)}=139$) with the exponential reliability functions. In the series system of the subsystem S_3 there are respectively:

– 1 belt marked by $E_{ij}^{(1)}$, $i=1$, $j=1$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(3)}(t,1)]^{(2)}=\exp[-0.0110t],\\ &[R_{ij}^{(2)}(t,2)]^{(2)}=\exp[-0.0120t],\ t\ge 0,\ i=1,\ j=1;\end{aligned}$$

– 2 drums marked by $E_{ij}^{(1)}$, $i=1$, $j=2,3$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(3)}(t,1)]^{(2)}=\exp[-0.0010t],\\ &[R_{ij}^{(3)}(t,2)]^{(2)}=\exp[-0.0012t],\ t\ge 0,\ i=1,21,\ j=2,3;\end{aligned}$$

– 117 channeled rollers marked by $E_{ij}^{(1)}$, $i=1$, $j=4,5,...,120$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(3)}(t,1)]^{(2)}=\exp[-0.003t],\\ &[R_{ij}^{(3)}(t,2)]^{(2)}=\exp[-0.006t],\ t\ge 0,\\ &i=1,\ j=4,5,...,120;\end{aligned}$$

– 19 supporting rollers marked by $E_{ij}^{(1)}$, $i=1$, $j=121,122,...,139$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(3)}(t,1)]^{(2)}=\exp[-0.002t],\\ &[R_{ij}^{(3)}(t,2)]^{(2)}=\exp[-0.003t],\ t\ge 0,\\ &i=1,\ j=121,122,...,129.\end{aligned}$$

Thus, at the operation state z_2, the subsystem S_3 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(1)}=1$, $l_1^{(2)}=139$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(3)}(t,\cdot)]^{(2)}=[1,[\boldsymbol{R}^{(3)}(t,1)]^{(2)},[\boldsymbol{R}^{(3)}(t,2)]^{(2)}],\ t\ge 0, \tag{35}$$

where

$$\begin{aligned}&[\boldsymbol{R}^{(3)}(t,1)]^{(2)}=\exp[-0.3910t],\\ &[\boldsymbol{R}^{(3)}(t,2)]^{(2)}=\exp[-0.7734t],\end{aligned} \tag{36}$$

The subsystem S_4 with the structure showed in Figure 3, consists of three identical chain conveyors forming series subsystems ($k^{(2)}=2$), each composed of a wheel driving the belt, a reversible driving wheel and 160 links ($l_1^{(2)}=162$, $l_2^{(2)}=162$) what means that the subsystem is a non-homogeneous non-regular three-state series-parallel system with the exponential reliability functions. In the series subsystems of the subsystem S_4 there are respectively:

– 2 two driving wheels marked by $E_{ij}^{(4)}$, $i=1,2$, $j=2$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(4)}(t,1)]^{(2)}=\exp[-0.002t],\\ &[R_{ij}^{(4)}(t,2)]^{(2)}=\exp[-0.004t],\ t\ge 0,\ i=1,2,\ j=2;\end{aligned}$$

– 160 links marked by $E_{ij}^{(4)}$, $i=1,2$, $j=3,4,...,162$, with a reliability function co-ordinates

$$\begin{aligned}&[R_{ij}^{(4)}(t,1)]^{(2)}=\exp[-0.008t],\\ &[R_{ij}^{(4)}(t,2)]^{(2)}=\exp[-0.010t],\ t\ge 0,\\ &i=1,2,\ j=3,4,...,162.\end{aligned}$$

Thus, at the operation state z_2, the subsystem S_4 is a three-state series-parallel system with its structure shape parameters $k^{(2)}=2$, $l_1^{(2)}=162$, $l_2^{(2)}=162$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(4)}(t,\cdot)]^{(2)}=[1,[\boldsymbol{R}^{(4)}(t,1)]^{(2)},[\boldsymbol{R}^{(4)}(t,2)]^{(2)}], \tag{37}$$

where

$$\begin{aligned}[\boldsymbol{R}^{(4)}(t,1)]^{(2)}&=2\exp[-1.284t]-\exp[-2.5680t],\\ [\boldsymbol{R}^{(4)}(t,2)]^{(2)}&=2\exp[-1.608t]-\exp[-3.2160t].\end{aligned} \tag{38}$$

Considering that the system at the operation state z_2 is a three-state series system composed of subsystems S_1, S_2, S_3 and S_4, after applying the formulae appearing after Definition 3.4 given in (Kołowrocki 2014) and the results (31)-(32), (33)-(34), (35)-(36) and (37)-(38), its conditional reliability function is given by

$$[\boldsymbol{R}(t,\cdot)]^{(2)}=[1,[\boldsymbol{R}(t,1)]^{(2)},[\boldsymbol{R}(t,2)]^{(2)}],\ t\ge 0, \tag{39}$$

where

$$\begin{aligned}[\boldsymbol{R}(t,1)]^{(2)}&=4\exp[-18.380t]-2\exp[-34.694t]\\ &\quad-2\exp[-19.664t]+\exp[-35.978t],\\ [\boldsymbol{R}(t,2)]^{(2)}&=4\exp[-21.6768t]-2\exp[-40.2288t]\\ &\quad-2\exp[-23.2848t]+\exp[-41.8368t].\end{aligned} \tag{40}$$

The expected values and standard deviations of the system conditional lifetimes in the reliability state subsets {1,2}, {2} at the operation state z_2, calculated from the results given by (39)-(40), according to (16), respectively are:

$$\mu_2(1) = \int_0^\infty [\boldsymbol{R}(t,1)]^{(2)}\,dt \cong 0.0861 \text{ month},$$
$$\mu_2(2) = \int_0^\infty [\boldsymbol{R}(t,2)]^{(2)}\,dt \cong 0.0728 \text{ month}. \quad (41)$$

At the system operational state z_3, the system is a series system with the structure showed in Figure 2, composed of four subsystems S_1, S_2, S_3 and S_4 illustrated respectively in Figure 4.

The subsystem S_1 with the structure showed in Figure 3, consists of one belt conveyor forming a series systems ($k^{(3)} = 1$) composed of 129 components ($l_1^{(3)} = 129$) with the exponential reliability functions. In the series system of the subsystem S_1 there are respectively:

– 1 belt marked by $E_{ij}^{(1)}$, $i = 1$, $j = 1$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(3)} = \exp[-0.0100t],$$
$$[R_{ij}^{(1)}(t,2)]^{(3)} = \exp[-0.0105t],\ t \geq 0,\ i = 1,\ j = 1;$$

– 2 drums marked by $E_{ij}^{(1)}$, $i = 1$, $j = 2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(3)} = \exp[-0.0009t],$$
$$[R_{ij}^{(1)}(t,2)]^{(3)} = \exp[-0.0011t],\ t \geq 0,\ i = 1,\ j = 2,3;$$

– 117 channeled rollers marked by $E_{ij}^{(1)}$, $i = 1$, $j = 4,5, ..., 120$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(3)} = \exp[-0.002t],$$
$$[R_{ij}^{(1)}(t,2)]^{(3)} = \exp[-0.004t],\ t \geq 0,$$
$$i = 1, j = 4,5, ..., 120;$$

– 9 supporting rollers marked by $E_{ij}^{(1)}$, $i = 1$, $j = 121,122, ..., 129$, with a reliability function co-ordinates

$$[R_{ij}^{(1)}(t,1)]^{(3)} = \exp[-0.001t],$$
$$[R_{ij}^{(1)}(t,2)]^{(3)} = \exp[-0.002t],\ t \geq 0,$$
$$i = 1, j = 121,122, ..., 129.$$

Thus, at the operation state z_3, the subsystem S_1 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(3)} = 1$, $l_1^{(3)} = 129$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(1)}(t,\cdot)]^{(3)} = [1,[\boldsymbol{R}^{(1)}(t,1)]^{(3)},[\boldsymbol{R}^{(1)}(t,2)]^{(3)}],\ t \geq 0, \quad (42)$$

where

$$[\boldsymbol{R}^{(1)}(t,1)]^{(3)} = \exp[-0.2548t],$$
$$[\boldsymbol{R}^{(1)}(t,2)]^{(3)} = \exp[-0.4987t], \quad (43)$$

The subsystem S_2 with the structure showed in Figure 4, consists of one bucket elevator forming a series system ($k^{(3)} = 1$) composed of 743 components ($l_1^{(3)} = 743$) with the exponential reliability functions. In the series stem of the subsystem S_2 there are respectively:

– 1 belt marked by $E_{ij}^{(2)}$, $i = 1$, $j = 1$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(3)} = \exp[-0.018t],$$
$$[R_{ij}^{(2)}(t,2)]^{(2)} = \exp[-0.022t],\ t \geq 0,\ i = 1,\ j = 1;$$

– 2 drums marked by $E_{ij}^{(2)}$, $i = 1$, $j = 2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(3)} = \exp[-0.0011t],$$
$$[R_{ij}^{(2)}(t,2)]^{(3)} = \exp[-0.0013t],\ t \geq 0,\ i = 1,\ j = 2,3;$$

– 740 buckets marked by $E_{ij}^{(2)}$, $i = 1$, $j = 4,5, ..., 743$, with a reliability function co-ordinates

$$[R_{ij}^{(2)}(t,1)]^{(3)} = \exp[-0.020t],$$
$$[R_{ij}^{(2)}(t,2)]^{(2)} = \exp[-0.024t],\ t \geq 0,$$
$$i = 1, j = 4,5, ..., 743.$$

Thus, at the operation state z_3, the subsystem S_2 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(3)} = 1$, $l_1^{(3)} = 743$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(2)}(t,\cdot)]^{(3)} = [1,[\boldsymbol{R}^{(2)}(t,1)]^{(3)},[\boldsymbol{R}^{(2)}(t,2)]^{(3)}],\ t \geq 0, \quad (44)$$

where

$$[\boldsymbol{R}^{(2)}(t,1)]^{(3)} = \exp[-14.840t],$$
$$[\boldsymbol{R}^{(2)}(t,2)]^{(3)} = \exp[-17.808t]. \quad (45)$$

The subsystem S_3 with the structure showed in Figure 4, consists of one belt conveyors forming a series system ($k^{(3)} = 1$) composed of 139 components ($l_1^{(3)} = 139$) with the exponential reliability functions. In the series system of the subsystem S_3 there are respectively:

– 1 belt marked by $E_{ij}^{(3)}$, $i=1,\ j=1$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(3)} = \exp[-0.0100t],$$
$$[R_{ij}^{(3)}(t,2)]^{(3)} = \exp[-0.0105t],\ t \geq 0,\ i=1,\ j=1;$$

– 2 drums marked by $E_{ij}^{(3)}$, $i=1,\ j=2,3$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(3)} = \exp[-0.0009t],$$
$$[R_{ij}^{(3)}(t,2)]^{(3)} = \exp[-0.0011t], t \geq 0,\ i=1,\ j=2,3;$$

– 117 channeled rollers marked by $E_{ij}^{(3)}$, $i=1,\ j=4,5,...,120$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(3)} = \exp[-0.002t],$$
$$[R_{ij}^{(3)}(t,2)]^{(3)} = \exp[-0.004t], t \geq 0,$$
$$i=1,\ j=4,5,...,120;$$

– 19 supporting rollers marked by $E_{ij}^{(3)}$, $i=1,\ j=121,122,...,129$, with a reliability function co-ordinates

$$[R_{ij}^{(3)}(t,1)]^{(3)} = \exp[-0.001t],$$
$$[R_{ij}^{(3)}(t,2)]^{(3)} = \exp[-0.002t],\ t \geq 0,$$
$$i=1, j=121,122,...,129.$$

Thus, at the operation state z_3, the subsystem S_3 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(3)}=1$, $l_1^{(3)}=139$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(3)}(t,\cdot)]^{(3)} = [1,[\boldsymbol{R}^{(3)}(t,1)]^{(3)},[\boldsymbol{R}^{(3)}(t,2)]^{(3)}],\ t \geq 0, \tag{46}$$

where

$$[\boldsymbol{R}^{(3)}(t,1)]^{(3)} = \exp[-0.2648t],$$
$$[\boldsymbol{R}^{(3)}(t,2)]^{(3)} = \exp[-0.5187t]. \tag{47}$$

The subsystem S_4 with the structure showed in Figure 4, consists of on chain conveyor forming a series system ($k^{(3)}=1$), composed of a wheel driving the belt, a reversible driving wheel and 160 links ($l_1^{(3)}=162$) with the exponential reliability functions. In the series system of the subsystem S_4 there are respectively:

– 2 two driving wheels marked by $E_{ij}^{(4)}$, $i=1,\ j=2$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(3)} = \exp[-0.001t],$$
$$[R_{ij}^{(4)}(t,2)]^{(3)} = \exp[-0.003t],\ t \geq 0,\ i=1,\ j=2;$$

– 160 links marked by $E_{ij}^{(4)}$, $i=1,\ j=3,4,...,162$, with a reliability function co-ordinates

$$[R_{ij}^{(4)}(t,1)]^{(3)} = \exp[-0.007t],$$
$$[R_{ij}^{(4)}(t,2)]^{(3)} = \exp[-0.009t],\ t \geq 0,$$
$$i=1, j=3,4,...,162.$$

Thus, at the operation state z_3, the subsystem S_4 is a three-state series-parallel system (a series system) with its structure shape parameters $k^{(3)}=1$, $l_1^{(3)}=162$, and according to Proposition 9.1 given in (Kołowrocki 2014), its conditional reliability function is given by

$$[\boldsymbol{R}^{(4)}(t,\cdot)]^{(3)} = [1,[\boldsymbol{R}^{(4)}(t,1)]^{(3)},[\boldsymbol{R}^{(4)}(t,2)]^{(3)}],\ t \geq 0, \tag{48}$$

where

$$[\boldsymbol{R}^{(4)}(t,1)]^{(3)} = \exp[-1.122t]$$
$$[\boldsymbol{R}^{(4)}(t,2)]^{(3)} = \exp[-1.446t] \tag{49}$$

Considering that the system at the operation state z_3 is a three-state series system composed of subsystems S_1, S_2, S_3 and S_4, after applying the formulae appearing after Definition 3.4 in (Kołowrocki 2014) and the results (42)-(43), (44)-(45), (46)-(47) and (48)-(49), its conditional reliability function is given by

$$[\boldsymbol{R}(t,\cdot)]^{(3)} = [1,[\boldsymbol{R}(t,1)]^{(3)},[\boldsymbol{R}(t,2)]^{(3)}],\ t \geq 0, \tag{50}$$

where

$$[\boldsymbol{R}(t,1)]^{(3)} = \exp[-16.4816t],$$
$$[\boldsymbol{R}(t,2)]^{(3)} = \exp[-20.2714t]. \tag{51}$$

The expected values and standard deviations of the system conditional lifetimes in the reliability state subsets {1,2}, {2} at the operation state z_3, calculated from the results given by (50)-(51), according to (16), respectively are:

$$\mu_3(1) = \int_0^\infty [\boldsymbol{R}(t,1)]^{(3)}\,dt / \cong 0.0607 \text{ month},$$
$$\mu_3(2) = \int_0^\infty [\boldsymbol{R}(t,2)]^{(3)}\,dt4 \cong 0.0493 \text{ month}. \tag{52}$$

In the case when the system operation time is large enough its unconditional three-state reliability function is given by the vector

$$\boldsymbol{R}(t,\cdot) = [1,\boldsymbol{R}(t,1),\boldsymbol{R}(t,2)]\ t \geq 0, \tag{53}$$

where according to (14) and considering the system operation process transient probabilities at the

operation states determined by (10), the vector coordinates are given respectively by

$$\begin{aligned}\boldsymbol{R}(t,1) &= p_1[\boldsymbol{R}(t,1)]^{(1)} + p_2[\boldsymbol{R}(t,1)]^{(2)} + p_3[\boldsymbol{R}(t,1)]^{(3)} \\ &= 0.530\cdot[\boldsymbol{R}(t,1)]^{(1)} + 0.109\cdot[\boldsymbol{R}(t,1)]^{(2)} \\ &\quad + 0.361\cdot[\boldsymbol{R}(t,1)]^{(3)} \ \text{for } t \ge 0, \\ \boldsymbol{R}(t,2) &= p_1[\boldsymbol{R}(t,2)]^{(1)} + p_2[\boldsymbol{R}(t,2)]^{(2)} + p_3[\boldsymbol{R}(t,2)]^{(3)} \\ &= 0.530\cdot[\boldsymbol{R}(t,2)]^{(1)} + 0.109\cdot[\boldsymbol{R}(t,2)]^{(2)} \\ &\quad + 0.361\cdot[\boldsymbol{R}(t,2)]^{(3)} \ \text{for } t \ge 0,\end{aligned} \tag{54}$$

where the reliability functions $[\boldsymbol{R}(t,1)]^{(1)}$, $[\boldsymbol{R}(t,1)]^{(2)}$, $[\boldsymbol{R}(t,1)]^{(3)}$, $[\boldsymbol{R}(t,2)]^{(1)}$, $[\boldsymbol{R}(t,2)]^{(2)}$, $[\boldsymbol{R}(t,2)]^{(3)}$ are given by (29), (40), (51).

In the Table 1, the values of the coordinates of the port grain transportation system unconditional reliability function $\boldsymbol{R}(t,\cdot)$ given by (53)-(54) are presented.

Table 1. The values of the port grain transportation system unconditional reliability function coordinates.

t	$R(t,1)$	$R(t,2)$
0.00	1.0000	1.0000
0.02	0.8638	0.8302
0.04	0.6884	0.6191
0.06	0.5133	0.4259
0.08	0.3665	0.2793
0.10	0.2549	0.1782
0.12	0.1745	0.1121
0.14	0.1184	0.0699
0.16	0.0800	0.0435
0.18	0.0540	0.0271
0.20	0.0364	0.0169
0.22	0.0246	0.0106
0.24	0.0167	0.0066
0.26	0.0113	0.0042
0.28	0.0077	0.0027
0.30	0.0053	0.0017
0.32	0.0036	0.0011
0.34	0.0025	0.0007
0.36	0.0017	0.0004
0.38	0.0012	0.0003
0.40	0.0008	0.0002
0.42	0.0006	0.0001
0.43	0.0005	0.0001
0.44	0.0004	0.0001
0.45	0.0003	0.0001
0.46	0.0003	0.0001
0.48	0.0002	0.0000
0.50	0.0001	0.0000
0.52	0.0001	0.0000
0.54	0.0001	0.0000
0.56	0.0000	0.0000

The graph of the three-state port grain transportation system unconditional reliability function is illustrated in Figure 5.

The expected value of the system unconditional lifetime in the reliability state subsets {1,2}, {2}, calculated according to (15) from the results given by (30), (41), (52) and (10), is

$$\begin{aligned}\mu(1) &= p_1\mu_1(1) + p_2\mu_2(1) + p_3\mu_3(1) \\ &= 0.530\cdot 0.0813 + 0.109\cdot 0.0861 \\ &\quad + 0.361\cdot 0.0607 \cong 0.0744 \text{ year}, \\ \mu(2) &= p_1\mu_1(2) + p_2\mu_2(2) + p_3\mu_3(2) \\ &= 0.530\cdot 0.0691 + 0.109\cdot 0.0728 \\ &\quad + 0.361\cdot 0.0493 \cong 0.0624 \text{ month}.\end{aligned} \tag{55}$$

Further, considering (17) and (55), the mean values of the unconditional lifetimes in the particular reliability states 1, 2, respectively are:

$$\begin{aligned}\bar{\mu}(1) &= \mu(1) - \mu(2) = 0.0120 \text{ month}, \\ \bar{\mu}(2) &= \mu(2) = 0.0624 \text{ month}.\end{aligned} \tag{56}$$

Since the critical reliability state is $r = 1$, then the system risk function, according to (18), is given by

$$r(t) = 1 - \boldsymbol{R}(t,1), \tag{57}$$

where $R(t,1)$ is are given by (54).

Hence, by (19), the moment when the system risk function exceeds a permitted level, for instance $\delta = 0.05$, is

$$\tau = r^{-1}(\delta) \cong 0.0100. \tag{58}$$

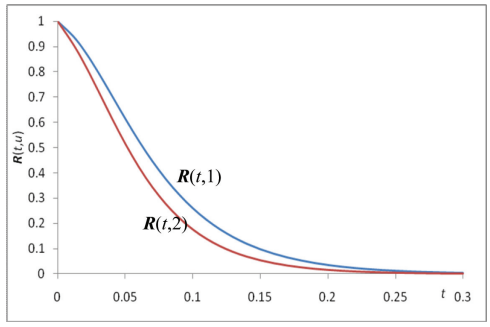


Figure 5. The graph of the port grain transportation system reliability function $\boldsymbol{R}(t,\cdot)$ coordinates.

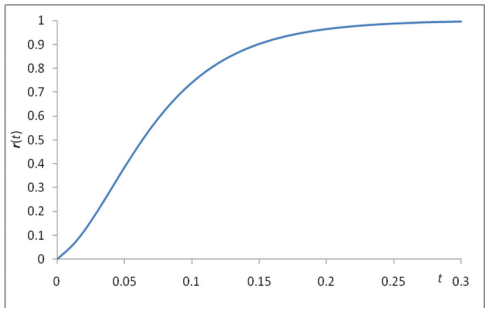


Figure 6. The graph of the port grain transportation system risk function $\boldsymbol{r}(t)$.

4 CONCLUSIONS

The integrated general model of complex systems' reliability, linking their reliability models and their operation processes models and considering variable at different operation states their reliability structures and their components reliability parameters is constructed and applied to the reliability evaluation of the port grain transportation system composed of three series-parallel subsystems linked in series. The predicted reliability characteristics of the considered system operating at the variable conditions are different from those determined for this system operating at constant conditions. This fact justifies the sensibility of considering real systems at the variable operation conditions that is appearing out in a natural way from practice. This approach, upon the good accuracy of the systems' operation processes and the systems' components reliability parameters identification, makes their reliability prediction more precise.

REFERENCES

Ferreira, F. and Pacheco, A., 2007. Comparison of level-crossing times for Markov and semi-Markov processes. *Statistics & Probability Letters,* 77(2): 151–157.

Glynn, P.W. and Haas P.J., 2006. Laws of large numbers and functional central limit theorems for generalized semi-Markov processes. *Stochastic Models,* 22(2): 201–231.

Grabski, F., 2002. Semi-Markov Models of Systems Reliability and Operations. Monograph. Warsaw: System Research Institute, Polish Academy of Science.

Kołowrocki, K., 2008. Reliability and risk analysis of multi-state systems with degrading components. *Proc. Summer Safety & Reliability Seminars,* 2(2): 205–216.

Kołowrocki, K., 2006. Reliability and risk evaluation of complex systems in their operation processes. *International Journal of Materials and Structural Reliability,* 4(2): 129–147.

Kołowrocki, K., 2014. *Reliability of Large and Complex Systems*. Elsevier.

Kołowrocki, K. and Soszyńska, J., 2006. Reliability and availability of complex systems. *Quality and Reliability Engineering International,* 22(1): 79–99.

Kołowrocki, K. and Soszyńska, J., 2010. Reliability, availability and safety of complex technical systems: modeling—identification—prediction—optimization. *Journal of Polish Safety and Reliability Association, Summer Safety & Reliability Seminar*s, 1(1): 133–158.

Kołowrocki, K. and Soszyńska-Budny, J., 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling-Identification-Prediction-Optimization. Springer.

Limnios, N. and Oprisan, G., 2001. Semi-Markov Processes and Reliability. Boston: Birkhauser.

Mercier, S. 2008. Numerical bounds for semi-Markovian quantities and application to reliability. *Methodology* and *Computing in Applied Probability,* 10(2): 179–198.

Soszyńska, J., 2007. Systems reliability analysis in variable operation conditions. International. *International Journal of Reliability, Quality and Safety Engineering,* 14(6): 617–634.

Soszyńska, J., Kołowrocki, K., Blokus-Roszkowska, A. and Guze, S., 2010. Prediction of complex technical systems operation processes. *Journal of Polish Safety and Reliability Association, Summer Safety & Reliability Seminar*s, 1(2): 379–510.

Xue, J., 1985. On multi-state system analysis. *IEEE Transactions* on *Reliability,* 34: 329–337.

Xue, J. and Yang, K., 1995. Dynamic reliability analysis of coherent multi-state systems. *IEEE Transactions* on *Reliability,* 4(44): 683–688.

Xue J. and Yang, K., 1995. Symmetric relations in multi-state systems. *IEEE Transactions* on *Reliability,* 4(44): 689–693.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability optimization of complex port transportation system

K. Kołowrocki & J. Soszyńska-Budny
Department of Mathematics, Maritime University, Gdynia, Poland

ABSTRACT: The method based on the results of the joint model linking a semi-Markov modelling of the system operation process with a multistate approach to system reliability and the linear programming are proposed to the operation and reliability optimization of complex technical systems at the variable operation conditions. The method consists in determining the optimal values of limit transient probabilities at the system operation states that maximize the system lifetimes in the reliability state subsets. The proposed method is applied to the operation and reliability optimization of the port grain transportation system composed of three multistate non-homogeneous series-parallel subsystems linked in series, changing its reliability structure and its components reliability parameters at variable operation conditions.

1 INTRODUCTION

The complex technical systems reliability improvement and decreasing the risk of exceeding a critical reliability state are of great value in the industrial practice (Kołowrocki & Soszyńska-Budny 2011, Kuo & Prasad 2000, Kuo & Zuo 2003, Vercellis 2009). In everyday practice, there are needed the tools that could be applied to improving the reliability characteristics of the multistate systems operating at variable conditions. There are needed the tools allowing for finding the distributions and the expected values of the optimal times until the exceeding by the system the reliability critical state, the optimal system risk function and the moment when the optimal system risk function exceeds a permitted reliability level and allowing for changing the system operation process after comparing the values of these characteristics with their values before the system operation process optimization in order to improve the system reliability (Kołowrocki & Soszyńska-Budny 2011, Klajban & Adelman 2006, Kołowrocki & Soszyńska 2010, Kołowrocki & Soszyńska-Budny 2014, Koowrocki 2014, Lisniansi & Levitin 2003, Tang, Yin & Xi 2007).

2 COMPLEX SYSTEM RELIABILITY AND OPERATION OPTIMIZATION

Considering the equation (14) in (Kołowrocki & Soszyńska-Budny 2014) it is natural to assume that the system operation process has a significant influence on the system reliability. This influence is also clearly expressed in the equation (15) in (Kołowrocki & Soszyńska-Budny 2014) for the mean values of the system unconditional lifetimes in the reliability state subsets.

From the linear equation (15) in (Kołowrocki & Soszyńska-Budny 2014), we can see that the mean value of the system unconditional lifetime $\mu(u)$, $u=1,2,...,z$, is determined by the limit values of transient probabilities p_b, $b=1,2,...,\nu$, of the system operation process at the operation states given by (3) and the mean values $\mu_b(u)$, $b=1,2,...,\nu$, $u=1,2,...,z$, of the system conditional lifetimes in the reliability state subsets $\{u,u+1,...,z\}$, $u=1,2,...,z$, given by (16) in (Kołowrocki & Soszyńska-Budny 2014). Therefore, the system lifetime optimization approach based on the linear programming ((Kołowrocki & Soszyńska-Budny 2011, Klajban & Adelman 2006, Kołowrocki & Soszyńska 2010, Tang, Yin & Xi 2007) can be proposed. Namely, we may look for the corresponding optimal values $\dot{p}_b$, $b=1,2,...,\nu$, of the transient probabilities p_b, $b=1,2,...,\nu$, of the system operation process at the operation states to maximize the mean value $\mu(u)$ of the unconditional system lifetimes in the reliability state subsets $\{u,u+1,...,z\}$, $u=1,2,...,z$, under the assumption that the mean values $\mu_b(u)$, $b=1,2,...,\nu$, $u=1,2,...,z$, of the system conditional lifetimes in the reliability state subsets are fixed. As a special and practically important case of the above formulated system lifetime optimization problem, if r, $r=1,2,...,z$ is a system critical reliability state, we may look for the optimal values $\dot{p}_b$, $b=1,2,...,\nu$, of the transient probabilities p_b, $b=1,2,...,\nu$, of the system operation process at the system operation states to maximize the mean value $\mu(r)$ of the unconditional system

lifetime in the reliability state subset $\{r, r+1, ..., z\}$, $r = 1,2, ..., z$, under the assumption that the mean values $\mu_b(r)$, $b = 1,2, ..., \nu$, $r = 1,2, ..., z$, of the system conditional lifetimes in this reliability state subset are fixed. More exactly, we may formulate the optimization problem as a linear programming model with the objective function of the following form

$$\mu(r) = \sum_{b=1}^{\nu} p_b \mu_b(r) \tag{1}$$

for a fixed $r \in \{1,2, ..., z\}$ and with the following bound constraints

$$\breve{p}_b \le p_b \le \hat{p}_b,\ b = 1,2, ..., \nu,\ \sum_{b=1}^{\nu} p_b = 1, \tag{2}$$

where $\mu_b(r)$, $\mu_b(r) \ge 0$, $b = 1,2, ..., \nu$, are fixed mean values of the system conditional lifetimes in the reliability state subset $\{r, r+1, ..., z\}$ and

$$\breve{p}_b, 0 \le \breve{p}_b \le 1 \text{ and } \hat{p}_b, 0 \le \hat{p}_b \le 1,\ \breve{p}_b \le \hat{p}_b,\ b = 1,2, ..., \nu, \tag{3}$$

are lower and upper bounds of the unknown transient probabilities p_b, $b = 1,2, ..., \nu$, respectively.

Now, we can obtain the optimal solution of the formulated by (1)–(3) the linear programming problem, i.e. we can find the optimal values $\dot{p}_b$ of the transient probabilities p_b, $b = 1,2, ..., \nu$, that maximize the objective function given by (1).

First, we arrange the system conditional lifetime mean values $\mu_b(r)$, $b = 1,2, ..., \nu$, in non-increasing order $\mu_{b_1}(r) \ge \mu_{b_2}(r) \ge \ldots \ge \mu_{b_\nu}(r)$, where $b_i \in \{1,2, ..., \nu\}$ for $i = 1,2, ..., \nu$.

Next, we substitute

$$x_i = p_{b_i},\ \breve{x}_i = \breve{p}_{b_i},\ \hat{x}_i = \hat{p}_{b_i} \text{ for } i = 1,2, ..., \nu \tag{4}$$

and we maximize with respect to x_i, $i = 1,2, ..., \nu$, the linear form (1) that after this transformation takes the form

$$\mu(r) = \sum_{i=1}^{\nu} x_i \mu_{b_i}(r) \tag{5}$$

for a fixed $r \in \{1,2, ..., z\}$ with the following bound constraints

$$\breve{x}_i \le x_i \le \hat{x}_i,\ i = 1,2, ..., \nu,\ \sum_{i=1}^{\nu} x_i = 1, \tag{6}$$

where $\mu_{b_i}(r)$, $\mu_{b_i}(r) \ge 0$, $i = 1,2, ..., \nu$, are fixed mean values of the system conditional lifetimes in the reliability state subset $\{r, r+1, ..., z\}$ arranged in non-increasing order and

$$\breve{x}_i, 0 \le \breve{x}_i \le 1 \text{ and } \hat{x}_i, 0 \le \hat{x}_i \le 1,\ \breve{x}_i \le \hat{x}_i,\ i = 1,2, ..., \nu, \tag{7}$$

are lower and upper bounds of the unknown probabilities x_i, $i = 1,2, ..., \nu$, respectively.

To find the optimal values of x_i, $i = 1,2, ..., \nu$, we define

$$\breve{x} = \sum_{i=1}^{\nu} \breve{x}_i,\ \hat{y} = 1 - \breve{x} \tag{8}$$

and

$$\breve{x}^0 = 0,\ \hat{x}^0 = 0 \text{ and } \breve{x}^I = \sum_{i=1}^{I} \breve{x}_i,\ \hat{x}^I = \sum_{i=1}^{I} \hat{x}_i \tag{9}$$

for $I = 1,2, ..., \nu$.

Next, we find the largest value $I \in \{0,1, ..., \nu\}$ such that

$$\hat{x}^I - \breve{x}^I < \hat{y} \tag{10}$$

and we fix the optimal solution that maximize (5) in the following way:

i. if $I = 0$, the optimal solution is

$$\dot{x}_1 = \hat{y} + \breve{x}_1 \text{ and } \dot{x}_i = \breve{x}_i \text{ for } i = 2,3, ..., \nu; \tag{11}$$

ii. if $0 < I < \nu$, the optimal solution is

$$\dot{x}_i = \hat{x}_i \text{ for } i = 1,2, ..., I,\ \dot{x}_{I+1} = \hat{y} - \hat{x}^I + \breve{x}^I + \breve{x}_{I+1} \text{ and } \dot{x}_i = \breve{x}_i \text{ for } i = I+2, I+3, ..., \nu; \tag{12}$$

iii. if $I = \nu$, the optimal solution is

$$\dot{x}_i = \hat{x}_i \text{ for } i = 1,2, ..., \nu. \tag{13}$$

Finally, after making the inverse to (4) substitution, we get the optimal limit transient probabilities

$$\dot{p}_{b_i} = \dot{x}_i \text{ for } i = 1,2, ..., \nu, \tag{14}$$

that maximize the system mean lifetime in the reliability state subset $\{r, r+1, ..., z\}$, defined by the linear form (1), giving its maximum value in the following form

$$\dot{\mu}(r) = \sum_{b=1}^{\nu} \dot{p}_b \mu_b(r) \tag{15}$$

for a fixed $r \in \{1,2, ..., z\}$.

From the expression (15) for the maximum mean value $\dot{\mu}(r)$ of the system unconditional lifetime in the reliability state subset $\{r, r+1, ..., z\}$, replacing

in it the critical reliability state r by the reliability state u, $u = 1,2, ..., z$, we obtain the corresponding optimal solutions for the mean values of the system unconditional lifetimes in the reliability state subsets $\{u, u+1, ..., z\}$ of the form

$$\dot{\mu}(u) = \sum_{b=1}^{\nu} \dot{p}_b \mu_b(u) \text{ for } u = 1,2, ..., z. \tag{16}$$

Further, according to (13)-(14), the corresponding optimal unconditional multistate reliability function of the system is the vector

$$\dot{\boldsymbol{R}}(t,\cdot) = [1, \dot{\boldsymbol{R}}(t,1), ..., \dot{\boldsymbol{R}}(t,z)], \tag{17}$$

with the coordinates given by

$$\dot{\boldsymbol{R}}(t,u) \cong \sum_{b=1}^{v} \dot{p}_b [\boldsymbol{R}(t,u)]^{(b)} \text{ for } t \geq 0, \tag{18}$$
$$u = 1,2, ..., z.$$

And, by (17), the optimal solutions for the mean values of the system unconditional lifetimes in the particular reliability states are

$$\ddot{\mu}(u) = \dot{\mu}(u) - \dot{\mu}(u+1), u = 1, ..., z-1,$$
$$\ddot{\mu}(z) = \dot{\mu}(z). \tag{19}$$

Moreover, considering (18) and (19), the corresponding optimal system risk function and the optimal moment when the risk exceeds a permitted level δ, respectively are given by

$$\dot{r}(t) = 1 - \dot{\boldsymbol{R}}(t,r), t \geq 0, \tag{20}$$

and

$$\dot{\tau} = \dot{r}^{-1}(\delta), \tag{21}$$

where $\dot{\boldsymbol{R}}(t,r)$ is given by (18) for $u = r$ and $\dot{r}^{-1}(t)$, if it exists, is the inverse function of the optimal risk function $\dot{r}(t)$.

Replacing in (3) given in (Kołowrocki & Soszyńska-Budny 2014), the limit transient probabilities p_b of the system operation process at the operation states by their optimal values $\dot{p}_b$, maximizing the mean value $\mu(r)$ of the system lifetime in the reliability states subset $\{r, r+1, ..., z\}$ defined by (1) and the mean values M_b of the unconditional sojourn times at the operation states by their corresponding unknown optimal values $\dot{M}_b$, we get the system of equations

$$\dot{p}_b = \frac{\pi_b \dot{M}_b}{\sum_{l=1}^{v} \pi_l \dot{M}_l}, b = 1,2, ..., v. \tag{22}$$

After simple transformations the above system takes the form

$$\begin{aligned}
&(\dot{p}_1 - 1)\pi_1 \dot{M}_1 + \dot{p}_1 \pi_2 \dot{M}_2 + ... + \dot{p}_1 \pi_\nu \dot{M}_\nu = 0 \\
&\dot{p}_2 \pi_1 \dot{M}_1 + (\dot{p}_2 - 1)\pi_2 \dot{M}_2 + ... + \dot{p}_2 \pi_\nu \dot{M}_\nu = 0 \\
&... \\
&\dot{p}_\nu \pi_1 \dot{M}_1 + \dot{p}_\nu \pi_2 \dot{M}_2 + ... + (\dot{p}_\nu - 1)\pi_\nu \dot{M}_\nu = 0,
\end{aligned} \tag{23}$$

where $\dot{M}_b$ are unknown variables we want to find, $\dot{p}_b$ are optimal transient probabilities determined by (14) and π_b are steady probabilities determined by (4) given in (Kołowrocki & Soszyńska-Budny 2014).

Since the system of equations (23) is homogeneous and it can be proved that the determinant of its main matrix is equal to zero, then it has nonzero solutions and moreover, these solutions are ambiguous. Thus, if we fix some of the optimal values $\dot{M}_b$ of the mean values M_b of the unconditional sojourn times at the operation states, for instance by arbitrary fixing one or a few of them, we may find the values of the remaining once and this way to get the solution of this equation.

Having this solution, it is also possible to look for the optimal values $\dot{M}_{bl}$ of the mean values M_{bl} of the conditional sojourn times at the operation states using the following system of equations

$$\sum_{l=1}^{v} p_{bl} \dot{M}_{bl} = \dot{M}_b, b = 1,2, ..., v, \tag{24}$$

obtained from (2) given in (Kołowrocki & Soszyńska-Budny 2014) by replacing M_b by $\dot{M}_b$ and M_{bl} by $\dot{M}_{bl}$, were p_{bl} are known probabilities of the system operation process transitions between the operation states z_b i z_l, $b,l = 1,2, ..., v$.

Another very useful and much easier to be applied in practice tool that can help in planning the operation processes of the complex technical systems are the system operation process optimal mean values of the total system operation process sojourn times $\hat{\theta}_b$ at the particular operation states z_b, $b = 1,2, ..., v$, during the fixed system operation time θ, that can be obtain by the replacing in the formula (5) given in (Kołowrocki & Soszyńska-Budny 2014), the transient probabilities p_b at the operation states z_b by their optimal values $\dot{p}_b$ and resulting in the following expession

$$\dot{\hat{M}}_b = \dot{E}[\hat{\theta}_b] = \dot{p}_b \theta, b = 1,2, ..., v. \tag{25}$$

The knowledge of the optimal values $\dot{M}_b$ of the mean values of the unconditional sojourn times and the optimal values $\dot{M}_{bl}$ of the mean values of the conditional sojourn times at the operation states and the optimal mean values $\dot{\hat{M}}_b$ of the total

sojourn times at the particular operation states during the fixed system operation time may by the basis for changing the complex technical systems operation processes in order to ensure these systems operation more reliable.

3 APPLICATION

We consider the port grain transportation system, presented in Figure 1, assigned to handle the clearing of exported and imported grain.

This system reliability structure and its components reliability parameters depend on its changing in time operation states with arbitrarily fixed the number of the system operation process states $\nu = 3$ and their influence on the system reliability indicated in (Kołowrocki & Soszyńska-Budny 2014) where its main reliability characteristics are predicted.

In the case when the system operation time is large enough its unconditional three-state reliability function determined in (Kołowrocki & Soszyńska-Budny 2014) is given by the vector

$$\boldsymbol{R}(t,\cdot)=[1,\boldsymbol{R}(t,1),\boldsymbol{R}(t,2)]\ \ t\geq 0, \tag{26}$$

where according to (14) given in (Kołowrocki & Soszyńska-Budny 2014) and considering the system operation process transient probabilities at the operation states determined by (10) given in (Kołowrocki & Soszyńska-Budny 2014), the vector co-ordinates are given respectively by

$$\begin{aligned}\boldsymbol{R}(t,1) &= p_1[\boldsymbol{R}(t,1)]^{(1)} + p_2[\boldsymbol{R}(t,1)]^{(2)} + p_3[\boldsymbol{R}(t,1)]^{(3)}\\ &= 0.530\cdot[\boldsymbol{R}(t,1)]^{(1)} + 0.109\cdot[\boldsymbol{R}(t,1)]^{(2)}\\ &\quad + 0.361\cdot[\boldsymbol{R}(t,1)]^{(3)} \text{ for } t\geq 0,\\ \boldsymbol{R}(t,2) &= p_1[\boldsymbol{R}(t,2)]^{(1)} + p_2[\boldsymbol{R}(t,2)]^{(2)} + p_3[\boldsymbol{R}(t,2)]^{(3)}\\ &= 0.530\cdot[\boldsymbol{R}(t,2)]^{(1)} + 0.109\cdot[\boldsymbol{R}(t,2)]^{(2)}\\ &\quad + 0.361\cdot[\boldsymbol{R}(t,2)]^{(3)} \text{ for } t\geq 0,\end{aligned} \tag{27}$$

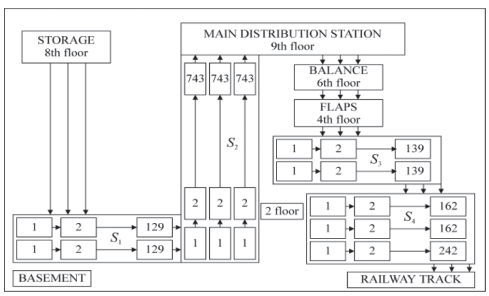


Figure 1. The scheme of the port grain transportation system structure at the operation state z_1.

where the reliability functions $[\boldsymbol{R}(t,1)]^{(1)}$, $[\boldsymbol{R}(t,1)]^{(2)}$, $[\boldsymbol{R}(t,1)]^{(3)}$, $[\boldsymbol{R}(t,2)]^{(1)}$, $[\boldsymbol{R}(t,2)]^{(2)}$, $[\boldsymbol{R}(t,2)]^{(3)}$ are given in (Kołowrocki & Soszyńska-Budny 2014).

The expected value of the system unconditional lifetime in the reliability state subsets $\{1,2\}$, $\{2\}$, calculated in (Kołowrocki & Soszyńska-Budny 2014) from the results given by (26)-(27), are

$$\begin{aligned}\mu(1) &= p_1\mu_1(1) + p_2\mu_2(1) + p_3\mu_3(1)\\ &= 0.530\cdot 0.0813 + 0.109\cdot 0.0861\\ &\quad + 0.361\cdot 0.0607 \cong 0.0744 \text{ year},\\ \mu(2) &= p_1\mu_1(2) + p_2\mu_2(2) + p_3\mu_3(2)\\ &= 0.530\cdot 0.0691 + 0.109\cdot 0.0728\\ &\quad + 0.361\cdot 0.0493 \cong 0.0624 \text{ year}.\end{aligned} \tag{28}$$

To find the optimal values of those system reliability characteristics, we conclude that the objective function defined by (1), in this case, as the system critical state is $r = 1$, according to (28), takes the form

$$\mu(1) = p_1\cdot 0.0813 + p_2\cdot 0.0861 + p_3\cdot 0.0607. \tag{29}$$

The lower $\breve{p}_b$ and upper $\hat{p}_b$ bounds of the unknown optimal values of transient probabilities p_b, $b = 1,2,3$, respectively are:

$$\begin{aligned}&\breve{p}_1 = 0.460, \breve{p}_2 = 0.080, \breve{p}_3 = 0.310;\\ &\hat{p}_1 = 0.600, \hat{p}_2 = 0.140, \hat{p}_3 = 0.410.\end{aligned}$$

Therefore, according to (2)-(3), we assume the following bound constraints

$$\begin{aligned}&0.460 \leq p_1 \leq 0.600,\ 0.080 \leq p_2 \leq 0.140,\\ &0.310 \leq p_3 \leq 0.410,\\ &\sum_{b=1}^{3} p_b = 1.\end{aligned} \tag{30}$$

Now, before we find optimal values $\dot{p}_b$ of the transient probabilities p_b, $b = 1,2,3$, that maximize the objective function (29), w arrange the system conditional lifetime mean values $\mu_b(1)$, $b = 1,2,3$, in non-increasing order

$$\mu_2(1) \geq \mu_1(1) \geq \mu_3(1).$$

Further, according to (4), we substitute

$$x_1 = p_2,\ x_2 = p_1,\ x_3 = p_3, \tag{31}$$

and

$$\begin{aligned}&\breve{x}_1 = \breve{p}_2 = 0.080,\ \breve{x}_2 = \breve{p}_1 = 0.460,\\ &\breve{x}_3 = \breve{p}_3 = 0.310;\end{aligned} \tag{32}$$

$$\begin{aligned}&\hat{x}_1 = \hat{p}_2 = 0.140,\ \hat{x}_2 = \hat{p}_1 = 0.600,\\ &\hat{x}_3 = \hat{p}_3 = 0.410.\end{aligned} \tag{33}$$

and we maximize with respect to x_i, $i=1,2,3$, the linear form (29) that according to (5)–(7) takes the form

$$\mu(1) = x_1 \cdot 0.0873 + x_2 \cdot 0.0812 + x_3 \cdot 0.0605, \tag{34}$$

with the following bound constraints

$$0.080 \le x_1 \le 0.140,\ 0.460 \le x_2 \le 0.600,$$
$$0.310 \le x_3 \le 0.410.$$
$$\sum_{i=1}^{3} x_i = 1. \tag{35}$$

According to (8), we calculate

$$\breve{x} = \sum_{i=1} \breve{x}_i = 0.850,$$
$$\hat{y} = 1 - \breve{x} = 1 - 0.850 = 0.150 \tag{36}$$

and according to (9), we determine

$$\breve{x}^0 = 0,\ \hat{x}^0 = 0,\ \hat{x}^0 - \breve{x}^0 = 0,$$
$$\breve{x}^1 = 0.080,\ \hat{x}^1 = 0.140,\ \hat{x}^1 - \breve{x}^1 = 0.060,$$
$$\breve{x}^2 = 0.540\ \hat{x}^2 = 0.740,\ \hat{x}^2 - \breve{x}^2 = 0.200,$$
$$\breve{x}^3 = 0.850,\ \hat{x}^3 = 1.150,\ \hat{x}^3 - \breve{x}^3 = 0.300. \tag{37}$$

From the above, as according to (36), the inequality (10) takes the form

$$\hat{x}^I - \breve{x}^I < 0.150, \tag{38}$$

it follows that the largest value $I \in \{0,1,2,3\}$ such that this inequality holds is $I = 1$.

Therefore, we fix the optimal solution that maximize linear function (34) according to the rule (12). Namely, we get

$$\dot{x}_1 = \hat{x}_1 = 0.140,$$
$$\dot{x}_2 = \hat{y} - \hat{x}^1 + \breve{x}^1 + \breve{x}_2$$
$$= 0.150 - 0.140 + 0.080 + 0.460 = 0.550,$$
$$\dot{x}_3 = \breve{x}_3 = 0.310. \tag{39}$$

Finally, after making the inverse to (31) substitution, we get the optimal transient probabilities

$$\dot{p}_1 = \dot{x}_2 = 0.550,\ \dot{p}_2 = \dot{x}_1 = 0.140,$$
$$\dot{p}_3 = \dot{x}_3 = 0.310, \tag{40}$$

that maximize the exemplary system mean lifetime $\mu(1)$ in the reliability state subset $\{1,2\}$ expressed by the linear form (29) giving, according to (15) and (40), its optimal value

$$\dot{\mu}(1) = \dot{p}_1 \cdot 0.0813 + \dot{p}_2 \cdot 0.0861 + \dot{p}_3 \cdot 0.0607$$
$$= 0.55 \cdot 0.0813 + 0.14 \cdot 0.0861$$
$$+ 0.31 \cdot 0.0607 = 0.0756\,\text{month}. \tag{41}$$

Substituting the optimal solution (40) into the formula (16), we obtain the optimal solution for the mean values of the exemplary system unconditional lifetimes in the reliability state subset $\{2\}$, that is as follows

$$\dot{\mu}(2) = \dot{p}_1 \cdot 0.0691 + \dot{p}_2 \cdot 0.0728 + \dot{p}_3 \cdot 0.0493$$
$$= 0.55 \cdot 0.0691 + 0.14 \cdot 0.0728$$
$$+ 0.31 \cdot 0.0493 = 0.0635\,\text{month}. \tag{42}$$

and according to (19), the optimal values of the mean values of the system unconditional lifetimes in the particular reliability states 1 and 2, respectively are

$$\dot{\tilde{\mu}}(1) = \dot{\mu}(1) - \dot{\mu}(2) = 0.0121\ \text{month},$$
$$\dot{\tilde{\mu}}(2) = \dot{\mu}(2) = 0.0635\ \text{month}. \tag{43}$$

Moreover, according to (17)-(18), the corresponding optimal unconditional multistate reliability function of the port grain transportation system is of the form

$$\dot{\boldsymbol{R}}(t,\cdot) = [1, \dot{\boldsymbol{R}}(t,1),\ \dot{\boldsymbol{R}}(t,2)],\ t \ge 0, \tag{44}$$

with the coordinates given by

$$\dot{\boldsymbol{R}}(t,1) = 0.55 \cdot [\boldsymbol{R}(t,1)]^{(1)} + 0.14 \cdot [\boldsymbol{R}(t,1)]^{(2)}$$
$$+ 0.31 \cdot [\boldsymbol{R}(t,1)]^{(3)} \text{ for } t \ge 0, \tag{45}$$

$$\dot{\boldsymbol{R}}(t,2) = 0.55 \cdot [\boldsymbol{R}(t,2)]^{(1)} + 0.14 \cdot [\boldsymbol{R}(t,2)]^{(2)}$$
$$+ 0.31 \cdot [\boldsymbol{R}(t,2)]^{(3)} \text{ for } t \ge 0, \tag{46}$$

where $[\boldsymbol{R}(t,1)]^{(b)}$, $[\boldsymbol{R}(t,2)]^{(b)}$, $b = 1,2,3$, are fixed in (Kołowrocki & Soszyńska-Budny 2014).

The graph of the port grain transportation system optimal reliability function $\dot{\boldsymbol{R}}(t,\cdot)$ given by (44)-(46) is presented in Figure 2.

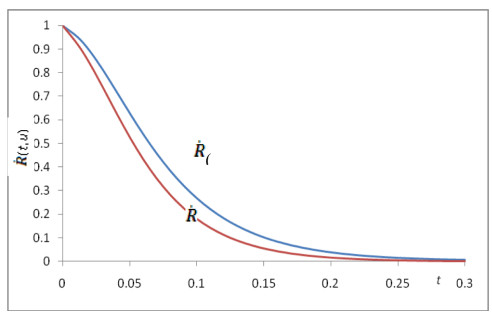


Figure 2. The graph of the port grain transportation system optimal reliability function $\dot{\boldsymbol{R}}(t,\cdot)$ coordinates.

As the critical reliability state is $r = 1$, then the optimal system risk function, according to (20), is given by (Fig. 3)

$$\dot{r}(t) = 1 - \dot{R}(t,1) \text{ for } t \geq 0, \tag{47}$$

where $\dot{R}(t,1)$ is given by (45).

Hence and considering (21), the moment when the optimal system risk function exceeds a permitted level, for instance $\delta = 0.05$, is

$$\dot{\tau} = \dot{r}^{-1}(\delta) \cong 0{,}0114 \text{ month}. \tag{48}$$

Substituting the exemplary operation process optimal transient probabilities at operation states

$$\dot{p}_1 = 0.5,\ \dot{p}_2 = 0.14,\ \dot{p}_3 = 0.31,$$

determined by (40) and the steady probabilities

$$\pi_1 \cong 0.279,\ \pi_2 \cong 0.344,\ \pi_3 \cong 0.377.$$

determined by (9) in (Kołowrocki & Soszyńska-Budny 2014) into (23), we get the following system of equations with the unknown optimal mean values $\hat{M}_b$ of the port grain transportation system operation process unconditional sojourn times at the operation states we are looking for

$$\begin{aligned} &-0.12555\dot{M}_1 + 0.18920\dot{M}_2 + 0.20735\dot{M}_3 = 0 \\ &0.03906\dot{M}_1 - 0.29584\dot{M}_2 + 0.05278\dot{M}_3 = 0 \\ &0.08649\dot{M}_1 + 0.10664\dot{M}_2 - 0.26013\dot{M}_3 = 0. \end{aligned} \tag{49}$$

The determinant of the main matrix of the above homogeneous system of equations is equal to zero and therefore there are non-zero solutions of this system of equations that are ambiguous and dependent on one or more parameters. Thus, we may fix some of them and determine the remaining ones. To show the way of solving this system of equations, we may suppose that we are arbitrarily interested in fixing the value of $\dot{M}_3$ and we put

$$\dot{M}_3 = 0.070.$$

Substituting the above value into the system of equations (49), we get

$$\begin{aligned} &-0.12555\dot{M}_1 + 0.18920\dot{M}_2 = -0.0145145 \\ &0.03906\dot{M}_1 - 0.29584\dot{M}_2 = -0.0036946 \\ &0.08649\dot{M}_1 + 0.10664\dot{M}_2 = 0.0182091. \end{aligned}$$

and we solve it with respect to $\dot{M}_1$ and $\dot{M}_2$, after omitting its last equation. This way obtained solutions that satisfy (49), are

$$\dot{M}_1 \cong 0.1678,\ \dot{M}_2 \cong 0.0346,\ \dot{M}_3 = 0.0700. \tag{50}$$

It can be seen that these solution are different from the values M_1, M_2 and M_3 estimated in (Kołowrocki & Soszyńska-Budny 2014).

Having these solutions, it is also possible to look for the optimal values $\dot{M}_{bl}$ of the mean values M_{bl} of the port grain transportation system operation process conditional sojourn times at operation states. Namely, substituting the values $\dot{M}_b$ instead of M_b, the probabilities

$$[p_{bl}]_{3x3} = \begin{bmatrix} 0 & \frac{1}{3} & \frac{2}{3} \\ \frac{4}{9} & 0 & \frac{5}{9} \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix}$$

of the port grain transportation system operation process transitions between the operation states given by (6) in (Kołowrocki & Soszyńska-Budny 2014) and replacing M_{bl} by $\dot{M}_{bl}$ in (24), we get the following system of equations

$$\begin{aligned} &\frac{1}{3}\dot{M}_{12} + \frac{2}{3}\dot{M}_{13} = 0.1678 \\ &\frac{4}{9}\dot{M}_{21} + \frac{5}{9}\dot{M}_{23} = 0.0346 \\ &\frac{1}{3}\dot{M}_{31} + \frac{2}{3}\dot{M}_{32} = 0.0700 \end{aligned} \tag{51}$$

with the unknown optimal values $\dot{M}_{bl}$ we want to find.

As the solutions of the above system of equations are ambiguous, then we fix some of them, say that because of practically important reasons, and we find the remaining ones. For instance:

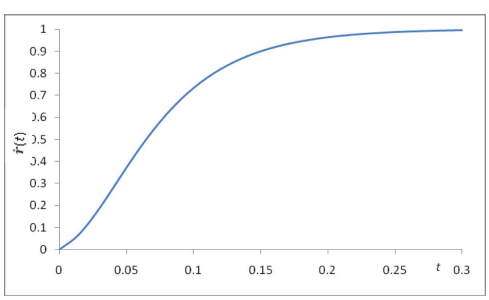


Figure 3. The graph of the port grain transportation system optimal risk function $\dot{r}(t)$.

– we fix in the first equation $\dot{M}_{13} = 0.050$ and we find $\dot{M}_{12} = 0.403$;
– we fix in the second equation $\dot{M}_{23} = 0.010$ and we find $\dot{M}_{21} = 0.065$;
– we fix in the third equation $\dot{M}_{32} = 0.100$ and we find $\dot{M}_{31} = 0.010$. (52)

It can be seen that these solutions differ much from the mean values of the port grain transportation system conditional sojourn times at the particular operation states before its operation process optimization given by (7) in (Kołowrocki & Soszyńska-Budny 2014).

Another very useful and much easier to be applied in practice tool that can help in planning the operation process of the port grain transportation system are the system operation process optimal mean values of the total sojourn times at the particular operation states during the system operation time that by the same assumpion as in (Kołowrocki & Soszyńska-Budny 2014) is equel to $\theta = 1$ year = 365 days. Under this assumption, after aplying (25), we get the optimal values of the exemplary system operation process total sojourn times at the particular operation states during 1 year

$$\dot{\hat{M}}_1 = \dot{E}[\hat{\theta}_1] = \dot{p}_1\theta = 0.55 \cdot 365 \cong 200.75,$$
$$\dot{\hat{M}}_2 = \dot{E}[\hat{\theta}_2] = \dot{p}_2\theta = 0.14 \cdot 365 \cong 51.1,$$
$$\dot{\hat{M}}_3 = \dot{E}[\hat{\theta}_3] = \dot{p}_3\theta = 0.31 \cdot 365 = 113.15, \quad (53)$$

that are different from the values of $\hat{M}_1$, $\hat{M}_2$, $\hat{M}_3$, determined by (8) in (Kołowrocki & Soszyńska-Budny 2014).

In practice, the knowledge of the optimal values of $\dot{M}_b$, $\dot{M}_{bl}$ and $\hat{M}_b$ given respectively by (50), (52), (53), can be very important and helpful for the system operation process planning and improving in order to make the system operation more reliable.

The comparison of the values of the selected port grain transportation system reliability characteristics before the system operation process optimization given in (Kołowrocki & Soszyńska-Budny 2014) by (55)-(56) and (58) with their values after the system operation process optimization respectively given by (41)-(43) and (48) justifies the sensibility of the performed system operation process optimization.

From the analysis of the results of the port grain transportation system operation process optimization it can be suggested to organize the system operation process in the way that causes the replacing (or the approaching/convergence to) the conditional mean sojourn times M_{bl} of the system at the particular operation states before the optimization given by (7) in (Kołowrocki & Soszyńska-Budny 2014) by their optimal values $\dot{M}_{bl}$ after the optimization given by (52). The possibility of fulfilling this suggestion of the operation process parameters changing is not easy and has to be checked in practice.

It seems to be practically a bit easier way, changing the operation process characteristics that results in replacing (or the approaching/convergence to) the unconditional mean sojourn times M_b of the port grain transportation system at the particular operation states before the optimization given by (8) in (Kołowrocki & Soszyńska-Budny 2014) by their optimal values $\dot{M}_b$ after the optimization given by (50).

The easiest way of the system operation process reorganizing is that leading to the replacing (or the approaching/convergence to) the total sojourn times $\hat{M}_b$ of the port grain transportation system operation process at the particular operation states during the operation time $\theta = 1$ year before the optimization given by (11) in (Kołowrocki & Sɒszyńska-Budny 2014) by their optimal values $\dot{\hat{M}}_b$ after the optimization given by (53).

The port grain transportation system operating at the varying in time operation conditions reliability evaluation and prediction are approximate because of non sufficiently exact input data. Therefore, the achieved results may only be considered as an illustration of the possibilities of applications of the proposed methods and procedures to this system operation and reliability analysis, prediction and optimization. However, the obtained evaluation may be a very useful example in other port grain transportation systems and other complex technical systems reliability characteristics prediction, especially during the design and when planning and improving their operation processes effectiveness.

4 CONCLUSIONS

Presented in this paper tool is useful in reliability and operation optimization of a very wide class of real technical systems operating at the varying conditions that have an influence on changing their reliability structures and their components reliability parameters. The results can be interesting for reliability practitioners from various industrial sectors.

REFERENCES

Klabjan, D. and Adelman, D., 2006. Existence of optimal policies for semi-Markov decision processes using duality for infinite linear programming, Siam Journal on Control and Optimization 44(6): 2104–2122.
Kołowrocki, K., 2014. Reliability of large and complex systems. Elsevier.

Kołowrocki, K. and Soszyńska, J., 2010. Reliability, availability and safety of complex technical systems: modeling-identification-prediction-optimization, Journal of Polish Safety and Reliability Associaion, Summer Safety & Reliability Seminars 1(1): 133–158.

Kołowrocki, K. and Soszyńska-Budny, J., 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling-Identification-Prediction-Optimization, Springer.

Kołowrocki, K. and Soszyńska-Budny, J., 2014. Modeling reliability of complex port transportation system, Proc. European Safety and Reliability Conference—ESREL 2014.

Kuo, W. and Prasad, V.R., 2000. An annotated overview of system-reliability optimization, IEEE Transactions on Reliability 49(2): 176–187.

Kuo, W. and Zuo, M.J., 2003. Optimal Reliability Modeling: Principles and Applications, Hoboken: John Wiley & Sons, Inc.

Lisnianski, A. and Levitin, G., 2003. Multi-State System Reliability. Assessment, Optimisation and Applications, World Scientific Publishing Co. Pte. Ltd.

Tang, H., Yin, B.Q. and Xi, H.S., 2007. Error bounds of optimization algorithms for semi-Markov decision processes, International Journal of Systems Science 38(9): 725–736.

Vercellis, S., 2009. Data mining and optimization for decision making, John Wiley & Sons.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Involvement of expert judgement in dynamic model

R. Krikštolaitis, A.E. Lutynska, S. Pečiulytė & I. Žutautaitė
Vytautas Magnus University, Kaunas, Lithuania

ABSTRACT: In many areas models of different processes take into account various factors that are time-dependent and dependent on each other. Thus, it is advisable to construct a dynamic model in order to describe these dependences. In the dynamic model we use indicators. An indicator is a special index, which provides numerical values to important factors for the investigated sector. The values of indicators are obtained from statistical data. Also this dynamic model enables to forecast the dynamics of the indicators according to different new factors. Since the parameters of new factors are not exactly known (got from expert judgement), their influences on indicators are expressed as random variables with known probabilistic distributions. Indicators model based on historic data is adjusted by probabilistic model with the influence of new factors on indicators using a Bayesian method.

1 INTRODUCTION

In many areas models of different processes take into account various factors that are time-dependent and dependent on each other. Thus, it is advisable to construct dynamic model in order to describe these dependences. In dynamic model we use indicators. An indicator is a special index, which provides numerical values to important factors for the investigated sector.

The paper presents a dynamic indicator model, involvement of expert judgement to dynamic model using a Bayesian method and pilot calculations. Pilot calculations of Lithuanian, Latvian and Estonian energy security from technical point of view were presented as an example. The calculations period was chosen from 2007 till 2012. Using the proposed model additional influence of two new energy facilities (LNG and VNPP) was evaluated. Liquefied Natural Gas (LNG) Terminal is one of the most important Lithuania's energy projects that will improve energy security situation in country, create conditions for natural gas market and provide economic boost for many local economies and residents. It is planned that LNG terminal is to be launched from the beginning of 2015. Visaginas Nuclear Power Plant (VNPP) is a new nuclear plant in Visaginas which could be one of the main electricity generating facilities. VNPP construction is still under discussion phase.

2 DYNAMIC INDICATOR MODEL

Let us construct a homogeneous differential equations system, according to the interdependencies between indicators

$$\begin{cases} \dfrac{\mathrm{d}I_1(t)}{dt} = a_{11}I_1(t) + a_{12}I_2(t) + \cdots + a_{1N}I_N(t), \\ \cdots \\ \dfrac{\mathrm{d}I_N(t)}{dt} = a_{N1}I_1(t) + a_{N2}I_2(t) + \cdots + a_{NN}I_N(t), \end{cases} \quad (1)$$

here a_{ij}, $i,j = 1, \ldots, N$ are coefficients, I_i, $i = 1, \ldots, N$—indicators, describing factors of different areas.

Coefficients a_{ij}, $i,j = 1, \ldots, N$ in formula (1) may be calculated using different methods: algebraic, statistical, etc. In (Augutis, Pečiulytė et al, 2012) we proposed to use algebraic method for calculation of these coefficients. This method is quite limited, as we should have square matrices. So, the number of indicators and the number of time moments (when factual values of indicators are observed) must be the same. So, it is better to use Least Square Method (LSM) for calculation of coefficients (Augutis, Krikštolaitis et al, 2013). Let us give the variation for each indicator $\Delta I_i(t) = \left(I_i(t+\Delta t) - I_i(t)\right)/\Delta t$, $i = 1, \ldots, N$ and construct system of algebraic equations

$$\begin{cases} \Delta I_1(t) = a_{11}I_1(t) + a_{12}I_2(t) + \cdots + a_{1N}I_N(t), \\ \cdots \\ \Delta I_N(t) = a_{N1}I_1(t) + a_{N2}I_2(t) + \cdots + a_{NN}I_N(t). \end{cases} \quad (2)$$

We take values of each indicator in time moments t_k, $k = 1, .., n$ and define $I_{ik} = I_i(t_k)$, $i = 1, \ldots, N$, $k = 1, \ldots, n$. So, we have N algebraic systems of N equations with N^2 unknowns

$$\Delta I_{ik} = a_{i1}I_{1k} + a_{i2}I_{2k} + \cdots + a_{iN}I_{Nk}, \quad i = 1, \ldots, N, k = 1, \ldots, n. \quad (3)$$

LSM is applied to calculate estimates of unknown coefficients of equation (3) with assumption that a_{ii}=0, i=1, …, N. For the application of LSM number of observed factual values of indicators $n : n \geq N-1$. In this way all collected statistical data on factual values of indicators may be used.

The expression of the solution of differential equations system (1) depends on eigenvalues λ of system coefficients matrix $\mathrm{A} = \{a_{ij}\}$, $i,j = 1, \ldots, N$. If all eigenvalues are real and different numbers, the solution may be found according to the formula (4) (Golokvosčius, 2000)

$$\left\{ \mathrm{I}(t) = \sum_{j=1}^{N} C_j B_j \mathrm{e}^{\lambda_j t}, \right. \tag{4}$$

here $\mathrm{I}(t) = (I_1(t), I_2(t), \ldots, I_N(t))^{\mathrm{T}}$. If eigenvalues are complex numbers $\lambda_j = \alpha_j + \beta_j \mathrm{i}$, $j = 1,2, ..., N/2$, (N is even number in this case) the solution may be found according to the formula (5)

$$\mathrm{I}(t) = \sum_{j=1}^{N/2} \left(\tilde{C}_{2j-1} B_{2j-1} e^{\alpha_{2j-1} t} \left(\cos\left(\beta_{2j-1} t\right) + \mathrm{i}\sin\left(\beta_{2j-1} t\right) \right) + \tilde{C}_{2j} B_{2j} e^{\alpha_{2j-1} t} \left(\cos\left(\beta_{2j-1} t\right) + \mathrm{i}\sin\left(\beta_{2j-1} t\right) \right) \right), \tag{5}$$

here $B = (b_1, \ldots, b_n)^{\mathrm{T}}$—vector of constants, $\tilde{C}_j = C_j + \mathrm{i}C_j$. Also the solution of differential equations system (1) may be the combination of expressions from formulas (4) and (5).

Aiming to find a particular solution for differential equations system (1), i.e. particular expression of each indicator as on time dependent function, we need to formulate initial conditions for differential equations system. Constants C_i, $i = 1, \ldots, N$ of general solution may be found by solving system of differential equations (1) in time moment t_0

$$I_1(t_0) = I_1^0, ..., I_N(t_0) = I_N^0, \tag{6}$$

here I_i^0, $i = 1, \ldots, N$—normalized factual value of indicator in time moment t_0.

Suppose, that coefficient matrix A of differential equations system (1) is normal, id est $\mathrm{P}^{-1} = \mathrm{P}^*$, here P is a matrix composed from eigenvectors of matrix A, P^*—joint matrix to matrix P. And if $\lambda_1 \leq ... \leq \lambda_k < 0 \leq \lambda_{k+1} \leq ... \leq \lambda_N$ then stability estimate of differential equations system (1) solution is

$$\left\| \mathrm{I}(t) \right\|_2 \leq \mathrm{e}^{|\lambda_1| t} \left\| \mathrm{I}(0) \right\|_2. \tag{7}$$

Created dynamic model will enable us to forecast alternation of different systems factors, such as energy security level according to introducing new objects. In this case we should correct the initial conditions (6) of differential equations system. Since parameters of new objects are not exactly known, these uncertainties should be reflected in the initial conditions. Thus, in such conditions, the values of indicators are random variables.

In mathematical statistics theory it is well known that Bayesian method allows a combination of two kinds of information: prior (for instance, generic statistic data, subjective option of experts) and measurements or observations (Bernardo et al, 2003; Berthold et al, 2003). Bayesian method allows updating estimates of all parameters in the model with a single new obtained observation, i.e. Bayesian method does not require to have new information on the values of all factors involved in the created model.

Bayesian method also allows taking into account the expert's opinion, i.e. when instead of real data we have experts opinion about factors behavior in the future. In our case, the pilot calculations are used for analyzing influence of two energy projects on energy security. One of the projects (LNG terminal) is almost at the completion stage, so the uncertainty due to the start of operation is minimal. The bigger uncertainty is with another project (VNPP). Currently it is not clear whether the project will be implemented. Therefore, the Bayesian method allows to include in the model not only the probable mean value, but also to evaluate the emerging uncertainties.

Also the expert opinion on new object parameters may be involved to dynamic model through initial conditions of differential equations system (6). In this case we should find a new separate solution of differential equations system (1). But there are weaknesses of this method: we need to have expert evaluation of all indicator values without uncertainties and this method does not allow to include more than one new object. So, while calculating the example, we used the Bayesian method for involving expert judgement on new objects, as it is more appropriate.

Expert judgment—probable mean values of indicators time t^*: $I(t^*) = (I_1^*, \ldots, I_N^*)$, with standard deviations σ_i, $i = 1, \ldots, N$, that represent uncertainties. C_i, $i = 1, \ldots, N$, in (4) or (5) solution of differential equations system (1) are independent random variables, with prior probability density functions (pdfs) $p_i(x_i)$, $i = 1, \ldots, N$.

In our case, non-stationary processes are analyzed, i.e. the values of factors depend on time t. Classical application of Bayesian method is not correct in this case, because observations obtained in different time moments represent the other state of the indicators. The modified application of Bayesian method for the calculation estimates of parameters of non-stationary process mathematical models is presented in research papers (Augutis et al, 2012; Žutautaitė-Šeputienė et al, 2010).

3 EXAMPLE OF CALCULATION

For practical demonstration of the proposed method technical blocks of energy security systems in three Baltic States—Lithuania, Latvia and Estonia were chosen. Three generalized indicators describing electricity ($I_1(t)$), gas ($I_2(t)$) and heat (district heat) ($I_3(t)$) were used. These indicators cover various aspects of technical infrastructure, aging of particular infrastructure, etc. The selection of such aggregated indicators was determined by the development of new energy facilities in Lithuania, which mainly influence the condition of technical infrastructure.

Statistical data of 2007–2012 was used for calculation of differential equations system (1) coefficients with least square method in cases of each country (8).

$$\mathrm{A}_{LT} = \begin{pmatrix} 0 & -0.09 & 0.08 \\ 1.74 & 0 & -1.48 \\ 0.52 & -0.48 & 0 \end{pmatrix},$$

$$\mathrm{A}_{LV} = \begin{pmatrix} 0 & -0.4 & 0.66 \\ 0.29 & 0 & -0.3 \\ 0.44 & -0.28 & 0 \end{pmatrix}, \quad (8)$$

$$\mathrm{A}_{EE} = \begin{pmatrix} 0 & 0.08 & -0.12 \\ 0.85 & 0 & -0.8 \\ 0.05 & -0.03 & 0 \end{pmatrix}.$$

All matrices A_{LT}, A_{LV}, and A_{EE} are normal.

As all eigenvalues of matrices (8) are real, so general solutions of (1) differential equations systems with coefficients (8) are constructed using expression of the solution (4):

$$\begin{cases} I_1^{LT}(t) = -0.17C_1\mathrm{e}^{0.77t} - 0.06C_2\mathrm{e}^{-0.76t} + 0.1\mathrm{e}^{-0.01t}, \\ I_2^{LT}(t) = 0.87C_1\mathrm{e}^{0.77t} - 1.05C_2\mathrm{e}^{-0.76t} + 0.11\mathrm{e}^{-0.01t}, \\ I_3^{LT}(t) = -0.65C_1\mathrm{e}^{0.77t} - 0.614C_2\mathrm{e}^{-0.76t} + 0.12\mathrm{e}^{-0.01t}, \end{cases} \quad (9)$$

$$\begin{cases} I_1^{LV}(t) = -0.49C_1\mathrm{e}^{-0.52t} - 0.73C_2\mathrm{e}^{0.51t} + 0.8\mathrm{e}^{0.01t}, \\ I_2^{LV}(t) = 0.77C_1\mathrm{e}^{-0.52t} - 0.06C_2\mathrm{e}^{0.51t} + 1.22\mathrm{e}^{0.01t}, \\ I_3^{LV}(t) = 0.84C_1\mathrm{e}^{-0.52t} - 0.6C_2\mathrm{e}^{0.51t} + 0.74\mathrm{e}^{0.01t}, \end{cases} \quad (10)$$

$$\begin{cases} I_1^{EE}(t) = 0.82C_1\mathrm{e}^{0.004t} + 1.35C_2\mathrm{e}^{0.28t} + 0.87\mathrm{e}^{-0.28t}, \\ I_2^{EE}(t) = 0.77C_1\mathrm{e}^{0.004t} - 0.06C_2\mathrm{e}^{0.28t} + 1.22\mathrm{e}^{-0.28t}, \\ I_3^{EE}(t) = 0.84C_1\mathrm{e}^{0.004t} - 0.6C_2\mathrm{e}^{0.28t} + 0.74\mathrm{e}^{-0.28t}. \end{cases} \quad (11)$$

Using stability estimate of differential equations system solution (7), there was checked up the stability of solutions (9)–(11) taking factual values of indicators in each year from 2007 till 2012 as initial conditions (I(0)) of differential equations systems. As all solutions are stable, constants C_i, $i = 1, 2, 3$ of general solution were chosen in each country case to calculate using normalized factual values of indicators I_i, $i = 1, 2, 3$ in 2012.

In Figures 1–3 are given functions of electricity, gas and heat indicators in each country (Lithuania, Latvia and Estonia) case in 2007–2015.

The decrease of electricity indicator for Lithuania is explainable by the fact that in the end of 2009 the main electricity generation source, Ignalina nuclear power plant, was shut down. The increase of electricity indicator of Latvia is explainable by the reconstruction of two blocks of Riga combined heat and power plant (Fig. 1).

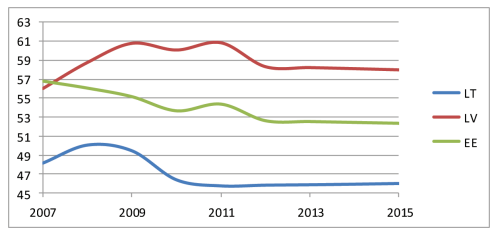


Figure 1. Electricity indicator $I_1(t)$.

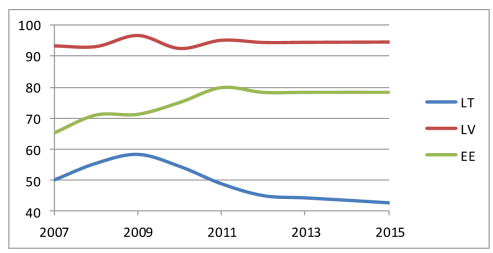


Figure 2. Gas indicator $I_2(t)$.

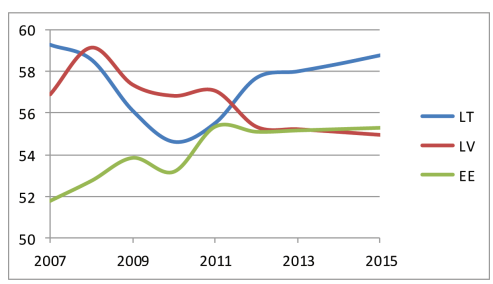


Figure 3. Heat indicator $I_3(t)$.

From 2010, the prevailing resource of electricity production in Lithuania has changed—basic production of electricity was ensured by power plants fuelled with gas. That is why we can see a decrease of gas indicator for Lithuania (Fig. 2).

In Figure 3 heat indicator of Lithuania is presented. This is determined by modernization of heat supply infrastructure.

In order to identify the technical blocks' state in each country, a 100 percent assessment scale is used. The scale is divided into three main parts: normal state (66.67–100 percent), pre-critical state (33.33–66.67 percent) and critical state (0–33.33 percent). These three parts are further subdivided into five equal parts accordingly. The value of each indicator is evaluated by percent during the research year. The state of technical blocks is evaluated using equal weights of all indicators according to the formula

$$TBS = s_1 I_1^p + s_2 I_2^p + s_3 I_3^p, \tag{12}$$

here I_i^p, $i = 1, 2, 3$–value of indicator in percent, s_i, $i = 1, 2, 3$–weight of each indicator (Augutis, Krikštolaitis et al, 2013). Integral characteristic of technical blocks states in Lithuania, Latvia and Estonia are presented in Figure 4. As changes of forecasted indicator values in 2013–2015 are very small, the assessment scale does not accurately reflect them. In order to be more accurate more a detailed scale is needed.

Three scenarios were investigated regarding practical demonstration of the proposed method how to involve expert judgement into a dynamic model:

- scenario 1—neither LNG terminal nor VNPP are constructed,
- scenario 2—LNG plant will start up in 2015,
- scenario 3—VNPP will start up in 2022.

Probable mean values I_i^* of indicators I_i in cases of two different scenarios are presented in Table 1.

Let's assume that at time moment t probability distributions of indicators $I_i(t)$ are normal with

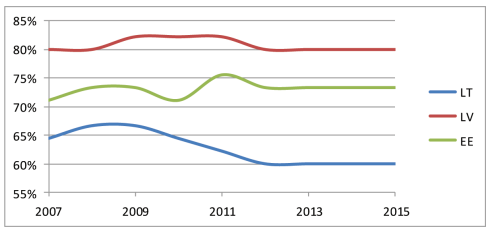


Figure 4. Technical blocks state in Lithuania, Latvia and Estonia.

Table 1. Probable mean values of indicators in cases of two scenarios.

	Indicator		
Scenario	I_1	I_2	I_3
SC2	47.65	63.23	61
SC3	57.5	45	61

means that satisfy equality (9), here C_i ($i = 1, 2, 3$) are independent random variables. C_i can be determined using sum of constants and indicator products (form system of equations (1) with coefficient matrix A_{LT} (8)). In case of normal distributions of indicators, probability distributions of random variables C_i ($i = 1, 2, 3$) are normal as well with means equal to values that are calculated for 2012, i.e. general solution of system of equations (1) with coefficient matrix A_{LT} (8). Denote means are $c_1 = -6.562$, $c_2 = -0.855$, $c_3 = 451.116$ and standard deviations are 10% of its means, i.e. $s_i = 0.1c_i$ ($i = 1, 2, 3$). Multidimensional probability density function (pdf)

$$p(x_1, x_2, x_3) = \prod_{i=1}^{3} \frac{1}{s_i\sqrt{2\pi}} \exp\left(-\frac{1}{2s_i^2}(x_i - c_i)^2\right). \tag{13}$$

BM was applied to obtain posterior pdf

$$p(x_1, x_2, x_3 \mid I_1^*, I_2^*, I_3^*) \propto p(x_1, x_2, x_3) L(I_1^*, I_2^*, I_3^* \mid x_1, x_2, x_3), \tag{14}$$

where $L(\cdot)$—likelihood function

$$L(I_1^*, I_2^*, I_3^* \mid x_1, x_2, x_3) = \prod_{i=1}^{3} \exp\left(-\frac{1}{2\sigma_i^2}\left(I_i^* - \sum_{j=1}^{3} x_j b_{ij} e^{\lambda_j t^*}\right)\right), \tag{15}$$

where σ_i—standard deviation as measure of uncertainty of indicator value forecast (of expert opinion).

The updated point estimates of random variables C_i ($i = 1, 2, 3$) are calculated using posterior pdf

$$\hat{C}_i = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x_i p(x_1, x_2, x_3 \mid I_1^*, I_2^*, I_3^*) \mathrm{d}x_1 \mathrm{d}x_2 \mathrm{d}x_3, \quad i = 1, 2, 3. \tag{16}$$

Forecasted mean values of indicators calculated with Bayesian method point estimates of random

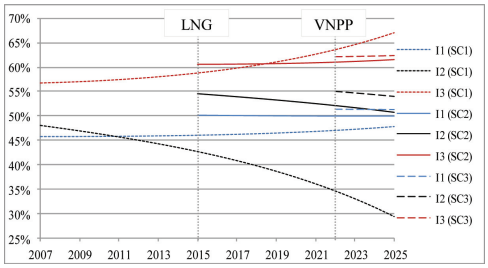


Figure 5. Electricity indicator $I_1(t)$ (blue line), gas indicator $I_2(t)$ (black line), heat indicator $I_3(t)$ (red line); indicators $I_i(t)$ of: SC1 (dot line), SC2 (solid line), SC3 (dash line), $i = 1, 2, 3$.

variables C_i ($i = 1, 2, 3$) was calculated in two scenario cases:

– SC2: LNG in 2015 (I_i^* probable values presented in Table 1, $\sigma_i = 0.5$, $i = 1, 2, 3$);
– SC3: LNG in 2015 (I_i^* probable values presented in Table 1, $\sigma_i = 0.5$, $i = 1, 2, 3$) and VNPP in 2022 (I_i^* probable values presented in Table 1, $\sigma_i = 1$, $i = 1, 2, 3$), i.e. BM was applied twice.

Obtained results presented in Figure 5.

In Figure 5 it is presented that in case business-as-usual (doing nothing) the better results can be expected only in the case of district heat. This can be explained by the fact that LNG terminal may encourage additional use of gas, while preventing the use of biofuel and other renewables for heating. In other cases, new energy objects improve the situation.

In order to be more accurate in long term construction of new facilities it is recommended to recalculate not only separate solution, but also differential equations system (1) coefficients matrix A.

4 CONCLUSIONS

1. The method, based on Bayesian method, explaining how to involve expert judgement as preliminary information with uncertainties on future projects into dynamic different indicator model, is proposed. The solution of this differential indicators system can be used for evaluation of indicators in the future according to the expert opinions.
2. The comparison of energy sector technical block states in three Baltic countries (Lithuania, Latvia and Estonia) was carried out according to the developed methodology. The technical block state is highest in Latvia (approx. 80 percent in 100 percent scale). In Estonia this state is equal to approx. 73 percent, and in Lithuania—approx. 60 percent.
3. The created method of involvement of expert judgement was illustrated by calculating examples for two scenarios—building liquefied natural gas terminal in 2015 and Visaginas nuclear power plant in 2022.

ACKNOWLEDGEMENTS

This research was funded by a grant (No. ATE-06/2012) from the Research Council of Lithuania.

REFERENCES

Augutis, J., Pečiulytė, S., Krikštolaitis, R., Žutautaitė, I. Ušpuras, E. 2012. Dynamic model for energy security level assessment. *Risk Analysis VIII:* 21–30. WitPress.

Augutis, J., Krikštolaitis, R., Lutynska, A.E., Pečiulytė, S., Žutautaitė. 2013. Evaluation of coefficients for energy security indicators system. *SAFE 5:* 21–30. WitPress.

Bernardo, J.M. & Smith A.F.M., 2003. Bayesian theory. John Wiley & Sons.

Berthold, M. & Hand D.J., 2003. Intelligent Data Analysis. 2nd edition.

Golokvosčius, P. 2000. *Differential equations*. Vilnius: TEV (in Lithuanian).

Liquefied Natural Gas Terminal. http://www.sgd.lt.

Žutautaitė-Šeputienė, I., Augutis, J., Telksnys, L., 2010. Parameters estimation in modelling of gas-gap in RBMK type reactor using Bayesian approach. Informatica, 21(2):295–306.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Anthropo-technical systems reliability

D. Laskowski & P. Łubkowski
Military University of Technology, Warsaw, Poland

E. Pawlak & P. Stańczyk
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: The development of new techniques, technology and the progress of civilization meant that man exploits Technical Objects (TO) offers a set of numerous and interrelated services implemented under different types of systems. In most cases, these are anthropo-technical systems (SA-T) taking into account the essential components of the process of exploitation: man—the operator, the technical object—hardware and software, and the environment—external and internal. Was developed a model of situational awareness SA-T in the implementation of services based on efficient transport of data between the operator and TO (machine, robot) using any interface. The result is a proposal to develop a comprehensive measure to estimate the reliability of SA-T using effectiveness and potentiality trajectories identifying the state of readiness of the system. The paper ends with conclusions of the research and a summary with prospects for further analysis SA-T.

1 INTRODUCTION

1.1 *Technical object*

Nowadays, various types of technical objects are exploited being the result of technology development and civilisation progress. Wide spectrum of properties characterising technical objects of the system nature designed today can be divided into subsets of fundamental discriminates (Laskowski D. 2011):

– people being significant participants of each object exploitation process,
– role of an object as a system component and a participant of system-environment relations,
– complexity of the structure and variety and complexity of functions and tasks.

The evolution of techniques, technology and the progress of civilization have made to society currently offers many services to help existence. The undeniable superiority of these services is the flow of data between sender and receiver. These can be both humans and machines (robots). The substrates for this are the various types of communication systems.

There are many indicators to split the system understood as a Complex Technical System/System (CTS, S). For the purposes of this publication, it is proposed to adopt a criterion in the form of: a man (operator), a technical object (hardware, software) and the environment (the impact of external and internal) operating system. So the system is divided into: classical (ST), anthropo-technical (SA-T) and social engineering (SS-T). These assumptions take into account the essential components of the process operation. Inability states of essential components in systems or destructive interactions of users can cause interruptions in transmission and loose of information. Considerable financial losses, human health or even life, depending on a type and the amount of information lost, can be a consequence of failures. That is why the more and more significant is to take widely understood operating requirements into considerations (particularly related to reliability). The required systems reliability can be achieved at least in two ways. Reliability of a system—it is a nondimensional feature of a system describing its readiness to render services and factors affecting this readiness, e.g.: unimpairability, maintainability and providing maintaining resources. From one hand the tendency should be to create a system with components of high unimpairability.

1.2 *Environment technical object*

Transmission of information between the terminal operator and the machine is connected with the flow of data through interfaces in stationary and mobile, simple and complex architectures CTS (S). This process is accompanied by anomalies related to the time-varying:

1. The state of technical and functional system.
2. Destructive: behavior of people, environmental factors (exposure).

Anomalies are different types of events that could disrupt the transport of data in the form of lost information. The consequences of adverse events are: reducing the number of services (e.g. telecommunications sector), financial loss (e.g. the banking, finance and insurance), human health or life (such as medical services, the transport sector ground, sea and air, uniformed services). Now, the growing importance of continuous—time identification of the state of airworthiness (technical and functional) of man and machine. Safety systems have a tendency to fail, which becomes the subject of a detailed analysis and examination procedure to eliminate such danger in the future. In most situations the direct cause of failure may be damage to the system, its exposure to unexpected load, or fault of the employee (Butlewski. & Sławińska 2014).

These important tasks from the perspective of situational awareness are the perception and understanding of events happening around in relation to time and space. Situation awareness is an essential determinant of operation CTS in which data flow is significant and "bad" decisions can lead to serious consequences. For more information we recommend reading e.g. (Nowakowski & Werbińska 2009), where issues on proper maintenance strategy selection and its influence on dependability state of the system are reviewed, or (Kowalski et al. 2014, 2011), where maintenance problems of complex technical systems are investigated in the context of different solution methodology use (Jasiulewicz-Kaczmarek & Drożyner 2013).

Taking into account the conclusions of the analysis of literature study area (reliability system) was assumed to have not been shown explicitly complex mathematical relationships that could be used to estimate the state of airworthiness man-machine system. There are grounds to conclude that the commonly used commercial solutions and research and implementation for many years used a piecemeal approach to achieve and maintain the declared level of airworthiness technical object (the system and its component) for continuous-time ability to implement services. The attention is focused on the analysis and synthesis of selected aspects of the research problem. Not defining numerical indicators and not taking into account technical and functional capabilities CTS and the effects of the conditions and environmental exposures and human origin. In addition, notes the lack of a clearly definite influence are methods of access to the system, data transport mechanisms and guarantee the level characteristics (i.e., reliability, safety, quality, efficiency, etc.) are important from the point of view of the system and the user who is the recipient of its products. This type of approach, particularly in the structures of the system, is focused on one or a few acquaint criteria,

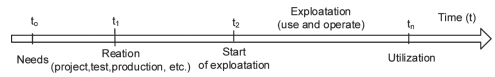


Figure 1. The cycle of existence CTS.

e.g. in the context of the optimization of financial resources, time or space.

It is, therefore definite conclusions from the available publications and the results of scientific research highlight the need for a comprehensive approach, correlating mutual projects in the areas of postulating, design and operational reality in terms of ensuring the proper operation of the OT (Fig. 1).

2 ANTHROPO-TECHNICAL SYSTEMS

2.1 *Model SA-T*

The main predicate research complex technical objects are the concept of "system". Manifested by the existence of a synergistic interaction of its parts was present in (Cempel 2012). The division of the system into components—elements (OTE)—addicted to the study aimed to validate the functionality of the system services. This division is hierarchical, multi-level. In many situations, is one of the initial stages of the development of the formal system description. Assuming assumptions general systems theory stands out, at least a few levels of the existence of systems (Berge 1961). The study adopted the interpretation of "cybernetic system", homeostat based on the transmission and interpretation of data.

In many scenarios, the analysis of the anomaly system is treated as an "or" indivisible. Substantive feature of the system as a whole is that its properties are not trivial functions of the properties of its components. In contrast instantiation is carried out taking into account the relationships between the elements. Become critical in the process of reliability of the item and the need for taking into account external factors (environmental impact). The process of reliability system modeling is a fundamental operation requiring the designer knowledge and technical skills. Supports are mathematical models, system engineering and simulation tools. The final step is to perform simulation studies and locals. For the issue in the article problems OTE collections are: man (operator behaviour), machine (device structures and mechanisms for proper operation) and exposure (resistance to destruction).

In the literature devoted to descriptions of systems you can find many definitions of the term appropriate for the specific situation of research. Therefore, they cannot be used universally for the entire test process system object. The aim of

unifying the nomenclature proposed to adopt a model system of human-machine (Fig. 2).

Depending on the level of detail of the system, its detailed articulation (including definitional) and the articulation of its elements and attributes may be different.

Accordance with the foregoing and publications (Dabrowski 2001), assumes that the measurable properties of a reliability system, respectively interpreted in a certain unit of time (t), are:

1. The potentiality required $(E_{p\text{-}wym}(t))$—determined by the number of services that start and continue the implementation of demanding users of the system.
2. The potential required $(F_{p\text{-}wym}(\Delta T))$—a measure of utility needs addressed at S. This measure to characterize the users' expectations regarding the number and type of services provided over a certain period of time.
3. The potentiality of fit $(E_{p\text{-}dys}(t))$—identified by the number of possible execution services ordered by the user or the probability of an ability condition (properly functioning) for their implementation:

$$E_{p-dys_S}(t,e_i) = f\left[P_{Pf_S}(t,e_i)\right] = \begin{cases} f\left[P_{Pf_ST}(t,e_i)\right] & for \quad ST \\ f\left[P_{Pf_SA-T}(t,e_i)\right] & for \quad SA-T \\ f\left[P_{Pf_SS-T}(t,n,\pi,e_i)\right] & for \quad SS-T \end{cases} \quad (1)$$

where:

– $P_{Pf_S}(t,e_i)$—the probability of an ability condition of the system (ST, SA-T and SS-T) or its components (e_i) taking into account the properties of the inner.

2.2 *Measure of system*

For research purposes, assume that the S classic data transport system (Fig. 3).

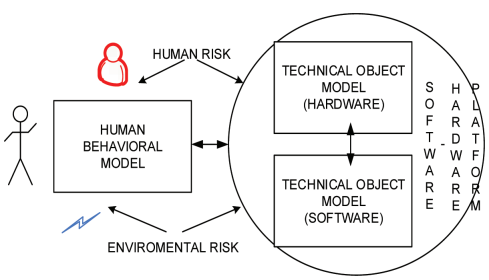


Figure 2. Human-machine system model.

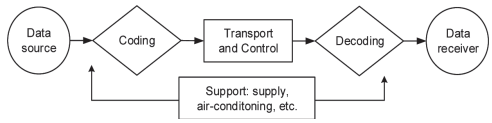


Figure 3. Data transport system model.

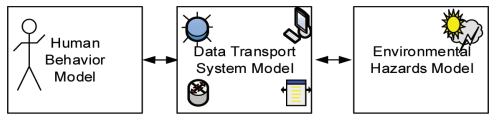


Figure 4. System operator—data transport system—exposure model.

Then it analyzed the system model takes into account the human machine and the environment will contain three elements (Fig. 4).

For the mathematical description of the observed reality in layers (physical, abstract and symbolic) in the S, it is proposed to use the relationship (Cempel 2012, Berge 1961):

$$TO \equiv \langle G, \{Fz\}, \{fk\} \rangle \quad (2)$$

where:

– F_z—attributes and properties,
– f_k—relationships and ties, cooperation,
– G—finite graph of system topology:

$$G = \langle W, K, R \rangle \quad (3)$$

where:

o $W=\{w_l: l=\overline{1, L}\}$, countable set of vertices of the graph (the nodes of the system);
o $K=\{k_m: m=1, M\}$, countable set of branches of the graph (transport channels);
o $R \subset W \otimes^1 K \otimes W$, tripartite relationship of incidence satisfies the condition;
o $B=\{e_i: i=1, I\}$, a size of a system components set is a sum of elements contains:

$$|B| = |W| + |K| \quad and \quad B = \left\{e_i : i = \overline{1, L+M}\right\} \quad (4)$$

In this case the states of system elements can be presented with the vector $\vec{X}^2$ of components $(L+M)$, which take the values *0* or *1*:

$$\vec{X}_{TO} = [\underbrace{x_1, \ldots, x_L}_{L}, \underbrace{x_{L+1} \ldots, x_{L+M}}_{M}] \quad (5)$$

[1]Symbol ⊗ represents the Cartesian product.
[2]Then the operating condition element can be described using the vector.

and components:

$$x_i = x(e_i) = \begin{cases} 1 & when \quad element \quad is \quad able \\ 0 & when \quad element \quad is \quad unable \end{cases} \tag{6}$$

Similarly, the operating states of the system in terms of reliability, it is advisable:
– generalized criterion of suitability of structural:

$$\Phi(S) = \begin{cases} 1 & when \quad system \quad is \quad able \\ 0 & when \quad system \quad is \quad unable \end{cases} \tag{7}$$

– criterion of fitness using the measure (1, 5 ÷ 7) for the system of temporary disablement (Fig. 5):

$$\bigvee_{t \in \Delta t_{zad}} \left[\bigvee_{\substack{E_{p-dys}(t) \in \Delta E_{p-d}(t) \\ E_{p-wym}(t) \in \Delta E_{p-d}(t)}} \left[\begin{array}{l} \left[E_{p-dys}(t) \geq E_{p-wym}(t) \right] \Rightarrow \\ \Rightarrow \left[\Phi(P_{pf_SA-T}, t) \equiv \Phi^{z}(t) \right] \end{array} \right] \right] \tag{8}$$

where:
– t—time, the current while,
– t_z—task time,
– Δt_{zad}—the time interval from the time the task adopted for the start of the task t_0 the moment of the t_z, $\Delta t_{zad} = [t_0, t_z]$,
– $E_{p\text{-}dys}(t)$—potentiality predisposed are value of the interval ($E_{p\text{-}d\text{-}min}(t) \div E_{p\text{-}d\text{-}max}(t)$):[3]

$$E_{p\text{-}dys}(t) \geq E_{p\text{-}wym}(t) \tag{9}$$

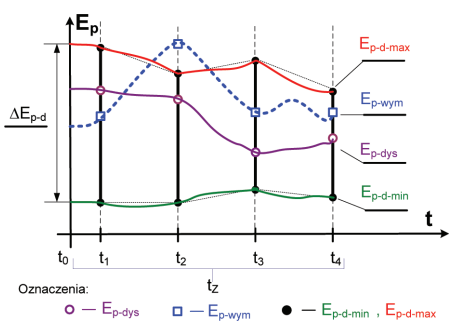


Figure 5. A graphical interpretation of the criterion (8) of an instantaneous system ability state (Dabrowski 2001).

[3]If at a certain time t potentiality predisposed is not less than the potentiality required, the system at time t is fit.

– $E_{p\text{-}wym}(t)$—potentiality required at the time of t,
– $E_{p\text{-}d}$—permissible value of potentiality at the moment t,
– $\Delta E_{p\text{-}d}(t) = [E_{p\text{-}d\text{-}min}(t), E_{p\text{-}d\text{-}max}(t)]$—the range of permissible values of potentiality,[4]
– $\Phi(P_{pf}, t)$—state of the system (P_{pf}—the probability of an airworthiness status),
– $\Phi^{Z}(t)$—the airworthiness status of the system at time t.

If there is even one moment of time t in the interval of the task, in which the potentiality predisposed of the set of potentialities limit is not less than the required potentiality, also belonging to the range of potentiality limit, the state of the system at the moment t is the state of availability (reliability).

The ability criterion is satisfied for the moment t_1, the ability criterion is not satisfied for the moment's t_2, t_3 and t_4. A principal conclusion resulting from the assumptions (6 ÷ 8) and the graphical interpretation of the criterion (Fog 5) of the instantaneous system ability is that, for the system to be able to satisfy functions stated for executing, a value of the required potentiality should at least be equal to a value of the disposed potentiality. In the case of a system it will be the state of executing a service, e.g. viewing electronic mails, viewing WWWs, loading ftp files, and so on.

Basing on accepted initial assumptions related to the criterion of the system ability was proposed to define the SA-T reliability as follows: "Reliability of a anthropo-technical system is defined as the capability to perform a system service for a defined user in conditions influenced by stresses[5], and to adaptation of components owned by the system in order to restore its correctness of operation".

The term "SA-T reliability" can be interpreted also as the ability of an application based on a communication component of a basic system to satisfy ordered critical requirements (e.g. related to security, reliability, real time response and faultlessness) in specified time in spite of unfavourable conditions. An influence range of harmful factors is in general definable, but some situations non-defined earlier should be expected.

Given the multiplicity and complexity of the factors proposed to be grouped into meaningful sets

[4]The range of permissible values of potentiality is determined, inter alia, the properties of the object, type your task, the task conditions, technical requirements, security, economic, administrative—it is, therefore, about the relative width of the interval.

[5]Stresses are sets of natural factors and the ones resulting from human activities, people, other living being and technical equipment presence.

of determinants in the form of intrinsic properties of the system, the properties of the operator and the harmful effects of the environment as a component of the formula for the probability of an ability condition:

$$P_{Pf_S}(t,e_i) \cong f\left(P_{wWi}, P_{pOpi}, P_{zOti}\right) \tag{10}$$

where:
P_{wWi}—probability of proper operation of the TO:

$$P_{wWi}(t,e_i) \cong f\left(K_{gi}, P_{sri}, P_{sni}\right) \tag{11}$$

where:
K_{gi}—unsteady readiness index (taking into account the intensity of damage λ and repair μ):

$$K_{gi}(t,e_i) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i}\ e^{-(\lambda_i+\mu_i)t} \tag{12}$$

P_{sri}—the likelihood of blockages in the ith element taking into account the model of service requests,

P_{sni}—the probability of loss of data in a stream of the ith element functioning as a result of incorrect synchronization (signalization)[6].

P_{pOpi}—the probability of correct operation of the operator TO with regard to knowledge and experience in project implementation time regimes (Fig. 6) determined on the basis of the method of HCR (*Human Cognitive Reliability*, Hannaman *i* in.):

$$P_{bOp_HCR} = \exp\left[-\left(\frac{t}{t_{0,5}} - C_{e,i}\right)C_{g,i}^{-1}\right]^{B_i} \tag{13}$$

where:
C_{ei}, C_{gi}, B_i—coefficients depend on the type of work being done (education, experience, reflexes, rules, etc.),

t—time available to complete the task,

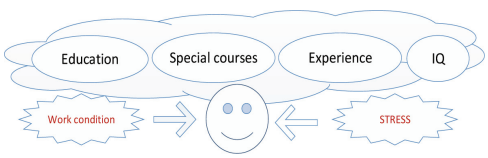


Figure 6. Behavior operator (determinants) model.

[6]Probability value is determined on the basis of technical parameters of the signaling system.

$t_{0,5}$—the average time usually sufficient to complete the task (k_1—experience, k_2—the level of stress, k_3—ergonomic workplace):

$$t_{0,5} = t_{0,5n}\left(1+k_1\right) + \left(1+k_2\right) + \left(1+k_3\right) \tag{14}$$

P_{zOti}—likely to remain CTS able to take into account the suitability of the environment impact:

$$P_{zOt}\left(t, U_k^{\times h}\right) = \left\langle E_{dys}(t) = f\left(P_{e_i}\left(U_k^{\times h}\right)\right)\right\rangle \tag{15}$$

where:
$P_{ei}(U_k^{xh})$—likely to remain in the state of airworthiness e_i after tripping on an object a series of factors U_k of multiplicity h[7]:

$$P_{e_i}\left(U_k^{\times h}\right) = \prod_{k=1}^{h}\left[1 - P_{de_i}^{U_k}\left(r_n^k\right)\right] \tag{16}$$

where:
$P_{de_i}^{U_k}(r_n^k)$—probability of destruction (electric, lower the state of airworthiness) e_i present in the nth (e.g. ring) the effect of factor U_k:

$$P_{de_i}^{U_k}\left(r_n^k, n, \pi, e_i\right) = 1 - \exp\left[-\delta\left(\frac{P\mathrm{r_n}}{P_{ue_i}}\right)^2\right] \tag{17}$$

where:
- δ—parameter of distribution,
- r_n^k—radius of influence of nth exposure of the πth set of types of exposures,
- P_{uei}—probability of damage e_i component systems of nth exposure of the πth-set of types of exposures.

Forms of measure (indicator) of the proper SA-T reliability are:

1) Comprehensive:

$$E_{p-dys_S}(t,e_i) = f\left[P_{Pf_S}(t,e_i)\right] = f\left[P_{wW}(t,e_i), P_{bOp_HCR}(t,e_i), P_{e_i}\left(t,e_i,U_k^{xh}\right)\right] \tag{18}$$

2) Elaborated for:
   - ST (11):

$$E_{p-dys_ST}(t,e_i) = q_1 P_{wWi}(t,e_i) \tag{19}$$

[7]The line may include the harvest Ω,Π factors, some of which may appear multiple times. It is understood that the impact area is divided into zones of different intensities of impact.

– SA–T (11,13):

$$E_{p-dys_SA-T}(t,e_i,U_k^{xh}) = q_1 P_{wW}(t,e_i)\cdot q_2 P_{bOp_HCR}(t,e_i) \quad (20)$$

– SS–T (11,13,16):

$$E_{p-dys_SS-T}(t,e_i,U_k^{xh}) = q_1 P_{wW}(t,e_i) \cdot q_2 P_{bOp_HCR}(t,e_i)\cdot q_3 P_{e_i}(t,e_i,U_k^{xh}) \quad (21)$$

where:
q_i—weight of component probability value depending on a number of components.

Inference on SA-T reliability was based on a statistical estimation fit potentiality based on the output patterns (19 ÷ 21) and the probability distributions. Below the critical value of $E_{p\text{-}dys}$ services will not be realized and OT will be able to unfitness technical and functional well.

3 RESEARCH SA-T

3.1 *Testbed*

Known scientific studies on the issues presented in the article show a diverse and inconsistent methodology of the identification CTS (ie, data transport system, goods or people). A multitude of solutions is closely linked with the selective choice of system characteristics and interests of researchers.

From the analysis of previous publications revealed that this issue is still a research model and design. Due to the ongoing process of analysis and research of the subject area, it was decided here on their own examination of the proposal taking into account the copyright approach to determine the measure of SA-T. These measures include hardware and software properties of the inner components, the proper operation of the operator in the presence of environmental hazards.

For the representative object of research and modeling adopted SA-T reflects the data transfer by classic architecture (Fig. 7). Survey methodology assumes the correctness of construction architecture SA-T in the context of its operation and comes to the implementation of a number of analytical and research work, which is important (Bajda et al. 2011, Laskowski D. 2013):

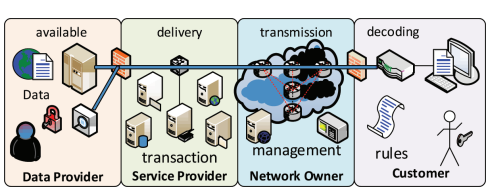


Figure 7. SA-T architecture.

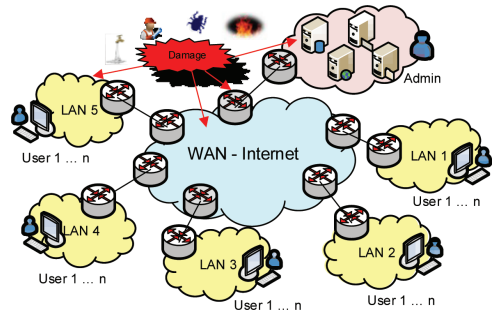


Figure 8. Reference architecture system testbed for research.

1. SA-T is a composition of elements in the chain functional implementation services (e.g. transfers).
2. Elements of SA-T are variable during the fitness of functional and are administered independently.
3. Contracts motor brings the maximum value of static data streams between the areas in SA-T.
4. The test plan included the verification of the suitability of the technical and functional variable traffic volumes and fixed structure research, randomness exposure and damage to components and a change in the level of knowledge of the operator.
5. The reliability of the results was based on the maximum mapping the actual conditions of use SA-T, the cardinality of measurement, reproducibility of results, etc.

This architecture is used in most current system services such as VoIP (Voice over IP), WWW, FTP and database (Lubkowski & Laskowski 2013).

It was therefore decided to extend it for the adopted research purposes (Fig. 8). SA-T contains important elements (testbed system architecture) for the realization of the services necessary to determine the potentiality trajectory.

4 RESULTS

On the basis of simulation studies and tests were obtained extensive collection of local data. Exemplary data is entered in the Table 1 and shown in the drawings (Figs. 9, 10).

Table 1. Example of output data for Group A scenarios.

Lp.	Parameter	Value		
		Minimum [%]	Maximum [%]	Average [%]
Scenario expert knowledge (Fig. 9)				
1	$E_{p\text{-}dys_ST}$	99,334735	99,7877975	99,56105
2	$E_{p\text{-}dys_SA\text{-}T}$	29,160907	89,8280945	54,16555
3	$E_{p\text{-}dys_SS\text{-}T}$	20,827015	80,8401576	44,53682
Scenario expert knowledge_difference (Fig. 10)				
4	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SA\text{-}T}$	9,9597030	70,173827	45,39550
5	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SS\text{-}T}$	18,947639	78,507719	55,02423
6	$E_{p\text{-}dys_SA\text{-}T}$—$E_{p\text{-}dys_SS\text{-}T}$	8,3338924	10,300253	9,628727
Scenario A1_advanced knowledge (Fig. 11)				
7	$E_{p\text{-}dys_SA\text{-}T}$	25,55337	78,7153405	47,46465
8	$E_{p\text{-}dys_SS\text{-}T}$	18,250477	70,8393134	39,02711
Scenario A1_advanced knowledge _ difference (Fig. 12)				
9	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SA\text{-}T}$	21,072457	73,7813622	52,09639
10	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SS\text{-}T}$	28,948484	81,0842576	60,53394
11	$E_{p\text{-}dys_SA\text{-}T}$—$E_{p\text{-}dys_SS\text{-}T}$	7,3028954	9,0259953	8,437544
Scenario A1_primary_knowledge (Fig. 13)				
12	$E_{p\text{-}dys_SA\text{-}T}$	9,0188375	27,7818849	16,75223
13	$E_{p\text{-}dys_SS\text{-}T}$	6,4413450	25,0021106	13,77427
Scenario A1_primary_knowledge_difference (Fig. 14)				
14	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SA\text{-}T}$	72,005912	90,3158976	82,80882
15	$E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SS\text{-}T}$	74,785686	92,8933901	85,78677
16	$E_{p\text{-}dys_SA\text{-}T}$—$E_{p\text{-}dys_SS\text{-}T}$	2,5774925	3,1856454	2,977956

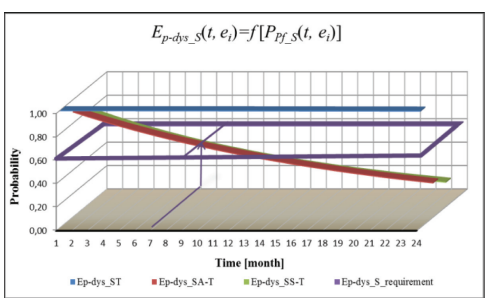


Figure 9. Scenarios 1_the knowledge of the expert.

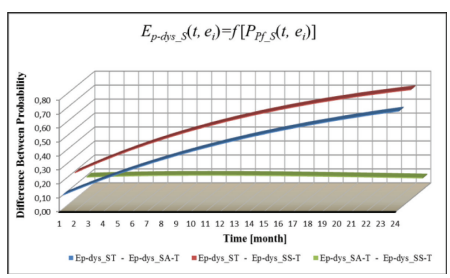


Figure 10. Scenarios A1_the knowledge of the expert difference.

The resulting trajectories of potentiality are taking into account:

1. Determinants:
   – base of stationary relations system and random occurrence of exposure,
   – detailed: change in the level of knowledge.
2. The result, values for charts:
   – Trajectory ST ($E_{p\text{-}dys_ST}$), SA-T ($E_{p\text{-}dys_SA\text{-}T}$) and SS-T ($E_{p\text{-}dys_SS\text{-}T}$) for the knowledge of the Expert (Fig. 9), Advanced (Fig. 11) and Primary (Fig. 13),
   – Differences in the probabilities of trajectories:
     o ST ($E_{p\text{-}dys_ST}$)—SA-T ($E_{p\text{-}dys_SA\text{-}T}$),
     o ST ($E_{p\text{-}dys_ST}$)—SS-T ($E_{p\text{-}dys_SS\text{-}T}$),
     o SA-T ($E_{p\text{-}dys_SA\text{-}T}$)—SS-T ($E_{p\text{-}dys_SS\text{-}T}$)

for the knowledge of the Expert (Fig. 10), Advanced (Fig. 12) and Primary (Fig. 13).

On the trajectory (Fig. 9), depending on the requirements of the operator, determining a required critical value ($E_{p\text{-}dys\text{-}requirment}$), below which it is believed that OT is no longer fit for operation.

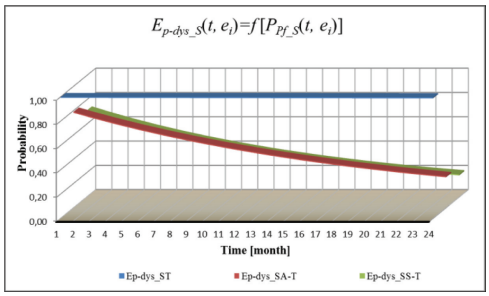


Figure 11. Scenarios A1_advanced knowledge.

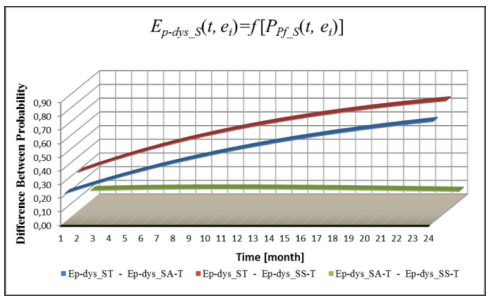


Figure 12. Scenarios A1_advanced knowledge_ difference.

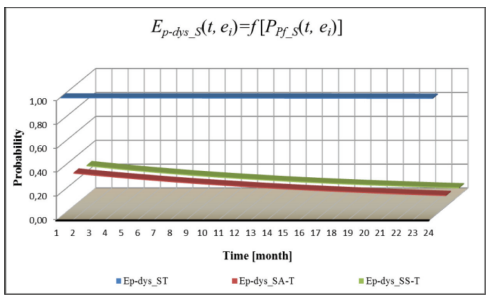


Figure 13. Scenarios A1_primary knowledge.

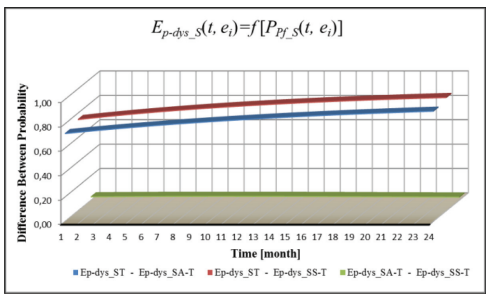


Figure 14. Scenarios A1_primary knowledge_ difference.

For example, the value may be 0.6, and the probability of $E_{p\text{-}dys\text{-}requirment}$ is reached after 7 months.

On the basis of the performed analysis and research projects of local output data were collected and subjected to statistical analysis. Such a procedure has facilitated clarification of observations for the period concerned (24 months), of which the main ones are:

1. Trajectories $E_{p\text{-}dys_ST}$, $E_{p\text{-}dys_SA\text{-}T}$, $E_{p\text{-}dys_SS\text{-}T}$ can be divided into several major collections are characterized by similar shapes depending on:
   – $E_{p\text{-}dys_ST}$—network traffic—"slightly" linearly decreasing (this effect is properly functioning and "high" reliability of hardware and software),
   – $E_{p\text{-}dys_SA\text{-}T}$: knowledge of the operator—"significantly" exponentially decreasing and value of traffic—"significantly" less than the influence of the human factor,
   – $E_{p\text{-}dys_SS\text{-}T}$: knowledge of the operator, environmental hazards and human—"significantly" exponentially decreasing and traffic value are smaller and oscillate at 1%.
2. The variability of the differences between the trajectories $E_{p\text{-}dys_ST}$, $E_{p\text{-}dys_SA\text{-}T}$, $E_{p\text{-}dys_SS\text{-}T}$ can be divided into two basic sets of relationships:
   – $E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SA\text{-}T}$ and $E_{p\text{-}dys_ST}$—$E_{p\text{-}dys_SS\text{-}T}$—"significantly" logarithmic growing,
   – $E_{p\text{-}dys_SA\text{-}T}$—$E_{p\text{-}dys_SS\text{-}T}$ – close to constant in time.

The data obtained on the basis of the concept developed, confirmed the need to consider many factors component. These factors determine the suitability of the technical SA-T (also ST, SS-T) and the correctness of the implementation of network services.

Used development tools have reduced the time and effort of research, and contributed to the reliability and reproducibility of the data. Also facilitate the removal of the trajectory of potentiality. Reasonable to conclude, that the results will enable the implementation of a synthetic analysis and clarification of observations with regard to the conduct of subsequent studies human-machine systems.

5 CONCLUSIONS

The main findings from the analysis of theories and research results in the field of system reliability during potentiality trajectory ($E_{p\text{-}dys_ST}$, $E_{p\text{-}dys_SA\text{-}T}$ and $E_{p\text{-}dys_SS\text{-}T}$) are:

1. It is possible to designate this kind of value for respectively the exact explicit baseline data identifying properties hardware and software platform, operator and environmental hazards.

2. Accuracy of change and shape of the trajectory depends on multiplicity and diversity of events occurring in the system environment.
3. The impact of the factors considered in the order of their weight (importance) is as follows:
   – environmental exposure and destructive human behavior (random) and knowledge operator hardware and software platform (Expert and Advanced),
   – traffic value (appropriate to the reported demand of the service and exchanged data synchronization) and technical parameters of the hardware and software platform.
4. The method is universal and is used to identify, by estimating selected parameters (i.e. potentiality), current and future technologies and network technologies used in the system (ST, SA-T, SS-T).
5. The components of this method may constitute a separate method to identify the impact of individual factors (ownership, i.e. technical, operator or exposure) environmental airworthiness status of the system or its component.

Potential measures proposed in the form of probabilities of system reliability can be used at any system operational step to restore or increase the SA-T ability state with taking into account stresses possible to occur. Therefore it is also advisable not to confine to design and establish an object rendering services, but to carry a permanent process of monitoring operational status of the network.

Knowledge related to the shape and location of potential trajectories, determined by using values of a reliability indices distribution for a anytime hour period of using, can considerably influence improving management of the operational process. This influence is possible first of all because of using the results of the trajectories synthesis in the formulation process of prognostic conclusions and operating decisions.

It seems reasonable to say that there is a need for further analysis and research undertaken scientific problem to accurately detail the relationship between the various elements of the COT analyzed in a broader spectrum of events anthropo-technical. The developed method can also be applied to other transport systems, and more.

REFERENCES

Bajda A., Wrażen M., Laskowski D. 2011. Diagnostics the quality of data transfer in the management of crisis situation, Electrical Review 87(9A), pp. 72–78, Poland.

Berge C. 1961. Théorie des graphes et ses applications, Collection Universitaire de Mathématiques II, Paris: Dunod. English edition, Wiley.

Butlewski, M., Slawinska, M. 2014. Ergonomic method for the implementation of occupational safety systems, Occupational Safety and Hygiene II—Selected Extended and Revised Contributions from the International Symposium Occupational Safety and Hygiene, SHO 2014, pp. 621–626.

Cempel Czesław. 2012. http://neur.am.put.poznan.pl/.

Dabrowski T.M. 2001. Diagnosing anthropo-technical systems in terms of potentially—effects. WAT, Poland.

Jasiulewicz-Kaczmarek M., Drozyner P., 2013. Social dimension of sustainable development—safety and ergonomics in maintenance activities, C. Stephanidis and M. Antona (Eds.): Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion, UAHCI/HCII 2013, Part I, LNCS 8009, pp. 175–184. Springer, Heidelberg

Kowalski, M., Magott, J., Nowakowski, T., Werbinska-Wojciechowska, S. 2014. Exact and approximation methods for dependability assessment of tram systems with time window. European Journal of Operational Research, vol. 235, nr 3, pp. 671–686.

Kowalski, M., Magott, J., Nowakowski, T., Werbinska-Wojciechowska, S. 2011. Analysis of transportation system with the use of Petri nets. Maintenance and Reliability, Issue: 1, pp.: 48–62.

Laskowski D. 2011. Problems of Dependability and Modeling Application of Unimpairability and Congestion Indices in Defining Survivability of a Teleinformation Network (STI), DepCoS-RELCOMEX '11, WUoT, p. 173–190, Poland.

Laskowski D., Lubkowski P, Kwasniewski M. 2013. Identification of suitability services for wireless networks, Electrical Review 89 9/2013, Sigma-Not, pp. 128–132, Poland.

Lubkowki P., Laskowski D. 2013. The end-to-end rate adaptation application for real-time video monitoring, Advances in Intelligent Systems and Computing, pp. 295–305, Springer International Publishing AG, Switzerland, Volume 224.

Nowakowski T., Werbinka S. 2009. On problems of multicomponent system maintenance modelling. International Journal of Automation and Computing, vol. 6, nr 4, pp. 364–378.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Cost-benefit analysis of surveillance technologies

Pei-Hui Lin & Coen van Gulijk
Safety Science, Technical University of Delft, Delft, The Netherlands

ABSTRACT: There are several types of surveillance devices in the market, each with its own operating characteristics. Since the terrorist attack of 9/11 there has been much focus on preventing or mitigating damages and causalities caused by terrorist activities. A key issue is whether the investment in fighting crime and counter-terrorism devices is well spent in a manner that optimizes public safety in a cost-effective manner. SURVEILLE is a research project funded within the EU Commission FP7 framework where one of the objectives is to assess the benefits and costs of surveillance technology. This paper reports on ongoing work of cost-benefit modelling for security that is performed within in this project.

This paper provides a brief overview of the quantification method for cost-benefit models for security devices. Currently, a straightforward and easy-to-use cost-benefit analysis of surveillance technologies is not available. A cost-benefit model considering probabilistic terrorism risk assessment is developed. The model developed here considers probability of attack, risk reduction, losses, and costs of security devices. However, it is found that a full cost-benefit analysis requires a substantial effort, even for a single surveillance device which may be difficult in operational organizations such as the Police. A brief discussion on mathematical modelling is shown in this paper. But more detail discussion can be found in the SURVEILLE project report that is available through the website[1]. Special attention was given to "cost" modelling of the security device in this paper. The paper ends with discussions of the use of cost modelling in a (semi-)quantitative cost-benefit analysis for surveillance. We are currently performing a case for the remainder of the SURVEILLE project, but cannot disclose the results. These results will be available on the SURVEILLE website later during the project.

1 INTRODUCTION

There are many types of surveillance devices that you can buy today. Since the terrorist attacks of 9/11 there has been much focus, and funding, on preventing or mitigating damage and casualties caused by terrorist activities. However, it is not quite transparent whether anti-terrorist spending's are cost-effective.

SURVEILLE is a research project funded within the EU Commission FP7 framework where one of the objectives is to assess the benefits and costs of surveillance technology. Work towards this objective is done through technology assessment experts operating in constant interaction with lawyers, ethicists and social scientists. Currently, a straightforward and easy-to-use cost-benefit analysis of surveillance technologies is not available. This paper reports on ongoing work of cost-benefit modelling for security that is performed within in this project.

Section 2 provides a brief overview of the quantification method for cost-benefit models for security devices. It is found that a full cost-benefit analysis requires a substantial effort, even for a single surveillance device which may be difficult in operational organizations such as the Police. The discussion on mathematical modelling is briefly summarized in Section 3. But more detail discussion can be found in the SURVEILLE project report that is available through the website[2]. Special attention was given to "cost" modelling of the security device in Section 4. Section 5 discusses the use of cost modelling in a (semi-)quantitative cost-benefit analysis for surveillance.

2 A BRIEF OVERVIEW OF THE QUANTIFICATION METHOD FOR COST-BENEFIT MODELS FOR SECURITY DEVICES

2.1 *Economic analysis*

A number of approaches exist for calculating and comparing the benefits and costs of a government policy. Cost-effectiveness analysis and cost-benefit analysis are among the most commonly used tools for this kind. Cost-benefit analysis compares a programme's benefits to a stakeholder with the costs to that stakeholder. This approach places benefits and costs in comparable terms, usually dollars. Cost-

[1]www.surveille.eu.
[2]www.surveille.eu.

effectiveness analysis determines how much is spent on a programme to produce a particular outcome (or how much of a particular benefit will result from a given expenditure). Unlike cost-benefit analysis, cost-effectiveness analysis only requires that costs be monetized (Dhiri & Brand, 1999; Cohen, 2004).

There are two principle types of formulation of cost-benefit analysis (European Commission, 2004). One is "net value of costs and benefits". This cost-benefit approach uses a net present value formula to make future costs and benefits comparable with present costs and benefits. It measures the benefits versus the costs in a well-defined period.

$$NPV = \sum_{t=0}^{T} \left(\frac{B_t - C_t}{(1+r)^t} \right) - K_o$$

NPV = net present value
B_t = benefits of the project at time t
C_t = operational costs of the project at time t
r = rate of discount
T = lifetime of the project
K_o = initial costs of the project in the base period

The project is considered as financially feasible if the calculated NPV > 0.

Alternatively one may also use a "cost-benefit ratio" formula. In this case a quotient of the net present benefits and the net present costs is calculated. If the ratio is >1 the social benefits outweigh the cost. The bigger the ratio, the better the project.

$$CBR = \frac{\sum_{t=0}^{T} \frac{B_t}{(1+r)^t}}{\sum_{t=0}^{T} \frac{C_t}{(1+r)^t}}$$

However, generally speaking cost-benefit analysis used in law enforcement and crime prevention policies is still rather simple and usually takes only some of the outcomes into account (European Commission, 2004). Moreover, after the terrorist attack of 9/11 there has been much focus on preventing or mitigating damage and causalities caused by terrorist activities. A key issue is whether the investment in counter-terrorism devices is well spent in a manner that optimizes public safety in a cost-effective manner. However, to compare costs and benefits requires the quantification of threat probability. Threat probability is the likelihood that a threat will occur. The formulas mentioned above do not include the issue of risk assessment or address the quantification of security risks (e.g., Stewart et al. 2006; Stewart and Netherton 2008; Dillon et al. 2009; Cox 2009). This is a challenging task, but necessary for probabilistic terrorism risk assessment. In next section, we will discuss the detail formulation of the net benefit of a security measure.

2.2 *Cost-benefit model for a security device*

As stated, a key issue often being raised in investing in security measures is the probability of crime. Considering the risk assessment, the formula of Stewart and Mueller (2011) is particularly useful for our project that is specifically designed for security devices. We can use this formula as a guideline to quantify the net benefit of a security device. A security measure is cost-effective when the benefit of the measure outweighs the costs of the security measure.

The net benefit of a security measure can be expressed as follows:

$$\begin{aligned} Net\,benefit = {} & P(attack) \times C(loss) \\ & \times \Delta R - C(Security) \end{aligned} \quad (1)$$

- P ($attack$): the probability of a successful attack is the likelihood that a successful terrorist attack will take place in the absence of the security measure.
- C ($loss$): the losses in the successful attack. This includes fatalities and damage to the infrastructures, as well as the psychological and political impact.
- ΔR: percentage reduction in risk. This is the degree to which the security measure protects against a terrorist attack. If a security device will foil every threat, then the risk reduction is 100%.
- C (security measure): cost of security measures. This includes public and private economic costs of applying a security device, and infringement of fundamental rights by this device.

The risk reduction ΔR in Stewart and Mueller (2011) is presented as risk percentage achieved by the presence of advanced image technology in airports. The paper by Stewart and Mueller (2011) considers a multidimensional decision problem with many possible interactions between security measures, threat scenarios, threat probabilities, risk reduction and losses. This means that it considers the risk reduction of several security measures. In this research, we will not consider the combination of different control measures, but rather focus on one security device at a time.

In equation (1) the amount of risk reduction is formulated as $P(attack) \times \Delta R$. In this research, we can re-formulate $P(attack) \times \Delta R$ as:

$$\begin{aligned} P(attack) \times \Delta R &= P(attack) \\ &\times P(success\,detect \mid attack) \\ &= P(attack) \times (1 - P(no\,detect \mid attack)) \end{aligned} \quad (2)$$

Thus, equation (1) becomes

$$\begin{aligned} Net\ benefit = {} & C(loss) \times P(attack) \\ & \times (1 - P(no\,detect \mid attack)) \\ & - C(Security\,measure) \end{aligned} \quad (3)$$

P(*no detect*|*attack*) is defined as 'false negative rate' which can be obtained based on the testing and evaluation of a security device. Such testing is normally required before a device can obtain state approval.

3 DISCUSSION ON MATHEMATICAL COST MODELLING

A full cost-benefit analysis requires a substantial effort for a single surveillance device. Each part of the parameters in equation (3) is discussed separately in the SURVEILLE project, but due to the length restriction of the ESREL paper submissions, the discussion on mathematical modelling for each parameter is briefly summarized here.

1. Cost of loss includes direct tangible costs of a terrorist incident, for example, the replacement costs of property damage after a terrorist incident; and intangible costs of terrorism includes, for instance, loss of lives after an attack, fear or social tensions in relation to terrorist activity, etc. When talking about cost-benefit analysis, a big concern in applying such a method to the case of security is that it requires the researcher to monetize the intangible costs of terrorism, such as value of life. It is very difficult, if not outright unethical, to obtain an objective value for a human life. There is now extensive literature on the value of life, which should not be interpreted as the value of any one particular life, but instead, of society's value of saving a "statistical" life.

   Other intangible costs are also legitimate costs to incorporate into cost-benefit analysis. These could be psychological and emotional costs, such as the cost of pain, suffering and loss of quality of life resulting from victimisation (Cohen et al. 2004). Estimation of these costs can be also difficult. However, a number of methods, such as method based on jury award data (Cohen 1988; Cohen 2000; Miller et al. 1996) or willingness to pay (Cohen 2000), have been developed to place monetary estimation on those intangible costs.

   During the development of cost-benefit model in this project, it is controversial if non-economic values are calculated. It can be argued that placing a monetary figure on a person's life is cold and detached; however, the alternative of not recognising this cost is probably also arguable. Currently placing monetary figure in those intangible costs is still arguable in our project. If the decision in the SURVEILLE project is to apply a formal cost-benefit analysis, then the information provided here give us an idea of how to quantify these impacts.
2. *P*(*attack*): The probability of a successful attack is the likelihood that a successful terrorist attack will take place in the absence of the security measure. Often, the data on the probability of attack is scarce and this makes the estimation of likelihood difficult. Due to this reason, Stewart and Mueller (2011) use a practical approach, "break even" cost-benefit analysis that finds the minimum probability of a successful attack required for the benefit of security measures to equal their cost. This means that they set net benefit in equation 1 to be zero and calculated the minimum attack probability necessary for full-body scanners to be cost-effective.

   In the safety domain, we also face the same severe limit on the availability of data to quantify failure probabilities. Expert opinion in the form of subjective probabilities has been a dominant source for failure probabilities in quantifying risk in safety science. Cooke (1991) and Cooke and Goossens (2000) presented a structured expert judgment procedure to combine experts' opinion in a scientifically defensible way. The overall goal of the method developed by these authors is to achieve rational consensus in the resulting assessments, and thus to enable the information of diverse experts or stakeholders to be incorporated into the process by which the results are reached. We have successfully applied this approach in a series of studies in the field of aviation and chemical industry studies (Ale et al. 2009; 2011; 2013) with Bayesian Belief Networks (BBNs) quantification. Although the structure expert judgement is not yet implemented in the security world, the scientific proof of such a method can be implemented in this domain.
3. 1 – *P*(*no detect*|*attack*) is the amount of risk reduction achieved by deploying a single device. This technical feature related to false negative rate often can be obtained based on the testing and evaluation of a security device before a device can obtain state approval. However, in reality, to decrease the false negative rate in the system, a practical solution for homeland security and international security is to choose a set of alternative devices to be combined together, to increase inspection criteria, or to incorporate operators to control risk. Stewart and Mueller (2011) assume the security measures are linear and use reliability block diagram to calculate risk reduction. However, in reality the inspection criteria, operators and security devices are not linear to foil terrorist attacks and there is uncertainty involved in risk reduction. In the SURVEILLE project report[3], Bayesian Belief Net approach

[3]www.surveille.eu.

is proposed to deal with uncertainty of risk reduction in a complex system/scenario.

4. Cost of a security device: as mentioned above in equation (1), the cost of a security device should include the economic costs of applying a security device, and indirect costs associated with using a device (e.g. infringement of fundamental rights as regards the protection of personal data, privacy, and freedom of thought) as defined in the project. It was decided by the project that analysis of cost security device is a precondition for evaluating the impacts of different surveillance systems for the security of the citizens. Therefore, special attention was given to cost modelling of the security device in the SURVEILLE project report. Next section shows the direct economic costs developed in that report.

4 COST MODELLING

4.1 *Literature review of cost models*

A literature review of cost modeling of security devices is conducted in this section. There is no general guideline on the cost modelling of security devices in technical scientific literature. Our literature review produced three topics which have contributed to our study:

- Assessing the impact of CCTV
- Selecting screening technologies for checked baggage inspection systems at airports
- Analyzing crime prevention programs

The first two topics are related to specific security measures. The last topic relates to national strategy on community safety and crime prevention. The purpose of the crime prevention programs studies is to build comprehensive and standard crime prevention measures for various types of programs. The governments of both the United Kingdom and Canada want to facilitate the comparison of cost-benefit analysis, thus building a comprehensive knowledge base in crime prevention programs to support the development of sound policy. The "cost parameters" incorporated in these three topics are particularly interesting for our research in cost modelling for surveillance technologies. As a result of the literature review, Table 1 summarizes all the variables considered in our literature review.

4.2 *Cost modelling of a security device*

The cost modelling of surveillance technology is exhibited as the annual cost of using devices to meet the security demand. The annual cost is based on the variables shown in Table 1. The cost model in our research includes the fixed cost and operational costs and also takes into account the costs associated with resolving false positive alarms.

There are two types of errors that any security device can make. A false positive reading when the device identifies an object (person or thing) as potential hazard when it is not. This is a problem because every such false reading leads to additional steps being taken that causes inconvenience to consumers, delays system operation, and costs money. The impact of this error reading is taken into account in the cost of the security measure that formulated in equation 4. Another type of errors is false negative reading when the hazard is actually present but a single device fails to recognize it. The designers of the system are most concerned with false negative readings, i.e. a situation with a real threat is not detected by the system. The consequence of this error may lead to loss of lives and infrastructure, and disruption of the transportation system. This is the type of error we do not want. The false negative error is incorporated in the cost-benefit equation showed in section 2.2.

Based on the analysis of Table 1, the cost model in this project considers:

- purchase price and installation cost—*P&I*
- space requirement cost—*S*
- human resources cost including any training that is required to operate the security equipment (start-up and in-service)—*H*
- maintenance and sustainability cost (e.g. renewing license, rental cost, and necessary manpower)—*M*
- cost of equipment operation such as power consumption—*O*
- other running costs (e.g. office furniture, transport, insurance, stationery items)—*R*
- false-positive rate—*FA*

The annual cost of a surveillance technology is modelled as follows:

$$C(\textit{security measure}) = \frac{[P\ \&\ I + S + H + M + O + R + FA]}{T_S} \tag{4}$$

- $\boldsymbol{T_S}$ = *desired system service time* (*year*). This is independent from which device is used.
- $\boldsymbol{P}\ \&\ \boldsymbol{I} = C_{p\&i} \times \lceil D_S / R_D \rceil \times \lceil T_S / T_D \rceil$

  $C_{p\&i}$ = purchase and install cost/per device;
  $\boldsymbol{D_S}$ = system operating demand;
  R_D = device processing rate including the waiting time (time/hour); $\lceil D_s / R_D \rceil$ determines the number of devices needed to meet the demand and the standard average waiting time; The processing

Table 1. Variables considered in the reviewed literature.

Aviation-checked baggage security system		Crime prevention program		CCTV
(Virta et al. 2003) (Jacobson et al. 2006)	(Blejcharova et al. 2012)	(Legg & Powell, 2000) (Hornick et al. 2000)	(Gill and Spriggs, 2005)	(Hornick et al. 2000)
Purchase and installation cost		Staff cost Recruitment	Personnel	Staff salaries and benefits
Expected annual maintenance costs		Training	Training	Staff training costs
Annual lease expenditure		Premises	Premises	
Operation of baggage screening security device per checked bag inspected		Equipment Purchase & rental costs: electrical appliances, office furniture, telephones, vehicles, fences, gates	Equipment	Equipment Purchase & rental costs (including office space)
		Research cost Publicity cost	Research, advertising and publicity	Advertising
		Running costs: (telephone, post, insurance, stationary items, vehicles, equipment maintenance)	Transport	– Furniture – Telephone, fax, mail, etc. – Office supplies – Utilities (heat, water, electricity) – Insurance (e.g., liability, automotive, property) – Transport
			Other overheads	Client expenses
False clear cost	False clear cost			Volunteer time for partner networks and administration
False alarm cost	False alarm cost			Volunteer time for client services
True clear cost				Victim costs
True alarm cost				In-kind resources (e.g., resources shared from host agency such as space, furniture, computers)

rate is an important factor that affects the number of devices required. For instance, the processing rate for automated x-rays for scanning baggage is 1200–1500 bags/hour. An EDS machine is 150–200 bags/hour. Thus, the annual processing capacity can be estimated by processing rate *operating hours/day*days/year. If the maximum annual requirement is denoted by D_S, the number of devices required is calculated as $\lceil D_s / R_D \rceil$.

$\boldsymbol{T_D}$ = lifetime of a surveillance device(year); $\lceil T_S / T_D \rceil$ determines the number of times that the security devices need to be purchased over a given time period.

- $\boldsymbol{S} = C_s \times \lceil D_s / R_D \rceil$
  C_s = space requirement cost/per device
- $\boldsymbol{H} = \boldsymbol{N}_P \times \lceil D_s / R_D \rceil \times C_P$
  $\boldsymbol{N_P}$ = number of personnel/per device
  C_P = salary/per personnel
- $\boldsymbol{M} = [C_{m1} + C_{m2}] \times \lceil D_s / R_D \rceil$
  C_{m1} = schedule maintenance cost; schedule maintenance is a preventive form of maintenance conducted at pre-set intervals to inspect and ensure that the device works properly;
  C_{m2} = unscheduled maintenance; unscheduled maintenance is needed after any failure event or the discovery of any unexpected technical wear or anomaly.
- $\boldsymbol{O} = C_O \times \lceil D_s / R_D \rceil$
  C_O = equipment operational cost/per device
- $\boldsymbol{FA} = C_{FA} \times P_{FA} \times (1 - P_T) \times D_s$
  False alarm cost, including inconvenience, delay, re-inspection cost of operators, re-

Table 2. Cost factors.

Categories	Cost factors proposed in this research
– Purchase cost	– Purchase price and installation cost – Space requirement cost
– Personnel cost	– Human resources cost including any training that is required to operate the security equipment
– Additional running costs	– Maintenance and sustainability cost (e.g. renewing license, rental cost, and necessary manpower) – Cost of equipment operation such as power consumption – Other running cost (e.g. office furniture, transport, insurance, stationary items) – Cost related to false-positive rate

inspection cost of device. Every false alarm leads to additional procedures being taken that waste money and man-hours, cause comsumer dissatisfaction, and reduce people's confidence in the security system.

Then, according to equation (4) the annual expected cost of a piece of surveillance technology can be calculated as:

$$C(security measure) = \frac{\left[C_{p\&i}\times\left\lceil\frac{D_S}{R_D}\right\rceil\times\left\lceil\frac{T_S}{T_D}\right\rceil + C_s\times\left\lceil\frac{D_s}{R_D}\right\rceil + N_P\times\left\lceil\frac{D_s}{R_D}\right\rceil\times C_P\right]}{T_S\times\left\lceil\frac{D_S}{R_D}\right\rceil} + \frac{[C_{m1}+C_{m2}]\times\left\lceil\frac{D_s}{R_D}\right\rceil + C_O\times\left\lceil\frac{D_s}{R_D}\right\rceil + C_{FA}\times P_{FA}\times(1-P_T)\times D_s}{T_S\times\left\lceil\frac{D_S}{R_D}\right\rceil} \quad (5)$$

5 DISCUSSION AND CONCLUSION

The objective of this paper is to show the ongoing work of cost-benefit modelling for security devices in this EU project. This research discusses the basic formulation of cost-benefit analysis. From there we extend the basic formula of the economic analysis model and develop a relatively straightforward modelling for cost-benefit analysis for security devices. However, as the factors in the model are closely examined, this relatively simple model becomes mathematically challenging, involving questions of uncertainties (e.g. probability of attack, amount of risk reduced) and modelling direct and indirect costs (e.g. loss of lives after an attack, fear or social tensions in relation to terrorist activity, infringement of fundamental rights to privacy).

As a full cost-benefit analysis requires a substantial effort for a single surveillance device, currently it is decided by the SURVEILLE project to utilize a (semi-)quantitative cost-benefit analysis for surveillance technology which includes costs other than financial cost. The multidimensional matrix for technology assessment includes (a) usability, in terms of effectiveness, cost, privacy-by-design features and overall excellence, (b) ethics, and (c) intrusiveness into fundamental legal rights. Significant insight gained in "cost" analysis in this research will contribute to the overall score for usability. Based on the cost factors found in section 4.2, Table 2 summarized three major cost categories that should be covered in SURVEILLE assessment matrix.

A matrix of surveillance technologies that reflects assessments of usability and of the risks of violating both ethical standards and fundamental rights is represented by numerical scores awarded in the usability and fundamental rights assessments and ethics assessment. The main conclusions that in the context of the matrix can be drawn from the combination of usability (technology), fundamental rights (law) and moral risk (ethics) assessments for 14 surveillance technologies.

It should be emphasized that this first version assessment measures the use of specific surveillance technologies and provide a basis for a general, all-things-considered assessment for surveillance technologies.

ACKNOWLEDGEMENT

This work reported above was fully funded by the European Union's Seventh Framework Programme. http://www.surveille.eu/.

REFERENCES

Ale, B.J.M., van Gulijk, C., Hanea, A., Hanea, D., Hudson, P.T.W., Lin, P.H., and Sillem, S. (2013), Towards BBN based risk modelling of process plants, Available online 10 January 2014, Journal of Safety Science.

Ale, B.J.M., Bellamy, L.J., Cooke, R.M., Kurowicka, D., Lin, P.H., Morales, O., Roelen, A.L.C., and Spouge, J. (2009), Causal Model for Air Transport Safety (final report), Ministerie van Verkeer en Waterstaat, Den Haag, Netherlands, ISBN: 9036917247.

Ale, B.J.M., Hanea, D., van Gulijk, C., Lin, P.H., Sillem, S., Hudson, P., (2011), Towards an integrated risk model for hydrocarbon industry operation, Proceedings of the European Safety and Reliability Conference, ESREL 2011 18–22 September 2011—Troyes France, Advances in Safety, Reliability and Risk Management—Berenguer, Grall & Guedes Soares (Eds.), Taylor & Francis Group, London, ISBN 978-0-415-68379-1.

Blejcharova, N., Cheu, R.L., and Bina, L. (2012), Framework for selecting screening technologies for checked baggage inspection system at airport, Journal of Transportation Security.

Cohen, M.A. (1988), Pain, suffering, and jury awards: A study of the cost of crime to victims. Law & Society Review, 22(3), 537–556.

Cohen, M.A., Rust, R.T., Steen, S., and Tidd, S.T. (2004), Willingness to pay for crime control programs. Criminology 42(1), pp. 89–109.

Cohen, M.A. (2004), The Costs of Crime and Justice, Taylor & Francis.

Cohen, M.A. (2000), Measuring the costs and benefits of crime and justice, in LaFree G, Measurement and analysis of crime and justice. Washington, DC: National Institute of Justice, US Department of Justice.

Cooke, R.M. (1991). Experts in Uncertainty: opinion and subjective probability in science, New York: Oxford University Press.

Cooke, R.M. and Goossens, L.H.J. (2000). Procedures guide for structured expert judgment. Technical Report EUR 18820. Brussels, Belgium, European Commission.

Cox, L.A. (2009), Improving risk-based decision-making for terrorism applications, Risk Analysis, 29(3), pp. 336–341.

Dhiri, S. and Brand, S. (1999), Analysis of costs and benefits: guidance for evaluators, Research, Development and statistics Directorate, Home office, UK.

Dillon, R.L., Liebe, R. and Bestafka, T. (2009), Risk-based decision making for terrorism applications, Risk Analysis, 29(3), pp. 321–335.

European Commission (2004), A review of costs and benefits analysis in crime prevention in the EU member states.

Gill, M. and Spriggs, A. (2005), Assessing the impact of CCTV, Research, Development and Statistics Directorate, Home Office, UK.

Hornick, J., Paetsch, J., and Bertrand, L. (2000) A manual on conducting economic analysis of crime prevention programs, Canadian Research Institute for Law and the Family.

Jacobson, S.H., Karnani, T., Kobza, J.E. and Ritchie, L. (2006), A cost-benefit analysis of alternative device configurations for aviation-checked baggage security screening, Risk Analysis, Volume 26, Issue 2, pp. 297–310.

Legg, D. and James, P. (2000), Measuring inputs: guidance for evaluators, Research, Development and Statistics Directorate, Home Office, UK.

Miller, T.R., Cohen, M.A. and Wiersema, B. (1996), Victim costs and consequences: A new look. National Institute of Justice Research Report (NCJ 155282). Washington, DC: National Institute of Justice.

Stewart, M.G., Netherton, M.D., and Rosowsky, D. (2006), Terrorism risks and blast damage to built infrastructure, Natural Hazards Review, 7(3), pp. 114–122.

Stewart, M.G. and Netherton, M.D. (2008), Security risks and probabilistic risk assessment of glazing subject to explosive blast loading, Reliability Engineering and System Safety, 93(4), pp. 627–638.

Stewart, M.G. and Mueller, J. (2011), Cost-benefit analyisis of advanced imaging technology full body scanners for airline passenger security screening, Journal of Homeland Security and Emergency Management.

Virta, J.L., Jacobson, S.H., Kobza, J.E. (2003), Analysing the cost of screening selectee and non-selectee baggage, Risk Analysis, Vol. 23, No. 5.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Integrated estimation of pipeline failure probability

I. Žutautaitė, G. Dundulis, S. Rimkevičius & R. Janulionis
Lithuanian Energy Institute, Kaunas, Lithuania

ABSTRACT: The estimation of pipeline failure probability based on the results of integrated deterministic-probabilistic structural integrity analysis and pipeline failure data analysis is presented in the paper. Deterministic-probabilistic structural integrity analysis evaluates the uncertainties associated with loads, material properties, and geometrical parameters. The application of Bayesian method allows us to update estimate of pipeline failure probability (obtained in deterministic-probabilistic structural integrity analysis) with regard to district heating network operation data. The developed methodology is applicable for district heating, gas and oil supply networks. Integrated failure analysis was performed for the selected part of Kaunas (Lithuania) district heating network to illustrate implementation of the proposed method.

1 INTRODUCTION

Piping networks as District Heating (DH) networks, natural gas transmission network or oil pipelines are very important elements of infrastructure of country energy system. District heating networks provide and distribute heat, generated in a heating source, for heating buildings and industry enterprises, heating water and technological needs. The consequences of loss of heating accidents are especially dangerous during the winter season in countries with harsh winters (for instance, in 2006 in Lithuania, Telšiai, an accident at –26.5 °C in the district heating system led to the loss of heat supply for thousands of people for almost a week). Natural gas and oil belong to the main energy resources which are needed for industry and public. The consequences of loss of gas supply could be catastrophic (for instance, loss of gas supply from Russia to Europe in 2009); therefore, the reliability of these networks is an issue of high concern. The reliability of all these systems depends on the degradation mechanisms and structural integrity of pipes. In this paper more attention is focused on the failure analysis of the district heating system. But all proposed methods are suitable for any piping network. In bigger cities of Lithuania and other Baltic countries the district heating systems were designed and installed more than 30 years ago. The degradation mechanisms and phenomena influence the ageing behavior of piping. The bigger part of piping and its components (valves, muffs, connections, etc.) are near at the end of their lifetime.

The methodology for the assessment of reliability of piping networks, presented in our previous work (Rimkevičius et al, 2012), was taken into account in this paper. This methodology includes the estimation of failure probability of each separate part of district heating systems.

There are research works devoted for assessment of piping system reliability based on statistical data (Suna et al, 2009; Gerbec, 2010). Other studies investigate piping degradation mechanisms (Filippov et al, 2006; Maesa et al, 2008) or present structural integrity analysis, which is performed using analytical formulas (Amirat et al, 2007; Davis et al, 2007) or finite element method (Chang et al, 2007).

In this paper authors present the method for the estimation of pipeline failure probability based on:

1. deterministic-probabilistic structural integrity analysis (taking into account loads, material properties, geometrical and boundaries parameters of pipes, defected zone thickness);
2. the application of Bayesian method (pipeline failure probability obtained by deterministic-probabilistic structural integrity analysis is updated with regard to network operation data (failure data)).

The estimate of failure probability of selected part of Kaunas (Lithuania) district heating (DH) network was calculated to illustrate implementation of the proposed method. The estimate of failure probability of selected part of DH network (with the highest failure rate) obtained by probabilistic structural integrity analysis using Bayesian method will be adjusted to other parts of DH network taking into account specific data of these parts. The estimate of failure probability will be used performing reliability and risk analysis of this network.

2 STATISTICAL DATA ANALYSIS AND DH NETWORK AGEING PROCESS ANALYSIS

2.1 *Operation data*

The following data were collected for the statistical failure analysis of district heating network:

1. general information about piping: diameters of pipes, material, piping laying technique, length, operating time;
2. information about failures (ruptures) of piping: identification of piping failure place, diameter of pipe, piping laying technique, groundwater levels, causes of the failures, repair time.

For the calculation example information of Kaunas (the second biggest city of Lithuania) district heating network of last three years was analyzed. Kaunas district heating network is one of the most complicated and oldest one in Lithuania, this system well represents other systems installed in bigger cities of Lithuanian.

2.2 *Statistical data analysis*

Practically all pipes failures are the final point of corrosion process. Approximately 3% of pipe failures are related to external effects. Performed initial statistical analysis shows failure rate dependence on pipeline laying technique and technical properties of pipes. Comparative reliability characteristic λ_i (failure rate per km per year) was calculated for the separate parts of district heating network. According performed calculations three parts of DH network were identified with higher failure rate (5K, 5T and 3Z, notation as it uses "Kaunas Energy" AB—the district heating supplier in Kaunas city).

5K pipeline failure data t_j, $j = 1, 2, \ldots, 28$, t_j—piping operation time till rupture (years), at 5 Bar pressure (normal operation condition).

In reliability theory the most common probability distributions for the modelling time to failure (Lewis, 1994, Zio, 2007): exponential $Exp(\lambda)$ (in case of constant failure rate); Weibull $W(k, \eta)$; log-normal $Log\text{-}N(\mu, \sigma^2)$; gamma $\Gamma(\alpha, \beta)$, etc.

The probability distribution of operation time T to failure is obtained by applying any of goodness of fit tests. Performed Kolmogorov-Smirnov and Anderson-Darling goodness of fit tests showed Weibull distribution is appropriate to model operation time to failure ($p\text{-value}_{(K\text{-}S)} = 0.7028$; $p\text{-value}_{(A\text{-}D)} = 0.6012$). Piping failure data histogram and obtained Weibull probability density function are presented in Figure 1.

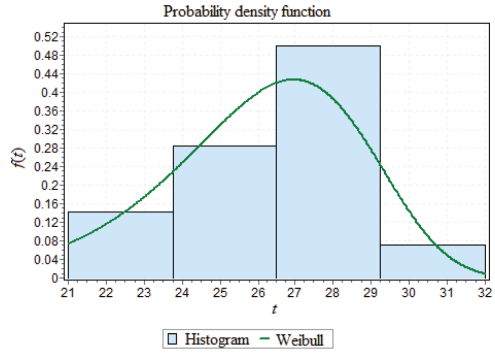


Figure 1. Histogram of failure data and probability density function (of Weibull distribution).

2.3 *The design and ageing mechanisms of DH network*

DH network are mainly built in underground channels. Pipes are supported by movable and immovable supports. To reduce the stresses caused by thermal loading movable supports are used which allow pipes to move in horizontal direction. The pipe elongation is compensated by loop compensators, stuffing boxes and by pipeline geometry itself. According to the specialists of Kaunas DH network operation organization the highest number of pipeline failures occurs at place of movable support. The schematic view of movable support is shown in Figure 2. Support is made of sheet metal bent to U shape beam with the stiffness plate and it is welded directly to the pipe as it is shown in Figure 2.

Movable supports are built each 8.5 to 10 meters depending on the diameter of the pipe. The deadweight load of 8.5–10 meter pipe with insulation and heating water is supported at two thin sheet metal edges welded to the pipe. The problem is that high stress fields are located at the welding zone where pipe material is weakened due to high temperatures during welding process. It is also known that corrosion rates are higher at higher stress fields. All these condition make the movable support as the weakest point of DH pipeline.

Kaunas district heating network is one of the oldest in Lithuania. The oldest pipelines were built in 1963. As it is up to 50 years old the main reason of pipeline failure is ageing mechanisms. And corrosion is the leading ageing mechanism. It is estimated that metal corrosion rate in the heating water vary from 0.05–0.2 mm/year ("Ekotermijos" service, 2007; Table 1 in section 4).

In this paper deterministic-probabilistic structural integrity analysis will be made for the pipe section with the movable support. As the movable support has unfavorable conditions for corrosion resistance high corrosion rates will be used in this paper. To select pipe section with movable support the statistical analysis of pipe failures and structural integrity analysis of pipelines were made. According to the statistical analysis results, three main pipelines 5K, 3Z and 5T were determined as

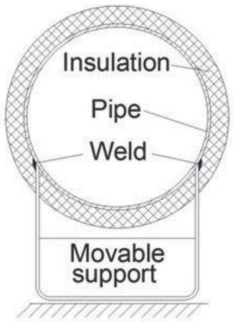


Figure 2. DH pipe movable support.

Table 1. Criteria for the assessment of corrosion rate ("Ekotermijos" service, 2007).

Assessment	Corrosion rate mm/year
No corrosion	0–0.02
Low	0.02–0.04
Allowable	0.04–0.05
High	0.05–0.2
Accident	>0.2

pipelines characterized by the highest failure rates. Pipeline 5K has the worst conditions in structural integrity analysis point of view. It has the highest stress level comparing to the other two. For deterministic-probabilistic structural integrity analysis the most loaded pipe section with movable support from pipeline 5K was selected.

The finite element model preparation requires a lot of human effort and deterministic-probabilistic structural integrity analysis is time consuming. Therefore conservatively it was assumed that all pipe sections with movable supports has the same failure probability as the most loaded pipe section with movable support from pipeline 5K.

3 PROBABILISTIC FAILURE ANALYSIS

In his section will be discussed probabilistic failure analysis made for previously selected pipe section with movable support. Probabilistic failure analysis combines deterministic and probabilistic analysis. Finite element method was used as deterministic method while the Monte Carlo Simulation and the combined Monte Carlo Simulation and Response Surface methods were used for the probabilistic analyses.

The FE software NEPTUNE (Dundulis et al, 2010; Kulak & Fiala, 1988) was used for deterministic calculations and ProFES software (Cesare & Sues, 1999) was used for probabilistic analysis.

During operation of DH pipelines due to various reasons (start and stop of the system, change of heat source, accidents in pipeline, etc.) the pressure in the pipeline can vary from its nominal value (5 bar), material properties are changing due to ageing and degradation mechanisms and also the pipe wall thickness at support and pipe welding zone due to corrosion can fluctuate from through-wall crack to un-defected pipe. Therefore probabilistic failure analysis was done using loads, material properties and defected zone thickness as random variables. As limit state the strength analysis of pipe wall in welding zone was selected. The calculated stresses in pipe welding zone were compared with allowable stresses (114.3 MPa), i.e. if the stresses in the pipe reach the allowable stress level the pipe failure can occur.

The failure dependence from wall thick-ness of defected zone of the movable support was defined in structural reliability analysis. "Response Surface/ Monte-Carlo simulation" method was used for determination of defected zone thickness probability functions. Rupture limit state dependence wall thickness and material properties is presented in equation (1)

$$\begin{aligned} y = \; & 7\cdot 10^{7} - 9.4P - 10.3P_a + 0.00023E_1 \\ & - 2.25\cdot 10^{9} b + 21.5P_b - 13.7P_c - 37.5P_d \\ & - 18672t - 1.3^{-5} E_1 - 0.044\sigma_{y1} \\ & - 2.4\cdot 10^{-5} E_2 - 0.009\sigma_{y2} - 6.4\cdot 10^{-5} E_3 \\ & - 0.04\sigma_{y3} + 3.7\cdot 10^{-5} E_4 - 0.02\sigma_{y4} \\ & + 8.2\cdot 10^{-6} E_5 - 0.02\sigma_{y5}, \end{aligned} \quad (1)$$

where y—limit state response variable; P, P_a, P_b, P_c and P_d—pressure inside the pipe, Pa; b—defected zone thickness, mm; t—temperature inside the pipe, °C; E_1, E_2, E_3, E_4 and E_5—elastic modulus of steel St3 at temperatures 20, 50, 100, 120 and 150 °C, Pa; σ_{y1}, σ_{y2}, σ_{y3}, σ_{y4} ir σ_{y5}—yield strength of steel St3 at temperatures 20, 50, 100, 120 and 150 °C, Pa.

The equation (1) was used as inner response function calculating rupture probabilities using "Monte-Carlo simulations" methods. It allows to define pipe rupture at movable support section dependence defected zone thickness were defined.

Described analysis was done for one selected movable support. The analysis results are presented in Figure 3.

It was defined that failure probability is $2.08\cdot 10^{-4}$ when pressure is 5 bars and when defected zone thickness is 1 mm.

4 RUPTURE PROBABILITY DEPENDENCE ON TIME

According to the research study ("Ekotermijos" service, 2007) for the estimation of metal corrosion

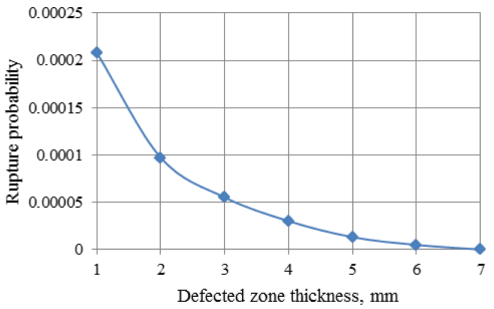


Figure 3. Pipe rupture probability (per year) dependence on defected zone thickness at pressure of 5 bars.

rate in heating water corrosion rates are classified (see Table 1).

Defected zone thickness (mm) dependence on operating time t (years) with regard to corrosion rate r (mm/year) is

$$b = 7 - rt, \tag{2}$$

where t—pipe operating time (years), new pipe are of 7 mm thickness of the wall.

The result of the deterministic-probabilistic structural integrity analysis is the estimates q_i, $i = 1, \ldots, 8$, of pipe rupture (failure) probability with in case of different defected zone thickness $b = \{ 0.1, 0.5, 1, 2, 3, 4, 5, 6\}$, mm (presented in Fig. 3). Rupture probability (per year) dependence on piping operating time t was calculated using corrosion rate $r = 0.2$ mm/year, conservatively (the worst case): $(q_i, b_i) \Rightarrow (q_i, t_i)$, $i = 1, \ldots, 8$.

5 BAYESIAN METHOD FOR FAILURE PROBABILITY ESTIMATE

5.1 *Bayesian method for the estimation of model parameters*

In general, according to the results of pipe Deterministic-Probabilistic Structural Integrity Analysis (DPSIA) (with regard to properties of materials, pressures, temperatures, etc.), failure probability function is known $F(t) = F(t, \theta_1, \ldots, \theta_m)$, the estimates of parameters $\theta_1, \ldots, \theta_m$ are known as well. Considered failure probability function can be updated by taking into account the statistical data about registered failures of operating pipelines. Updating is based on application of Bayesian method.

The parameters $\theta_1, \ldots, \theta_m$ are assumed as random variables with known prior probability density functions (pdfs) $p_l(x_l)$, $l = 1, \ldots, m$, with mean values equal to its estimates (of DPSIA). With respect to available failure data the posterior (updated) pdf of random parameters is obtained by Bayesian Method (BM):

$$p(x_1, \ldots, x_m \mid t_1, \ldots, t_n) = \frac{\prod_{l=1}^{s} p_l(x_l) \cdot L(t_1, \ldots, t_n, x_1, \ldots, x_m)}{\int_{D_1} \ldots \int_{D_m} \prod_{l=1}^{m} p_l(u_l) \cdot L(t_1, \ldots, t_n, u_1, \ldots, u_m) \mathrm{d}u_1 \ldots \mathrm{d}u_m} \tag{3}$$

where t_j—piping operation time till failure (years), $j = 1, 2, \ldots, n$, $L(\cdot)$—likelihood function (with regard to operation time till failure T distribution), D_l—range of parameter θ_l, $l = 1, \ldots, m$, values.

Usually in reliability theory (of technical system) probability distributions of random variable T (time-to-failure) are exponential $Exp(\lambda)$ (in case of constant failure rate), Weibull $W(k, \eta)$ (with appropriate choice of parameters a variety of failure rate behaviors can be modeled), lognormal $Log\text{-}N(\mu, \sigma^2)$, gamma $\Gamma(\alpha, \beta)$, etc. (Lewis, 1994, Zio, 2007).

Bayesian point estimate of parameter θ_l is an expected value calculated using posterior pdf

$$\hat{\theta}_l = \int_{D_1} \ldots \int_{D_m} x_l p(x_1, \ldots, x_m \mid t_1, \ldots, t_n) \mathrm{d}u_1 \ldots \mathrm{d}u_m, \tag{4}$$

where $l = 1, \ldots, m$.

The updated failure probability function is

$$F(t, \hat{\theta}_1, \ldots, \hat{\theta}_m). \tag{5}$$

If the pipe is required to have design-life reliability of p_r, design-life t_{DL} is the solution of equation

$$R(t_{DL}, \hat{\theta}_1, \ldots, \hat{\theta}_m) = p_r, \tag{6}$$

where reliability function

$$R(t, \hat{\theta}_1, \ldots, \hat{\theta}_m) = 1 - F(t, \hat{\theta}_1, \ldots, \hat{\theta}_m). \tag{7}$$

5.2 *Selected district heating network pipeline analysis*

For the implementation of the presented method application one part of district heating network was selected: 5K pipeline of 8,62 km length. 1 km DH pipeline has approximately 95 movable supports. Conservatively it was assumed that failure of pipe can occur at any movable support. Therefore ProFES analysis results (pipe failure probability) determined for one pipe section of movable

support was recalculated to pipe failure probability per 1 km per year or failure probability of 5K pipeline (per year). 5K pipeline is constructed of approximately 819 movable supports.

Failure probability (per year) of analyzed part of DH is calculated

$$q_{(5K),i} = 1-(1-q_i)^{819}, \quad i = 1, \ldots, 8. \tag{8}$$

Failure probability (per year) function $F(t)$ obtained using pipe failure probability dependence on the defected zone thickness (Fig. 3) is

$$F(t,k^*,\eta^*) = 1-\mathrm{e}^{-\left(\frac{t}{\eta^*}\right)^{k^*}}, \tag{9}$$

with shape parameter $k^* = 4.366$ and scale parameter $\eta^* = 44.65$ (cumulative distribution function of Weibull distribution). Loss function is defined

$$S(k,\eta) = \sum_{i=1}^{8} \left| q_{(5K),i} - F(t_i,k,\eta) \right|, \tag{10}$$

where $q_{(5\,\mathrm{K}),i}$—the estimate of failure probability at the time t_i., $i = 1, \ldots, 8$.

$$(k^*, \eta^*)^T := \arg\min_{k,\eta\,>\,0} S(k,\eta), \tag{11}$$

in analysed case $S(k^*, \eta^*) = 0.0559$.

Function $F(t)$ obtained using pipe rupture probability dependence on operation the defected zone thickness (Fig. 3) is presented in Figure 4 (dot line).

Statistical data analysis of operation time till failure shows that operation time till failure T as random variable follows Weibull distribution (according to performed goodness of fit tests). The parameters k and η are assumed as independent random variables with prior probability density functions: $p_1(x)$—gamma pdf with mean value equals to prior (DPSIA) estimate of k^* and variance—10% of estimate value, $p_2(y)$—inverse gamma (as conjugate prior (Bernardo et al, 2003; Berthold et al, 2003)) pdf with mean value equals to prior (DPSIA) estimate of η^* and variance—10% of estimate value. Failure data t_j, $j = 1, 2, \ldots, 28$. Thus, likelihood function is

$$L(t_1, \ldots, t_n \mid x, y) = \prod_{j=1}^{n} \left(\frac{x}{y}\right)\left(\frac{t_j}{y}\right)^{y-1} \mathrm{e}^{-\left(\frac{t_j}{y}\right)^{x}}. \tag{12}$$

BM was applied to calculate posterior probability density functions of the parameters of Weibull distribution (formula (3)), Bayesian point estimates of parameters are calculated using formula (4) as well

$$\hat{k} = 4.92,$$
$$\hat{\eta} = 34.85.$$

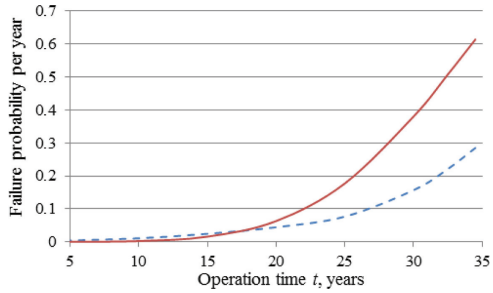


Figure 4. Failure probability $F(t)$ per year of 5 K pipeline (of 8,62 km length, at 5 Bar pressure): failure probability obtained by DPSIA (dot line), updated failure probability by BM (solid line).

Updated failure probability $F(t, 4.92, 34.85)$ (per year) of 5K pipeline (8.62 km length) is presented in Figure 4 (solid line).

Comparative measure as failure probability per 1 km per year was calculated

$$F_{(1km)}(t,\hat{k}',\hat{\eta}') = 1-\mathrm{e}^{-\left(\frac{t}{\hat{\eta}'}\right)^{\hat{k}'}}, \tag{13}$$

where $\hat{k}' = \hat{k}$, $\hat{\eta}' = \hat{\eta}\left(\frac{819}{95}\right)^{\frac{1}{\hat{k}}} = 53.995$.

Failure probability $F_{(1\mathrm{km})}(t,\ 4.92,\ 53.995)$ (per 1 km per year) is presented in Figure 5 ("solid line").

In analyzed case the design-life (solution of equation (6)) of 5K pipeline and 1 km of pipeline with reliability $p_r = 0.9$ are

$$t_{DL} = \hat{\eta}\left(-\ln p_r\right)^{\frac{1}{\hat{k}}} = 22.01 \text{ years}, \tag{14}$$

$$t_{(1km)DL} = \hat{\eta}\left(-\frac{819}{95}\ln p_r\right)^{\frac{1}{\hat{k}}} = 34.18 \text{ years}. \tag{15}$$

The updated failure probability function (Figs. 4 or 5) is significantly increasing when operation time is over 30 years. The renovation of pipeline is recommended. The results of analyzed case show (Figs. 4 and 5) that failures in piping of considered part of district heating main network occur more frequently than it was forecasted with failure probability obtained in deterministic-probabilistic structural integrity analysis. More frequent failures

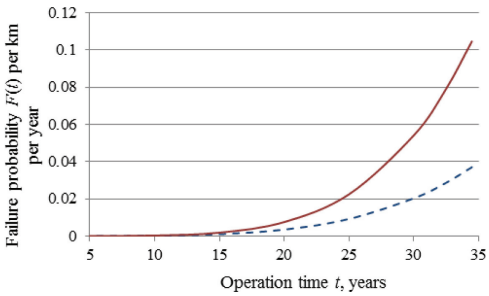


Figure 5. Failure probability $F(t)$ per km per year (at 5 bar pressure): failure probability obtained by DPSIA (dot line), updated failure probability by BM (solid line).

in district heating main network can be related to higher corrosion rate, groundwater, inappropriate drainage, etc.

The estimate of failure probability of selected part of DH network (with the highest failure rate) obtained by probabilistic structural integrity analysis using Bayesian method will be adjusted to other parts of DH network taking into account specific data of these parts. The estimate of failure probability will be used performing reliability and risk analysis of this network.

6 CONCLUSIONS

The estimation of pipeline failure probability based on the results of integrated deterministic-probabilistic structural integrity analysis and pipeline failure data analysis is presented in the paper.

The pipe rupture probability dependence on the defected zone thickness and loading was calculated using deterministic-probabilistic structural integrity analysis. Deterministic-probabilistic structural integrity analysis evaluates the uncertainties associated with loads, material properties, and geometrical parameters as well.

The obtained estimate of pipeline failure probability was updated with regard to network operation data (failure data)) by application of Bayesian method.

The implementation of the proposed method was presented by method application to obtain failure probability estimates of one part of Kaunas (Lithuania) district heating network.

The developed methodology is applicable for district heating, gas and oil supply networks.

ACKNOWLEDGEMENTS

This research was funded by a grant (No. ATE-04/2012) from the Research Council of Lithuania.

REFERENCES

Amirat, A., Chateauneuf A. & Chaoui, K., 2006. Reliability assessment of underground pipelines under the combined effect of active corrosion and residual stress. Int J of Pressure Vessels Piping. 83(2):107–117.

Bernardo, J.M. & Smith A.F.M., 2003. Bayesian theory. John Wiley & Sons.

Berthold, M. & Hand D.J., 2003. Intelligent Data Analysis. 2nd edition.

Cesare, M.A. & Sues, R.H., 1999. PROFES Probabilistic FE System—Bringing Probabilistic Mechanics to the Desktop. American Institute of Aeronautics and Astronautics; AIAA 99-1607:1–11.

Chang, Y.S., Jung, S.W., Lee, S.M., Choi, J.B. & Kim, Y.J. 2007. Fatigue data acquisition, evaluation and optimization of district heating pipes. Applied Thermal Engineering. 27(14–15): 2524–2535.

Davis, P., Burn, S., Moglia, M. & Gould, S. 2007. A physical probabilistic model to predict failure rates in buried PVC pipelines. Reliability Engineering and System Safety. 92:1258–1266.

Dundulis, G., Kulak, R., Alzbutas, R., Uščpuras, E., 2010. Application of probabilistic methods to the structural integrity analysis of RBMK reactor critical structures. In Pavel V. Tsvetkov. (eds), Nuclear Power: 163–189. Croatia: Sciyo.

"Ekotermijos" service, 2007. Hot water for central heating systems preparation analysis, assessment and recommendations for improving the condition of preparation. Applied research work (in Lithuanian).

Filippov, G.A. & Litvinov, O.V., 2006. Degradation processes and their effect on fracture strength of pipe steels after long term operation. Proc. of scientific-practical seminar "Aging problems of steel of main pipelines", Nizhny Novgorod, Russia, 197–211 (In Russian).

Gerbec, M., 2010. A reliability analysis of a natural-gas pressure—regulating installation. Reliability Engineering and System Safety. 95:1154–1163.

Kulak, R.F. & Fiala, C., 1988. Neptune a system of FE programs for three dimensional nonlinear analysis. Nuclear Engineering and Design 106:47–68.

Kulak, R.F. & Marchertas, P., 2003. Development of a FE Based Probabilistic Analysis Tool. Transaction 17th International Conference on Structural Mechanics in Reactor Technology, Prague, Czech Republic, August 17–22, 2003 (CD-ROM), Paper B215.

Lewis, E.E. 1994. Introduction to reliability engineering. John Wiley & Sons, Inc.

Maesa, M.A., Danna, M. & Salama, M.M., 2008. Influence of grade on the reliability of corroding pipelines. Reliability Engineering and System Safety, 93:447–455.

Rimkevičius, S., Kaliatka, A., Valinčius, M., Dundulis, G., Janulionis, R., Grybėnas, A. & Žutautaitė-Šeputienė, I., 2012. Development of approach for reliability assessment of pipeline network systems. Applied energy. 94:22–33.

Suna, Y., Ma, L. & Morris, J., 2009. A practical approach for reliability prediction of pipeline systems. European Journal of Operational Research. 198-1:210–214.

Zio, E., 2007. An introduction to the basics of reliability and risk analysis. World Scientific Prienters (S) Pte Ltd.

Reliability and safety management

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability engineering interactions in aerospace products

E.N. Çetin & A.Ş. Temiz
TAI, Turkish Aerospace Industries Inc., Ankara, Turkey

ABSTRACT: Reliability is an engineering discipline that mainly deals with the systems' or equipment's failures. Therefore, data produced by the reliability engineers becomes very essential for the design team and the rest of the specialty engineering professionals. When the concerned product is a complex one like an aircraft, the data transfer between the specialty engineering disciplines become more and more important. In this paper reliability engineering analysis [like modeling, allocation, prediction and Failure Mode Effects and Criticality Analysis (FMECA)] and relations with the other specialty engineering disciplines during the design of different aerospace products will be discussed in terms of input and output data. And the lessons learned that is gained about the reliability process and the management of the different subcontractors, during the development of Training Aircraft and different avionics modernization products of Turkish Aerospace Industries, Inc. (TAI), will be shared.

1 INTRODUCTION

Reliability is a discipline concerned with ensuring that system performs its mission successfully. It aims at finding potential failures; determine their causes and probabilities in order to ensure more robust products. Reliability is an important attribute of final product. For this reason; the manufacturer must ensure that reliability is considered during the design phase.

Specialty engineering disciplines include analysis of specific features of a system that requires special skills to identify requirements and assess their impact on the system life cycle. Reliability, testability, maintainability, safety, availability, electromagnetic compatibility and human systems integration disciplines are specialty engineering areas.

Specialty engineering disciplines management is becoming more important as the systems are becoming more complex. Complex systems, which are composed of many subsystems, require more people dealing with those specialty engineering disciplines, and sometimes under different groups of the organization. And also it becomes necessary to work with different subcontractors. Different subcontractors have a different way of managing those disciplines; and sometimes no knowledge of how to do.

Reliability is one of the main disciplines of specialty engineering which provides both qualitative and quantitative data to the rest of the specialty engineering disciplines. System safety, testability, maintainability and logistics all require reliability data in order to proceed.

Therefore, in an organization it is very important to establish the relations between these disciplines in order to complete the projects in a timely and cost effective manner.

2 RELIABILITY PROCESS

The data produced by reliability engineering are used by the rest of the specialty engineering disciplines and most of the time those data are the pre—requisite as the starting point. (Dikbaş 2011).

There are four main reliability engineering processes that are carried over at the very early phases of a design project and updated during the development phase of the project. Those are modeling, allocation, prediction and Failure Modes Effects and Criticality Analysis (FMECA). MIL-STD-785B can be used as a reference for conducting a reliability program. (Department of Defense 1980, Aydın & Çetin 2009, Demirel & Çetin 2010).

2.1 *Reliability modeling and allocation*

A Reliability Model presents a clear picture of the interdependencies within a system. A Reliability Block Diagram (RBD) is very helpful for evaluating complex redundant systems by showing all series and parallel relationships of the system. MIL-HDBK-338B well defines the types of RBDs as serial, active-parallel, standby-parallel and complex mixed serial-parallel types. (Department of Defense 2007) A complex system will require a large number of RBDs; so it should be started by drawing a top level RBD and then the next down level RBDs. An example of RBD reflecting the

fuel system of an aircraft for levels I and II is given in Figures 1 and 2 respectively. Level I contain all series blocks; whereas level II is made up of both parallel and series string of blocks.

Hardware reliability models can be used for making numerical allocations and showing redundancies. While a reliability engineer is drawing RBDs showing the system architecture and making some allocations, in the meanwhile maintainability engineers need those RBDs for the maintainability budgeting, like repair times. And also a RBD showing the system structure is also used by the logistics engineers who are in charge with the spare parts planning.

Once a system RBD is drawn; there are several different techniques for the allocation of the reliability goals to the subsystem/equipment levels. Those include "equal apportionment technique", "ARINC apportionment technique" and "feasibility of objectives technique", which are defined in detail in MIL-HDBK-338B. (Department of Defense 2007) However, experience coming from the similar projects will be the best way for making allocations.

RBDs are most effective for easy identification of single point failures and this can be achieved by drawing functional RBDs. When a reliability engineer is drawing the RBD of any subsystem of a complex system, he/she should always be keep in touch with his/her collogue who is dealing with the RBD of the other subsystem. What I mean, the reliability engineer dealing with the landing gears of an aircraft, should keep in touch with his/her friend who is dealing with the hydraulics. Functional RBDs require all the systems' interactions and should be evaluated together. Functional RBDs are good tools for the prediction of mission reliability. While preparing RBDs for mission success, alternative modes of operation shall be modelled parallel as well as redundant equipment. An example RBD is provided in Figure 3 about "video recording" function.

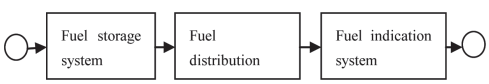


Figure 1. Level I RBD of fuel system.

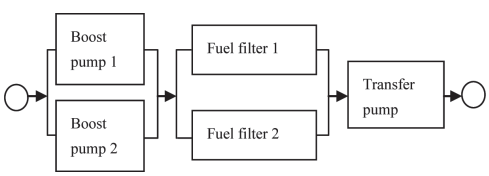


Figure 2. Level II RBD of fuel system. This RBD reflects the "fuel distribution system" portion of the fuel system.

2.2 *Reliability prediction*

Reliability prediction is performed for estimation of the system's ability to meet the specified reliability goals. Basic reliability prediction estimates the ability of a system to perform its function failure free without demand on the support system. (Reliability Information Analysis Center 2005) That is why basic reliability is also called as logistic reliability. At the operational phase, failure rates can be obtained by test data or by field operation data evaluation. At the design phase, different reliability prediction techniques can be used depending on the depth of the knowledge of the system design. At the very early phases, "parts count method" and then as the design progresses "parts stress method" is used; details of which are defined in MIL-HDBK-217F. (Department of Defense 1995) In common sense, part failure rates are predicted by using "parts stress method" during detailed design phase. However, it is a common practice to calculate equipment Mean-Time-Between-Failures (MTBF) by using "parts count method" in order to save time and effort. Furthermore reliability data banks like NPRD and EPRD can be also used for easy gathering of part failure rates. By using the predicted MTBF data it is checked whether the system level and aircraft level reliability goals are met or not. Predicted MTBF data is also used to estimate the demand for maintenance and logistic support in case of an item's unreliability. As the maintainability engineers have the MTBF data in their hand they start to estimate the Mean-Time-To-Repair (MTTR) data of the system. Also, logistics engineers start to make the spare parts planning.

Mission reliability prediction estimates the probability that the system is operable and capable of performing its required function for stated mission

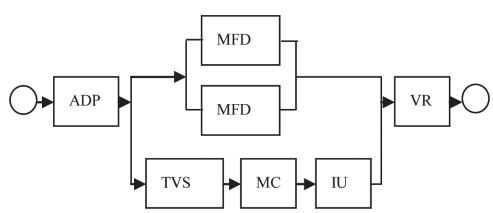


Figure 3. RBD for "video recording" function; where ADP stands for Avionics-Distribution-Panel, MFD stands for Multi-Function-Display, TVS stands for Television-Sensor, MC stands for Mission-Computer, IU stands for Interface-Unit, VR stands for Video-Recorder.

duration. Mission reliability is predicted by using the functional RBDs with the associated mathematical model and predicted reliability figures of the system equipment with the applicable time of the mission. Mission reliability is increased by redundancy; however always keep in mind that increasing redundancy decreases basic reliability figures. While the MTBF data is used to calculate inherent availability of the equipment, mission reliability data is an essential input for the system availability studies.

Therefore, while the reliability engineer is performing predictions in order to check if the specified reliability goal is met; those data should be shared at the same time with the maintainability and logistic engineers. Meanwhile they will perform predictions in order to estimate the repair times, demand for maintenance, demand for logistic support and whether the availability goals are met or not.

2.3 *Failure Modes Effects and Criticality Analysis (FMECA)*

A very important and powerful reliability analysis tool is the FMECA. FMECA identifies all potential weaknesses of a system by systematically identifying all the potential failure modes, their causes, failure frequencies, effects of the failure modes to the item, system and aircraft, severities of those effects, detection method of the failures and finally possible compensating provisions of the failures. There are several different standards and guidelines available which outlines how a FMECA can be performed and documented. For the aircraft programs MIL-STD-1629 A can be used as a reference and can be tailored in accordance with the program needs. (Department of Defense 1998) Steps to be followed while performing a FMECA, is shown in Figure 4.

A generic FMECA worksheet includes the following columns;

- Identification number: which is a unique number defining the each failure mode,
- Function: defines the functions that the related item is supposed to perform,
- Failure mode: defines all the failure modes of the item,
- Failure cause: defines possible causes of the failure modes,
- Failure rate: defines the failure rate of each failure mode,
- Failure effect: the consequence(s) of a failure mode on the function, operation or status of the item being analyzed is evaluated at the equipment, system and aircraft level,
- Failure detection method: the means or methods by which a failure is discovered by the operator during operation or by the maintenance people by some diagnostics.
- Severity: severity classification is given in accordance with the effects of the failure on the system,
- Compensating provisions: includes the actions that are available or can be taken to negate or mitigate the effects of failure.

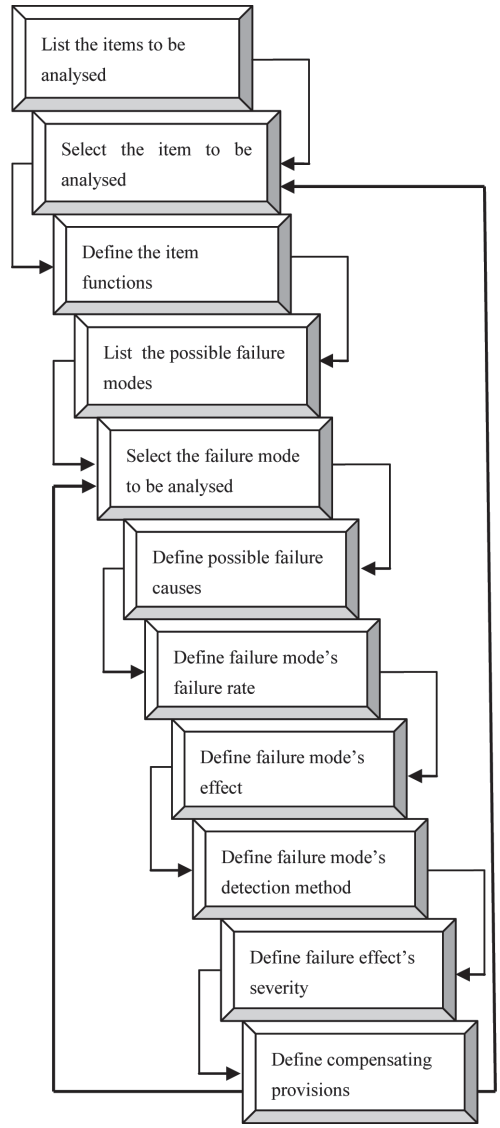


Figure 4. FMECA steps.

An example of FMECA worksheet covering some of the failure modes of "fuel distribution system boost pump" is given in Figure 5.

Item Function	Boost Pump Supply fuel flow		
ID	Failure Mode	Failure Cause	Failure Rate
28.01.01	Open circuit of electric motor	Stator winding	0,004
28.01.02	Rubbing rotor	Bearings wiring/ binding/ sticking	1,023
28.01.03	Cracks in pump housing	Mechanical damage	0,001

Local Effect	Next Effect	End Effect	Detection Method
Motor inoperative	Loss of boosted fuel supply	Mission degradation	Pressure switch signal
Motor speed falls	Reduced fuel supply	Mission degradation	Pressure monitoring
Leakage	External leakage	Mission cancels	Fuel quantity indicators/ Visual

Severity	Compensating provisions
Marginal	The other boost pump is used
Marginal	
Marginal	Pre/ Post Flight check required

Figure 5. FMECA worksheet example.

A well-studied FMECA Report is a very comprehensive report and has many customers in the design team;

- System designers require FMECA in order to see single point failures with their severity. System designers try to eliminate the single point failure cases in an acceptable level.
- Testability engineers require FMECA in order to calculate the FDR (Fault Detection Rate) and FIR (Fault Isolation Rate) of the system,
- Maintainability engineers require FMECA in order to perform the scheduled maintenance analysis like Maintenance Steering Group-3 (MSG-3) or Reliability Centered Maintenance (RCM) analysis,
- System safety engineers require FMECA in order to complete the FTA (Fault Tree Analysis) of the system and use the FR (Failure Rate) data,
- Logistic engineers require FMECA in order to prepare the troubleshooting procedures.
- If the FMECA is for mechanical systems; structural design and analyst engineers use FMECA in order to decide on the items which require further analysis or tests,
- Also, assembly planning engineers use FMECA in order to decide on the inspection points during assembly, if FMECA is performed for mechanical items.

Therefore, after completion of a FMECA of an aircraft's subsystem it is not enough to distribute the resulting report to the whole design team; but also to;

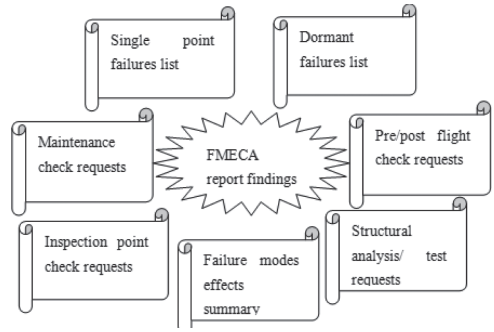


Figure 6. FMECA report findings.

- list the failure modes effects summary and pass to system safety engineers,
- list all the single points leading to "catastrophic" and "hazardous" effects and pass to the system safety engineers and to system design engineers,
- list the dormant failures and pass to maintainability and testability engineers,
- list the failure modes that can be compensated by pre-flight or post-flight check and pass to logistic engineers
- list the periodic check/maintenance requests and pass to maintenance engineers
- list the structural analysis or test requests and pass to the structural design and analyst engineers
- list the inspection points requests and pass to the production planning engineers

FMECA Report findings are shown in Figure 6.

3 INTERACTIONS WITH THE SPECIALTY ENGINEERING DISCIPLINES

3.1 *Reliability interfaces with system safety*

System safety is a discipline which identifies potential hazards and provides controls and certain counter measures by applying several safety assessment methods. System safety requires equipment MTBF data and FMECA Report findings in order to complete the Fault Tree Analysis (FTA)s and System Safety Assessments (SSA)s. A FMECA may be used to supplement the FTA by providing a complementary list of failure effects from the bottom up.

The SSA uses the quantitative values obtained from the Failure Modes and Effects Summary (FMES). The FMES is a summary of failures identified by the FMECA(s) which are grouped together on the basis of their failure effects. (Society of Automotive Engineers 1996).

The FTA Basic Events get their failure rates from the FMECAs and/or FMESs. The SSA should verify that all significant effects identified in the FMES are considered for inclusion as primary events in the FTA. Equipment MTBF data are provided to system safety groups via reliability reports; and reliability reports are revised as the design progresses. Single point failures list and dormant failures list, which is the part of FMECA report is used by the system safety group while performing SSAs. FMECA report findings (FMES, single point failures list, dormant failures list) are distributed to the system safety groups by engineering coordination memos as well as FMECA reports.

3.2 *Reliability interfaces with testability*

Testability is defined as the design characteristic which allows the status (operable, inoperable, or degraded) of an item to be determined and the isolation of faults within the item to be performed in a timely manner. From this definition it is obvious that testability includes both the detection and isolation of faults within a system. Testability engineers do the necessary trade-offs for designing an easily testable and cost effective system.

In order to configure optimum testable design solution and assign the degree of self-test capability, reliability prediction and FMECA are used as input. Reliability predictions must be performed so that high failure rate items can be identified. In conjunction with the prediction, a Failure Mode, Effects and Criticality Analysis (FMECA) should be done to ensure that malfunctions will not adversely affect other units and to determine the exact level of BIT (Build in Test) achieved. (Raytheon Company 1991).

FMECA is a good tool to assess the testability parameters of a system. Dormant failures list with severity information is provided to testability engineers via engineering coordination memos as well as FMECA reports. Testability engineers use "failure detection method" and "failure rate" columns of FMECA in order to calculate Fault Detection Rate (FDR) and Fault Isolation Rate (FIR) of a system. And also perform necessary revisions in order to lessen the number of dormant failures by taking into account the failure severities.

3.3 *Reliability interfaces with maintainability*

Maintainability is defined as the ability of an item to be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources. Maintainability is concerned with the relative ease and economy of preventing or correcting failures by the use of maintenance actions.

Maintainability is considered to be complementary to reliability. RBDs are used in order to allocate and predict numerical maintainability parameters. Numerical maintainability requirements are allocated from system level to sub-system levels by the use of RBDs and MTBF data. Main sources for performing preventive/scheduled maintenance analysis are the FMECA and system safety assessment. Failure modes considered in FMECA are used to determine preventive/scheduled maintenance tasks and intervals in MSG-3 analysis or RCM analysis. MTBF data of the equipment is used while planning the Qualitative Maintainability Analysis (QMA) of a system and performing MTTR predictions. MTTR predictions are used to estimate the maintainability of the system and to make a determination of whether or not the required maintainability could be achieved with the proposed design.

Maintainability engineers are one of the main customers of reliability reports and FMECA reports. Maintenance check requests list is also provided to the maintainability engineers by engineering coordination memos.

3.4 *Reliability interfaces with logistics*

Logistics is the degree to which system design characteristics and planned logistics resources like diagnostic equipment, spares and technical data etc. allow meeting system availability. Logistics engineers perform Logistics Support Analysis (LSA) in order to include supportability during the design process. LSA is based on a Data Element Definition (DED) list and MTBF data is one of the many data required by the standard. For each LSA candidate FMECA gives the necessary potential failure modes, failure effects on equipment, subsystem and product operation with severities. FMECA also describes the means by which the occurrence of a specific failure mode is detected and localized by the operator and the maintenance person. Any applicable warning device, Built-In-Test (BIT) indication or any other indication that make evident that an item has failed or malfunctioned is clearly identified in the FMECA; so that FMECA is well used while preparation of the troubleshoot check lists. Reliability reports and FMECA reports are distributed to the Logistics group with an engineering coordination memo including the pre/post flight check requests list.

3.5 *Reliability interfaces with environmental qualification studies*

During development and installation of airborne equipment and systems, the anticipated external

and internal airplane environmental conditions should be considered.

For environmental qualification studies, the airplane is divided into zones and environmental characteristics of each zone are defined. Equipment's are selected and installed considering these environmental condition requirements.

While performing reliability models and predictions, the environmental conditions of the equipment is taken into account. A Reliability Prediction frequently needs to be revised or updated because the equipment is operated in an environment different than what the original prediction assumed. (Marvin & Willie 2006).

4 LESSONS LEARNED

Below some of the lessons learned are listed in groups about the reliability process during modernization programs of C-130 and CN-235 transport aircrafts and T-38 trainer aircraft;

4.1 *Reliability management*

- Giving trainings at the beginning of a project and repeating for the integrated design teams increases the reliability awareness within the project team.
- Working side by side all the specialty engineering groups is very useful for the quick communication and easy management.
- It is more powerful to distribute the FMECA findings in the form of lists by some engineering coordination memos or by the use of a software tool for the attention of the related FMECA customer for quick action and traceability.
- Using software tools for FMECA is useful for easy management of design changes.
- FMECA and FTA are complementary safety tools. Using a common software tool is time saving while establishing links between the FTA events and FMECA failure modes.
- Using the Bill-Of-Material (BOM) printed out from a centralized system will ensure that all the items in a system are analyzed by the use of FMECA.

4.2 *Sub-contractor management*

- Detailed guidelines for the preparation of reliability reports and FMECA reports are very useful when the subcontractors have no or limited experience of the reliability process. Just referring the standards in the contracts is not enough, because generally standards tell what to do but not how to do.
- Requesting FMECA sheets from subcontractors in soft form and in terms of the applicable project template will lessen the workload while incorporating to the total system FMECA.
- While requesting reliability reports from the subcontractors always give the environmental and temperature factors and reliability prediction methods; and request the reliability data sources.
- When working with the equipment suppliers always query the availability of the reliability data, otherwise it will be very difficult to incorporate the equipment with no reliability data into the system design.

4.3 *Reliability process*

- Using reliability allocation models defined in military standards is an appropriate way when there is no existing data in hand; but always update the data with the ones acquired from the subcontractors or as the system designs starts to shape; and use the previous projects data as the starting point if any available.
- It is more meaningful to give reliability requirements to the system functions rather than system equipment.
- While performing system FMECA it is useful to take into consideration the FHA events as system effects so as to easily harmonize FMECA and FHA in the next step.

5 CONCLUSIONS

Reliability is an engineering discipline concerning with the systems/equipment performance for completing their mission successfully. Reliability improves the design of the product and reduces the life cycle cost by finding potential failures of the design and determining their causes and probabilities. Reliability process approach of TAI Aircraft Group is briefly described in this study. Reliability analysis methods are defined with reference to the standards.

Interfaces with the other specialty engineering disciplines are explained by the data flow between each other. Lessons learned during several design projects are shared. With a well-planned specialty engineering organization, it will be easier to design a user friendly and maintainable system by reducing the life cycle cost.

ACKNOWLEDGMENT

This study has been prepared with the permission and support of TAI Aircraft Group. The authors

wish to express their deepest gratitude to all their managers for support.

REFERENCES

Aydın P., Çetin E.N. 2009 *Application of Mil-Std-785B "Reliability program for systems and equipment development and production*" in aerospace programs.

Demirel A., Çetin E.N. 2010 *Reliability analysis process in UAS development programs*.

Department of Defense (DoD), 1980. MIL-STD-785B *Reliability program for systems and equipment development and production*.

Department of Defense (DoD), 1998. MIL-STD-1629A *Procedures for performing a failure mode effects and criticality analysis*.

Department of Defense (DoD), 2007. MIL-HDBK-338B *Electronic reliability design handbook*.

Department of Defense (DoD), 1995. MIL-HDBK-217F Reliability prediction of electronic equipment.

Dikbaş Z., 2011 *Reliability analysis process for aircraft systems and interfaces between reliability and other specialty engineering disciplines*.

Marvin L Roush, Willie M Webb, 2006, *Applied reliability engineering volume I*.

Raytheon Company, 1991, *Testability design rating system—Testability handbook*.

Reliability Information Analysis Center (RIAC), 2005 *System reliability toolkit*.

Society of Automotive Engineers (SAE), 1996, ARP4761 *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An influence of the lifetime assessment in aviation technology

K. Kustroń
Faculty of Power and Aeronautical Engineering, Institute of Aeronautics and Applied Mechanics, Warsaw University of Technology, Poland

J. Lewitowicz
Air Force Institute of Technology, Poland

ABSTRACT: There are many properties correlated with maintenance costs. Due to minimize the maintenance costs we should recognize them and assess the level of influence and choose them of which the mitigation is the most cost effective. One of the most important property is lifetime which is assessed using statistical methods during accelerated tests. And may be improved based on real data. The parametric and non-parametric statistics could be applied to assessment the lifetime of aviation items. In the paper their advantages and disadvantages were recognized.

1 INTRODUCTION

Effective methods to reduce costs of servicing aircraft are welcome. The servicing costs include operation as well as maintenance costs. In the paper we are focused on cutting the maintenance costs. Optimization of maintenance programs directly affects the cost of aircraft maintenance and it is a key factor in air carrier's profitability. Due to improving aircraft maintenance solutions which directly cut servicing costs we must recognize all factors affected both safety and costs, assess them and their uncertainty. It is sure that in commercial aviation the downtime for maintenance double costs because of spending money for different activities connected with sustaining the airworthiness and losses of no operation. In military aviation the longer downtime reduced readiness and there is desirable to shorten it.

One of the ways to increase the efficiency of servicing is finding the best suitable model of lifetime, taken in this paper. The most suitable lifetime model with the acquisition of operating data decrease uncertainty and better assess the prevention activities reduced them to only the needed based on more real behavior of fleet in comparison to the initial assumptions which are assessed by manufacturer in accelerated tests. In (Nelson 2003) are recommends greater use of available advances in accelerating tests that are not yet being fully utilized in practice. Also, it suggests advances that need to be developed. Aircraft maintenance activities ensure security and the continued airworthiness of the fleet as well as on-time performance. Aircraft maintenance is based on pre-established programs and during servicing should be improve.

The high reliable systems undergo Reliability Centered Maintenance (RCM) strategy that is implemented to optimize the maintenance program. In aviation the strategy based on RCM for assessment maintenance tasks was developed and is involving as MSG-3 which implement the newest research achievements.

Second problem is the classification aircraft items into Significant Structural Item (SSI) influenced safety when damaged and have to be prevent and other which may be servicing to failure and then replace as correction maintenance or could be replace according to assessed life-time. This is very important classification and generate the maintenance costs and influence on safety. Mentioned above problems of the activities before or after failure based on statistical assessments of the accelerated tests data.

Third problem, which has to be implemented to maintenance improvement process, is using appropriate statistics to number of sample.

Presented in (Kustroń et al. 2012) study is an introduction to research in the field of process automation to optimize aircraft maintenance programs using expert systems in the form of available software. The analysis indicates that the best distribution of the random variable T for the failure rate data collected by non-renewable component of the aircraft due to the maximization of technical readiness, a log-normal distribution, for which the time interval preventive replacement component is 103 hours. In order to assess the accuracy of the analysis determined time intervals under

consideration component for gamma distribution, Weibull and normal. Intervals for these distributions differed for the benefit of the log-normal distribution, was chosen as best for the accumulation of data on a non-revolving component failure rate about five hours for the gamma distribution, about 16 hours for the Weibull distribution, and up to 29 hours for a normal distribution. The benefits of proper selection of random variable distribution of correct non-revolving facility is fundamentally due to the costs generated by double-under-the real component durability and losses as a result of the fault and the ground plane at the time of exchange. This work constitutes a development of the subject to identify appropriate methods of statistical analysis-nonparametric and statements for and against in the analysis of lifetime.

2 THE LIFETIME ASSESSMENT AND MANAGEMENT

The lifetime is created by appropriate requirements set by regulations managed by Aviation Authorities as relatives to States' constitutional rights to ensure the safety of its citizens, including the safety and security of transport means including air transport. Although the safety is a priority the ICAO's Annex 19 safety management was established in November last year. This Annex ensures safety of flight and will be implemented in the near future.

Lifetime of aircraft is created in design process according to Annex 8 and during accelerated tests have to be assessed. In manufacturing process the lifetime is materialized with appropriate quality. During the process of servicing the lifetime have to be sustain. All these processes creates maintenance costs which air carriers spend on ensuring safety.

The lifetime of an aircraft is recognized by longtime servicing with required safety. To ensure the safety we can used method of prevention the failures influenced the safety. To prevent failure we can assess risk of occurrence damages with an influence on safety. Additional we should have appropriate diagnostic system to assess health of the structure. The health assessment is the base of classification the aircraft to airworthy or non-airworthy stage. For commercial aircraft the strategy to list checks is ATA MSG-3. According to this strategy checks are the periodic routine and detailed inspections that have to be done in the set periods of time or usage. Commercial operators of large or turbine-powered aircraft are obligated for continuous inspection programs approved by national aviation authorities e.g. the European Aviation Safety Agency (EASA), Federal Aviation Administration (FAA) in the United States, Transport Canada. Each operator prepares a continuous airworthiness maintenance program under its operations specifications. The continuous airworthiness maintenance program includes: A, B, C, and D checks. A and B checks are lighter checks, while C and D are considered heavier checks. The checks are set in accelerated tests using statistical calculation. The maintenance cost could be reduced by appropriate statistic method of failures rates which correspond with real data. Due to this the maintenance program have to be improve while servicing aircraft.

3 PARAMETRIC VS. NONPARAMETRIC STATISTICS

The parametric and nonparametric statistics could be applied to assessment the lifetime of aviation items.

Both for parametric and nonparametric statistics have to be set assumptions. For parametric are:

- the observations must be independent,
- the observations must be drawn from normally distributed populations,
- these populations must have the same variances,
- the means of these normal and homoscedastic populations must be linear combinations of effects due to columns and/or rows;

And for nonparametric:

- observations are independent and
- variable under study has underlying continuity.

There is at least one nonparametric test equivalent to a parametric test.

Power of the test can be measured as statistical power and it is the probability of rejecting the null hypothesis when it is in fact false and should be rejected. Power of parametric tests is calculated from formula, tables, and graphs based on their underlying distribution. Power of nonparametric tests is less straightforward and can be calculated using Monte Carlo simulation methods (Mumby 2002).

The statistical methods based on assumption that the lifetime were drawn from known distributed populations such as normal etc., and below there are techniques that do not make such assumptions. The methods are recognized as distribution-free statistics or nonparametric statistics. In situations where the known assumption holds, the nonparametric tests are less efficient than parametric methods.

There are used many models in nonparametric statistics. Nonparametric models differ from parametric ones in that the model structure is not specified a priori but is instead determined from data. The term nonparametric means that the number and nature of the parameters are flexible and not

fixed in advance. A simple nonparametric estimate of a probability distribution is a histogram. Kernel density estimation provides better estimates of the density than histograms. There are too nonparametric regression and semi-parametric regresion and data envelopment analysis provides efficiency coefficients.

The tests which we can use to assess lifetime are: Wilcoxon Rank Sum Test or Mann-Whitney U Test, Wilcoxon Signed Rank Test and Kruskal-Wallis test.

Wilcoxon Rank Sum Test or Mann-Whitney U Test is the technique tests whether the medians of two populations are the same, when the two samples are independent of each other. This test is comparable to the parametric t-test on the difference between two means that we considered previously. Technique is followed merge and rank the observations and find the sum of the ranks R_1 and R_2 for each of the two samples. Compute the T_1 statistic (based on the smaller of the two samples, or either sample if same sizes) and its mean μ_{T_1} and standard deviation σ_{T_1} is written as:

$$T_1 = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1$$

$$\mu_{T_1} = \frac{n_1 n_2}{2}$$

$$\sigma_{T_1} = \sqrt{\frac{n_1 n_2 (n_1 + n_2 + 1)}{12}}$$

If the two sample sizes are each greater than 10, then U is approximately normal and we can standardize to get:

$$Z = (T_1 - \mu_{T1})/\sigma_{T1}$$

Then if Z is statistically different from zero, we conclude that the medians are not the same.

Wilcoxon Signed Rank Test is the technique tests whether the medians of two populations are the same, when the samples are not independent of each other. This test is comparable to the parametric matched-pairs test that we considered previously. Technique follows calculate the differences between the two sample values for each pair of observations, drop the zero values, of the n non-zero values, rank the absolute values of the differences and sum the ranks of the positive and negative differences separately. Let W be the sum of the positive ranks.

The mean and standard deviation of W are:

$$\mu_W = \frac{n(n+1)}{4}$$

$$\sigma_W = \sqrt{\frac{n(n+1)(2n+1)}{24}}$$

If the number of non-zero differences is at least 20, then W is approximately normal and we can standardize to get:

$$Z = \frac{W - \mu_W}{\sigma_W}$$

If Z is statistically different from zero, we conclude that the medians are not the same.

Kruskal-Wallis test is the technique tests the null hypothesis that several populations have the same median. It is the nonparametric equivalent of the one-factor ANOVA. The test statistic is:

$$K = \frac{12}{n(n+1)}\left(\sum \frac{R_j^2}{n_j}\right) - 3(n+1)$$

where n_j is the number of observations in the j-th sample, n is the total number of observations, and R_j is the sum of the ranks for the jth sample. If each n_j is at least 5 and the null hypothesis is true, then the distribution of K is χ^2 with $c-1$ degrees of freedom, where c is the number of sample groups. If testing at the level α and K is in the α-tail, then we conclude that the medians are not the same. In the case of ties, a corrected statistic K_c should be computed:

$$K_c = \frac{K}{1 - \left[\frac{\Sigma(t_j^3 - t_j)}{n^3 - n}\right]}$$

where t_j is the number of ties in the jth sample.

The nonparametric tests have plenty of advantages but some criticisms too. The nonparametric tests advantages are:

- probability statements obtained from most nonparametric statistics are exact probabilities, regardless of the shape of the population distribution from which the random sample was drawn,
- if sample sizes as small as N = 6 are used, there is no alternative to using a nonparametric test,
- treat samples made up of observations from several different populations,
- can treat data which are inherently in ranks as well as data whose seemingly numerical scores have the strength in ranks,
- available to treat data which are classificatory,
- easier to learn and apply than parametric tests (Hebel 2002).

Criticisms of nonparametric procedures are losing precision/wasteful of data, low power, false sense of security, lack of software, testing distributions only and higher-ordered interactions not dealt with.

Table 1. Summary the statistical methods according to analysis type.

Analysis type	Parametric test Nonparametric test
Differences between independent groups. Compare means of two independent groups	Independent sample t-test Wilcoxon Rank Sum Test Wald-Wolfowitz runs test Kolmogorov-Smirnov two sample test
Differences between independent groups. Compare means of the same group at two time points	Paired sample t-test Wilcoxon Signed Rank Test
Differences between independent groups. Compare means between three or more independent groups	Analysis of variance (ANOVA/MANOVA) Kruskal-Wallis analysis of rank Median Test
Differences between dependent groups. Compare two variables measured in the same sample	T-test for dependent sample Sgh test Wilcoxon's patched pair test
Differences between dependent groups	Related measures ANOVA Friedman's two way analysis of variance Cochran Q
Relationship between variables. Estimate degree of association	Spearman's Product Moment Correlation coefficient Spearman's Rank Correlation Kendall Tau Coefficient gamma Chi square Phi coefficient Fisher exact test Kendall coefficient of concordance

4 CONCLUSIONS

This paper is next step to improvement maintenance program. Here were presented comparison to potential implementation parametric and nonparametric statistics to assess lifetime in design stage as well as manage it during servicing aircraft.

Both groups of statistics method will be used in expert system improving maintenance of aircraft in Air Carrier's fleet.

REFERENCES

Hebel A. 2002. Parametric versus Nonparametric Statistics—When to use them and which is more powerful? Department of Natural Sciences, University of Maryland Eastern Shore, April 5, 2002.

Kustroń K. & Cieślak Ł. 2012. The Optimization of the Replacement Time for Non-Repairable Aircraft Component. Journal of KONBiN 2(22).

Luvalle, M.J. 2004. Statistical Reliability Physics: Theory and Practice of Accelerated Testing Integrating Physics and Statistics, in progress, Chapman & Hall, London.

Mumby P.J. 2002. Statistical power of non-parametric tests: A quick guide for designing sampling strategies.

Nelson, W. 1990. Accelerated testing: statistical model test plans, and data analyses. Wiley, New York.

Nelson, W. 2003, Better Accelerated Tests. ISSAT International Conference on Reliability and Quality in Design, Honolulu. Published in the Proceedings of the Ninth International Society of Science and Applied Technologies (ISSAT) Conference on Reliability and Quality in Design, Honolulu, August 2003.

Nelson, W. & Doganaksoy, N. 1995. Statistical Analysis of Life or Strength Data from Specimens of Various Sizes Using the Power-Lognormal Model. Chapter 21 in Recent Advances in Life-Testing and Reliability. N. Balakrishnan, ed., CRC Press, Boca Raton, FL.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

How managers should think about risk—a case study from the oil and gas industry

T. Bjerga & T. Aven
University of Stavanger, Norway

ABSTRACT: We discuss how managers should think about risk when facing challenging decision-making situations with large uncertainties and high values at stake. The paper is based on the thesis that managers are well qualified for the proper understanding and management of such risk and uncertainties, but that there has been a lack of suitable conceptual frameworks available. We argue that the key to success in this respect is to be open to broader risk perspectives than the common damage-probability view. Risk also has to reflect uncertainties and knowledge, and potential surprises relative to this knowledge. A case taken from the oil and gas industry is used to illustrate the discussion. The main aim of the paper is to guide managers and analysts on the conceptualization of risk and on which principles to adopt in order to understand, assess, manage and communicate risk in relation to situations of large uncertainties and high values at stake.

1 INTRODUCTION

Back in 2003 the Board of Directors of the Norwegian oil company Statoil made a decision to acquire 50% of BP's interest in the In Amenas project in Algeria (STO 2013). Statoil's global footprint and experience base at the time was rather limited, and this acquisition represented a major move subject to high risk and a new type of risk events. The major operational risk identified and discussed in the time prior to the decision was the security risk for personnel, both at the gas facility and in transit between the gas facility and the airport. Algeria had just come out of a decade of unrest, and terrorist kidnapping for ransom was a quite common phenomenon. Reassured by having BP and Algerian Sonatrach as partners with global and local experience, and by relying strongly on the Algerian military for protection, the decision to invest was made. The security was found to be satisfactory. In other words the risk of terrorist attacks was found to be within company standard and conduct—assuming the army would protect the facility and the workers from terror. This assumption was considered to be solid, as the government was heavily reliant on the income from the oil and gas industry. The strong track record for the Algerian army demonstrated this. The assumption failed, as a surprising attack materialized in the early morning hours of January 16th, 2013. It became one of the largest terrorist attacks in the history of the industry with 69 casualties (including 29 killed terrorists) (STO 2013).

In the aftermath it seems obvious that the assumption and background knowledge should have been better analyzed and given weight to in some way, as it turned out to be a major source of the surprising attack. The current paper is based on the thesis that managers are well qualified for understanding and managing risk and uncertainties, but that there has been a lack of suitable conceptual frameworks available that adequately address the knowledge dimension. It is for instance common to consider risk to contain a combination of consequences (loss) and probabilities (Lowrence 1976, Kaplan & Garrick 1981, Ale 2002), which pays little attention to the knowledge base, including the assumptions, underpinning the numbers. Deviations in the knowledge base can lead to quite different numbers. The risk, uncertainty and potential for surprises associated with this knowledge base need to be addressed and given weight to in some way. Giving weight to risk, uncertainties and potential surprises, in synthesis and balance with other concerns, is primarily the responsibility of the managers, though risk analysts need to contribute to the analysis part, informing the managers. The aim of the paper is to guide managers and analysts on how to conceptualize risk—giving due attention to the knowledge dimension—and on what principles to use in order to understand, assess, manage and communicate risk in relation to situations of large uncertainties and high values at stake.

The remainder of the paper is organized as follows. In Section 2 we will introduce a conceptual

framework of risk, giving attention to the knowledge and surprise dimensions. Section 3 applies the framework to the In Amenas case introduced above. Section 4 discusses the findings, and Section 5 concludes.

2 RISK, KNOWLEDGE AND BLACK SWANS

The general setting is this. We are at the present time interested in the future outcomes of an activity. The activity can be ongoing or in the planning stage. The aim is to avoid negative outcomes and nurture positive ones in the period considered. In this setting: Risk is defined as (C, U), where C is the consequences of the activity, and U is the associated uncertainty (what will C be) (Aven 2012). Sometimes (A, C, U) is used to account for initiating events A. The consequences C are relative to something that humans value (health, environment, assets).

Under this definition, risk is described generally as (C′, Q, K) (or (A′, C′, Q, K)), where C′ represents some specific consequences, Q is a measure of uncertainty like subjective probability P, and K represents the background knowledge on which C′ and Q are based.

2.1 *Knowledge in risk analysis and risk descriptions*

What we mean by knowledge needs to be clarified. There are numerous definitions, classifications and theories to explain knowledge. See for instance the many definitions and categories in Alavi and Leidner (2001). One common categorization is to distinguish between three types of knowledge: as know-how (skill), know-that of propositional knowledge, and acquaintance knowledge (Lemos 2007). "Knowing how to ride a bicycle" is an example of know-how, and the statement "I know that Algiers is the capital of Algeria" is an example of propositional knowledge, while "I know John" is an instance of acquaintance knowledge. In relation to risk analysis and risk descriptions, we are primarily dealing with propositional knowledge. A traditional perspective on (propositional) knowledge, often credited to the Greek philosopher Plato, is that knowledge is justified true beliefs. However, the propositions made in risk analysis are typically in the form of assumptions and phenomenological understanding—perhaps shaped by history and present, but which concerns the future. It implies that we cannot talk about something being a "true belief". For example, we cannot say today that it is an absolute true belief that "Algiers will be the capital of Algeria in 10 years." No one can! The way we will understand knowledge is as justified beliefs. Some comments are in order. Firstly, in practice beliefs are in degrees. This means that we can for instance have a strong belief about something: "I strongly believe that Algiers will be the capital of Algeria in 10 years." The degree of belief can even be quantified using for example subjective probabilities. Secondly, it is necessary that the belief is justified. This means that it is not sufficient to proclaim, "I strongly believe …." Justification must be provided in addition to *why* you strongly believe (or have a low belief if that is the case). A belief is someone's belief, i.e. it is subjective, and it is not of much value in risk analysis unless it can be justified. At the very least it should be informed when justification cannot be provided. As for the statement above, one could argue that Algiers is the current capital, and has been for nearly 200 years, and nothing on the horizon appears to be capable of changing that. This would provide fairly strong justification. However, in risk analysis there are many cases where (strong) justification cannot be provided, i.e. it is just a belief, or a belief with varying degrees of justification. The degree of justification—the strength of the knowledge—can also be assessed, for example using a scoring system as described in Appendix A.

2.2 *Black swans in a risk context*

Knowledge, in a risk context, being justified beliefs for a future time period implies that knowledge is not an absolute and objective truth, and sometimes surprises can emerge relative to the justified beliefs. A black swan in a risk analysis context is here understood as a surprising extreme event relative to current knowledge/beliefs (Aven 2013b). Black swans are relative to the knowledge of the risk analysts, reflected by the risk description (A′, C′, Q, K). Three types are used:

- Unknown unknown – strictly unknown to all (at least in the scientific community). This means an actual event A that was not captured by the list A′ in the risk description.
- Unknown known – known to someone, not to all (in the scientific community). The event A is not on the list A′ of the current analyst, but might have been on someone else's list.
- Events judged not to occur because of negligible probability.

3 HOW MANAGERS SHOULD THINK ABOUT RISK

Let us start again with the case introduced in Section 1, turn back in time to 2003 and take the stand of a manager. Assume an investment

opportunity—the In Amenas project—has been presented. At first glance it seems like a good fit for the company's strategic ambitions. The decision problem is whether to invest here or in other alternatives including waiting for a better option, but also if controlling actions should be taken in case an investment is made. The investment prospect will ordinarily only be chosen if it represents a good/best mean to achieve the strategic objectives of the company, including to maximize profits and ensure security for the personnel.

The In Amenas is located far away from home, not only geographically speaking. Algeria has had unrest lasting for a decade that has just come to an end, but terrorist groups are still active. Undoubtedly, there are opportunities that may pay off very well for those who dare, but there are uncertainties, and there may be large negative surprises hidden in the future. There is risk; and an analysis of risk is in place. To provide support with this task is the job of the risk analysts, and their services are requested.

3.1 *The request for a risk analysis focusing on knowledge and surprises*

Now, giving attention to knowledge and uncertainties starts already with the request for a risk analysis. The first thing a manager needs to do is to reflect on what information the analysts should provide. What is it important and useful to know in order to make the decision? Financial risk obviously, but security risk is also important in this case given the presence of terrorist groups and the recent political unrest. Other aspects are also important, but we focus only on these two to illustrate our points. Secondly, and most importantly, attention must be devoted to uncertainty, knowledge and potential black swans in relation to these two: finance and security. A manager and leader should motivate, facilitate and request this from the risk analysts. One way to do this for financial risk, focusing on the cost side, is to request expected values and best estimates, but the use of uncertainty intervals may also be applied. In this case, say that the In Amenas project cost is estimated at $750 m, but a 90% uncertainty interval within which the analyst believes the "true" cost will lie, say $[600, 1,500] m, can also be informative. It is equally important to request an accompanying assessment of the strength of the knowledge underpinning all these numbers. This can be done by using a crude scale and scoring criteria like the one in Appendix A. Next, all key assumptions must be made visible for scrutiny about their importance. One way to do this is by assessing the assumption-deviation-risk (Aven 2013a), i.e. analyzing what deviations from the assumptions could occur and what consequences such deviation would have on the cost. See Appendix A for more details. In addition, evaluations of black swans types ii) and iii) should be requested. Assessment and judgments should be made for:

1. Potential thematic knowledge not possessed by the risk analyst group. In search for potential black swans type ii).
2. Evaluation of events judged negligible due to low probability—black swans type iii). This can include looking into historical events and experts not following the dominant way of thinking.
3. Evaluations of weaknesses and gaps in the underpinning knowledge K.

For the case of security, the request should not only cover scenarios, probabilities and expected consequences given an attack or quantities like Individual Risk (IR), Fatal Accident Rate (FAR), Potential Loss of Life (PLL), f-n curves etc., but also, and equally importantly, that the background knowledge underpinning these numbers and potential black swans is assessed in the same way as for financial risk. Take for example the assumption that the military will prevent terror—what if it fails? What could be the consequences? An assessment of the assumption deviation risk needs to be requested.

Table 1 summarizes the request. The request can cover alternatives other than to invest in the In Amenas, also the alternative of not investing at all. A comparison can then be made between the alternatives, which focuses knowledge, uncertainties and black swans.

In search for black swans, i.e. large surprises relative to the existing knowledge, it is essential that the existing knowledge is scrutinized and other sources of knowledge accessed. In practice this means that not only self-evaluation is mandatory. It is also essential that people with other competences be brought in to have a critical and independent view of the risk analysis. They could act as a "red team", taking the side of an opposing view, and for example argue for the occurrence of rare events (black swans type iii)), look for holes in the knowledge (black swans type ii)), and check how precursors and warnings have been dealt with. Constraints on time and resources may hamper such evaluations, yet they are necessary. Good planning and routines are keys to success in this respect.

In this case it might also be interesting to consider protecting measures to reduce the risk, for instance in case the Algerian military forces fail to prevent terrorist attacks. It is common to use cost-benefit type of analysis based on the Expected Net Present Value formula (E[NPV]), to say something about Implied Cost Per Averted Fatality (ICAF)

Table 1. Summary of the risk analysis request, covering different aspects and alternatives.

	Alternative		
Attribute	1: Invest in In Amenas	2: Second alternative	n: nth alternative
Cost	(Best) estimates		
	90% uncertainty intervals*		
	Strength of knowledge assessment		
	Key assumptions		
	Assumption deviation risk assessment		
	Evaluations to reveal potential unknown knowns (black swans type ii)), i.e. knowledge about the topic not possessed by the group, but which others may possess		
	Evaluations of events judged to not occur due to negligible probability (black swans type iii))		
	Evaluations to reveal potential weaknesses and gaps in the knowledge underpinning the risk analysis		
Security	Scenarios/consequences		
	Probabilities		
	Strength of knowledge assessment		
	Key assumptions		
	Assumption-deviation-risk assessment		
	Evaluations to reveal potential unknown knowns (black swans type ii)), i.e. knowledge about the topic not possessed by the group, but which others may possess		
	Evaluations of events judged to not occur due to negligible probability (black swans type iii))		
	Evaluations to reveal potential weaknesses and gaps in the knowledge underpinning the risk analysis		
…			

*An x% uncertainty interval is an interval that the assessor is x% confident will contain the "true" number. For example, 10% confident is comparable with drawing 1 favorable ball out of an urn containing 10 balls (Lindley 2000).

in such cases. Again the uncertainties, strength of knowledge, and potential surprises must be assessed in a similar manner as above, since expected values and probabilities are not a good way to reflect risk.

The risk analysts will then perform the analysis, and return a risk description. The risk description covers requested information and knowledge in relation to the risk, assessed through the eyes of the risk analyst and experts.

3.2 *Managerial review and judgment focusing on knowledge and surprises*

Eventually the risk analyst hands over the risk description of the aspects and alternatives requested. At this point, there is a very important question that needs to be reflected upon by the manager, preferably even before reading the report. Should the risk description be indiscriminately accepted and assimilated as the manager's own? Informal arguments in favor could be that risk analysts are professional experts paid to do the job and it could be difficult to challenge that from a manager's "ignorant" position. Say too that something surprising and bad should occur in the future; then one can always say that one did what the experts advised. However, from the point of view of what a black swan is, this cannot be defended. Remember, black swans are surprises relative to present knowledge/beliefs. This means that if a black swan were to occur in the future it would be a surprise relative to the knowledge/beliefs of the risk analysts—explicitly engraved in the risk description. A manager constitutes a different knowledge source and a different set of lenses with which to view the risk description, which can be useful to reveal potential black swans. The role of a manager is to be a critical and independent reviewer of the risk description; a similar approach as that of the "red team" introduced above—taking an opposing view. The same bullet points 1) through 3) need to be evaluated by the manager: What if the military turn their guns? What would weaken the incentives the government has to protect the facility? What would strengthen them? What about an invasion by neighboring countries? What if large terrorist groups should reach the facility? The knowledge needs to be scrutinized and critical questions asked. In many

real cases, there may not be time and resources to employ a full-scale, independent, "red team", as recommended in Section 3.1. More important is the manager's review as a last "filter" to reveal potential black swans before an action is taken. Requesting an assessment of the knowledge and potential black swans, as in Section 3.1, is certainly useful and a step in the right direction, but a manager has the responsibility for carrying out evaluations and scrutiny of the work performed by the risk analyst for him/herself before accepting it. Ultimately the manager and decision maker is also the top risk analyst.

A related topic is also that the risk analysts themselves might be "biased". For instance, could the risk analysts have personal interests for a decision to enter In Amenas, or a particular security technology? This issue is often seen in political decisions. Administrative staff performs the analysis, prepares the case and advises the elected officials on a decision. Of course the administrators try to be objective in their assessment, but they too have political or financial interests of their own which may influence the analysis and advice. The manager must also take similar concerns into account when presented with a risk description, as such "biases" could lead to unpleasant surprises.

Also relevant is the fact that the risk analysis with its qualitative flaws and weaknesses is only one contribution of many. The risk description is limited and targets only some aspects and events. In this case only finance and security risk is considered. What about technical challenges? Or third party risk? Or the environment? The manager also has to bring these elements to the table.

A decision is risk informed, not risk based (Apostolakis 2004). The risk description will only target some aspects and events, and has weaknesses and limitations both in its quality and scope.

In the end, the foundation for the decision will constitute the risk description covering elements of risk, knowledge, uncertainty and black swans placed in a greater context which takes into account 1) limitations and weaknesses of the risk description, and 2) other concerns and inputs (analysis). Now, judging how to give weight to all of these elements and inputs, and use them in order to reach a choice—a decision—is the job of the manager.

3.3 *Giving weight to uncertainties and black swans in the decision*

At the point when the risk description is judged eligible to be input to the decision, and all elements are on the table, the next role of the manager begins: to give weight to consequences and surprises, uncertainties and knowledge in balance and synthesis with other concerns. Many principles are applicable to that end.

Giving weight to uncertainty is giving weight to principles like the cautionary and precautionary principles. The cautionary principle says that when uncertainty is present caution is advised (Aven & Vinnem 2007). An example of its use is found on the Norwegian continental shelf, where it is mandatory to have a firewall protecting the living quarters on platforms in case a fire occurs in the production zone. The precautionary principle can be considered a special case of the cautionary principle and applies when scientific uncertainties are present (Aven 2011). This means situations in which the phenomena and processes are poorly understood by the scientists, and reliable models are lacking. In the In Amenas case here discussed, there are large uncertainties and poor knowledge, and both principles can apply. This could mean that the investment is not made, or that further measures to reduce risk and uncertainty are taken. Some potential candidates to reduce the risk for terrorist attacks would be to hire more security personnel, arm the security personnel, invest in intruder safe shelters, put more efforts into training in case of emergencies, and surveillance. How much caution is taken needs to be balanced against attributes like cost, and they all come with security risks of their own. For instance, armor given to security personnel can potentially also be used against the personnel they are supposed to protect.

In line with cautionary thinking and the case when the question is whether or not to implement an identified mitigating measure, like armored shelters designed to withstand a terrorist attack, the ALARP principle might be used. It says that risk should be as low as reasonably practicable. In the way that risk is understood here, it means that the (C′, Q, K) should be as low as reasonably practicable, where 'reasonably practicable' needs to be seen in relation to other costs and benefits. The ALARP principle means a reversed burden of proof, i.e. identified reducing measures shall be implemented unless gross disproportion between cost and benefits can be demonstrated. It is common to use a cost-benefit type of analysis as mentioned in Section 3.1 for such demonstration. However, when giving attention to uncertainties and surprises, a decision cannot be made based on the expected numbers alone. This especially concerns the cases when the cost is high, and the cost-benefit analysis demonstrates gross disproportion. Still, the measure should be considered implemented if the strength of knowledge is poor, provided it can strengthen knowledge, or the measure will reduce the risk of surprises and black swans.

It is also common to use risk acceptance criterion. If the risk is below a predefined limit, then the risk should be accepted. Giving weight to knowledge, uncertainty and black swans means

that the acceptance criteria cannot be defined solely on probability except in the case of strong background knowledge and small potential for black swans. In cases of poor knowledge and/or large risk for black swans, the risk may not be accepted regardless of the probability. This could have been the case for the In Amenas investment prospect, as it was accepted back in 2003, without introducing further measures.

Another way to give weight to surprises is by giving weight to resilience, i.e. the ability to prepare and cope with consequences and uncertainty given the occurrence of any type of event including new types (Hollnagel et al. 2006, Steen & Aven 2011), for instance various attack scenarios. In practice, there is always a trade-off between resilience and efficiency, i.e. how much weight and resources the manager is willing to give resilience.

4 DISCUSSION

How the manager should think about risk when large uncertainties are present and high values are at stake has been elaborated in Section 3. At the very center is the conceptualization of risk and the associated request/description summarized in Table 1. This request/description can be generalized into three primary elements. The first element contains the specified consequences C' and the measures of uncertainty Q, which are both conditioned on the background knowledge K. We refer to this pair as element Z, hence $Z = (C', Q)$. The second element is a description of the knowledge K including a judgment of the strength of this knowledge, and the third element is an assessment of surprises S relative to the knowledge and beliefs as expressed by (Z, K). We can combine these three elements in a triplet, (Z, K, S). There are various tools and measures applicable for carrying out the evaluations of these elements. In our case for security, scenarios, probabilities and expected consequences were requested, while for finance best estimates and uncertainty intervals were requested. Other measures like imprecise probabilities could also apply. From a practical point of view, it may be preferable to use the same way of measuring aspects, for all alternatives, as this would make comparison fairly straightforward. Equally important are the qualitative aspects linked to the knowledge K, and surprises S. Without these knowledge assessments there is no expression of the level of justification of the beliefs Z, and relevant comparisons and the decision-making can accordingly lack basis.

Concerning surprises and black swans, the careful reader may have noticed that we primarily have been addressing black swans of types ii) and iii). These can be addressed at the current time of the analysis, and be dealt with to some degree by means of scrutiny and knowledge sharing/transfer. The knowledge exists; it is just a matter of finding it, or using it the right way. That is what one would do when employing a red team, or hiring specialists. It is also the same thing a manager would do when using his/her knowledge to review the work done. Black swans of type i), however, are by definition very hard to do something about at the current time (unknown to the entire scientific community). Fortunately, knowledge is changing and growing with time, so that what is unknown at the current time may not be unknown at a future point in time. Research and development can reveal potential unknown unknowns. In addition, there are often signals and warnings, also for this type of events. Paté-Cornell (2012) recommends a mix of alertness, quick detection and early response to cope with type i) black swans, but this also applies to types ii) and iii). The thinking is in line with collective mindfulness principles linked to High Reliability Organizations (HROs) (Weick & Sutcliffe 2007, Aven & Krohn 2014), as well as ideas of resilience engineering (Hollnagel et al. 2006). Take the HRO principle of sensitivity to operations, i.e. sensing what is happening and taking the necessary action. It addresses (rapidly) changing knowledge in an operational setting.

Lastly, we would like to highlight the use of the cautionary principle. The ideas highlighted in the present paper acknowledge the importance of uncertainty in risk descriptions and characterizations, and the need for management to be aware of these uncertainties and give them proper weight in the decision-making when balancing different concerns, such as safety/security and costs. Common decision-making practice is often risk-based (Aven & Vinnem 2007), where the uncertainties are concealed. In accordance with the proposed methods presented above, the proper management regime is risk-informed where due consideration is given to the uncertainties, and the cautionary principle is seen as an integrated part.

5 CONCLUSION

This paper has primarily been concerned with how managers should think about risk and what principles they should apply in related decision-making. The work is based on the thesis that there has been a lack of suitable conceptual frameworks to account for the knowledge and surprise dimensions of risk. A decision process case from the oil and gas industry has been used to exemplify various aspects of how to account for these dimensions. At the very center is the way risk is understood, and the request/

description of risk it leads to, which addresses specified consequences and measures of uncertainty, assessments of underpinning knowledge, and surprises relative to the knowledge. It is argued that the cautionary principle needs to play an important role in the decision making, to give proper weight to the uncertainty component of risk. The management task is to balance different concerns, such as security/safety and costs, but in order to do this in a meaningful way, the full spectrum of the uncertainty dimension must be reflected. The present paper has pointed to some key aspects to consider, which extend beyond current practice.

ACKNOWLEDGEMENTS

The work has been partly funded by the Petromaks 2 program of the Research Council of Norway.

REFERENCES

Alavi, M. & Leidner, D.E. 2001. Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*: 107–136.

Ale, B.J.M. 2002. Risk assessment practices in The Netherlands. *Safety Science* 40: 105–26.

Apostolakis, G.E. 2004. How useful is quantitative risk assessment? *Risk Analysis* 24: 515–20.

Aven, T. 2011. On different types of uncertainties in the context of the precautionary principle. *Risk Analysis* 31: 1515–1525. (With discussion pp. 1538–1542).

Aven, T. 2012. The risk concept—historical and recent development trends. *Reliability Engineering and System Safety* 99: 33–44.

Aven, T. 2013a. Practical implications of the new risk perspectives. *Reliability Engineering and System Safety* 115: 136–145.

Aven, T. 2013b. On the meaning of a black swan in a risk context. *Safety Science* 57: 44–51.

Aven, T. & Krohn, B.S. 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and System Safety* 121: 1–10.

Aven, T. & Vinnem, J.E. 2007. *Risk Management, with Applications from the Offshore Oil and Gas Industry*. NY: Springer Verlag.

Flage, R. & Aven, T. 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability and Risk Analysis: Theory & Application* 2: 9–18.

Hollnagel, E., Woods, D.D and Leveson, N. 2006. *Resilience Engineering*. Burlington,VT: Ashgate.

Kaplan, S. & Garrick, B.J. 1981. On the quantitative definition of risk. *Risk Analysis* 1: 11–27.

Lemos, N.M. 2007. *An Introduction to the Theory of Knowledge*. Cambridge: Cambridge University Press.

Lindley, D.V. 2000. The philosophy of statistics. *Journal of the Royal Statistical Society: Series D* (The Statistician) 49: 293–337.

Lowrance, W. 1976. *Of Acceptable Risk—Science and the Determination of Safety*. Los Altos, CA: William Kaufmann Inc.

Paté-Cornell, E. 2012. On "black swans" and "perfect storms": Risk analysis and management when statistics are not enough. *Risk Analysis* 32: 1823–1833.

Steen, R., & Aven, T. 2011. A risk perspective suitable for resilience engineering. *Safety Science* 49(2): 292–297.

STO. 2013. Statoil. *The In Amenas Attack*. http://www.statoil.com/no/NewsAndMedia/News/2013/Downloads/In Amenas report.pdf.

Weick, K.E. & Sutcliffe, K.M. 2007. Managing the Unexpected: Resilient Performance in an Age of Uncertainty. San Francisco: Jossey-Bass.

APPENDIX A—KNOWLEDGE ASSESSMENTS

The knowledge K in the risk description includes assumptions and phenomenological/contextual understanding. One way to assess the strength of the knowledge is by using a scoring system based on Flage and Aven (2009). The strength of knowledge is poor if one or more of the following conditions are met:

- The assumptions made represent strong simplifications.
- Data is not available, or is unreliable.
- There is a lack of agreement/consensus among experts.
- The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions.

The strength of knowledge is strong if all of the following conditions are met:

- The assumptions made are seen as very reasonable.
- Much reliable data is available.
- There is broad agreement/consensus among experts.
- The phenomena involved are well understood; the models used are known/believed to give poor predictions.

The strength of knowledge is graded medium in cases in between.

More detailed analysis of assumption-deviation-risk (Aven 2013a) can be performed by considering 1) the magnitude of a potential assumption deviation, 2) how likely the deviation is (the probability), 3) the consequences given a deviation, and 4) a strength of knowledge assessment of preceding points 1)–3).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Balancing safety and performance through QRA and RAM analyses

Victor Borges & Colin Hickey
DNV GL Software, London, UK

ABSTRACT: Improving safety through risk management and improving economic viability through asset management are crucial elements of sustainable business success. However, what if the needs of these initiatives conflict? The impact of risk management on asset performance and the impact of asset management on risk can be assessed and thus an iterative analysis begins. Loss prevention tools and methods can be summarised under two main headings: Risk management and asset management. In using these approaches, operators ensure that assets are running optimally with a known and managed level of risk. We find that sometimes the methods to assure safety and asset management methodologies may at times conflict; changes recommended from risk management work can directly impact the performance of a system- and vice-versa.

1 INTRODUCTION

This paper presents a case study where a conflict in risk management and asset management is found and a balance sought. Managing assets encompasses different techniques to ensure that a system is running at optimum capacity in a safe manner. Loss prevention contains a range of methodologies—some integrated, some not—under one business' management system or systems.

Two management methods that are vital to ensure optimum performance and safe operations are risk management and asset management.

1.1 *Risk management*

Risk management is a process used in many industries. Very plainly it is the process of identifying what might go wrong in terms of consequence and likelihood, and using this factored view of the incident to inform us when deciding which steps we will take prevent or protect against the incident. Risk management is a powerful method to—in some cases—quantify or at least qualify the intangible wealth of possible futures of an activity. The process of risk management therefore contains an ever evolving array of tools and methods such as HAZOP, a systematic procedure for imagining all undesirable behaviour from the process flow diagrams of a process plant, to cutting edge experiments used to look at how newly popular materials such as Hydrogen and CO2 behave when they escape from containment. These methods—and everything in between—offer the safety engineer, or risk analyst and design and process engineers the tools required to build and run safe plant.

1.2 *Asset management*

Asset management is the process used to maintain production in a wide range of industries. In its application in the process industry, asset management is used to ensure the optimum performance of a process plant by balancing design configurations, maintenance strategies and operational bottlenecks with capital investments. By considering each of the factors involved in asset management in a strategic manner the "asset manager" can define and aim for the enterprise's optimum.

Asset management contains an array of complex range of tools and methods. From data management and storage systems used for handling vast quantities of information related to inspection and maintenance to the advanced technology of remotely operated vehicles used for inspection of subsea equipment.

This paper presents a case study of a separation unit where a conflict arises between advice given by risk management and asset management techniques and a balance is sought.

2 LOSS PREVENTION TECHNIQUES

The loss prevention pyramid, as shown in Figure 1, provides a description of the array of tools and

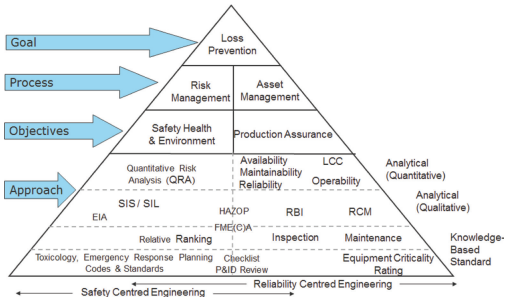


Figure 1. Loss prevention pyramid.

methods within risk management and asset management and how they can be combined to create an available and safe system.

The main goal of the activities in the pyramid is to prevent loss. From the risk management point of view, loss prevention refers to preventing loss of lives and property and avoiding environmental impact. From the asset management point of view, loss prevention refers to assuring production by ensuring that a system is available to perform its intended function.

As the pyramid describes, both domains are supported by qualitative and quantitative analyses, simulation techniques, management processes and standards.

Two well established and advanced methodologies that are widely used by the process industry to assess risk and performance are Quantitative Risk Analysis (QRA) and Reliability, Availability and Maintainability (RAM) Analysis.

2.1 *Quantitative risk analysis*

QRA is a method for systematically analyzing major accident hazards within an operation. QRA methods have been well documented and the approach is now ubiquitous within the process industry, with regulatory demand for it in some countries. Examples of guidance are the CCPS guide book (CCPS, 1989) and the Dutch BEVI guidelines (RIVM, 2009). The general approach is to take the following steps:

1. Identify hazards
2. Qualitatively assess the consequence and likelihood of the hazards and postulate major accident hazards
3. Quantify the extent of consequences
4. Quantify the extent of likelihood
5. Sum the risks
6. Compare the risks against some criteria

The quantification and assessment of risks is a powerful tool which can help you identify a risk profile. Knowing which hazards pose the most harm in a relative context can inform many factors of loss prevention such as plant design, building siting, emergency preparedness, and can inform cost benefit decisions on all manner of risk management activities. In general QRA will point to the core, common sense approach of "what you don't have can't leak" and other inherent safety approaches. The QRA can be conducted throughout all stages of the lifecycle of the asset; from the conceptual design through to decommissioning. Importantly, changes in design and operation may have significant impact on the total risk and the risk profile across the plant. Quantity of, physical and hazardous properties of products, location and vulnerability of population and location of ignition sources all have a relation to the risk. Presence of sources of loss of containment, potential for loss of containment from operational activities and their preventive and protective barriers form the root hazards across the site. For this reason, information relating to all of these factors must be considered as accurately as possible.

Typical outputs of a risk analysis are risk contours, FN curves and risk ranking measures. These are used in a variety of ways, for example to direct application of resources when considering layers of protection or for providing details required for emergency response planning.

2.2 *RAM analysis*

RAM analysis is a methodology (Smith, 2011) used to predict the performance of a system and is made possible through evaluating three factors:

- Reliability; typically expressed as the mean time between failures under given operating conditions.
- Maintainability; typically expressed as the mean time needed to return failed or shutdown equipment back to normal service. Influencing factors are the equipment's design, working conditions, organisation of work, procedures, and the location and availability of people and spare equipment.
- Availability; typically expressed as the fraction of time the equipment is able to perform its intended function under given operating conditions. Availability is a function of reliability and maintainability.

The main output of the analysis is an availability value, which is the fraction of the time where the system is available.

This methodology has been applied to a wide range of industries and throughout all stages of asset lifecycle from early design to decommissioning.

RAM analysis helps in the decision making process as it highlights areas which will cause system downtime or which will require continuous effort and resource to keep the system in a serviceable state. With the information that RAM analysis can provide, decisions can be made with regard to design and maintenance strategies, optimising production and reducing maintenance resources usage and cost.

In order to obtain a complete picture of the performance, we must not only evaluate the uptime of the system from generic reliability of hardware and the general 'time it takes to fix or replace things', but also the effects on performance from operations. For example, upon failure of a piece of equipment used to process gas leaving a 2-phase separator, can we bypass the failed equipment and flare the gas so that we can keep the liquid fraction of the product flowing? This is particularly important for oil and gas developments where systems are complex, time dependant and interrelated. To extend the traditional RAM analysis approach and account for operability factors a combined method utilising traditional RAM analysis with flow assessment is used.

By adding flow assessment, another dimension is introduced—the production rate. This enables the methodology to account for a range of results containing:

- Flaring operations
- Export requirements
- Recovery Mechanisms
- Buffer and Tank management
- Logistics and transportation
- Ramping time

3 CASE STUDY: SEPARATION SYSTEM

3.1 *Process description*

The process serves to remove unwanted liquids from a high pressure and low pressure gas lines providing fuel gas to a downstream utility plant. The arrangement of equipment is shown in the process flow diagram of Figure 2.

The process takes high pressure and low pressure gas feeds, which pass through separators used to remove liquids. Each of the two separators has a liquid outlet on the bottom. Each of the separators has a gas outlet on the top, which send the gas to be compressed and used as fuel. The low pressure system takes the liquids removed from the high pressure separator vessel, after the low pressure separator the liquids are removed from the system. The gas lines all have a connection to a flare line through pressure relief valves.

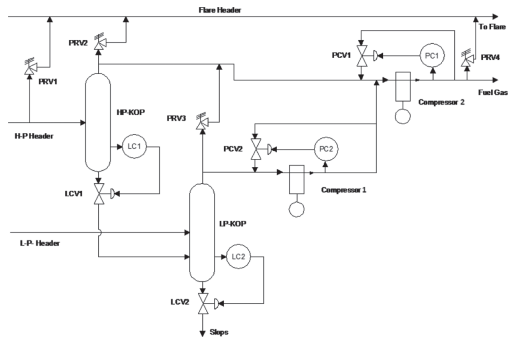


Figure 2. Process flow diagram of separation unit.

3.1.1 *The safety and operational performance analyses*

The performance will be evaluated by running a RAM study and the risk assessment will be performed using QRA.

The base case must fulfil safety and performance requirements. If the system does not meet the safety and performance requirement, changes must be suggested satisfying both risk and asset performance criteria. The principles adopted for this case study are that base case risks must be proven to be as low as reasonably practicable, by adopting economically viable risk reduction measures on the primary risk contributors. The RAM analysis will aim to establish the base case production efficiency and then further analysis will determine what changes should be made to the design to achieve a more reliable and maintainable selection and arrangement of equipment resulting in an improved production efficiency which more than pays for itself.

3.2 *QRA model*

3.2.1 *Description of QRA analysis case study*

A hazard and operability study was used to identify hazardous scenarios arising from the process. These were qualitatively assessed and a risk ranking was established. With knowledge of the operational procedures and intended layout of the plant, the key potential accidents identified in the HAZOP have been rationalised for the purposes of the case study to:

1. Rupture of HP-KOP
2. Ignition of relief from HP-KOP
3. Line Rupture at gas outlet of HP-KOP
4. Leak from Compressor 2 kick-back loop
5. Ignition of relief from LP-KOP
6. Line Rupture of gas outlet of LP-KOP
7. Leak from Compressor 1 kick-back loop

The domain of loss prevention is helpfully supported by an array of tools and techniques with

which to identify and manage risks from hazardous activities, and each of the above accidental events would be investigated further using techniques such as Layer of Protection Analysis, Bow-Tie analysis so as to determine the presence and effectiveness of barriers to prevent and protect against their failures. In this case study, QRA is used to support and enhance the qualitative risk ranking of the above scenarios by using best available science to estimate the extent of harm from each scenario.

A plot plan, shown in Figure 3 is used in the QRA tool. QRA software is used to simulate the range of flammable hazards including fireballs, jet fires, flash fires and explosions. There are no toxics present. As can be seen in Figure 3, there are congested regions around the compressor units. Ignition in these regions would give rise to overpressures. Also shown in Figure 3 is a risk ranking point; this is a geographical location of interest representing a point which if impacted would give rise to an escalation event. Following QRA calculations for the accidental scenarios and their predicted outcomes, Location Specific Individual Risk contours (LSIR) are developed, as shown in Figure 4.

The spikes in the risk contours are generated from elongated jet fire radiation zones. The risk ranking point is in an area which appears to be impacted by various outcomes. This can be confirmed by looking to the individual risk ranking results for the point. These are shown in Table 1.

The risk ranking results of Table 1 show us that the majority of escalation risk comes from jet fires resulting from leaks from the two compressors. The percentage risk shows the relative contribution to risk at the risk ranking point from each source.

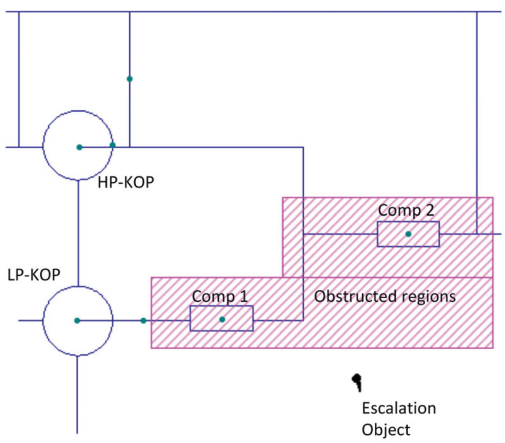


Figure 3. Plot plan with obstructed regions and risk ranking point.

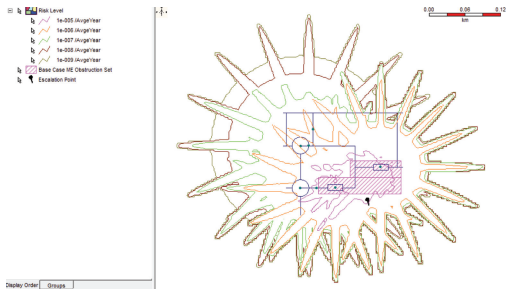


Figure 4. Risk contours for the base case.

Table 1. Ranking of risk contributions at escalation location.

Model name	Risk (/yr)	% risk
7 Leak from Compressor 1 kick-back	8.11E-7	47.37
Jet Fire	8.11E-7	47.37
4 Leak from Compressor 2 kick-back	8.11E-7	47.37
Jet Fire	8.11E-7	47.37
3 Line Rupture at gas outlet of HP-KOP	8.92E-8	5.21
Flash Fire	5.35E-8	3.13
Explosion	3.57E-8	2.09
1 rupture HP-KOP	6.98E-10	0.04
Fireball	6.98E-10	0.04
TOTAL	1.71E-6	

3.3 *RAM model*

The RAM study was performed to calculate the production efficiency of the base case design and identify the critical items impacting the production of fuel gas.

3.3.1 *Study boundary*

Boundary plays an important role in this study. The separation system might be assumed to be part of pool of utilities systems. Utilities systems refer to any essential services required by a process plant. For example, water supply, compressed air, gas, electricity, steam, nitrogen etc.

Loss of utility supplies can cause substantial disruptions to process operations for example, loss of compressed air, steam for heating, water for cooling or electricity for running pumps. In the case of this separation system, failures will have direct impact to any unit that requires fuel gas to operate. Fuel gas can be used for a wide range of application from power generation to heating products.

A total failure of this system may lead to a complete or partial shutdown of the processing

facilities upstream and downstream. Additionally, in certain conditions to safely shut down the plant, chemical may be routed to flare systems and burnt in order to reduce the potential safety hazard on the process plant.

This case study aims at calculating the availability and production efficiency of the separation system but it could be extended if needed.

3.3.2 *Flow network and flow rates*

The most important and thought provoking step in RAM analysis is to formulate a logic network which will reflect the functionality of the system and interdependence of the elements. In order to produce a flow network, it is necessary to decide from the outset which primary function of the system is to be monitored and then create a flow network mimicking that operation.

For this case study, the primary function of the system is to produce fuel gas. Armed with this information, the logic flow network is constructed as shown Figure 5.

The flow network in Figure 5 imposes that failures on the LP or HP separation will partially shut down the system. Failures at the compression system will prevent the system from exporting fuel gas and cause a full shut down of the system.

The overall flow exported from this system is 100 mmscf per day. The high and low pressure gas systems are assumed to have equal contribution to the end product quantity exported: 50% LP Gas and 50% HP Gas.

3.3.3 *Reliability block diagram*

One level below the flow network, the analyst must define the Reliability Block Diagrams. Reliability Block Diagrams (RBD) are similar to logic flow networks and describe the interdependency between equipment items. Two configurations are to be defined: blocks in series or blocks in parallel. Equipment items in series are required to be operational at all times to keep the system available. Equipment items in parallel, also known as being in redundancy, require more information to be properly defined. Apart from the number of trains, the definition includes flow rates available in each train as well as its mode of operation, active or stand-by. Depending on the combination of the elements defined above, the impact of losing each one of the trains can be assessed.

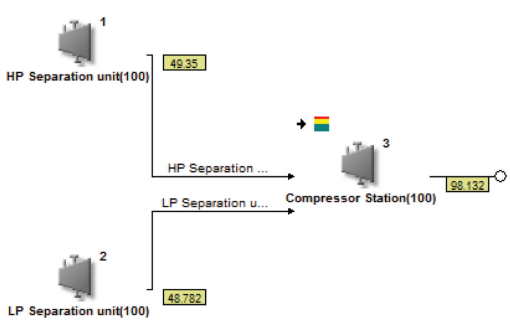


Figure 5. Separation plant flow network.

This process flow diagram does not show any redundancy at the equipment level. Hence, losing any equipment item will impose a production loss to the system.

Figure 6 shows the RBD for the HP Compression system and Figure 7 shows the RBD for the HP Separation system.

3.3.4 *Failure events and impact*

The failure of different systems will cause different impacts on the system. For example, different types of failures of the *Process Control Valve 1* will produce different losses. If the *Process Control Valve 1*:

- Fails open—half of the fuel gas production is lost because the flow is split between the recycle flow and the export pipe flow
- Fails close—full shut down of production to protect units downstream to the separation system

An evaluation of each of the possible failure modes must be carried out for all equipment items.

3.3.5 *Failure data*

The reliability data for this study is a modified version of OREDA's data (Det Norske Veritas AS, 2002). OREDA is a database of reliability data used for the offshore industry. As this system is operating onshore, the failure data and repair data is factored to more accurately represent the plant.

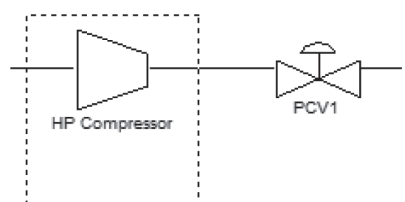


Figure 6. RBD Representation of the HP compression System.

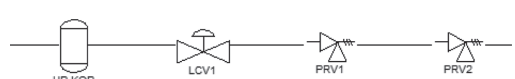


Figure 7. RBD representation of the HP separation system.

Table 2. Failure rates of equipment items.

Subsystem	Equipment	MTTF (years)	MTTR (hours)
HP compressor	HP compressor	0.106	24
	PCV1	7.189	17.28
HP separation	HP-KOP	7.189	17.28
	LCV1	2.327	22.08
	PRV1	7.189	17.28
	PRV2	7.189	17.28
LP compressor	LP compressor	0.106	24
	PCV2	7.189	17.28
LP separation	LP-KOP	7.189	17.28
	LCV2	2.327	22.08
	PRV3	7.189	17.28

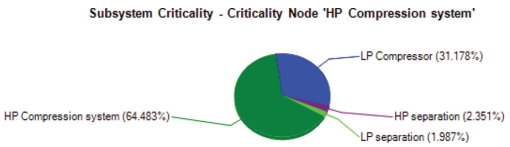


Figure 8. Criticality ranking of equipment contribution to unavailability.

All equipment items use statistical distributions which use a constant repair time and a constant failure rate.

3.3.6 *Maintenance strategy*

In this case study maintenance resources are assumed to be available at all times to perform repairs upon failure. It is important to bear in mind that maintenance strategies could impose delays to repair and increase the unavailability of the system.

3.3.7 *Performance results*

For the base design configuration the overall production efficiency of the system is 96.05%. The criticality ranking is shown in Figure 8 and tells us that the compression systems contribute the majority of production losses. The HP compression system causes 64% of losses and the LP compression system causes 31% of losses.

4 IMPROVEMENT CASE 1—IMPLEMENT WARM RUNNING REDUNDANCY TO COMPRESSORS

4.1 *RAM analysis*

The compression system including parallel redundancy for the HP compressor is shown in Figure 9.

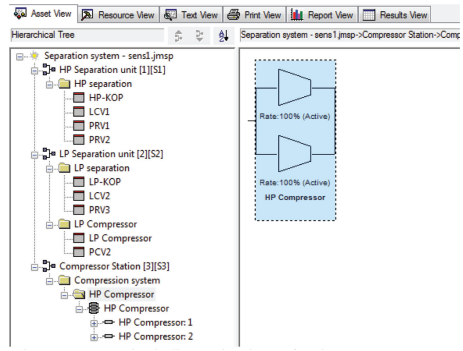


Figure 9. RBD including redundancy for the HP compressors.

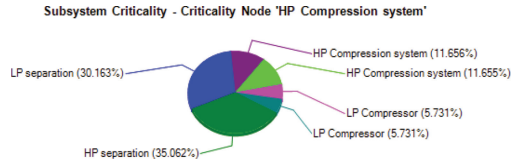


Figure 10. New criticality ranking of equipment contribution to unavailability.

Warm running parallel redundancy is a selected option for investigation as it offers instant switchover without ramping of the equipment should the operating compressors fail or be taken out for scheduled maintenance.

The improvement in availability and production flow from introduction of parallel redundancy to the compressors is of 3.7% resulting in 99.7% production efficiency.

4.2 *QRA analysis*

By adding parallel compressors which are running warm, so as to ensure instant switch over capability we are introducing two new parallel compressors. The plot plan of the suggested design is shown in Figure 11.

Following HAZOP of this modified design it was found that additional failure cases were present at the new compressors. Due to the need for immediate switchover to the parallel compressors, the equipment items would be at process conditions and therefore pose identical hazards as the operational compressors. In the QRA duplicate failure cases are used to represent loss of containment from the kick-back loops around each compressor. As this is a simplified case study no other changes were made to the QRA.

The LSIR contours resulting from analysis of this case are shown in Figure 12.

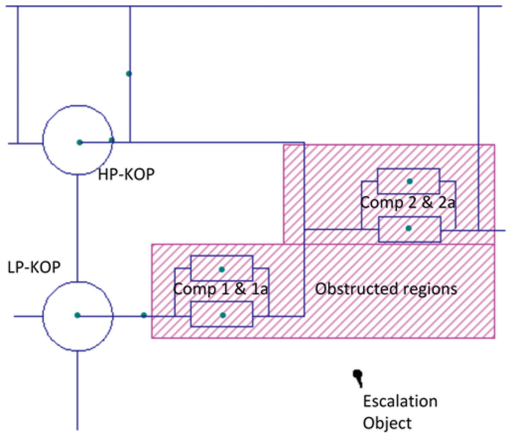


Figure 11. Plot plan of separation plant with parallel redundancy compressors.

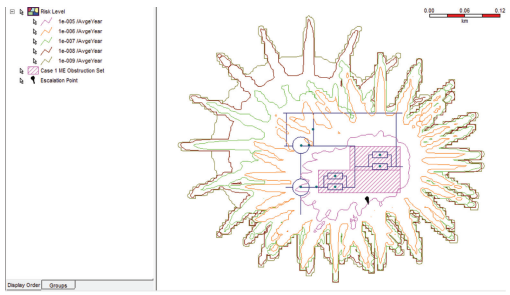


Figure 12. Risk contours for case with parallel compressors.

The risk contours indicate several changes to the risk results. The increase in size of the obstructed regions appears to have increased the size of the 1E-5/yr risk contour, which largely follows the shape of the obstructed regions. Larger congested and confined volumes will increase the flammable mass, flame path length and possibly turbulence patterns and thus increase the blast extents. Compounding the additional equipment is the increase in the number of failure sources. This of course increases the number of and thus frequency of hazardous outcomes. The risk ranking results in Table 3 for the escalation location tells us more.

The total location specific individual risk, as shown in Table 3 has increased by 30% to 2.21E-06/yr compared to the base case. Interestingly, the increased risk does not come from the new release location as the source term. Instead, the risk comes from expansion of the congested volume and its effect on the extent of blast potential on the escalation point. The increased risk from introducing the parallel compressors must now be assessed against the benefits derived.

Table 3. Risk ranking at escalation location after introduction of parallel compressors.

Model name	Risk (/yr)	Pct. risk
7 Leak from Compressor 1 kick-back	1.28E-06	58.07
Jet Fire	8.11E-07	36.67
Explosion	4.73E-07	21.40
4 Leak from Compressor 2 kick-back	8.11E-07	36.67
Jet Fire	8.11E-07	36.67
3 Line Rupture at gas outlet of HP-KOP	8.92E-08	4.04
Flash Fire	5.35E-08	2.42
Explosion	3.57E-08	1.61
7a Leak from Compressor 1a kick-back	2.63E-08	1.19
Jet Fire	2.63E-08	1.19
1 Rupture HP-KOP	6.98E-10	0.03
Fireball	6.98E-10	0.03
TOTAL	2.21E-06	

5 DISCUSSION

Clearly the increase in production availability has caused an increase in risk. The method used to increase availability from to 96.05% to 99.7% has increased individual risk at the escalation location from 1.71E-6/yr to 2.21E-6/yr.

The decision of whether this is tolerable must take into account a range of factors:

- local regulations for individual risk criteria
- corporate risk tolerance criteria
- the nature of the escalation location
- the increased value of the production efficiency gain from introducing improved availability
- the lifecycle cost of the improved availability initiative

5.1 *What other options do we have?*

Engineers are pragmatic and creative. Armed with analysis tools such as those used above for QRA and RAM we can perform sensitivity analyses to check the risk and production performance of a range of other ideas. Ideas we could adopt include but are not limited to:

- Offer standby (cold) redundancy, so as to reduce the potential for full pressure leaks from the parallel compressors—this would have an adverse but tolerable effect on the production efficiency

– Move the object that poses as the risk ranking point location. This might be a control room, an expensive or safety critical piece of equipment. Given that fuel gas production has increased we may have further funding available to invest in making a change to the site layout.
– Do nothing—perhaps the production efficiency gains outweigh the increase in risk

This case study highlights the benefits of having a unified asset data system that can be called upon by QRA and RAM analyses. By taking instances of the base case and making changes we can efficiently analyse a range of options. Each option will have production efficiency, risk and cost impact. Using quantified measures of production efficiency and risk we can make informed decisions about plant design and operation and take a holistic view of Loss Prevention.

6 CONCLUSIONS

In conclusion this case study has highlighted the benefits of the quantified analyses within the domain of Loss Prevention. By using QRA and RAM we are able to assess the design of a plant from a safety and performance perspective. The values of Risk and Production Efficiency and by performing sensitivity analyses we are able to make informed decisions about the impact of changes to design over a base case.

In this study we saw that a plant modification involving introduction of parallel redundancy to gas compressors provided a 3.5% increase in production efficiency, but a 30% increase in individual risk to a sensitive location.

Using quantified analysis allows us to check what other options we may have and to compare the pros and cons of each in an informed and numerate manner.

This holistic approach to the safety and asset management sides of Loss Prevention would be more accessible and improved if a repository of plant asset data were available on which to perform the analyses. QRA and RAM analysis are multi-faceted techniques which themselves require an underlying appreciable platform of good information. QRA requires thorough hazard identification and failure frequencies and RAM requires sound reliability data and well thought out flow networks and reliability block diagrams. The approaches in this case study made use of QRA and RAM analysis software tools. It is the opinion of the authors that such tools are crucial for freeing up the analyst to spend time working on the most important factor in these analyses: the information input to and output from the analyses.

REFERENCES

CCPS. (1989). *Chemical Process Quantitative Risk Analysis.* New York: AiChE Centre for Chemical Process Safety.

Det Norske Veritas AS. (2002). *Offshore Reliability Handbook.* Oslo: OREDA Participants.

RIVM. (2009). *Reference Manual Bevi Risk Assessments.* Bilthoven: National Institute of Public Health and the Environment (RIVM).

Smith, D.J. (2011). *Reliability, Maintainability and Risk: Practical Safety-Related Systems Engineering Methods. Elsevier*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Public risk perception towards chemical process industry: Comprehension and response planning

D. Botheju & K. Abeysinghe
Agility Group AS, Sandefjord, Norway

ABSTRACT: The chemical process industry is a vastly diversified entity which effectively involved in every facet of human life. Public perception of risks associated with chemical process industry is not necessarily aligned with the risk evaluation methods used by safety professionals. The risk perception by public is a subjective, emotional, and contextual process. This article is an attempt to elucidate this phenomenon in relation to chemical process industry and to provide a general guide for safety managers and decision makers to formulate responsive actions.

Several contextual factors which influence the public risk perception are identified and their impacts are described. The necessity of two way risk communication is emphasized as a mean of avoiding public concerns escalating into outrage. A case example is provided in this regard. Correct understanding of social dimensions of the concept of risk and timely engagement with the public are recognized as crucial aspects of modern day safety management in chemical process industry.

1 INTRODUCTION

1.1 *General*

The chemical process industry is a vastly diversified entity which effectively involved in every facet of human life. The essential life requirements like medications, foods, energy; as well as day-to-day use chemicals like detergents, fragrances, agrochemicals; and also the basic ingredients of modern high tech products (e.g. semiconductors, polymers) are all among the products of chemical process industry.

Chemical process industry involves many risk elements as all other human activities. However, it has been widely observed that public (including media) perception of risks associated with chemical process industry is being highly amplified in a distorted way. It is clearly noted that public is willing to accept far more dangerous events from other sectors (such as construction industry, transport, foods and healthcare, etc.) compared to probabilistically less risky activities emanating from chemical process industry.

Quite different to the way risks are quantified by safety professionals having associated scientific and engineering knowledge, the public risk perception is heavily affected by various emotional and contextual aspects. Laypersons often gauge risks mostly by the associated hazard which generates the risk, and also based on a number of other factors including various emotional states (Byrd, 2005).

It is seriously important for decision and policy makers within the industry and for other stakeholders to understand this phenomenon and accordingly plan their responsive activities to minimize negative repercussions arising from this distorted public risk pictures towards chemical process industry.

Also, the future progress of many technologies such as nuclear and genetic technologies (Huang et al., 2013) heavily depends on the social acceptability, other than any other factor. Therefore high attention on public risk pictures associated with the process industry is more crucial than ever.

1.2 *Objectives*

One objective of this paper is to discuss the above mentioned public risk perception scenarios associated with chemical process industry and to explain why this distortion is happening. The article provides a common understanding and recognizes a few key aspects which can be used to understand the basis of public risk perception towards chemical process industry.

The paper also suggests several strategies of communication that can be adopted by safety and risk management systems and by regulative authorities to correctly respond to the recognized public risk perception scenarios.

Table 1. Relative safety of chemical process industry (data adopted from Sanders, 2005).

	Risk related to chemical process industry	Comparison
Estimated loss of life expectancy (no. of "days")	Dangerous job (in general): 300	Cigarette smoking (male): 2250; Being overweight (30%): 1300; Vehicle accident: 207; Average job: 74
Relative occupational risk in US (1995)	Chemical and allied products industry: 0.6	Fishermen: 21.3, Timber cutter: 0.6, Taxi driver: 9.5, Average job: 1 Finance sector: 0.4
Fatal accident rate in UK (1987–90)	Chemical and allied industry: 1.2	Deep sea fishing: 42; Construction: 5; Agriculture 3.7; All manufacturing industries: 1.2.

1.3 *Relative safety in chemical process industry*

Despite the common misperception of chemical process industry being dangerous to occupants and surrounding communities, which is promoted by isolated case histories, such as the Bhopal tragedy, regular statistics show a very different picture. According to the data presented by Sanders (2005) the relative risk index of workplace accidents in chemical and allied products industry (value of 0.6) is about 20 times less than the relative risk faced by Fishermen (index of 21.3) and Timber cutters (index of 20.6). It is even less than the relative risk of an average job (index of 1.0). This fact is further emphasized when it comes to the fatal accidents and death. The relative risk index is a method of expressing workplace risk and it gives the ratio of the rate of quantified risk (such as the rate of fatal accidents) for a particular group of workers against the rate for the total number of workers (Bureau of Labor Statistics, 1997).

Table 1 indicates several other statistical figures related to chemical process industry compared against other occupations. If the comparison is made against other potential risks faced in life (other than occupation), the figures become even more intriguing. It can be underlined that doing a dangerous job (in broad perspective) carries only a 13% of risk compared to smoking habit (Table 1).

2 PUBLIC RISK PERCEPTION

2.1 *Risk*

Let us first indicate how the term "risk" is understood by its usual meaning, and by the typical definitions given in scientific literature (Table 2).

Except for the first 2 dictionary references, the rest of the definitions reflect the standard way "risk" is "defined" by scientific community, or by the "experts" opinion.

Table 2. Different definitions of "risk".

Definition	Source
A situation involving exposure to danger.	Oxford dictionary
Possibility of loss or injury.	Merriam Webster dictionary
Probability of an unwanted event that results in negative consequences.	Ostrom & Wilhelmsen (2012)
A measure of economic loss, human injury, or environmental damage in terms of both the incident likelihood and the magnitude of the loss, injury, or damage.	Bollinger et al. (1996)
The combination of the expected frequency (events/year) and severity (effects/event) of a single incident or a group of incidents.	Center for chemical process safety (2008)
Mathematical probability of a specified undesired event occurring, in specified circumstances or within a specified period	Mannan, 2014
Combination of the probability of occurrence of harm and the severity of that harm	NORSOK Z-013 Standard
Combination of the probability of an event and the consequences of the event	ISO 17776 Standard

But when it comes to the domain of public or the "laypersons", the way they perceive "risk" may not necessarily bounded by any of the above definitions. That is when one needs to consider the concept of risk perception.

2.2 *Risk perception*

It is understood that public's risk perception or relative risk ranking is affected by a number of qualitative factors or modifiers; hence they do not restrict themselves by the rational judgments

presented by experts regarding the quantitative likelihood of a specified risk. In other words, inexpert people may carry drastic biases when they come to judge the acceptability of a certain risk. This means, two similar risk events can be judged very differently by the public if the associated "context" is different, while experts' opinion may put both risks at the same threshold number. Note that the "perception" is subjective and will vary while the "actual risk" is constant.

In the following sections several factors recognized as important when analyzing the public risk perception phenomena related to chemical process industry are described. Note that some of these factors can be interrelated.

2.2.1 *Familiarity*

Risks posed by familiar establishments or events are seen as more acceptable compared to completely strange and new events. The communities living close to an old process plant may see a less and less risk when time goes by due to their experience that nothing dangerous has ever happened during previous years of their experience. However, in the eyes of experts, the risk of that process plant might be increasing when the plant nears its operational life time with aging equipment and older safety systems.

2.2.2 *Complexity*

The public can perceive a higher risk with the industrial processes and plants that seem hard to be understood. They feel a certain degree of mystery surrounding such facilities, but in most of the cases people have never even had a chance to see inside of such facilities.

For example: A community living nearby a water dam might face a statistically higher risk of dam failure compared to any risk posed by a nearby process plants. Still, public will "see" a higher risk with the plant than that "simple dam" which they can easily comprehend its arrangement and the purpose.

This implies that, in association with risk communication, it might sometimes be a good idea to let people come and visit a process facility and get them explained the processes happening there.

2.2.3 *Media*

Media can significantly influence public opinion on risks related to industrial activities. Media coverage most of the time leads to accelerate the risk perception, i.e.: amplification of perceived risk than what the risk really is. When it comes to chemical process industry, media coverage can be inherently biased. This is due to a characteristic nature of public media. The commercial media is usually based on popular incidents (for obvious reasons) rather than true scientific reporting. Hence, media tend to report "sudden, dreadful, sellable" incidents with a heavy weight rather than any news about "a peaceful operation of a chemical plant for a long time". This deposits an idea in public mind resembling chemical process industry to all-time "Bhopal gas tragedy", "Piper Alpha accident", or "Deepwater Horizon disaster". This should however be seen in the context that public media is always more interested in "disturbed, dangerous, and unsteady" occurrences rather than "steady, safe, slow phase" situations. That is where the "news" exists. Thus, this should be understood as the ground reality rather than a reason to blame the media. An industry should always try to maintain good relations with public media despite any past encounters with bad publicity.

Analysts suggest that the effect of media is more prominent among the less educated sectors of the public. Similarly if the targeted public is less experienced or knowledgeable regarding the particular hazard, then they can be more rigorously mediated by media coverage (Williamson & Weyman, 2005).

However some studies suggest that the relationship between media coverage and the public risk perception is not directly proportional as one might expect (Williamson & Weyman, 2005). Authors believe this may be due to the interrelated complexity between different demographic and other factors (modifiers) affecting risk perception, such as level of education, familiarity to the specific hazard, etc.

2.2.4 *Previous fatal experience*

If the community of concern has had a previous fatal encounter with similar risk, they would have a high intolerance for the same risk despite of the fact that reoccurrence of the same incident is statistically highly unlikely. This is especially relevant for highly dreadful incidents (Williamson & Weyman, 2005) Looking at an example of a natural event; 2004 tsunami which hit the eastern and southern coastlines of Sri Lanka claimed a casualty rate of about 15–20% of population lived within 1 km distance from the coast (Fehr, et al., 2006). After experiencing such a deadly event, people developed a high fear level of the risk of reoccurring tsunamis. There were several occurrences that coastline populations were scared themselves off and self-evacuated by false alarms. Meanwhile the "expert" opinion is that it will take another 300–400 years before any significant risk of a similar mega thrust seismic event can surface (NGI, 2006).

2.2.5 *Equity*

Public accepts more of the risks which are fairly distributed compared to the ones those are specifically

affecting a sector or an isolated community (Sinisi, 2004).

2.2.6 *Benefits*
Sometimes risks are perceived based on their relative benefits. A risk with high benefits to the local community might be perceived as less risky than it really is, and vice versa. Example: Some expressway road construction projects are opposed by some farming communities in Sri Lanka, because they do not gain much from the expressways which only serves rapid transit between big cities while these roads claim parts of their agricultural land.

As discussed for the case study in Section 4, this vital aspect is neglected by the controversial Rathupaswala latex factory (name of the locality in Sri Lanka) by deciding (unofficially) not to employ personnel from the nearby community.

2.2.7 *Cultural values and social norms*
Some industries are repulsed by the communities simply based on their cultural values. For example: poultry industry and associated meat processing facilities such as slaughter houses are highly repulsive to the rural communities in Sri Lanka where common public disapproves animal farming for meat production. The slightest of the emergence of any risk, such as an untreated effluent release, may be aggressively protested. In that case the protest may weigh way beyond the expected harm. In that example case, the design of the effluent treatment facility should include this dimension of public risk perception, and might need to invest for additional treatment stages.

Risk tolerance can heavily depend on the social norms of a particular society at a particular era. For example: Extremely high fatality rates of coal mine labors were an acceptable norm in Europe about a century ago.

2.2.8 *Voluntariness and control*
People give less weight to the risks that they are voluntarily subjected to (Sanders, 2005). Similarly they feel less risk in activities that they have control over (Sinisi, 2004). Meanwhile they might fiercely oppose an industrial activity that might have a very low risk compared to their day today activities (such as driving, sports, air travel, etc.) but in which they do not have "a say". This is where risk communication can play a major role in diffusing such amplified risk perceptions, by giving the public a chance to express their say and being listened.

2.2.9 *Artificiality*
Compared to natural disasters, people have a less acceptability to risks posed by manmade events such as a process plant explosion, or a chemical release. This is key perception modifier regarding chemical process industry. People have a general fear of all sorts of chemicals (perhaps except for water!) which in turn results in an amplified risk perception towards chemical process industry. Risk managements in chemical industry need to bear this additional weight compared to their colleagues in other industries, e.g civil engineering constructions, or electrical manufacturing. For example; Sanders (2005) pointed out that a particular dam collapse occurred in 1979 might have killed more people in India than the fatality count in Bhopal tragedy. The failure of Machchhu dam on August 11, 1979, in Rajkot district of Gujarat might have killed 1800–25 000 people (exact count is disputed). Yet, seemingly everyone has forgotten that dam collapse accident, but still a lot of talk is going on Bhopal tragedy that occurred five years later on 3rd December 1984. The official death toll was given as 3787 (the worst of the estimates put it at 16 000). The killing agent of the dam incident is water which is naturally familiar to people; while Bhopal tragedy involves methyl isocyanate (CH_3NCO), an artificial gaseous agent unknown to the public.

In risk communication, communicators must bear in mind the fact that repeated comparison of a chemical process plant risk to risks faced by natural events might make public angry and agitated; because they simply do not see the connection. (e.g. comparing the risk of industrial effluent release incident to a tsunami event).

2.2.10 *Permanency*
Risks leading to irreversible or long term persisting consequences are likely to be resisted extensively by the public, in comparison with risks leading to short term and recoverable consequences. In this context, a nuclear power plant which may have low statistical risk of fatality can be highly resisted by the public, while high fatality risk caused by flooding of the nearby river is easily forgotten.

2.2.11 *Dreadfulness*
There is a tendency that the public and media give overweight to highly dreadful incidents (Sanders, 2005) such as Bhopal tragedy or Piper Alpha accident; and they remember such events for a long time. But in reality the likelihood of such events can be quite low by modern day industrial safety practice. That means the "risk" (experts' risk) is low, but the "perceived risk" by the public is still high. The basic reason for this is that people are scared of violent scary ways of danger (such as an explosion) despite their low probability (hence the low risk) compared to slowly occurring (but perhaps more frequent and hence high risky) events such as disease caused by unhealthy life habits (e.g. smoking).

For example; public often react negatively to nuclear power generation, despite its statistically low fatality rate compared to other power generation means. This may associate with a couple of past incidents with catastrophic outcomes, including use of nuclear energy as a weapon.

2.2.12 *Phase of consequences*

When the consequences are readily observable, people react more negatively. Some risks emerge in so slow phase that people do not notice them for a long time. In an incident at Rathupaswala (Sri Lanka) where ground water acidification occurred (as explained in the Case Study, Section 4) reaction of the surrounding community was rapid. Meanwhile in an another region in Sri Lanka, where the heavy use of agricultural herbicides might have led to heavy metal contamination of ground water and associated widespread kidney decease, no public outcry was observed for decades, until recently the widespread danger is eventually surfaced. Higher risks with slow consequences are likely to be forgotten while smaller risks with rapidly observable consequences get largely magnified public reactions.

2.2.13 *Demographic factors*

Various studies suggest the influence of demographic factors on public risk perception. Factors such as education level, ethnicity, gender, age, income, occupation, etc, can have bearing on the risk perception. Investigating on such demographic effects on the public risk acceptability based on survey results conducted covering three provinces in China, Huang et al. (2013) observed that men had a higher risk acceptance to chemical industry compared women; younger people were more likely to accept chemical industry risks compared over 50 age people; farmers, retired persons, and house wives had less risk acceptability compared to other occupations. The same study by Huang et al. (2013) further suggested that highly educated people were more likely to accept chemical industry risks compared to the people with lower education. They further observed that people in the middle income category were highly resistive to chemical industry risks, compared to lower or higher income categories. This might be due to the fact that high income people are better shielded from risk elements, while the lower income category considers the potential benefits from the local industry. Such demographic factors must be given proper consideration by the industrial decision makers when they evaluate investments on new plants or when modifying existing plants.

Sometimes certain ethnic groups are more disturbed by new industries arriving at their localities. An example case: In an attempt to build a coal based power generation plant in Sri Lanka, strong opposition had been initiated by a certain minor religious group who were residing close to the suggested location. The location was chosen based on strategic considerations with the aim of minimized environmental effects, and was perhaps among the best locations for such plant. However, the perceived environmental risk by that local ethnic group was highly exaggerated which could be related to their perception that might have its roots in being a minor ethnic group.

This shows that industrial decision makers need to consider a very wide spectrum of social phenomena before they dare to invest in new projects which can trigger sensitive demographic factors.

2.2.14 *Trust*

Public's trust (or distrust) of the authorities and of the personnel responsible for handling any disaster aftermath and the experts who are advising public, is among the most critical elements which affect industrial risk acceptance by public.

A strong trust can overcome many other factors such as media influence, lack of knowledge, uncertainty, complex technologies, etc. Trust can be seen as a kind of compensation factor (Huang et al., 2013) that people can use to overcome other influential perception modifiers (Williamson & Weyman, 2005).

The trust can be based on four key aspects, i.e. impartiality, competence, openness, and past track records. If the concerned party is known to have high vested interests in other things than public safety, people may not trust them considering them as prejudice. This is very applicable for regulative and government authorities, perhaps for the whole political structure of a government. Trust can also be easily broken when a management or a particular expert is exposed by lack of knowledge or incompetence or negligence to carry out a particular task. Openness in sharing accurate details and presenting the whole picture increases the public trust. Managements and individuals with poor track records of safety and competence may need additional efforts to build public trust again.

What this means is that "trust" is one of the best assets an industry can build to defend themselves against unfavorable public risk perceptions. A community or the general public may after all accept a perceived high risk from a trusted company management, that they would not have accepted from a suspicious management which is known to have made past mistakes or have not kept their promises to the public (or to their employees). This point is further emphasized in the case study mentioned in Sec. 4.

The most critical aspect of public trust is that it takes a long time to build while it can be quite easily broken within a very short duration.

For example: A soft drink manufacturer might have been building public reputation for many decades while it takes one single news article in one day to break the whole trust, if it mentions that "an item" has been found inside one of their drink bottles.

3 RESPONSE PLANNING

3.1 *Policy decisions*

In decision making regarding safety, it is essential that regulators or industrial safety managers base their decisions not only on the expert opinion but they should seriously evaluate also the public perception of the associated risks. One might argue that publics' opinion is habitually inaccurate, unscientific, irrational, or biased. However, often the ground reality is that industry has to deal with public *en masse*, other than a bunch of safety experts; also to remember that it is the public who shapes the political arena which eventually takes higher-up policy decisions. In other words, the industry has to address this *perceived risk*, even if the experts' risk picture is quite different.

This expert verses layperson debate has its roots in two different world views. One school of thought is that the reality can only be scientifically explained and hence the decisions must be made based on tangible scientific evidence (such as the statistical probability of an event).

However, there exists an entirely different school of thoughts suggesting that there is no such thing as absolute reality, and the reality is relative to the perception of an observer. Hence the concept of risk itself is relative and the "real risk" is the one that is perceived by the majority of a society that represents cultural values and demographic factors. In this view point, opinion of the public may carry a similar or even higher validity than the experts' opinion. Williamson & Weyman (2005) indicated that even the experts can sometimes be culturally biased, making their opinions based on perception too, rather than founded on hard science and mathematics.

This effectively suggests that the concept of "risk" has a scientific dimension as well as a social dimension. Authors believe that "safety" shall not only be physically guaranteed but it shall be "felt" by the individuals who are being protected. One example of this concept: There is an elevated water storage tank situated in one of the large public hospitals in Sri Lanka where the water tank is purposefully constructed with a unique structural design. The massive concrete tank lies on an apparently narrow beam of straighten up single concrete column. Although the structural design is unique, extremely "safe" and showcases the skills of its designers, many patients coming to the hospital have expressed their worry about the "risky position" of the water tank. In this context, even though the tank is "safe" the public sees a "risk" in it. This may not be a good "and safe" design for a hospital after all (perhaps very good for a structural engineering faculty of a university). A good engineering designer must be able to combine both scientific and social dimensions into their designs.

Hence it is essential that modern-day chemical process facilities affectively engage the public, and also even more importantly the local communities, in a continuous dialogue throughout all life cycle phases of a process plant (i.e. from concept studies to operation, modifications and eventually until decommissioning). The safety policies and associated decisions must reflect, at least to a reasonable extent, that the public has been heard and their views are respected.

3.2 *Redefining risk*

The conventional formulation of the concept of risk is based on the extent of negative consequences of predefined events and the frequencies or probabilities of the occurrence of the defined events (Table 1). This definition of risk may be modified to include social dimensions as shown in (Formula 1), where risk (R) is defined as a function of threat events (e), consequences (c), probabilities (p) and social perceptions (s)

$$R = f(e,c,p,s) \tag{1}$$

Any eventual true formula based on Eq. 1 can be very complex and hard to estimate, since some of the associated social contexts can be extremely complicated and of varying nature. However, Eq. 1 can be a useful mean of emphasizing the impact of social dimensions in risk based decisions.

3.3 *Risk communication*

Risk communication is an integral part of modern day industrial safety management. Risk communication involves exchange of information related to the nature, magnitude, expected effects, and control of associated risks. The communication can happen between different stakeholders, such as safety management, the general public, media, investors, pressure groups, local communities, etc. In many situations, two way dialogues are essentially emphasized rather than unidirectional communications (Ng and Hamby, 1997).

Understanding of the nature of public risk perception towards a particular industrial activity is critical for the communicators to plan and execute proper communication strategies. Risk communication has become a vital topic among modern day process industries, instigated by new national and

international legislations mandating the obligatory requirements of industries producing or using hazardous chemicals or materials to inform general public regarding type, quantities, and other details related to their use of hazardous materials. In addition, "right to know" principal is now a widely accepted principle throughout the world.

In many process industry related cases, timely engagement with the public through constructive dialogues can prevent public opinion from escalating into public uproars and outrage. Note that if the matters are escalated into the higher levels, different pressure groups such as environmental groups (Sheppard et al., 2012) and media may involve and then the communication can be significantly complicated and difficult. This has been noted in the Rathupaswala latex industry incident which is mentioned under the case study in Section 4.

Communications related to risk details should be carefully planned based on public risk perception factors. Following guidelines must be paid with due attention in this regard.

3.3.1 *Key guidelines for risk communication*

Give a full picture of the involved risk: Even though it is likely to suggest that common lay people may not be able to comprehend complex concepts involving technology and physics, a number of studies has indicated that if the facts are properly presented common public is able to understand quite complicated information (Williamson & Weyman, 2005; other references). Hence, it is important to present the risk picture without withholding critical information. If the public get to know later that the company has withheld such info, it can totally ruin the trust between the communicating parties. Sinisi (2004) indicated several categories of key information that should be included in risk communications.

Public must be heard: The outcomes resulting from the engagement processes should not be disregarded eventually. This means that the dialogues with the public shall not be used as a mere face-saving mean. The public must be able to see that their viewpoints has been appreciated and taken care of. In some situations, full implementation of public opinions might not be feasible, but that should not result in total disregard of their voices.

Do not over-impose scientific opinion: Communicators must well understand the complexity of public risk perception factors and hence should be open to receive diverse opinions. Public must feel that their perspectives have been respected. Any attempt from communicator's side to overemphasize scientific opinion while downplaying the public views can lead to the collapse of any constructive dialog. Public may be expressing their true feelings and hence their view points are equally legitimate, whatever extent they might be distant from scientific reality.

Targeted communications if necessary: Sometimes it may be necessary to carry out targeted risk communication. E.g. certain ethnic groups in the area, or certain well respected community leaders in the area.

Communicators must have necessary knowledge and trust: Communicators shall not be only skillful in public communication but they should also have enough knowledge to present correct facts, figures and data. They must be able to answer questions raised by the public. It is to remember that there can indeed be technology experts among general public. If the public to see that communicators become speechless in certain questions raised, they will immediately loose the trust on the communicators. If such situations are likely, the management should use additional technical experts in the communication team to back the communicators up.

Do education campaigns if needed: In some situations, it will indeed need to do certain education of the public. Public seminars, handbills, electronic media, newspapers, or any such suitable mean can be used.

Maintain good relations with media: In many industrial risk scenarios media publicity can escalate public perception; at least that will be the apparent view point from industry's side. But it is truly important for the management to maintain good relations with public media. Be open to them and provide necessary information upon demand. Hostile attitudes towards media will always worsen the situation. Fighting with media is unwinnable and can be interpreted as fighting an invincible enemy. On the other hand, bad media publicity can be counteracted through industry's own media campaigns. Such campaigns should not however look like advertisements or blowing your own trumpet, but should carry some impartiality and deliver correct information.

4 CASE STUDY

4.1 *Rathupaswala (Sri Lanka) incident*

In 2013 there was a huge outrage related to a latex manufacturing facility in Sri Lanka, which was then known as Rathupaswala incident (Rathupaswala is the area name of the locality). The local manufacturing company which is known to be a global entity in latex industry, for supplying almost 5% of the world demand of rubber gloves (non-medical), was accused of polluting the ground water resource which is used by local community for drinking and other.

The company rejected downright the accusation telling that they had nothing to do with ground water acidification issue and had a proper wastewater treatment facility and all their activities were under the environmental license.

But the local community did not accept the claims and went ahead to continuous public demonstrations, picketing, hunger strikes and some violence. Media were covering the incident with 24 hr. broadcasts and cameras permanently located at the industrial facility, making it a public relations nightmare for the company. The government and the judicial had to involve as an urgent matter and the company was ordered to stop the production immediately. Eventually the large scale latex manufacturer was ordered to close down the facility and asked to move out of the area and relocate itself in a designated industrial zone.

Later research done by several independent research institution, public safety authorities, and local universities, indicated perhaps the accused industry might have nothing to do with the ground water acidification issue. Analysis and groundwater infiltration simulations suggested that other natural reasons may have led to the generally observed low pH of the ground water.

The important lesson here is that the company management did not maintain a public trust and credibility at the time of this incident occurred. They did not have a proper risk communication or public engagement strategy. They have had a number of past shaky deals related to effluent treatment. In the past, they were accused of ground infiltrating latex wash water (known to be acidic) which were stored in deep wells. After those past confrontations with the local community the factory did seem to resort to retorting actions like not to employ any one from the surrounding community. Also they did not seem to have trustworthy relations with media. This antagonist approach escalated the public risk perception and distrust among the surrounding communities that eventually led to a huge outrage.

If the factory management had had a constructive discussion (before the incidents) and had resort to effective risk communication techniques, this eventuality could have been avoided which almost ruined the company both by economically by enormous relocation and rebuilding cost, and by losing its reputation.

5 CONCLUSIONS

Social dimensions of the concept of risk is emphasized and explained in differentiation with typically accepted view point of statistical risk.

Different factors influencing the amplification and attenuation of public risk perception and tolerance in relation to chemical process industry have been documented.

Importance of timely risk communication has been pointed out and a general guide for managing risk communication is provided.

REFERENCES

Bollinger, R.E., Clark, D.G., Dowell III, A.M., Rwbank, R.M., Hendershot, D.C., Lutz, W.K., Meszaros, S.I., Park, D.E., Wixom, E.D., 1996. *Inherently safer chemical processes: A life cycle approach*. Book published by American Institute of Chemical Engineers.

Bureau of Labor Statistics, 1997. Compensation and working conditions, summer 1997 report. Accessed online; http://www.bls.gov/iif/oshwc/cfar0020.pdf.

Byrd, T., 2005. Avoiding outrage in risk communication. On Tap, Winter 2005 (Magazine).

Center for Chemical Process Safety, 2008. *Guidelines for hazard evaluation procedures.* 3rd Edition. Book published by Wiley Interscience.

Fehr, I., Grossi, P. Hernandez, S., Krebs, T., Mckay, S., Muir-wood, R., Pomonis, A., Re, D. d., Souch, C., Windeler, D., Xie, Y., 2006. Managing Tsunami Risk in the Aftermath of the 2004 Indian Ocean Earthquake & Tsunami. Report published by Risk Management Solutions (RMS).

Huang, L., Ban, J., Sun, K., Han, Y., Yuan, Z., Bi, J., 2013. The influence of public perception on risk acceptance of the chemical industry and the assistance for risk communication. *Safety Science*, 51, 232–240.

International Standard, ISO 17776, First Edition, 2000. Petroleum and natural gas industries—Offshore production installations—Guidelines on tools and techniques for hazard identification and risk assessment. Published by International Organization for Standardization.

Mannan, S., 2014. *Lees' process safety essentials: Hazard identification, assessment and control.* Book published by Elsevier Inc.

Ng, K.L., and Hamby, D.M., 1997. Fundamentals for establishing a risk communication program. Health Phys. 73 (3), 473–482.

NGI (Norwegian Geotechnical Institute), 2006. Tsunami risk reduction measures with focus on land use and rehabilitation. Main Report, CCOP-DMR Project.

NORSOK Standard Z-013, Edition 3, 2010. Risk and emergency preparedness assessment. Published by Standards Norway.

Ostrom, L.T. and Wilhelmsen, C.A., 2012. *Risk assessment: Tools, techniques and their applications*. Book published by John Wiley & Sons, Inc.

Sanders, R.E., 2005. *Chemical process safety: Learning from case histories*. 3rd Edition. Book published by Elsevier.

Sheppard, B., Janoske, M., Liu, B., 2012. Understanding risk communication theory: A guide for emergency managers and communicators. Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security.

Sinisi, L., 2004. Public concerns and risk communication. World Health Organization (WHO) publication.

Williamson, J. and Weyman, A., 2005. Review of the public perception of risk and stakeholder engagement. Health & Safety Laboratory, HSL/2005/16.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk assessment system for verifying the safety guards system based on the HAZOP analysis information

A. Nakai, K. Isshiki & K. Suzuki
Okayama University, Okayama, Japan

ABSTRACT: In recent years, serious accidents in chemical plants occurred frequently in Japan. Also in order to prevent deserters/accidents caused by natural disasters, it is needed to re-evaluate risks which consider reliability of existed safety guards system in chemical plants. In order to identify hazards in chemical plants, HAZOP (Hazard and Operability Study) is used as one of effective measures. In this paper, we propose the method to calculate the probability of occurrence of hazards in chemical plants by considering of existed safety guards system. The method is based on the HAZOP information and reliability of safety equipment arrangement.

1 INTRODUCTION

In past few years, serious accidents in chemical plants occurred frequently in Japan. Large-scale and complexity of chemical plants are growing. After the severe accident of Fukushima Daiichi nuclear power plants due to the Great East Japan Earthquake and Tsunami, the safety management of large industrial facilities has taken on increasing importance. Since then most Japanese people feel anxiety about not only nuclear engineering but also chemical engineering. In other words, our society required to build up a believable safety and reliability of chemical plants. As well-known many kinds of hazardous materials are under controlled in facilities. If a severe accident occurs, there is a possibility of a serious damage to employees and also local residents in the community. Therefore "risk assessment" is more important to identify the cause of the accident. Before an accident occurs, we should calculate the risk based on the frequency and scale of the damage of industrial facilities (Isshiki et al. 2013). This paper shows how to re-evaluate risks in chemical plants by considering reliability of existed safety guards system in plants.

2 PURPOSE AND APPROACH

In order to identify hazards in chemical plants, HAZOP (Hazard and Operability Study) is used as one of effective measures (Klets, T.A. 1992). When the risk assessment is performed, there is a problem whether the current measures are sufficient enough to evaluate the hazard. Therefore various methods are proposed to solve this problem. For example the system used in the risk assessment to create a statistical model based on the accident database (Meel et al. 2007). In chemical plants, the safety guards system is installed to prevent the accidents and the damage from spreading. The control system and the safety instrumented system perform in order to operate safely the existing chemical plant as the safety guards system. In this paper, we have proposed the method to calculate the probability of occurrence of hazards in chemical plants by considering of existed safety guards system. It is based on the HAZOP information and reliability of safety equipment arrangement. In this study, function for synthesis scenario trees is introduced HAZOP analysis system. Figure 1 shows overview the proposed system. After hazards are identified by HAZOP analysis system, the fault propagation scenarios are created automatically.

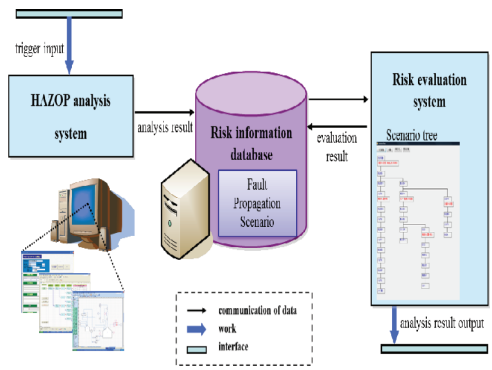


Figure 1. Outline of proposed system.

In this step, the information of abnormal states with the safety measures in IPL (Independent Protection Layer) is added to fault propagation scenarios. The system that we developed creates a scenario tree using fault propagation scenarios. Two or more causes are shown to one hazard in the created scenario tree.

We can calculate the probability of hazard using the information by HAZOP analysis system and layout of safety equipment in the fault propagation scenario. The probability of hazard is cut down by the suitable safety measures for the fault propagation scenario. The system can calculates likelihood of fault propagation scenario and evaluate of the risks which consider reliability of existed safety guards system in chemical plants. Based on this information, it is possible to verify and design safety guards system in plants to prevent accidents/disasters. The results can be used to assess risk of the chemical plant according to this method. When adding a safety measures after risk assessment, prepared method can determine a valid location to stop the fault propagation.

3 PROPOSED SYSTEM

3.1 *Add function to HAZOP system*

HAZOP analysis is a technique to identify hazard by using 'deviation' from the design intent. HAZOP used in the preliminary safety assessment of new plant or modification to existing ones. HazopNavi was developed to clarify the operation, behavior of the chemical plant (Kawamura et al. 2008).

Deviation is expressed 'guide word' and 'process parameter'. Guide word is a keyword used in analysis. Process parameters are flow, pressure, temperature and etc. In analysis, deviation is applied the pipe that is a part of process and propagated next equipment. Fault propagation is process that deviation is propagated. Fault propagation is used to identify hazards and to assess safety measures in HAZOP (Isshiki et al. 2013). Figure 2 shows the model expressing HAZOP analysis. This proposed system analysis is based on the HAZOP information and safety guards system arrangement. When hazards in plant are identified, at the same time, it can be recognized the location that safety measures work.

The instruments and equipment are arranged in the process for control to operate. If the deviation is propagated, the change and the propagation of the deviation are defined by each of the internal function of the equipment. Then the fault propagation consist of the deviation that perform safety guards system, the data is stored in the system database.

The following shows these procedures.

1. "Deviation" is defined
2. "Deviation" is converted into electrical signal
3. It performs control equipment, "Deviation" propagate safety measures
4. Parameter indicating by instrument is controlled.
5. The information of HAZOP analysis is stored in the risk information data base.

Using result by HAZOP system, the fault propagation scenario is created. The information of propagation is stored to the data base in the system. The analysis result shows the cause of propagation and identifies the hazards by the database. From this data base, it can remove the necessary information to create scenario tree. The proposed system creates the scenario tree of fault propagation automatically. This scenario tree system is developed to calculate automatically the accident frequency quantitatively. The model of the fault propagation scenario is created from many results of HAZOP system. It is shown in Figure 3. Ei0 is

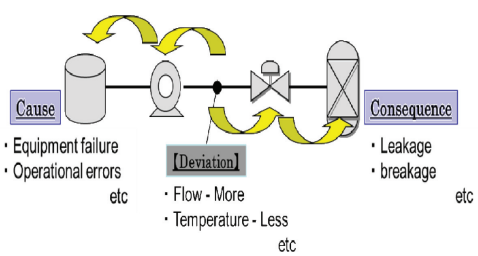


Figure 2. HAZOP analysis.

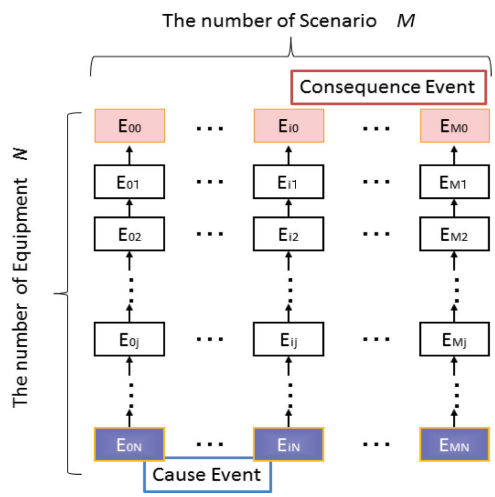


Figure 3. The model of fault propagation scenario.

the consequence event and EiN is the cause event in the fault propagation scenario. In this scenario tree system, it is possible to create a scenario tree indicating the cause of multiple hazards using fault propagation scenarios. Figure 4 shows scenario tree created from the propagation scenario. First the branch conditions are determined. When the system is generating the scenario tree, the scenario with the same consequence event is detected from the database.

To search information of hazards in the database is repeated. It is retrieved in the same way about branch condition. A search with some conditions perform on all equipment in the fault propagation scenario. By using the fault propagation scenarios, it is cleared that there are multiple causes for one consequence event. To visualize the position of the equipment that causes the fault propagation in chemical plant is very important. Since effect of fault propagation involved in the equipment becomes clear, it is possible to determine where to add new safety equipment by this technique. The safety equipment that located in a higher place from a branch point in the scenario tree can reduces the probability of hazard to two or more scenarios.

3.2 *Calculating the probability of consequence event*

3.2.1 *One cause event in the scenario*

There is one consequence event and one cause event in the fault propagation scenario. In this case, the probability of consequence event is as equal to the probability of cause event. This is the unavailability of the equipment causing failure. The unavailability of the cause equipment is given by $\overline{A}$. The probability of consequence event is expressed by (1) when the safety measure is not installed in the scenario.

λ = Failure rate of the cause equipment,

μ = Repair rate of the cause equipment,

MTTR = mean time to repair

P = the probability of occurrence of the consequence event

$$P = \overline{A}$$

$$\overline{A} = \lambda \times MTTR = \frac{\lambda}{\mu}$$

$$P = \lambda / \mu \tag{1}$$

There are more than one cause event in the scenario tree. The probability of occurrence of consequence event is equal to the sum of the probability of occurrence of each cause event as expressed in (2).

$$P = \sum_{i=1}^{n} (\lambda_i / \mu_i) \tag{2}$$

3.2.2 *One cause event and one safety measure in the scenario*

The probability of occurrence of hazards depends on the allocation of the safety measures in fault propagation scenario. By calculating likelihood of fault propagation scenario, the proposed system conduct evaluation of the risks which consider reliability of existed safety guards system in chemical plants.

In order to calculate probability safety measures, the PFD (Probability of Failure on Demand) is installed to calculate. The PFD means the probability that the equipment does not work properly when it is required (CCPS 2001). The PFD used on this system reference to "Guidelines for Process Equipment Reliability Data with Data Tables" (CCPS 1989). The Probability of consequence events caused by equipment failure can be calculated by equation (3).

λ = Failure rate of the cause equipment,

μ = Repair rate of the cause equipment,

P = the probability of occurrence of the consequence event

$$P = (\lambda / \mu) \times a \cdot 10^{-3} \tag{3}$$

3.2.3 *One cause event and more than one safety measures in the scenario*

In the scenario tree, there is one consequence event and one cause event. Safety measures placed more than one in the fault propagation scenario. And they work effectively. The probability of occurrence of consequence event is given by equation (4).

N = the number of safety equipment placed in the scenario tree

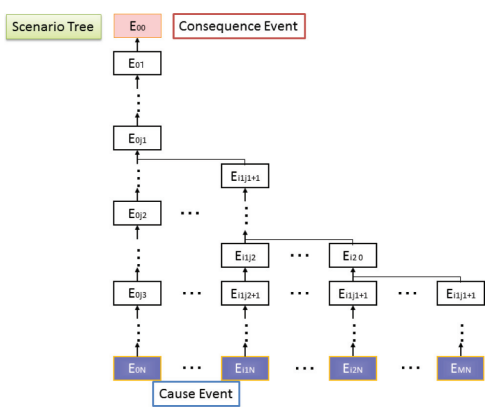


Figure 4. Scenario tree created from fault propagation scenario.

When the safety equipment does not exist, i.e., n = 0, PFD0 = 1

$$P = (\lambda / \mu) \times \prod_{i=0}^{n} PFD_i \tag{4}$$

3.2.4 *More than one cause event and safety measures in the scenario*

The safety equipment is placed appropriately in the fault propagation scenario. At this time, it will be expressed in the same tree that the same equipment causes failure in the scenario. There are more than one cause event and safety measures. Then the formula that calculates the probability of consequence event is generalized by (5).

$$P = \sum_{i=0}^{M} \left\{ \left(\lambda_{in_i} / \mu_{in_i} \right) \times \prod_{j=0}^{L_i} PFD_{ij} \right\} \tag{5}$$

3.3 *Changes in the probability of occurrence*

Therefore the system can calculate the probability of the effect of reducing the hazard by arranging the safety equipment. When the safety equipment is installed to control "deviation" in fault propagation scenario, the probability of occurrence of hazard of that scenario is reduced. The probability of occurrence of hazard varies depending on the placement of the safety equipment for the branch of the scenario tree. When safety measures are located on the side of the cause event branch, it works for only one scenario to reduce the probability of occurrence hazard. When safety equipment is located on the side of the consequence event, it works for more than one scenario to reduce the probability of occurrence hazard. When safety measures are placed to work effectively to the fault propagation, they can reduce the risk of hazard.

4 CASE STUDY

4.1 *Analysis range*

This method is supposed to the ethylene production plant. Analysis range is shown in Figure 5.

Prerequisite at this time is as follows.

1. Chemical plant analyzed by this system is a continuous operation plant.
2. The safety measures and the control system are analyzed in this investigation. (For example, safety valve and transmitter, instrument, control cable, and control valve)
3. All sensors are in order.

Safety measures are defined not to prevent hazard identification. Safety valve function linked parameter "pressure-more".

After the HAZOP analysis including safety measures, the information of a safety measures

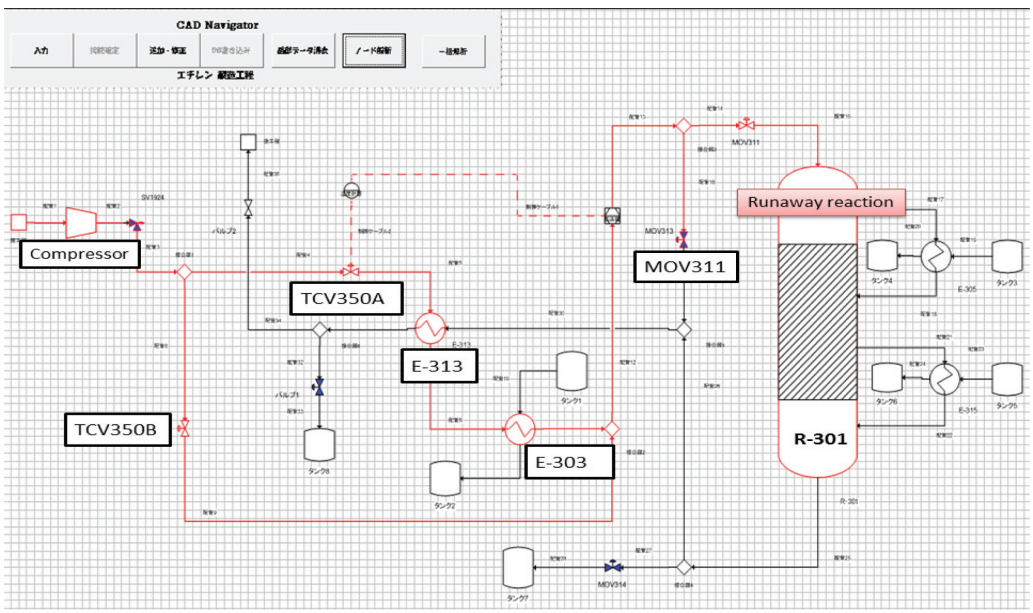


Figure 5. Analysis range in the ethylene production plant.

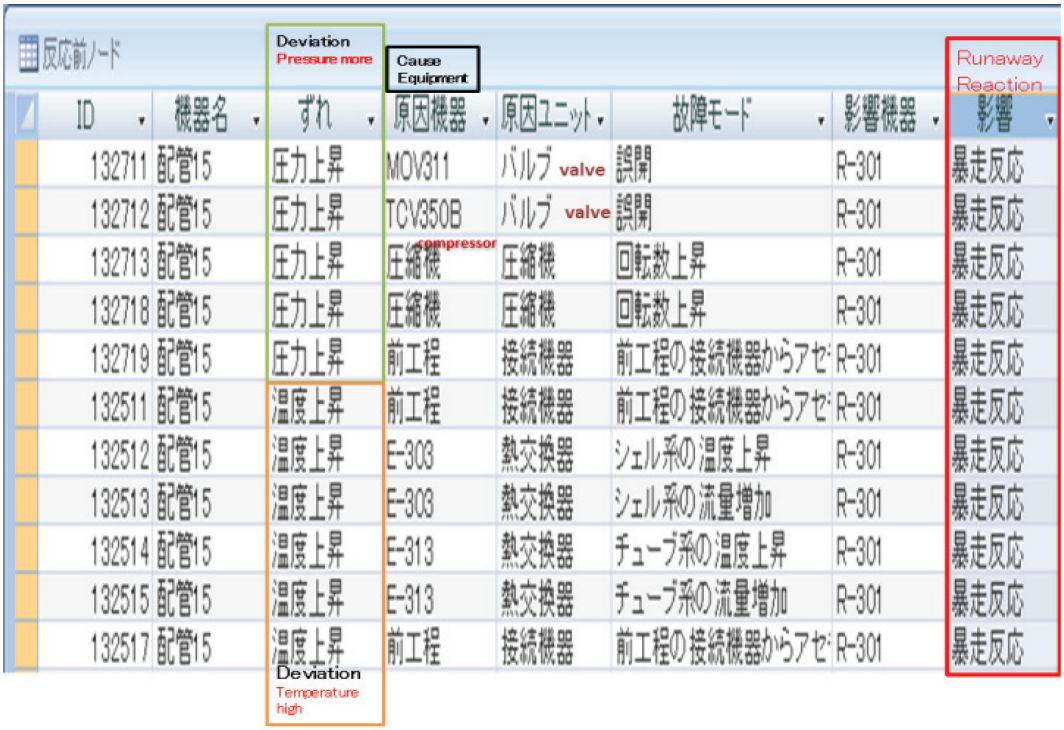


Figure 6. Fault propagation scenario.

is stored as a result. Repeat HAZOP analysis in the analysis range, the fault propagation scenario that has a top influence event in the reaction vessel of "runaway reaction" is created. The scenarios created are shown in Figure 6. By using the fault propagation scenario, the scenario tree including the safeguards equipment is created. This system can calculate the probability of the consequence event.

Figure 7 shows the scenario tree.

The probability of consequence event in the scenario tree is calculated according to equation (5). The probability of consequence events is obtained by summing the probability each scenario including the safety measures. Two deviations propagate in the scenario tree in Figure 7. The deviations are "temperature high" and "pressure more". There are seven cause events in the analysis range in Figure 7.

The probability of consequence event in the scenario tree is calculated according to equation (5). The probability of consequence events is obtained by summing the probability each scenario including the safety measures. Two deviations propagate in the scenario tree in Figure 7. The deviations are

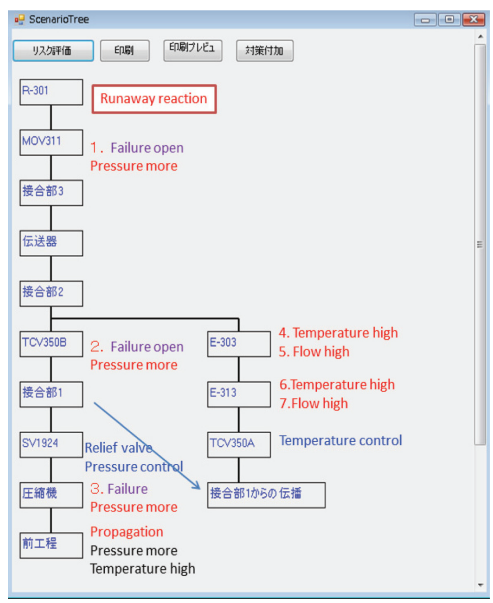


Figure 7. Scenario tree of the ethylene production plant.

"temperature high" and "pressure more". There are seven cause events in the analysis range in Figure 7.

The probability of occurrence of a runaway reaction in the reactor R-301 is calculated as follows.

1. MOV311: $P_1 = (\lambda_1/\mu_1) \times \mathrm{PFD}_0$
2. TCV350B: $P_2 = (\lambda_2/\mu_2) \times \mathrm{PFD}_0$
3. Compressor: $P_3 = (\lambda_3/\mu_3) \times \mathrm{PFD}_1$
4. E-303: $P_4 = (\lambda_4/\mu_4) \times \mathrm{PFD}_0$
5. E-303: $P_5 = (\lambda_5/\mu_5) \times \mathrm{PFD}_0$
6. E-313: $P_6 = (\lambda_6/\mu_6) \times \mathrm{PFD}_0$
7. E-313: $P_7 = (\lambda_7/\mu_7) \times \mathrm{PFD}_0$

$$P = \sum_{i=1}^{7} P_i = 0.00072 / \mathrm{year}$$

Therefore the probability of occurrence of the top event of this scenario tree is 0.00072 per year.

This result can be used for risk assessment in risk management.

5 CONCLUSION

In this study, we have proposed the risk assessment system for verifying the safety guards system based on the HAZOP analysis information. The system is developed to identify hazard and to calculate the probability of occurrence of consequence event. Safety guards system is installed in the existing chemical plants in operation. The effect of safety guards system is evaluated explicitly by using our system. This paper can clearly explain elucidated the linkage between the fault propagation and safety measures. It becomes possible to add information of the arrangement of the safety measures in fault propagation scenario without interfering hazard identified by them. The method included here can create a scenario tree based on the fault propagation scenario automatically. The scenario tree shows the placement of the equipment of the plant with safety measures. As a result of the analysis by the method included in this paper will become possible to consider the best placement of safety measures. Result of calculation by this method is the occurrence probability of the hazard based on the information of safety measures placement. This proposed method can re-evaluate the risk of chemical plants currently in operation. If an accident occurs, emergency shutdown is required rapidly. Furthermore, accident prevention is necessary not only for chemical plant and but also other industrial facilities. But still there exists the possibility that unexpected accident could occur in chemical plants. Therefore risk management is required to recognize and to examine all the angles of the situation in the plant. It is expected that the proposed method will become valid for this purpose and present useful information to support for plant operation.

REFERENCES

Center for Chemical Process Safety (CCPS)., 1989. Guidelines for Process Equipment Reliability Data with Data Tables. American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety (CCPS)., 2001. Layer of protection analysis: Simplified process risk assessment. American Institute of Chemical Engineers, New York.

Isshiki, K. and Munesawa, Y and Nakai, A. and Suzuki. K., 2013. HAZOP Analysis System Compliant with Equipment Models based on SDG. Recent Trends in Applied Artificial Intelligence: 460–469.

Kletz, T.A., 1992. Hazop and Hazan: Identifying and Assessing Process Industry Hazards Third Edition, Bristol.

Kawamura, K. and Naka, Y. and Fuchino, A. and Aoyama, A. and Takagi, N., 2008. Hazop Support System And Its Use For Operation. Computer-Aided Chemical Engineering, 25, 1003–1008.

Meel, A and O'Neill L.M. and Levin, J.H. and Seider, W.D. and Oktem, U. and Keren, N., 2007. Operational risk assessment of chemical Industries by exploiting accident databases. Journal of Loss Prevention in the Process Industries, 20, 113–127.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Development of the Safety Requirements Specification (SRS) in oil and gas industry

E.H. Park, K.P. Chang & S.T. Kim
Advanced Technology Institute, Hyundai Heavy Industries, Yongin-si, Gyeonggi-do, Korea

ABSTRACT: This paper presents the technical interpretations for Safety Requirements Specification (SRS) preparations in oil and gas industries based on international standards such as IEC 61508, 61511, and OLF 070. Development of SRS is an important activity to design the Safety Instrumented System (SIS). Some difficulties are explained to reflect international standards and fulfill all requirements of the standards in SRS during design phase of oil and gas plant. A new approach suggests a feasible systematic approach for SRS preparation to satisfy the safety requirement clauses by using case study. Also, an example of SRS based on above methodology is provided.

1 INTRODUCTION

The importance of safety systems has been gradually increasing in oil and gas industry. In general, safety systems, which are different and independent from each other, are considered to provide multiple protection layers. The typical multiple protection layers installed in oil and gas facilities are BPCS (Basic Process Control System), SIS (Safety Instrumented System) and Physical Mitigation System.

BPCS is a system which handles process control and monitoring for oil and gas facilities. SIS is a system composed of sensors, logic solvers and final elements to keep "people", "environment", "assets" in safe conditions during operation periods often oil and gas facility. Physical mitigation system is a system which consists of active fire protection and fire/blast walls. Among the various multiple protection layers, SIS is the most important and critical protection layer to prevent or reduce the risk of abnormal process condition which may be hazardous. A variety of SISs are installed in the oil and gas plants such as fire & gas system, emergency shutdown system and process shutdown system. SIS is the next layer of protection following BPCS and alarm/operator intervention.

In accordance with IEC 61508/61511, the overall required safety management and proper technical activities relates with all documentation for SIS are summarized in safety life cycle. The purpose of analysis phase is to identify hazards and assess safety requirements of SIS. Safety Requirements Specification (SRS) of SIS should contain critical information which includes functional description of each System Instrumented Function (SIF), target SIL, mitigated hazards, process parameters, maintenance requirements, response time, etc. Next phase of safety life cycle is the realization of SIS based on SRS results. All performance targets and functional requirements defined in SRS are the key information for design, installation and operation of SIS. The development of the SRS is one of the most important activities during the design of SISs. If important information regarding safety protection is missing, the design of the SIS may not be performed in a safe way.

According to the study by Health and Safety Executive (HSE) in the United Kingdom, improper SRSs are classified as the most significant cause of accident relating to control systems including SIS. Therefore, demands for well-prepared SRS are increasing in oil and gas industry.

However, there is lack of practical guidelines or systematic approaches to prepare SRS based on the technical interpretations of standards such as IEC 61508/61511 and OLF 070. For example, most standards just give a requirement description and the list with general level. On the other hand, more detail and quantitative information should be prepared and involved in SRS. Therefore, there are always technical gaps between detail SRS preparation and general guidance summarized in the standards during practical oil and gas projects.

So, the objective of this paper is to provide effective way to prepare SRS which can save cost and time. It is expected that this new approach reduces difficulties to prepare the SRS, and make the procedure of safety documentation simple. An example of SRS preparation is provided briefly.

2 SRS GUIDANCE REQUIREMENT REVIEWS

2.1 *Review of safety standards for SRS*

The general contents of SRS are based on standards such as IEC 61508, IEC61511 and OLF 070. The definition of SRS is given in the IEC 61508 (2010), "specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems." Also, the objective of SRS preparation is stated in the IEC 61511 (2003), "The SRS shall specify all requirements of safety instrumented systems, SIS, needed for detailed engineering and process safety information purposes." According to these standards, it is important that the documentation covers all safety aspects to be addressed during the safety lifecycle. In OLF 070 (2004), the SRS contents are the same as IEC 61511 (2003). Typically, the SRS of a SIS includes requirements for design, reliability, availability, installation, testing, maintenance, hardware specification, software development, and so on. The requirement is quite clear in the IEC 61511-1 (2003), chapter 10.

The SRS are divided in two components such as general parts and specific parts. The input information and general requirements are applicable to all SIFs implemented by SISs. Each SIF must fulfill specified functional requirements and integrity requirements.

The specific requirements for SIF are divided in three parts: requirements of function, safety integrity and software safety. Therefore, main content of SRS for SIF should involve quantitative safety integrity requirements as well as functional ones. The SRS input requirement documentation is used to give detailed information regarding functional requirements. These functional requirements consist of safe state, response time, reset function, trip point, output actions, etc. The integrity requirements for the SRS include assigned SIL, reliability requirements, demand mode, proof testing, environmental stress, and so on. The application software safety requirements are specified in IEC 61511-1 (2003), chapter 10.3.1. Several critical requirements such as common cause failure, spurious trip rate, response time and so on are discussed in Appendix A. The specification should be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and the assessment of functional safety.

2.2 *Safety requirements in IEC 61511-1*

SRS contains three types of requirements such as functional requirements, integrity requirements and software safety requirements. The description of the requirements in IEC 61511-1 (2003) is presented in Table 1. The following contents consist of 27 requirements and include general/specific requirements.

The safety requirements specification is followed by SIL assignments in the safety lifecycle. In order to fulfill a complete SRS, the required safety input information should be accessible. A typical set of input information includes process conditions, existing hazards, required SISs, required SIFs,

Table 1. Description of the requirements (ref. IEC 61511-1).

	Description of Requirements (IEC 61511-1)
SRS-1	Description of all the SIFs
SRS-2	Identify common cause failure
SRS-3	Definition of the safe state of the process (each SIF)
SRS-4	Definition of any individually safe process state (create a separate hazard)
SRS-5	Assumed sources of demand and demand rate
SRS-6	Requirements for proof-test interval
SRS-7	Response time requirements
SRS-8	The SIL and mode of operation for each SIF
SRS-9	Description of SIS process measurements and their trip points
SRS-10	Description of SIS process output action and criteria for successful operation
SRS-11	The functional relationship between process inputs and outputs
SRS-12	Requirements for manual shutdown
SRS-13	Requirements relating to energize or de-energize to trip
SRS-14	Requirements for resetting the SIS after a shutdown
SRS-15	Maximum allowable spurious trip rate
SRS-16	Failure modes and desired response of the SIS
SRS-17	Any specific requirements for starting up and restarting the SIS
SRS-18	All interfaces between the SIS and any other system
SRS-19	Description of the modes of operation and identification of the SIFs required to operate within each mode
SRS-20	The application software safety requirements
SRS-21	Requirements for overrides/inhibits/bypass
SRS-22	The specification of any action necessary to achieve or maintain a safe state
SRS-23	The mean time to repair
SRS-24	Identification of the dangerous combination of output states
SRS-25	The extremes of all environmental conditions
SRS-26	Identification to normal and abnormal modes and individual plant operational procedure
SRS-27	Definition of the requirements for any SIF necessary to survive a major accident event

target SILs, common cause failures, and so on. This input information is taken in various documents such as P&ID, HAZID/HAZOP report, C&E charts, logic diagrams, etc.

2.3 *SRS documentation*

The SRS is prepared before hazard and risk analysis and the allocation of safety function to protective layers in the safety lifecycle according to IEC 61511-1 (2003). It is important that the documentation covers all SIFs to be addressed during the safety lifecycle. After completing the risk analysis and SIL allocation, the SRS is created and updated according to the procedure in Figure 1. Revision process of SRS is needed in each phase according to the safety lifecycle. The average number of revisions is commonly more than 5 times.

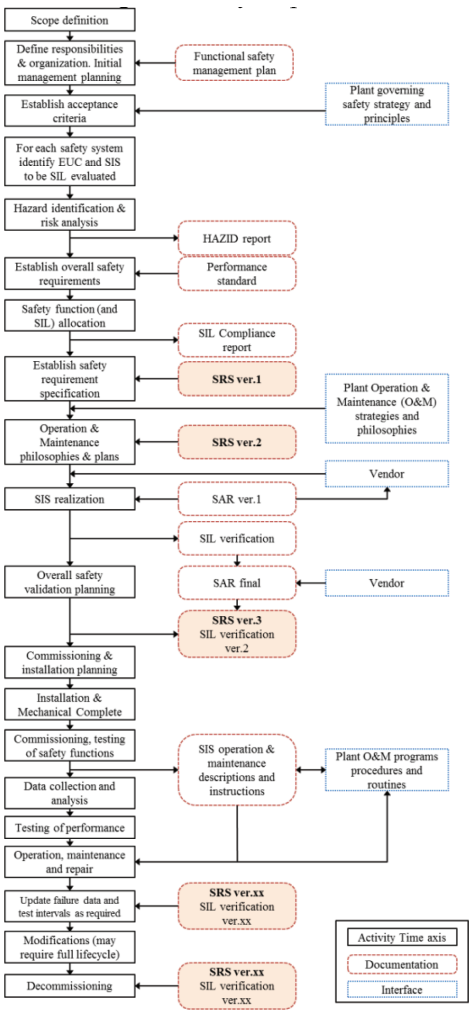


Figure 1. Procedure of SRS documentation (OLF 070 2004).

Generally, the SRS contains the relevant information to specify and operate the instrumented safety functions and provides the basis for design. The required information for the SRS is normally included in previous documents such as HAZID report, SIL compliance report, and so on. Most of the required contents of the SRS would not be available during early project phases because the actual data is not reflected on these documents. The SRS document is subject to follow-up and updating by vendor data through all lifecycle phases of the SIS.

Also, the SRS is an important document for the validation process. The SRS must cover all safety aspects for the actual SIS. During the validation phase, the SRS is served as the reference to check where the safety requirements are implemented in the SIS.

3 SUGGESTION OF MODIFIED FORMAT FOR THE SRS

3.1 *Problems of conventional SRS format—Comparison between IEC 61511 and practical projects*

The elements of SRS described in IEC 61511 are selectively involved based on characteristics of projects with respect of practicality. All requirements are not always engaged in practical projects during preparation of SRS documentation.

There is information of practical projects in Table 2. SRSs containing different contents are summarized in Table 3. If the requirement agrees with IEC 61511, circle is marked. And if the requirements have differences, it is X. The triangle is shown when the requirement is matched with a part of the IEC 61511. As shown in Table 3, requirements for SRS documentation differ from each project. For instance, although all 27 requirements can be mentioned in SRS documentation

Table 2. Details about 3 practical projects.

	Project A	Project B	Project C
Onshore/ offshore	Offshore	Onshore	Onshore
Site	Norway	United Arab Emirates	Saudi Arabia
Division	Oil & Gas production facilities	Gas processing plants	Refineries

Table 3. Comparison of requirements between IEC 61511 and practical projects.

IEC 61511	Project A	Project B	Project C
SRS-1	O	O	O
SRS-2	O	O	Δ
SRS-3	O	O	O
SRS-4	O	Δ	X
SRS-5	O	O	O
SRS-6	O	O	O
SRS-7	O	O	O
SRS-8	O	O	Δ
SRS-9	O	O	O
SRS-10	O	O	Δ
SRS-11	O	O	O
SRS-12	O	O	O
SRS-13	O	O	O
SRS-14	O	O	O
SRS-15	O	O	O
SRS-16	O	X	O
SRS-17	O	O	X
SRS-18	O	O	X
SRS-19	O	O	O
SRS-20	O	O	X
SRS-21	O	O	Δ
SRS-22	O	X	X
SRS-23	O	O	Δ
SRS-24	O	O	X
SRS-25	O	O	X
SRS-26	O	X	X
SRS-27	O	X	X

like project A, some requirements may be omitted in SRS documentation like project B or C. Also, some requirements are added to the SRS contents in project C.

Some contents which are related to SIF, safe state, proof test interval, response time, manual shutdown, and etc. are commonly included as main requirements in all projects. However, safe process state, additional action, normal/abnormal mode and major accident event are sometimes dropped. There are some occasions that new requirements are often added to SRS such as design intent, consequence of failure and so on.

Therefore, if all of the requirements in IEC 61511 are used as the format for SRS, there are a few difficulties. Although most of functional requirements for SRS can be handled, there are still concerns to miss some elements relating to integrity requirements. These include diagnostic coverage, maintenance requirements, concrete proof testing and reliability requirements, which may lack on the conventional SRS format as described in Table 4. Therefore, SRS format would be modified to include any necessary elements for integrity requirements which can be used in SIL verification followed by SRS documentation.

If input information for SRS is not available, the requirement must assume the empirical values with approximation. These assumptions may induce uncertainties of the elements.

Some requirements covering similar topics exist in IEC 61511. These are composed of several categorized items with similar subject. However, information on the requirements is redundant. This redundancy is unreasonable in terms of waste

Table 4. Suggested requirements for the SRS.

No.	IEC 61511	Suggested requirements
1	SRS-1, 10, 11, 24	Description of all the SIFs (Initiator, logic solver, final element)
2	SRS-2	Identify common cause failure
3	SRS-3, 4, 22	Specification of the safe state of the process and any action to achieve or maintain a safe state
4	SRS-5	Assumed sources of demand and demand rate
5	SRS-6	Requirements for proof testing(Interval, Coverage)
6	SRS-7	Response time requirements
7	SRS-8, 19	The SIL and mode of operation for each SIF
8	SRS-9	Description of SIS process measurements and their trip points
9	SRS-12	Requirements for manual shutdown
10	SRS-13	Requirements relating to energize or de-energize to trip
11	SRS-14	Requirements for resetting the SIS after a shutdown
12	SRS-15	Maximum allowable spurious trip rate
13	SRS-16	Failure modes and desired response of the SIS
14	SRS-17	Any specific requirements for starting up and restarting the SIS
15	SRS-18	All interfaces between the SIS and any other systems
16	SRS-20	The application software safety requirements
17	SRS-21	Requirements for overrides/inhibits/ bypass
18	SRS-23	The mean time to repair
19	SRS-25	The extremes of all environmental conditions
20	SRS-26	Identification to normal and abnormal modes and individual plant operational procedure
21	SRS-27	Definition of the requirements for any SIF necessary to survive a major accident event
22	-	Requirements for partial stroke testing (Interval, Coverage)

of time and cost consumption. Duplication of information should be avoided for managing the safety lifecycle as efficient ways. Therefore, process of integration to combine the redundant elements into one is needed.

3.2 *Suggestion of modified format*

It is necessary to define SRS elements thoroughly because there is no specified format in filling with the SRS. The duplicated requirements are removed and the necessary requirements are supplemented through the analysis in IEC 61511.

Incomplete elements that have deficiencies in existing format are eliminated by adding others which can reflect integrity requirements. Furthermore required data for the following phase is SIL verification, is added. Partial stroke testing and proof test coverage, for example, are supplemented in order to relieve the problem of insufficient integrity requirements.

Proof Test Coverage (PTC) is conditional probability that a DU fault will be detected by proof tests, given that the fault is present when initiating the proof test. PTC can also be expressed as the percentage of DU faults which will be detected by proof test among all the DU faults which are present when the proof test is initiated.

Partial Stroke Testing (PST) is sometimes used as a supplement to full proof testing of safety valves.

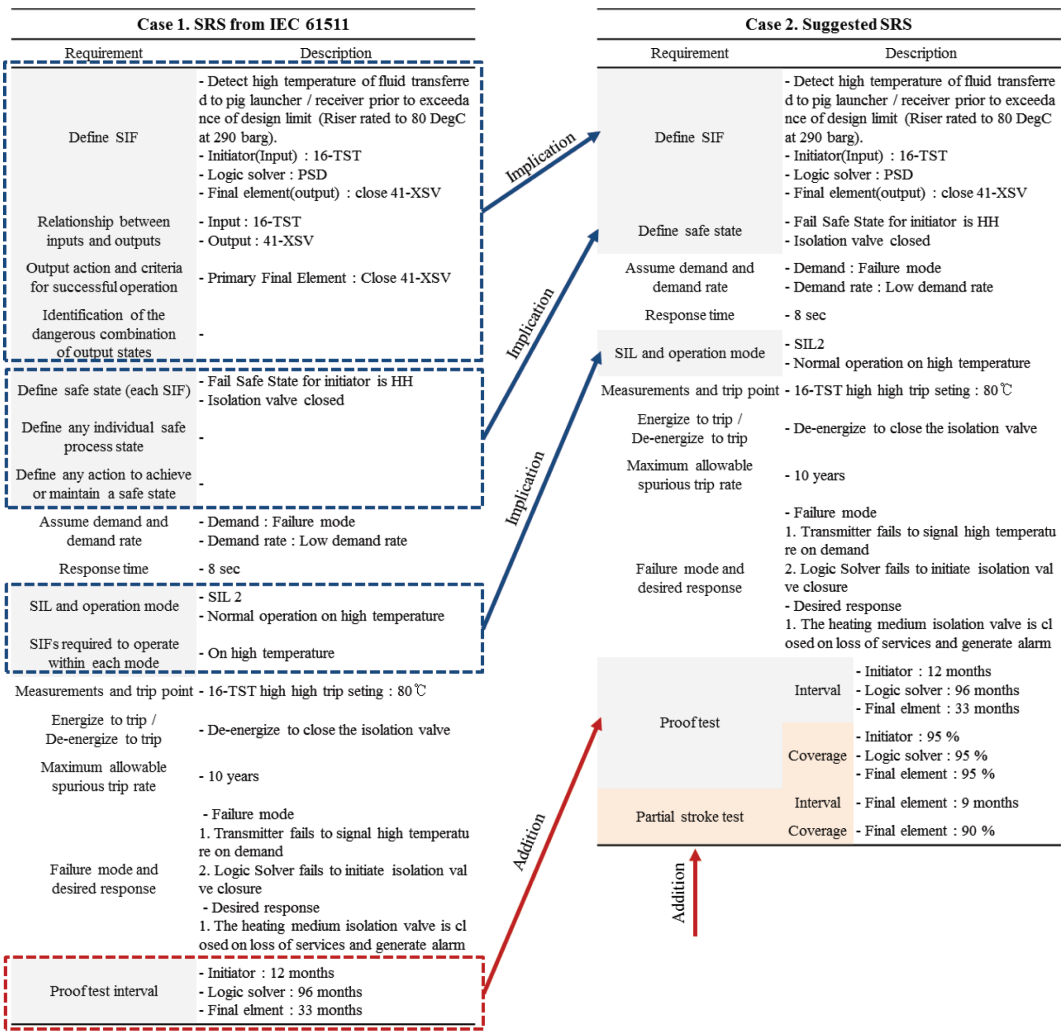


Figure 2. Case study for comparison with IEC 61511 and suggested SRS.

PST is performed by partially opening or closing a valve and returning the valve to the initial position. Assumptions related to PST coverage should be made for plant specific application rather than for an average valve performance in ISA-TR-84.00.03. The PST coverage is typically in the range of 60% to 70% (Summers & Zachary, 2000).

The requirements related to duplication topics are integrated into a single requirement as follows to prevent duplication of contents.

For instance, the similar requirements (SRS-4, SRS-10, SRS-11, SRS-19, SRS-22, SRS-24) are deleted according to the previous analysis. The value of input is described in the SRS-5 and the description of the output is SRS-10. The contents of SRS-5 and SRS-10 have the same contents as SRS-11's. Also, SRS-10 and SRS-24 describe SIS process output actions. SRS-3 and SRS-4 are definitions of the safe state of the process and SRS-22 is the specification of any necessary action to achieve or maintain a safe state. These requirements are similar to each other. Moreover SRS-8 explains SIL and mode of operation and SRS-19 does the latter. Thus, SRS-4, SRS-10, SRS-11, SRS-19, SRS-22 and SRS-24 can be omitted.

3.3 *Advantages of modified format*

All requirements for the SRS in IEC 61511 are difficult to fulfill. The conventional format has some problems regarding incompleteness, uncertainty and duplication. This paper proposes a modified format of the requirements to solve these problems.

Figure 2 shows case study for comparison with IEC 61511 and suggested SRS. The case study is carried out to compare specific requirements for the same SIF. Some requirements combine several similar requirements into one in the suggested SRS format. The requirements related to proof test and partial stroke test are added to the SRS, respectively. Therefore, the list of suggested requirements has simpler form than the conventional one.

Also, the brief list of the requirements can be bigger profit in time and cost when the number of SIF and revision of the SRS is great. Table 5 shows that there is acquirable profit by modifying the SRS. Total saving cost has been calculated by *(Total saving costs) = (Average number of SIFs) X (Reduced analysis time) X (Average number of revision) X (Daily rate)*. If the number of revisions increases, the saving cost will also increase.

Also, the new requirements, proof test coverage and partial stroke testing, are added to the original requirements. They are usefully available value in SIL verification phase.

The suggested requirement format keeps it simple while holding more contents. Management for safety lifecycle can be more convenient and time to prepare and update the SRS can be reduced by the change of format.

Table 5. Suggested requirements for the SRS.

Cost item	Value
Average number of SIFs	200
Reduced requirements	5
Reduced analysis time for each SIF (day)	0.03
Average number of revisions in the safety management plan	5
Daily rate for SRS (USD) (These daily rates are based on 8 hours per day)	2000
Total saving cost (USD)	60,000

4 CONCLUSIONS

SRS should be developed to cover all Safety Instrumented Functions (SIFs). The SRS, based on the contents from standards, has been set but the format has not yet been decided. This paper notes that some difficulties, such as incompleteness, uncertainty and duplication of the requirements in the standard, can be revealed through the analysis for the requirements of SRS. The modified format for the SRS is suggested in order to improve the problems. Multiple requirements dealing with similar topics are integrated and simplified. Moreover, systematic data management can be performed by adding other necessary elements for SIL verification. The suggested requirement format is simpler than the conventional one while holding more contents and management for safety lifecycle can be more convenient. Additional advantage by the change of proposed format is that time to prepare and update the SRS can be reduced.

Analyses in this study are performed to develop the format for the SRS. Some methodologies are suggested to obtain the values for several critical requirements such as common cause failure and spurious trip. However, the approach method for all of the requirements could not be described in more detail because there is no prescribe way for each requirement. A methodology which minimizes the incompleteness and uncertainty between practical data and assumed requirement should be developed. The development of the methodology for each requirement will be discussed in the further study.

REFERENCES

AIChE In-dustry Technology Allience. 2007. Guidelines for Safe and Reliable Instrumnted Protective Systems. An AIChE In-dustry Technology Allience. Wiley.

IEC 61508. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electro technical Commission.
IEC 61511. 2003. Functional safety—safety instrumented systems for the process industry. Geneva: International Electro technical Commission.
ISA-84.00.01. 2004. Functional safety: safety instrumented systems for the process industry sector. Research Triangle ark, NC: The Instrumentation, Systems, and Automation Society.
ISA-TR84.00.02. 2002. Safety instrumented functions (SIF)-safety integrity level (SIL) evaluation techniques part 1: Introduction. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.
Marvin Rausand. 2013. Reliability of Safety-Critical Systems. Wiley.
OLF-070. 2004. Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. Technical report. Stavanger, Norway: The Norwegian Oil Industry Association.
Rausand, M. and Høyland, A. 2004. System Reliability Theory. Models, Statistical Method, and Applications. 2nd edition. Wiley.
Sintef. 2010. Reliability data for safety instrumented systems, PDS method handbook. Trondheim, Norway: Sintef.
Sintef. 2010. Reliability prediction methods for safety instrumented systems, PDS method handbook. Trondheim, Norway: Sintef.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Development of functional safety standards for civil engineering

E. Nachtigall
Quantum Brandschutz GmbH, Basel, Switzerland

V. Shcherbina
WASCS Research Center, Moscow, Russia

ABSTRACT: Functional safety, as well as other topics related to safety, usually considered in each industry and also on the level of different standalone systems separately. Thus, each developer considering, basically, only their systems without take account adequately the relationship with other safety systems in buildings. Current standards for safety systems in buildings also do not include a comprehensive approach to safety systems. The aims of the paper are to present why functional safety methods are necessary for development of safety-related systems in civil engineering. Moreover, such methods are to develop in order to manage the increasing complexity of safety-related systems in modern buildings. The paper presents recent developments in the Russian Federation and describes ready to use, GOST R 53195 and interrelated standards focused on functional safety of safety-related systems in buildings.

1 INTRODUCTION

The approach to standardization of functional safety of systems as properties of those systems to fulfill the safety functions in an environment during an interval of time with the established probability (safety integrity) appeared at the very end of the XX century (Smith & Simpson 2004 and Börcsök 2007). A milestone in this approach was the development of IEC 61508 series for functional safety of the electric/electronic/programmable electronic safety-related systems (IEC 2010). This approach began to develop rapidly.

Now there are about 200 standards in more than 40 sectors of standardization of ISO and IEC in this field e.g. IEC (2000, 2005, 2007, 2008, 2012). The key features of standards are: implementation of an iterative process of the analysis of dangers and risks, the general assessment of risk and taking measures to decrease the risks to an acceptable level (according to ISO/IEC Guide 51 on safety aspects), and also the possibility of ensuring management of risk by repeating regular processes at all stages of the life cycle of systems and their components (Rolle 2013a).

Many procedures of risk management have been implemented in different areas after development of ISO Guide 73, ISO 31000 and ISO 31010 ISO (2009, 2011), Hasofer & et al. (2007). Also the acceptance of risk management methods given in those standards, which are related to standards of functional safety, has increased. In IEC according to Administrative Circular AC/7/2004 and Administrative Circular AC/33/2013 steps for transition from standardization of separate units of production to standardization of systems in which separate units of production (components) are structurally and functionally interconnected to work in the common uniform system for ensuring requirement are taken.

Thus, now there are all prerequisites for standardization and sustainable development of complex sociotechnical systems with use methods and means of risk management for safety.

The international standardization in the construction branch develops more slowly, than in other branches. Perhaps it generated a certain conservatism of thinking because of centuries-old traditions in one of the most ancient and, general successful activity of the people. In civil-engineering branch standards are traditionally developed in groups, whose interests often coincide, and members of the group are often from the same industry.

For example, developers and the technical committees of developing standards of automatic fire alarm systems, as a rule, for several reasons don't consider existing functional safety approaches described in IEC 61508 or other standards, claiming that sufficient reliability of systems is completely ensured with their compliance to national norms and standards of the branch ISO/IEC (2009), Rausand & Hoyland (2004).

Thus, each developer of standards and the producer of systems consider, generally only their systems without adequately taking into account

the relation with other safety-related systems in buildings. We know from the general theory of systems, that the properties of system cannot be completely defined by the sum of properties of its components (Ropohl 2012). Therefore there is no possibility to evaluate the level of functional safety or life and fire safety in the building without considering multiple interconnections of the fire alarm system with other systems, such as a fire extinguishing system, smoke extraction systems, security systems etc. (Nachtigall 2013b).

2 COMPLEX APPROACH TO FUNCTIONAL SAFETY IN CIVIL ENGINEERING

Systematic, comprehensive approach to functional safety, systems safety and security of buildings and structures can be seen in a series of national Russian basic standard GOST R 53195 "Functional safety of building/erection safety-related systems" (Shcherbina, Puzyrevskaya, Lubimov, & Matveev 2011, Nachtigall 2013a). The series consists of seven parts, five of which are already in place, and two additional parts are planned for development. Below the seven interrelated parts of the standard are listed.

- Part 1: General
- Part 2: General requirements
- Part 3: Requirements for systems
- Part 4: Software requirements
- Part 5: Techniques and measures on risk reduction, estimation methods
- Part 6: External resources for risk reduction, monitoring systems
- Part 7: Application requirements, sample calculations.

In parts 1 and 2, both first developed in 2008 general definitions and requirements of the standard are given. Parts 3 and 4 define requirements for hard- and software of safety-related systems used in buildings and constructions. In part 5 techniques and measures on risk reduction for those systems are presented. Parts 6 and 7 are in development. The focus of those parts is on methods for risk reduction and monitoring of systems as well as on application requirements and sample calculations.

The basis of GOST R 53195 laid down the basic definitions, philosophy, approaches and methods in accordance to IEC 61508 series, the requirements for quality assurance according to ISO 9000, safety aspects according to ISO Guide/IEC 51 (ISO 1999), with respect to the specificity and demands of civil engineering. During development of GOST R 53195 since the year 2008, current standards as e.g. ISO/IEC 14762 (ISO/IEC 2009) as well as experiences of applications from standards IEC (2000, 2005, 2007, 2008) were taken into account in the development process.

Standards focus on specifications providing improvements of safety to people and properties. They provide methods for analysis of hazards, risks and quantifying the safety of technical means to ensure the safety of buildings and erection or structures in order to achieve an acceptable level of safety, and provide a systematic approach to the facilities in civil engineering. Technical and safety related subsystems used in facilities of civil engineering are considered as systems of system. Also a holistic view of the entire system is given in Shcherbina, Lubimov, Puzyrevskaya & Matveev (2012).

3 TWO TYPES OF APPROACHES TO SAFETY AND RISK REDUCTION AS APPLICATION OF GOST R 53195

Production as a result of activity differs in industrial and construction branches. In Figure 1 the lifecycle of production of industrial manufacturing is shown.

Goods of industrial production are usually created in the design office and made at the factory. Those goods can be tested for compliance to be used in any situation and places according to its specifications.

Such goods, usually of mass production, can be stored in a warehouse, transported and delivered to the consumer, including with crossing of customs borders (Meyna & Pauli 2010).

In contrast to the life cycle of goods of industrial production in civil engineering the lifecycle of goods differs. In Figure 2 a simplified lifecycle of production in civil engineering is shown.

Typically, the lifecycle in civil engineering for most stakeholders begins with some engineering surveys followed by the process of design. After the examination of the project the construction work follows. At the end of this phase installation

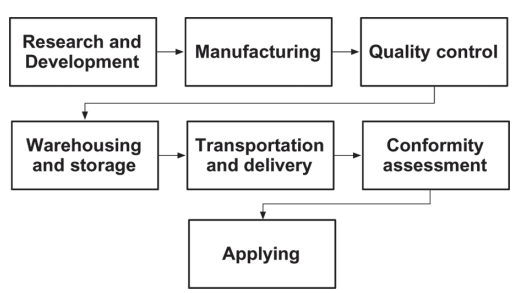


Figure 1. Life cycle of production of industrial manufacturing (after Ryan & Faulconbridge 2014).

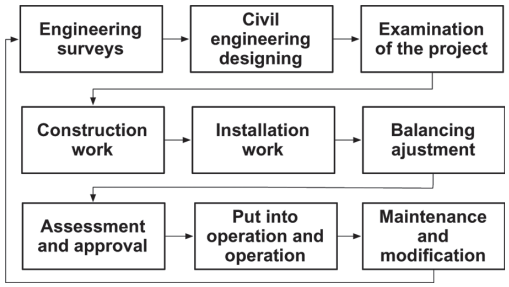


Figure 2. Life cycle of production in civil engineering (compare Mumovic & Santamouris 2009).

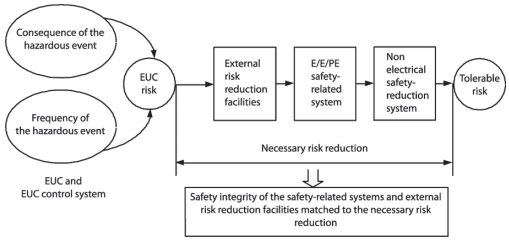


Figure 3. General approach to decrease risk (after DIN 1994, Börcsök 2007).

of technical systems is performed. This is followed by phases of adjustment, assessment and approval. Finally phases of put into operation, operation, maintenance and modifications start.

Due to different life cycles in industrial manufacturing and in civil engineering the approach to functional safety and risk reduction should take into account these differences.

In Figure 3 the general approach to decrease risk is shown.

In general, the risk is the result of a combination of consequence of the hazardous event and the probability of occurrence of these hazardous events. This combination influences the equipment under control risk. If this risk is higher than the tolerable risk, than necessary risk reduction measures are to apply to reach the tolerable risk level. To reach the tolerable risk level external risk reduction measures, the implementation of safety-related systems and the application of non electrical safety reduction systems are to be considered.

With a combination of measures and systems the risk level achieved is usually even lesser than the tolerable risk. In Figure 4 the relationships of risk and safety integrity are shown.

The actual risk reduction should usually be greater than the necessary. By judicious selection of shown modules the risk reduction achieved by all the safety-related systems and external risk

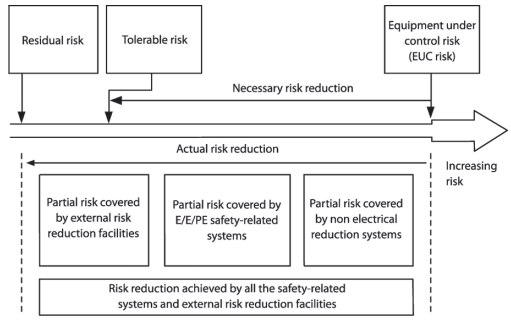


Figure 4. Risk and safety integrity (compare Börcsök 2007).

reduction facilities can be optimized especially for the needs of civil engineering.

During the process of evaluation of different risks not only the safety-related systems are to be considered. This is because in modern buildings many very complex and interrelated systems are usually used (Novak 2008). Therefore for different scenarios different initially non-safety or security-related systems can become crucial for safety or security. This results from the complexity of modern high performance systems in civil engineering. To take this into account GOST R 53195 provides methods and show examples of interrelated systems to consider different safety- and security-related scenarios and systems.

First practical applications of standard show positive experiences in modern and complex buildings. It is reported by the practical users that the use of standards real-world problems can be solved. Furthermore, it is reported that using the standards the safety can be significantly improved as a whole. Since the standards are new and still largely unknown, so far the application was limited to large objects that have an outstanding importance for national safety in Russia.

4 FURTHER DEVELOPMENT OF STANDARDIZATION

Along with independent application of the GOST R 53195 this standards created a basis for development of new standards for functional safety for special buildings and constructions.

Within National association of builders of Russia (NOSTROY), which itself is part of 270 self-regulating organizations uniting over 100.000 enterprises of the construction branch of Russia, the STO NOSTROY 2.35.73-2012 “Engineering networks of high-rise buildings. Systems of complex safety of high-rise buildings

and constructions." was developed and approved (NOSTROY 2014). Both authors of the presented paper are involved in the development and implementation of GOST R 53195 and STO NOSTROY 2.35.73-2012 in Russia and abroad. One of the authors is the coordinator of GOST R 53195.

The STO NOSTROY 2.35.73-2012 standard is applicable on safety- and security-related and other systems installed in high-rise buildings or constructions. Because of the importance of this type of buildings the engineering networks and other boundary conditions play a very important role to ensure the safety needs.

As features and factors influencing safety especially in high-rise buildings following examples can be listed:

- Difficult infrastructure of the building or construction and high saturation power-intensive engineering systems which may contain large volumes of harmful substances
- Large number vertically and horizontally directed supply channels which can be ways of fire propagation
- Vertical layout and natural updraft of air
- Large number of people in the high-rise building
- Limited possibility of safe evacuation of people from the building in emergency situations
- Lack of the effective technical means, allowing to organize rescue of people from high-rise buildings
- Attractiveness to carry out terrorist acts and actions of a criminal nature
- Possible considerable weight of consequences at realization of events doing harm.

5 PECULIAR PROPERTIES OF NOSTROY 2.35.73-2012

The standard establishes the main requirements to functional safety of safety- and security related systems according to GOST R 53195 and IEC 61508, and also considers the systems interrelated to engineering life support systems. Other engineering systems that are initially non-safety or security-related such as comfort maintenance systems according to the IEC 61511series are considered, too (IEC 2003).

It contains requirements for functional safety of about 28 types of safety- and security related systems, including complex system of safety. The standard establishes requirements for actions and procedures, which have to be executed in stages of the life cycle of these systems for achievement and maintenance of their functional and complex safety and antiterrorist and ant-criminal security of the high-rise buildings as a whole. The standard enables planning a control center to manage crisis situations and of evacuation of people. It contains requirements to elevators and their controls for safe evacuation of people, including the evacuation during a fire.

In the standard as well as in GOST R 53195 a systemic process approach is used (Meyers 2009, Ropohl 2012). Lifecycle of system or building is a process, which breaks into subprocesses, etc. Each of them has an input (e.g. information, energy or materials), an output (e.g. information, energy or goods) and functionality (actions in transformation of in- to outputs). A process can have some in- and outputs. The outputs of the previous process are used as inputs of the subsequent processes. Processes can also branch and unite.

In the standard besides requirements to systems also requirements for responsible persons influencing safety at each stage of the life cycle of systems, subsystems and complex systems or safety systems, and to their actions for reduction of influence of a subjective factor are established.

On the basis of presented standards similar standards for different types of construction objects in civil-engineering branch can be developed. Currently the possibility of development of standards for safety-related systems for underground objects is discussed in NOSTROY.

6 ADVANTAGES AND DISADVANTAGES OF FUNCTIONAL SAFETY APPROACH IN CIVIL ENGINEERING

As shown in the examples of the development of functional safety in civil engineering in the Russian Federation the role of functional safety approach is becoming more important.

Below some advantages and disadvantages of the approach of functional safety in civil engineering are listed.

Advantages:

- The society's needs for safety and security can be better achieved
- Civil engineering industry can learn from other industries (compare Rolle 2013b)
- Civil engineering industry can adopt and use best practice processes from other industries (e.g. IEC 2003, 2012)
- Civil engineering industry can use certified and reliable hardware and software from other industries
- Quality of safety and safety-related systems can be improved in the civil engineering industry
- Achieved safety level can be quantified.

Disadvantages:

- The adoption of standards and processes in the civil engineering industry can take long time
- The adoption of hardware and software can, in some cases, be expensive
- Expertise is necessary
- Certificate processes are to develop.

In spite of the disadvantages the advantages of the shown approach predominate from the point of view of the authors.

7 WORLDWIDE DEVELOPMENT OF FUNCTIONAL SAFETY IN CIVIL ENGINEERING

The importance of functional safety has grown steadily in recent years. This, on the one side, is because no other adequate solution to challenges in areas of safety, security and complexity can be observed. And on the other side for fast growing complexity of safety systems e.g. as for fire protection systems a solution to this problem has to be found rapidly as shown in Nachtigall & Klingsch (2011).

In Germany the standard VDI 6010 Part 4 "Safety Technology-Application of SIL classifications in the technical building equipment" is planned. The development of this standard by the Association of German Engineers begins in 2014 and will build on existing parts of the standard VDI 6010 parts 1–3 (VDI 2005). Also other commissions in Germany e.g. in German Commission for Electrical, Electronic & Information Technologies of DIN and VDE develop new standards in functional safety for the special needs of electrical engineering in the civil engineering industry.

Besides the identified national developments and discussed Russian standards the letter are planned to launch to international standards.

8 CONCLUSIONS

The paper shows clear and global trends and needs for safety in civil engineering. Furthermore the need to handle the growing complexity in civil engineering, and the need for new approaches to handle safety and complexity in this area are identified.

With presented and discussed current and interesting developments and ready to use standards a way to deal with growing complexity in civil engineering by implement and use special functional safety developments and standards is shown. First positive experiences of application of presented approach and standards in modern and complex buildings are available.

The discussed functional safety approach can be understood as the beginning of a new era of functional safety in civil engineering. Furthermore, the conclusion can be drawn that it is necessary to consider systems theory approach in functional safety to address the complexity in modern buildings.

Further development of standards will show whether the functional safety approach can solve the presented challenges of modern civil engineering industry. In addition, the development of standards will show whether they can give a new fresh impetus to the improvement of safety and security in civil engineering.

REFERENCES

Börcsök, J. (2007). *Functional Safety evacuation. Basic Principles of Safety-related Systems.* Heidelberg, Germany: Hüthig.

DIN (1994) DIN V 19250:1994-05 Leittechnik—Grundsätze für Rechner in *Systemen mit Sicherheitsaufgaben, Änderung* 1:1994-10.

Hasofer, A.M. & et al. (2007). Risk Analysis in: *Building Fire Safety Engineering*. Amsterdam, Netherlands: Elsevier.

IEC (2000). IEC 60204–1. *Safety of machinery—Electrical equipment of machines—Part 1: General requirements,* Edition 4.1 2000–05.

IEC (2003). IEC 61511. *Functional safety—Safety instrumented systems for the process industry sector, All parts.*

IEC (2005). IEC 62061. *Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems,* Edition 1.0 2005–01.

IEC (2007). *IEC 61131-2. Programmable controllers—Part 2: Equipment requirements and tests,* Edition 3.0 2007–07.

IEC (2008). IEC/TS 61000-1-2. *Electronic compatibility (EMC)—Part 1+2: General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena,* Edition 2.0 2008–11.

IEC (2010). *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems,* All parts.

IEC (2012). *Programmable controllers—Part 6: Functional safety,* Edition 1.0 2012-10.

ISO (1999). *ISO Guide 51 Safety aspects—Guidelines for their inclusion in standards.*

ISO (2009). *ISO Guide 73 Risk management. Vocabulary.*

ISO/IEC (2009). *ISO/IEC 14762 Information technology—Functional safety requirements for Home and Building Electronic Systems (HBES).*

ISO (Entwurf, 2011). *DIN ISO 31000 Risikomanagement. Grundsätze und Leitlinie.*

Meyers, R.A. (Ed.) (2009). *Encyclopedia of Complexity and Systems Science.* Springer.

Meyna, A. & B. Pauli (2010). *Zuverlässigkeitstechnik—Quantitative Bewertungsverfahren.* Hanser.

Mumovic, D. & M. Santamouris (2009). *A Handbook of Sustainable Building Design and Engineering,* Earthscan.

Nachtigall, E. (2013a). Functional Safety in Civil Engineering: On the example of the GOST R 53195 Functional safety of building/erection safety-related systems. *Standards and Quality*. *February 2013.*

Nachtigall, E. (2013b). Systems Analysis Methods for Consideration of Fire Safety. *Science and Safety 1 (6)*.

Nachtigall, E. & W. Klingsch (2011). Perspektiven anlagentechnischer Komponenten im ganzheitlichen Brandschutz. sicher ist sicher—*Arbeitsschutz aktuell 04, 160–163*.

NOSTROY (2014). STO NOSTROY 2.35.73-2012 *Engineering networks of high-rise buildings; Systems of complex safety of high-rise buildings and constructions.*

Novak, T. (2008). *Functional Safety and Systems Security in Building Automation and Control Systems—A Common Approach,* PhD-Thesis, Vienna.

Rausand, M. & A. Hoyland (2004). *System Reliability Theory Models, Statistical Methods and Applications.* Hoboken: John Wiley.

Rolle, I. (2013a). Die Sicherheit eingebetteter Systeme. *Elektronik 3*.

Rolle, I. (2013b). Modelle der funktionalen Sicherheit. *Elektronik 3*.

Ropohl, G. (2012). *Allgemeine Systemtheorie Einführung in transdisziplinares Denken.* Germany: edition sigma.

Ryan, M.J. & R.I. Faulconbridge (2014). *Systems Engineering Practice*. ArgosPress.

Shcherbina, V.I., M.M. Lubimov, E.I., Puzyrevskaya, & V.P. Matveev (2012). Functional safety of the safety-related systems in construction. *Globalnaya bezopasnost, Yubileyny vypusk*.

Shcherbina,V.I., E.I. Puzyrevskaya, M.M., Lubimov, & V.P. Matveev (2011). *Functional safety of the safety-related systems in construction*. Technical Report 2126.

Smith, D.J. & K.G.L. Simpson (2004). Functional Safety. A straightforward guide to applying IEC 61508 and related standards. Elsevier Butterworth-Heinemann.

VDI (2005). VDI 6010 Technical safety installations Systems overlapping functions, All parts.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Mechanism design for risk allocation and benefit sharing in the development of a Geological Disposal Facility for nuclear radioactive waste

Oscar Nieto-Cerezo, Edoardo Patelli, Jan Wenzelburger & Michael Beer
Institute of Risk and Uncertainty, The Quadrangle, University of Liverpool, Liverpool, UK

ABSTRACT: In this research, we analyse a mathematical model using principal-agent theory where NDA delegates the implementation of a GDF to site licenced companies through the take-it-or-leave-it offer of a contract. A risk sharing incentive mechanism is designed to overcome the moral hazard problem when agents hide information on the level of risk, in order to accomplish the highest level of economic, environmental and social performance. An application to a simplified model will show the potential of the proposed approach. This paper will be of interest to academic and consultants concerned with the design of incentive contracts in the nuclear industry.

1 INTRODUCTION

Atomic power plays an important role in the mix of energy in the UK supplying 18% of the electricity consumed (World Nuclear Association 2014).

Since the first world's reactor started operating for commercial purposes in Sellafield, the UK has accumulated around 1,000 cubic meters of High Level radioactive Waste (HLW) which represents 95% radioactivity in radioactive waste (NDA 2010).

The viability of the development of the new generation of nuclear plants announced by the government in 2013 is subject to the effective management of radioactive waste.

The proposed solution to manage HLW is the development of a Geological Disposal Facility (GDF) where HLW is placed in a deep rock environment which is stable and unaffected by environmental change for hundred thousands of years. Under this condition radioactive waste which is protected from underground water by a geological, concrete and metallic barrier undertakes a natural process of radiation reduction called radioactive decay (NDA 2010).

The primary risks associated with nuclear activities arise from the radiation released by radioactive materials in the reactor and during the disposal. Nuclear risk can be interpreted from two perspectives, as the probability of death as a result of nuclear explosion, which in the UK is about 1 in 100 million or the probability of death as a result of long time exposure to radiation (HSE 2001).

GDF is an example of a complex project comprising a large number of interrelated risks affecting every-thing from technical feasibility to cost as well as large number of stakeholders including Government, Parent Body Organizations, Site Licensed Companies and financial institution.

This complexity requires a sophisticated multidisciplinary approach to secure a robust balance among all parties in view of sharing risk and benefits. Benefits and risks associated with large energy projects have to be considered from an economic, environmental, engineering and societal point of view.

It is obvious that an optimal solution is often not achieved such as the UK public rejection to GDF and the Fukushima nuclear accident have shown. Fukushima Daiichi reactor accident is an example

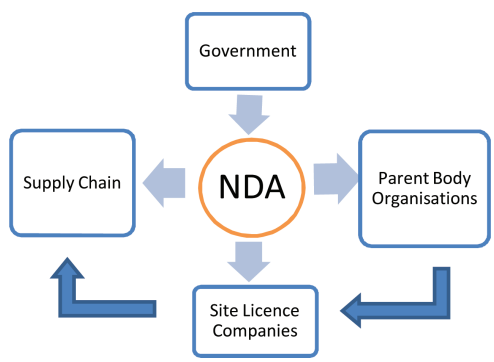


Figure 1. Structural NDA contracts (NDA 2010).

of benefit and risk sharing failure due to the moral hazard problem. As a result of underestimating the level of risk associated with tsunamis, Tokyo Electric Power Company (Tepco) took the decision of cutting down the original 35 meters cliff of the island and replaced it with a shorter concrete seawall to facilitate the access to docked ships. This decision brought some initial savings to the overall project cost but quite tragic consequences (Japan Nuclear Institute 2011).

The contribution of this paper is the introduction of an incentive mechanism to overcome the moral hazard problem when SLC's hide information on the level of risk under asymmetric information. When economic actors make profit—maximizing but inefficient decisions because they are able to avoid the cost associated with the conduct, the incentive mechanism will encourage stakeholders to reveal their private information on risk to accomplish the highest level of economic, environmental and social performance.

2 PRINCIPAL AND AGENT FRAMEWORK

Classical risk management approaches take the perspective of a single player for which the risk analysis is being carried out. Nevertheless, a game theoretical approach can be regarded as a decision making tool to model and predict the outcome of the strategic interactions between principal and agent. This enables managers to take the most efficient action in a given scenario. Strategic interactions comprising government and a consortium of companies to implement energy projects can be model in the framework of principal and multiagents. Principal–agent theory is concerned with the design of incentives by the principal when the principal and agents conflict in their personal objectives and exits asymmetric information between them (Laffont & Martimort 2001). In this setting, the presence of a consortium of site licensed companies requires the coordination of their efforts for joint a team production. The agents' problem is to decide, given a contract, whether to contribute to a public good when costly contribution is unobservable by the principal (Whitford 2002). In this paper, we model the coordination problem between agents in the framework of prisoner's dilemma.

Several authors have attempted to address efficient risk sharing allocations in the framework of principal and agent. Shavel states that a Pareto optimal payment fee by a principal to his agents is subject to the attitudes towards risk of the principal and the agent. The most appropriate payment fee (incentive) to a risk neutral agent is the outcome minus a constant, the principal share. On the other hand, if the agents are risk averse will not accept to bear all risk if an intolerable risk scenario is realized (Shavell 1979).

3 FORMULATION OF THE MECHANISM

NDA as the principal delegates the implementation of the geological disposal facility to the winner of a competitive tendering—PBO's and SLC's.

The asymmetric information of the strategic interaction between NDA and SLC's makes NDA unable to observe the actions taken by SLC's to complete the task. This prevents an efficient resolution of players' conflict of interest. This is known as the moral hazard problem (Laffont & Martimort 2001).

In this context, SLC's are rational companies in a game theoretical sense presented with the dilemma of how many financial resources should be invested in risk reduction when profit-maximizing is the objective.

The level of investment in risk reduction can affect the feasibility of the project as well as NDA and SLC's payoffs.

To this end, NDA faces two questions:

a. How to design an incentive mechanism so that efficient investment in risk reduction is desirable for SLC's
b. How the cost of risk should be shared in relation to possible scenarios

These questions can be answered by defining a game in the principal and agent framework.

3.1 *The game—interaction between SLC's*

Risks of different nature in complex systems are interrelated causing propagation phenomena such as reaction chains and loops (Fang et al. 2012). Thus, risk management in large energy projects requires the cooperation of site license companies as well as the parent body organizations to reduce risks to acceptable levels.

3.1.1 *Notation*

π_i	Payoff function of the Site Licenced Companies.
α	Revenue share allocated to each SLC's.
δ	Percentage of electricity trade-off revenue transferred to SLC's.
$E(\tau_{C_P})$	Expected monetary transfer from NDA to SLC's as a function of the cost of implementing risk mitigation actions.
P	Price of a KWh of electricity generated by nuclear power plants in the UK.
Q	Quantity of KWh of electricity generated by Nuclear Power Plants in the UK.
C_P	Total cost of electricity generation including the cost associated with construction,

maintenance, dismantling of the power plant and managing radioactive waste through a geological disposal facility.

θ Risk associated with nuclear waste; environmental damage (e.g.: contamination of soil, pollution of water bodies) and health effects of radiation (e.g.: cancer).

C_r Cost per unit of risk. When the cost is higher than 0 an investment in risk mitigation has been made. When the cost is equal to 0, companies maintain the status quo.

P_r Probability of a natural hazard.

N Monetary loss when a hazard occurs.

3.1.2 *Payoff function of site licensed companies*

The generation of electricity from nuclear sources has an associated economic revenue from trading off in the energy market as well as some cost related to the construction, maintenance, running and decommissioning of the nuclear plant.

The payoff of SLC's is subject to the outcome realized. Consequently, SLCs' payoff can be represented as follow:

$$\pi_i = \alpha(\delta(E(t_{C_{r>0}}))) - (\theta * C_{r>0}) \quad (1)$$

where α the revenue share to each SLC, δ is the fixed payment agreed between NDA and SLC's $E(t_{Cr})$ δ is the expected monetary transfer from NDA to the SLC's as a function of the level of investment in risk reduction. Risk (θ) is defined as the multiplication of the probability of a hazard to occur times the consequences in monetary loss. C_r is the cost associated with implementing risk mitigation to reduce the current levels of risks.

$$\theta = P_R * N \quad (2)$$

The investment required will depend on the level of risk. Thus, the outcome of the project is a function of the level of risk and the risk mitigation investment.

The consequence of risk in this study is taken as the number of fatalities resulting from nuclear accidents or exposure to high radioactivity levels.

The cost per unit public risk reduction (C_r) can be derived from the compensation for fatalities. (Zhao, et al 2012).

In the UK, 1,000,000 GB pounds (2001) is presented as the Value of Preventing a Fatality (VPF) related to a reduction in risk of one in a hundred thousand (HSE 2001).

3.1.3 *Analysis of the game*

This game setting can be viewed as a prisoners' dilemma paradigm which illustrates the conflict between social incentives to cooperate or private incentives to defect (Auman 1987) as shown in Table 1.

In this setting, Site Licensed Companies strategically interact and take decisions on whether or not to invest in risk reduction or maintain the status quo.

The Nuclear Decommissioning Authority intervenes by offering a contract which includes a payment transfer that encourages companies to jointly contribute to risk reduction.

This payment transfer should satisfy two constraints

a. The incentive constraint

$$\alpha\left(\delta\left(E(t_{C_{r=0}})\right)\right) < \alpha\left(\delta\left(E(t_{C_{r>0}})\right)\right) - (\theta * C_r) \quad (3)$$

Higher levels of investment yields higher revenue to SLC's

b. The participation constraint.

$$p\left(\alpha\left(\delta(E(t_{C_{r=0}}))\right)\right) + (1-p)\left(\alpha\left(\delta\left(E(t_{C_{r>0}})\right)\right) - (\theta * C_r)\right) \geq reservation\ price \quad (4)$$

The expected utility of the payment transfer minus the risk investment should be at least as great as joining another alternative project.

In this study, we assume that NDA and SLC's have a risk neutral behavior.

However, in many real scenarios, it has been observed that SLC's are risk averse with a strictly concave utility function. Equation 5. This is due to NDA being less sensitive to risk and SLC's

Table 1. Site licensed companies' payoff matrix.

Actions	Maintain levels of risk $C_r = 0$	Reduce risk to acceptable levels $C_r > 0$
Maintain levels of risk $C_r = 0$	$\pi_1 = \alpha(\delta(E(t_{C_r} = 0))$ $\pi_2 = (1-\alpha)(\delta(E(t_{C_r=0})))$	$\pi_1 = \alpha(\delta(E(t_{C_r>0})))$ $\pi_2 = (1-\alpha)(\delta(E(t_{C_r>0}) - (\theta * C_{r>0})))$
Reduce levels risk $C_r > 0$	$\pi_1 = \alpha(\delta(E(t_{C_r>0}) - (\theta * C_{r>0})))$ $\pi_2 = (1-\alpha)(\delta(E(t_{C_r>0})))$	$\pi_1 = \alpha(\delta(E(t_{C_r>0}) - (\theta * C_{r>0})))$ $\pi_2 = (1-\alpha)(\delta(E(t_{C_r>0}) - (\theta * C_{r>0})))$

having limited liability. (Laffont & Martimort 2001)

$$p\left(\alpha\left(\delta\left(\sqrt{E(t_{C_{r=0}})}\right)\right)\right) + (1-p)(\alpha(\delta(\sqrt{E(t_{C_{r>0}})}) - (\theta^* C_r))) \geq C_r \quad (5)$$

The best outcome for the companies is that both companies cooperate. Nevertheless, each player has an incentive to be a "free rider". In other words, those companies which do not contribute will still benefit from the additional input of the other companies to risk reduction obtaining even a higher payoff than those companies which invested capital. And finally, if neither of the companies contributes to risk reduction will receive a payoff lower than contributing but higher than contributing if the other company does not.

The game has a unique Nash equilibrium (Maintain, Maintain) as whatever one company does, the other prefers maintain to reduce. Table 1.

As companies are rational and driven by profit maximization, it will be in their best interest to underestimate their level of risk to increase their benefit. This behavior causes uncertainty about the payoffs of the game and information asymmetry between NDA and SLC's (Neuman & Morgenstern 1944). Under these circumstances, a Bayesian game is induced where each company has some beliefs about the level of risk hold by the other companies by assigning a continuous probability distribution over the interval of the level of risk. This distribution is common knowledge. In this paper, we assume that the companies' interval type is the same for both companies (low levels of risk $\underline{\theta}$, high levels of risk $\overline{\theta}$). Each type profile induces a state of the game with different payoffs. Table 1.

Companies will choose a strategy that maximizes their expected payoff in each state of the game. The solution to this game is a Bayesian Nash Equilibrium.

Underestimating the level of risk will decrease the probability of achieving a desirable outcome. In light with this, it is necessary the implementation of an incentive mechanism by NDA to enforce companies to reveal their actual levels of risk.

3.1.4 *The principal and agent model—NDA and SLC'S*

Current practice of risk management allocates all project risks to government (NDA) being passed onto customers as a result. Thus, customers become vulnerable to the consequences of accidents and disruptions of energy services. In line with this, it is necessary the introduction of a risk sharing scheme.

3.1.5 *Tolerability of risk*

The Office for Nuclear Regulation (ONR), regulator for the civil nuclear industry in the UK, has proposed a framework of social risk tolerability which has been established as a benchmark to assess how optimal and desirable each potential outcome is.

The regulation nuclear risk is defined by the introduction of boundaries for each outcome with regards to the risk of death or serious injury (HSE 1988)

a. When risk levels are higher than 1 in 10^4 per annum to any member of the public, the outcome is regarded as intolerable and should be rejected. (HSE 1988)
b. When risk levels are lower than 1 in 10^6 per annum to any member of the public, the outcome is regarded as acceptable and no further precaution is necessary (HSE 1988)
c. When risk levels falls between 1 in 10^4 and 1 in 10^6, the outcome is regarded as tolerable and a cost-benefit analysis can be performed to evaluate if risks levels are as low as reasonable possible (ALARP) (HSE 1988).

3.1.6 *NDA's payoff*

In the principal and agent framework, the revenue of the project depends on the Site Licensed Companies' investment in risk.

$$\sum_{s_i \in s} p(S \mid C_r) * ((P * Q) - C_p + R_b - t_{C_r}) \quad (6)$$

The project revenue is the expected payoff of each possible scenario given the level of investment in risk reduction by Site Licensed Companies. Equation 6. The conditional probability distribution increases from scenario 1 to scenario 3 when high risk investments have been made whereas decreases when lower investments of risk

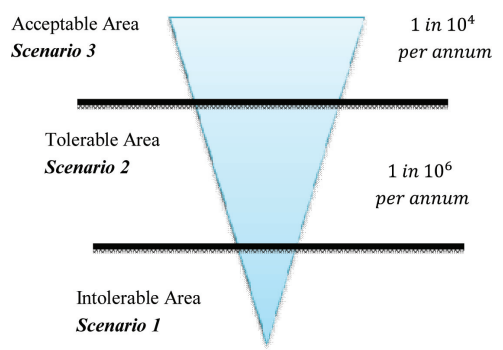


Figure 2. Acceptable, tolerable, intolerable risk scenario and criteria (HSE 1988).

Table 2. Project revenue at different scenario.

	Scenario 1 Socially intolerable level of risk Risk >1 in 10^4 per annum	Scenario 2 Socially tolerable level of risk 1 in $10^4 \geq$ Risk > 1 in 10^6 per annum	Scenario 3 Socially acceptable level of risk Risk ≤ 1 in 10^6 per annum	Expected payoff
$C_r = 0$	$p\,(S1\|C_r = 0) * ((P * Q) - C_p - t_{C_r}$	$p\,(S2\|C_r = 0) * ((P * Q) - C_p + R_b - t_{C_r})$	$p\,(S3\|C_r = 0) * ((P * Q) - C_p + R_b - t_{C_r})$	$\sum_{S_i \in S} p(S\|C_r = 0) * ((P * Q) - C_p + R_b - t_{C_r})$
$C_r > 0$	$p\,(S1\|C_r > 0) * ((P * Q) - C_p - t_{C_r}))$	$p\,(S2\|C_r > 0) * ((P * Q) - C_p + R_b - t_{C_r}))$	$p\,(S3\|C_r > 0) * ((P * Q) - C_p + R_b - t_{C_r}))$	$\sum_{S_i \in S} p(S\|C_r > 0) * ((P * Q) - C_p + R_b - t_{C_r})$

Table 3. Project revenue at different scenarios.

	NDA's revenue	Risk cost sharing and payment transfer
Scenario 1	$((P * Q) - C_p - t_{C_r}) - \sum_{S_i \in S} p(S\|h) * u(S)$	$((P * Q) - C_p - t_{C_r}) - \sum_{S_i \in S} p(S\|h) * u(S) + \pi_i$
Scenario 2	$((P * Q) - C_p - t_{C_r} + R_b) - \sum_{S_i \in S} p(S\|h) * u(S)$	$((P * Q) - C_p - t_{C_r} + R_b) - \sum_{S_i \in S} p(S\|h) * u(S) + \pi_i$
Scenario 3	$((P * Q) - C_p - t_{C_r} + R_b) - \sum_{S_i \in S} p(S\|h) * u(S)$	$((P * Q) - C_p - t_{C_r} + R_b) - \sum_{S_i \in S} p(S\|h) * u(S) + \pi_i$

have been realized. R_b is the economic benefit of improving the environmental and social performance of the project through risk reduction and t_{C_r} is the monetary transfer to SLC's. Table 2. Cost and benefit analysis needs to be perform to convert non-marketable environmental and social benefits into monetary values.

The NDA designs a contract with a variable share of the production depending on the outcome realized. The Site Licensed Companies will decide whether to accept NDA's offer based on the expected payment and the cost associated with performing that action.

$$\left((P * Q) - C_p + R_b - t_{C_r}\right) - \sum_{s_i \in s} p(S \mid h) * u(S) + \pi_i \quad (7)$$

The risk sharing incentive mechanism takes the form of the utility function in equation 7.

If the payoff of the scenario realised under a level of risk reduction is lower (negative) than the expected payoff an equivalent payment transfer will be discounted from the SLC's payoff and transferred to NDA. If, on the contrary, the payoff of the scenario realised under a level of risk reduction is higher a payment is added to SLC's expected payoff.

3.1.7 *Analysis of the principal and agent model*

The contract between NDA and SLC's consists of NDA offering a fixed shared of the production realized. Such a sharing rule should satisfy the participation constraint and be at least as great as the reservation price. However, this payment does not guarantee the effective management of risk by SLC's.

In order to overcome the moral hazard problem with respect to the investment in risk reduction made by SLC's, an incentive mechanism is designed to reduce the degree of information asymmetry in the form of profit sharing scheme. If the revenue of the scenario realized is less than the expected revenue at a given risk investment, SLC's will make an equivalent payment to NDA minus her own share of the expected utility. If the revenue of the scenario realized is higher than the expected revenue at a given risk investment, SLC's will receive an equivalent payment by NDA. As principal and agents have different goals, the non-observability of the agent's action may prevent an efficient resolution of the conflict of interest. Incentive schemes that satisfies incentive constraint and participation constraint, restores efficiency by inducing a higher level of risk investment (Shavell 1979).

4 CONCLUSION

We have built a model of principal—agent theory on the assumption that the NDA and Site Licensed Companies are risk neutral. It has been shown that under this setting, the cost of risk related when an adverse social and environmental outcome is realized, is fully borne by the SLC's. The optimal investment in risk reduction maximizes the payoff of the NDA and SLC's preventing inefficiency associated with asymmetric information.

We also state the necessity of internalizing externalities in risk sharing mechanisms by allocating a monetary value to benefits associated with

an improvement of social and environmental performance through a cost and benefit analysis.

The authors have identified some limitations in the game. For simplicity, it has been assumed that the two players in the game are risk neutral and that the payoffs of the SLC's includes revenue from electricity generation. Further study will be focused on refining the game with more than two risk averse companies and the introduction of a cost and benefit analysis in each project risk scenario to investigate payment transfers when electricity revenue cannot be distributed.

REFERENCES

Auman, R., 1987. Game theory. In J. Eatwell, M. Milgate, & P. Newman (eds), *The New Palgrave*. London: MacMillan Press.

Fang, C., Marle, F., Zio, E. & Bocquet, J.C., 2012. Network theory based analysis of risk interactions in large engineering projects. *Reliability Engineering and System Safety* 106(1–10).

HSE, 1988. HSE (Health and Safety Executive). *The tolerability of risk form nuclear power stations*. Available from www.hse.gov.uk/nucleartolerability.pdf. Accessed 12/01/2014.

HSE, 2001. HSE (Health and Safety Executive). *Reducing risk, protecting; HSE's decision making process*. Available from www.hse.gov.uk. Accessed 14/01/2014.

Japan Nuclear Technology Institute, 2001. Examination Committee on Accident at Fukushima Daiichi Nuclear.

Laffont, J.J. & Martimort, D., 2001. *The theory of incentives; the principal and agent model*. Princeton: Princeton University Press.

NDA, 2010. NDA (Nuclear Decommissioning Authority). *Geological disposal facility; an* overview *of the generic disposal system safety case*. Available from www.nda.gov.uk. Accessed 10/12/2013.

Neuman, V. & Morgenstern, O., 1944. *Theory of games and economic behaviour.* Princeton: Princeton University Press.

Shavell, S., 1979. Risk sharing and incentives in the principal and agent relationship. *The Bell Journal of Economics* 10(1): 55–73.

Whitford, A.B., 2002. Trust and incentives in principal agent negotiations; the insurance/incentive trade off. *Journal of Theoretical Politics,* 14(2): 231–267.

World Nuclear Association, 2014. *Energy and environment* http://www.world-nuclear.org/info/Energy-and-Environment/Environment-and-Health-in-Electricity-Generation/Accessed 14/01/2014.

Zhao, R., Neighbour, G., Han, J., Mcguire, M. & Deutz, P., 2012. Using game theory to describe strategy selection for environmental risk and carbon emissions reduction in the green supply chain. *Journal of Loss Prevention in the Process Industries,* 25(6): 927–936.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimization of the drinking water coagulation and filtration system as a result of reliability analysis and Life Cycle Costing

J. Szymik-Gralewska & I. Zimoch
Institute of Water and Sewage Engineering, Silesian University of Technology, Gliwice, Poland

ABSTRACT: Application of reliability theory allows an evaluation of technical and technological operation of all technical systems including water provision systems. Many other industrial branches like transport or energetics expanded the analysis on existing systems by including costs factors. Authors of this paper propose to implement this approach and develop new model of combined reliability and economic theory dedicated for water systems. Proposed model would include determination of reliability factor and economical part would be represented by Life Cycle Costing which allows to establish all incoming and outgoing of cash for each element and structure.

In this paper, basing on real exploitation data (collected 2005–2012) authors presented an innovation approach of application of reliability and Life Cycle Cost theories.

1 INTRODUCTION

In many scientific articles and presentations the authors present results of reliability analyses undertaken for various types of technical installations, devices and equipment (Möller & Hansson 2008, Zio 2009, Tchorzewska—Cieslak 2008). For a number of decades the reliability theory has been widely applied for drinking water systems and with the development of this field of knowledge today's operators of water systems are able to optimize their technical inspection programmes without the risk of any reduction in the level of reliability. The operator is also able to identify objects/subsystem with high performance risks and/or compare reliability of different devices & systems.

The reliability of a device is not the only factor taken into consideration when the operator plans to buy or build a new installation or system. The capital and upkeep costs also plays a major role in the process. The operator also has to consider the cost and reliability when deciding on the future usage of already operating devices.

After analysis of accounting papers it can be noticed that one of the cost accounting concepts—product Life Cycle Costing (LCC) is particularly applicable in cost management (Sierpinska & Niedbala 2003, Sobczyk 1997). The basic of LCC is to establish future costs, based on the adopted model. Polish norm P*N-EN 60300-3-3* defines LCC as "*the total cost incurred during the life cycle of the product*."

Researchers have determined that the Product Life Cycle Costing can be applied for technical systems such as the transport, power engineering etc. (Aggarwal 1977, Asiedu & Gu 1998, Barringer & Weber 1996, Nizinski & Zoltowski 2002, Li Du, Wang & Huang H. 2010, Selech & Kurczewski 2012).

For the last 20 years researchers have been applying Life Cycle Costing to optimize the operation of pumping units (Jedral 2007). The Hydraulic Institute, and Europump, created a program to allow for efficient energy management based on LCC analysis. Costing analysis requires a combination of economic and technical approaches when considering the projected operating time. The main aim of the research on pumps is to find an optimal system with low energy consumption. The analysis proved that the design process gives the greatest opportunity to optimize the total value of LCC; even though that the higher costs usually occur in the final phases of a pump's life.

Authors of this paper propose to implement the LCC methodology to analyze every device/object of a Drinking Water Treatment Plant (DWTP) (Zimoch & Szymik-Gralewska 2013, 2014).

This approach will allow a full economic efficiency analysis which is especially important when the Operator has to plan future utilization or modernization of any devices.

The authors decided use the approach to combined reliability and economic research based on the existing coagulation and filtration system at one of the largest DWTP in Poland. The coagulation and filtration system includes the following processes; rapid water and coagulant mixing, slow

mixing (Flocculation), sedimentation in Sedimentation Tanks and filtration by Sand Filters.

2 AIM AND SCOPE OF THE RESEARCH

The purpose of this study is to evaluate the existing coagulation and filtration system and to propose future optimization. In this paper "optimized utilization" means usage of a system which can be described with reliability factors higher than required and which also generate associated lower operational costs.

The scope of research includes the calculation of basic reliability factors, recognition of all operational and capital costs and the application of a new index—"indicator of operational readiness" (R), describing the probability of economic readiness of operation.

All of these factors are based on real data i.e. all included data related to any technical events that influence the reliability factors were provided by the operator. Furthermore all cash flows related to the operation of the system were investigated and taken into consideration.

3 METHODOLOGY

3.1 *Reliability model*

During the research the authors identified all operational events which occurred between 01 January 2005 and 30 June 2012. In case of the Sedimentation Tank's rapid and slow mixing subsystems the most common was the failures of the mixers. For the actual Sedimentation Tanks the cleaning of the tanks was only event which influences the ability to operate a Tank. In the case of the Filters some failures took place but the main factor which determines the reliability factor is the backwash procedure. Due account was taken of the time required for backwashing and rearranging the sand beds. During the backwashing the Filter is not able to treat the water, however this results not from a failure but from normal technological/operational activities.

As mentioned above reliability theory has been used in the drinking water sector for a number of years (Wieczysty & others 2001). According to common used formulas (Wieczysty & others 2001, Zimoch & Szymik-Gralewska 2014), and based on two-parametric methods and using operational data, the following indicators for each object (Mixing Chamber, Sedimentation Tank, Filter) were calculated:

- T_p—average operating time between failures—hr
- T_o—average renewal time—hr
- μ—renewal intensity—1/hr
- λ—damage intensity—1/hr
- f—frequency of damage—1/hr
- "K"—readiness index—dimensionless.

In using reliability theory the authors divided the complete system into groups based on their technological role. Taking into account the connections between technical elements all possible reliability structures (parallel or serial) were found. In order to fully describe all parallel structures, basing on actual water production, the authors of this paper calculated reliability characteristic "n of M" where "n" represent the number of operating objects and "M" is represents the number of all existing objects of each type. The reliability indicators (T_p, T_o, μ, λ, f, K) for each structure were calculated, however due to the limited form of this article only values of T_p, T_o, "K" are presented.

For this research, indicator "K" plays a major role in the evaluation of an object/structures. The definition of "K" means that it describes the possibility of future correct operation basing on past events. "Correct operation" is understood as the production of water with the required quality and volume at any time.

3.1.1 *Required reliability level*

To allow the estimation of the operation of each structure, the associated "K" indicator will be calculated and compared to a required value. Based on research conducted on the Polish water supply systems for over 30 years, suitable reliability standards were established (Wieczysty 2001). Depending on the size of the supplied city relevant values of "K" were described. In the case of the Drinking Water Plant considered by the authors the number of water consumer is higher than 500 000 people, therefore the required "K" indicator for whole Water Supply System (WSS) equates to 0,9827329 (Wieczysty 2001).

Taking into account all parallel and serial connections between subsystems and groups of elements, each required value was established (Wieczysty 2001, Zimoch & Szymik-Gralewska 2014). The authors assumed in parallel the reliability of the water production (DWTP) subsystem and the distribution (water pipe network) subsystem.

During the calculations each of the technological processes were divided into groups (Fig. 1):

1. I step of water purification includes initial ozonation, coagulation, filtration (serial structures),
2. I step of water purification is carried out in two technological lines (parallel structure),
3. Coagulation involves mixing (coagulant with water) and flocculation (serial structures),
4. Coagulation and sedimentation are technical groups which create a serial system,

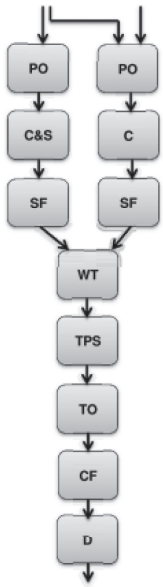


Figure 1. DWTP flow diagram.
PO—Pre-ozonation chambers; C&S—Coagulation and sedimentation; SF—Sand Filters; C—Coagulations (Pulsators); WT—Water Tank; TPS—Transitional pumping station; TO—Transitional ozonation chambers; CF—Carbon filters; D—Disinfection.

5. II step of water purification includes pumping, middle ozonation, sorption on activated carbon & disinfection (serial structure).

The conducted calculations show that the rate of K readiness for the analyzed groups should be as follows:

– for Coagulation K required = 0.9966290;
– for Sedimentation K required = 0.9966290;
– for Filtration K required = 0.9799436.

3.2 *Costing model*

To determinate which model of cost analysis is the most adequate for the DWTP system, different types of analysis were taken into consideration. As combined reliability and economic research in water supply systems is a novel approach the authors reviewed literature from other sectors (Dziaduch 2011). It was assumed that the concept of Life Cycle Costing (LCC) is most applicable. LCC analysis involves specifying the total cost incurred during the life cycle of an object and it can be described with the following equation:

$$LCC = CF_d + CF_b + CF_u + CF_{di} \quad (1)$$

where symbols stand for:
CF_d—cash flows of design phase
CF_b—cash flows of construction phase
CF_u—cash flows of usage phase
CF_{di}—cash flows of disposal phase

Mentioned costs of design, construction and disposal are relatively easy to define, however costs related to the usage phase is much more complicated. To describe all cash flows occurring in that phase Activity Based Costing (ABC) was applied (Sierpinska & Niedbala 2003). This method assigns indirect overhead costs and activity costs to the objects, facilities, systems & devices, and uses "cause—effect" relations between factors that generate costs and activities. In other words the ABC concept allows the grouping of the costs by actions i.e. causes of cost.

In the case of the water supply systems, the type of actions which cause costs are; maintenance works, replacement of failed equipment, & technological activities (filter backwashing). To find the total cost of the operational phase, costs related to materials (spare parts, water for backwashing), labour and energy was calculated.

Another aspect of Life Cycle Costing is the fact that it must allow for the change of money value over time. For this reason all cash flows must be "discounted" and the equation below shows the connection between the future and present value of money:

$$PV = \frac{FV}{(1+r)^t} \quad (2)$$

where:
PV—present value e.g. of a cash flow—PLN,
FV—future value—PLN,
r—the discount rate—dimensionless,
t—the time of the cash flow (here 30 years)—dimensionless.

According to "*Guide to Cost-Benefit Analysis of Major Projects in the context of EC Regional Policy*" by European Commission "r" factor for Poland is 0,05.

It should also be stated, that from an economic point of view, by referring to Cash Flows (CF) we mean the incoming and outgoing of cash, representing the operating activities of a water supply company (Sierpinska & Niedbala 2003). Cash flows can be divided into cash outlays e.g. for design, construction or modernization, costs generated during the operation of an object and cash income e.g. savings from lower energy consumption.

With reference to the above, it can be concluded that during the design and construction phases only cash outlays occur, while during the usage phase costs for maintenance cash outlays for moderniza-

tion and possible income can be observed. During the disposal phase costs related to the demolition, and income from selling the debris can appear. The total value of each life phase is a balance of all the cash flows, and for this reason outlay costs are given a minus signs (as these are expenses) and income is given a plus sign. It can however be seen that the majority of the considered CF has a negative sign i.e. it is an outgoing cost/money In order to facilitate the calculations in this paper, minus signs will be omitted.

Taking all of the above into consideration, the discounted balance of cash flow—Present Value of Cash Flow (PVCF) related to each life phase is presented by the following formula:

$$PVCF = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^n} \tag{3}$$

where:
PVCF—Present Value of Cash Flows—PLN,
CF_t—the net cash flow at time t—PLN,
N—following periods—years.

3.2.1 *Identified costs*
A significant part of the research was to identify and specify all Cash Flows related to each group of elements. Basing on water company records, documentation of analogical DWTP and the author's calculations, the incoming and outgoing of cash was determined. Results are shown in Tables 1–4.

3.2.1.1 *Mixing chamber*
For the Mixing Chamber the authors determined the following costs (divided into life phases):

Design phase
According to Polish legislation acts for investor's costing, it was assumed that design costs equal 5% of the construction costs. This phase included costs related to the provision of executive design, all necessary expertise surveys, land surveys and obtaining all required permits.

Construction phase
Based on cost documentation of analogical chamber built in other DTWP, construction phase was established. The authors took into consideration the value of construction and assembly works, the value of direct used materials and direct labor costs.

Usage phase
Due to fact, that the Mixing Chamber is a reinforced concrete structure which is not equipped with any machinery, concrete repair is the only associated cost. According to *Guide to cost-benefit analysis of investment projects* by the European Commission, concrete structure durability is normally 50 years. Based on the author's experience, and using data obtained from professional contractors, it was assumed that the concrete surface will require repairs once every 20 years with an average costs of 30% of construction.

Disposal phase
Normally the cost of this phase is mainly the cost of dismantling works and associated disposal.

As the Mixing Chamber is the widening of the water channel it is impossible to demolish this element. Consequently the costs related to the disposal phase equal 0.

3.2.1.2 *Flocculation chamber*
The authors have carried out an investigation of the costs of the Flocculation Chamber and the following costs have been determined:

Design phase
Similar to the Mixing Chamber, in accordance with Polish legislation it was assumed that design phase costs equal 5% of construction costs.

Construction phase
Basing on a cost estimation carried out in accordance with Polish legislation, and using average costs from the first quarter 2014, cash flows for the construction phase were established. The following particular aspect were taken under considera-

Table 1. Summary of required values of indictor K for each groups.

Type	Symbol	Elements no.	Function	Value of K indicator
Serial structure of water production and the subsystem	Wa	2	$\sqrt[2]{K_{WSS}}$	0.9827329
Serial structure of I and II step of water purification	Wb	5	$\sqrt[5]{K_{W_a}}$	0.9965225
Parallel structure of two technological lines of I step of water purification	Wc	2	$1-\sqrt{1-K_{wb}}$	0.9410295
Serial structure of technological system which build one of line of I step of water purification	Wd	3	$\sqrt[3]{K_{W_c}}$	0.9799436
Serial structure of technological groups which build technological system	We	2	$\sqrt[2]{K_{W_d}}$	0.9966290

Table 2. LCC for mixing chamber.

Phase of mixing chamber's life cycle	Cash flows (net value) PLN
Design	27 207.96
Production	544 159.16
Usage	656 082.12
Disposal	0.00
LCC	1 227 449.23

Table 3. LCC for flocculation chamber.

Phase of flocculation chamber's life cycle	Cash flows (net value) PLN
Design	35 423.00
Production	708 459.93
Usage	1 732 162.28
Disposal	10 246.94
LCC	2 486 292.14

Table 4. LCC for coagulation subsystem.

LCC of element	Cash flows (net value) PLN
Mixing chamber (2 elements)	2 454 898.47
Flocculation chamber (4 elements)	9 945 168.57
LCC	7 364 695.40

tion; direct costs associated with the purchase and installation of materials and equipment, the cost of construction and assembly/installation works, the cost of installed equipment, the cost of direct used materials and direct labor costs.

Usage phase
As stated for the Mixing Chamber, according to *Guide to cost-benefit analysis of investment projects* by the European Commission, concrete structure durability is normally 50 years. Based on the author's experience, and using data obtained from professional contractors, it was assumed that the concrete surface will require repairs once every 20 years with an average costs of 30% of construction.

To provide a correct flocculation process, Slow Mixers are installed in the chamber. According to *Guide to cost-benefit analysis of investment projects* by the European Commission equipment durability is up to 30 years. For that reason the analysis assumes Mixer replacement after 30 years.

In accordance with the ABC concept costs are being generated during technical activities. Each chamber is cleaned once a year and this action results in costs (labor, material, overheads).

The cost of possible repairs can be illustrated by an average renewal time T_o. For this study the highest T_o was taken into account.

Disposal phase
Cost of this phase is mainly associated with dismantling works and waste disposal. The Flocculation Chamber is a reinforced structure which is a part of the Coagulation Building and for this reason demolition works were not taken into consideration.

Costs related to Mixer demolition was established basing on average costs in the first quarter of 2014.

Profit from the sale of dismantled scrap metal is negligible.

3.2.1.3 *Sedimentation tank*
For the Sedimentation Tank the following costs were found:

Design phase
Similarly to the other analyzed concrete structures, the design phase costs were assumed to be 5% of the construction costs.

Construction phase
For the Sedimentation Tank, the authors carried out a cost estimate based on the average costs in the first quarter 2014. The following aspect were taken under consideration; the value of construction and assembly works, the value of direct used materials & direct labor costs.

Usage phase
The design life of the tank is assumed to be 50 years. As the tank is reinforced hydro concrete the authors assumed that the repairing of the concrete surface once every 20 years would be required and that the repairs have an average costs 30% of construction. This is based on information obtained from the operator.

In accordance with the ABC cost model cash outflows are generated during technical activities; i.e. the cleaning process which takes place once a year.

Disposal phase
Cost of this phase is mainly associated with dismantling works and waste disposal. The authors carried out a cost estimate based on average costs in the first quarter 2014, and the following aspects were taken into consideration; the value of demolition construction and dismantling works, the value of direct used materials, direct labor and the cost of debris removal & disposal.

3.2.1.4 *Sand filter*
Based on a cost estimate provided by a potential contractor for the renewal of the Sand Filters, the following costs were indicated (Zimoch & Szymik-Gralewska 2014):

Design phase
This phase included costs related to the provision of the executive design, all necessary "expertise" surveys and land surveys together with obtaining all required permits.

In contrast to the other analyzed elements, the costs related to the design phase for the Sand Filter were assumed to be real contractor's costs.

Construction phase
The costs of this phase consist of; direct costs associated with the purchase and installation of materials & equipment, the value of construction & assembly works, the value of installed machinery & equipment, the value of direct used materials, direct labor costs, fees & charges related to required permits and the costs of preparing the construction site.

Usage phase
In the life cycle of the Sand Filter the backwash time plays the major role. In the analyzed case the backwash time equals 0.25 hr, and in accordance with the ABC concept costs are being generated during this 0.25 hr period. Rising process results in the following costs; wages of employees directly involved in this process, consumed energy of the pump units (pumps provide purified water to the tower tank) & cost of used backwash water.

The cost of possible repairs can be illustrated by an average renewal time T_o. For this study the highest T_o was taken into account.

What is more, during the data analysis it was noted that on an average of once every 10 years, a Filter must be renovated, i.e. the anthracite bed must be replaced. This operation requires the emptying of the Filter Chamber, removal of the filter bed, disposal of sand and provision of new filter bed material.

For this research, it was assumed that the Sand Filter has an operational life of 30 years.

Disposal
The cost of this phase is mainly the cost of dismantling works and associated disposal. As the Filter Chambers are part of Filters Building, the authors assumed that the structure will be not demolished.

Costs occurred in this phase relate to refer to demolition works, the value of direct used materials, direct labor costs, cost of scrap metal and the cost of used sand disposal.

4 DESCRIPTION OF COAGULATION AND FILTRATION SYSTEM

The Coagulation and Filtration System is part of the DWTP which purifies surface water. The DWTP with other ten local Plants provides water to more than 3 million Silesian citizen. Its design capacity is 500 000 m^3/d and average production equals 213 800 m^3/d. The examined system is one of two parallel coagulation and filtration subsystems (Fig. 1).

During the observed time the average capacity was 37% of the design capacity (150 000 m^3/d) and it equals 55 500 m^3/d. The maximum capacity in this period was 97 700 m^3/d.

The system includes; rapid water and coagulant mixing, slow mixing (flocculation), sedimentation in Sedimentation Tanks and filtration by sand Filters (Fig. 2).

There are three parallel coagulation lines in which water is purified with a coagulant (aluminum sulfate) dosed into the three supply pipes (DN 800) serving the Coagulation Building.

Coagulant is dissolved to an appropriate concentration in 4 concrete tank each with 13.5 m^3 capacity. The coagulant solution is then transferred to tanks by membrane dosing pumps. Each coagulation line has 2 labyrinth Mixing Chambers (MC) and each reinforced concrete MC has five inclined baffles which create turbulent flow. The retention time of Mixing Chambers is 3 minutes.

After the mixing process the water divides into four Flocculation Chambers (FC). Each FC is equipped with two mixers and the capacity of one FC is 67.67 m^2. The maximum design water level in the Flocculation Chamber is 4.1 m and the minimum is 3.8 m. The retention time depends on rate of the water flow, and at the maximum fulfilment and with twelve chambers in operation, the retention time is 27 minutes and with a min fulfilment and 12 chambers in operation—it is 23 minutes.

Further water by three pipelines DN 1200 is transported to the Division Chamber and then to three horizontal post-coagulation Sedimentation Tanks (S). These are roofed reinforced concrete buildings, located below ground level. Each tank is divided into three chambers connected with overflows. The design retention time is 1 hr

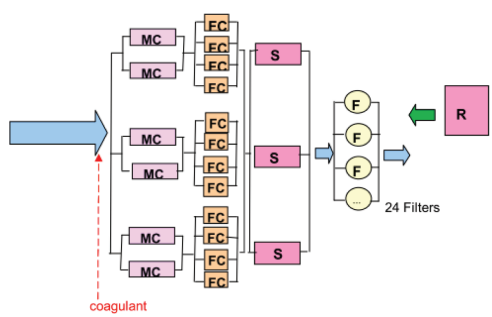


Figure 2. Coagulation and filtration flow diagram (Symbols as in text).

45 min but due to current production levels the actual retention time is a few hours. The capacity of the Sedimentation Tank equals 21 500 m^3.

The clarified water is forwarded to the Filtration Building. The filtration system consists of 24 identical reinforced concrete Filter chambers (F) filled with an anthracite bed. The filtration area equals 46 m^2 and the chamber volume is 115 m^3.

Each Filter bed is provided with a 55 cm layer of sand and a 35-centimeter support layer. The base of the Filter chamber is covered by plates with mushroom shape drainage nozzles. The Filters are backwashed gravitationally with water from the Retention Tank (R).

5 OBTAINED RESULTS

5.1 *LCC calculation*

Based on the assumptions described in point 3.2 and on formulas (1), (2), (3) the Life Cycle Costs for each element were calculated. Due to the limited form of this article only final results are presented.

It can be seen, that two Mixing Chambers are connected only to specific four Flocculation Chambers (Fig. 2). And this means that when the operator decides to stop operating one MC the second MC and related four FC cannot be operated.

For this reason elements arrangement "2MC+ 4FC" should be consider as one Coagulation Subsystem. LCC for Coagulation Subsystem is a sum of LCC for the Mixing and Flocculation Chamber (Table 4).

Regardless to which configuration of the chambers is adopted the water can be provided to any of the Sedimentation Tanks. Therefore the Sedimentation Tanks can be consider as a separate Sedimentation Subsystem.

Similarly the Sedimentation Filtration is a separate subsystem and the following LCC was calculated.

Table 5. LCC for sedimentation tank.

Phase of sedimentation tank's life cycle	Cash flows (net value) PLN
Design	224 759.04
Production	4 495 180.89
Usage	5 439 724.15
Disposal	10 008 017.82
LCC	20 167 681.90

Table 6. LCC for filter.

Phase of Filter's life cycle	Cash flows (net value) PLN
Design	300 000.00
Production	1 277 000.00
Usage	2 769 946.46
Disposal	19 898.46
LCC	4 366 844.92

5.2 *Reliability index calculation*

5.2.1 *Objects*

Based on the assumption of reliability theory described in point 3.1 on this paper, the reliability indicators were established as in Table 7.

At the end of study period only 18 Filters were in operation. The remaining 6 were out of operation due to drainage plate failure.

Table 7. Reliability indicators for elements.

Object	Tp hr	To hr	K dimensionless
Mixing chamber	32 844.00	0.00	1.0000000
Flocc. chamber no. 1 with mixers	222.60	17.15	0.9284552
Flocc. chamber no. 2 with mixers	438.43	5.78	0.9869821
Flocc. chamber no. 3 with mixers	5 051.76	4.69	0.9990717
Sedimentation tank no. 1	5 460.08	15.18	0.9972272
Sedimentation tank no. 2	3 844.65	20.56	0.9946801
Sedimentation tank no. 3	4 093.63	12.67	0.9969153
Filter no. 1	31.64	0.25	0.9921599
Filter no. 2	31.58	15.25	0.6744530
Filter no. 3	31.64	0.25	0.9921599
Filter no. 5	31.64	0.25	0.9921599
Filter no. 8	31.64	0.25	0.9921599
Filter no. 9	31.64	0.25	0.9921599
Filter no. 10	31.64	0.25	0.9921599
Filter no. 11	26.87	9.05	0.7481501
Filter no. 12	31.64	0.25	0.9921599
Filter no. 13	31.64	0.25	0.9921599
Filter no. 14	31.60	18.03	0.6367376
Filter no. 15	31.64	0.25	0.9921599
Filter no. 16	31.64	0.25	0.9921599
Filter no. 17	31.61	18.32	0.6331126
Filter no. 19	31.64	0.25	0.9921599
Filter no. 21	31.64	0.25	0.9921599
Filter no. 22	31.62	9.75	0.7644022
Filter no. 23	31.64	0.25	0.9921599
Filter no. 24	31.64	0.25	0.9921599

Filters no. 4, 6, 7, 18, 20 were unexploited throughout the study period and the drainage plate to Filter no. 22 was damaged during the course of the study.

It can be seen that T_o for the Mixing Chamber equals 0,00. This is a result of the fact that from 2005–2012 maintenance works were executed. As the chamber has no mechanical equipment no failure was recorded.

In case of the Sedimentation Tanks a very long average renewal time (T_o) is observed as the water production rate is considerably lower than the design value (two Tanks can provide the max water capacity) and consequently the Operator does not endeavour to optimise the cleaning period.

Calculations for the Flocculation Chamber with Mixers were calculated based of the Flocculation Chamber (structure) and the associated four mixers being considered as a serial structure. In Chamber no 1, Mixers no 1, 2, 11 & 12 are in operation, in Chamber no 2 there are Mixers no 3, 4, 9 & 10 and in Chamber nr 3—Mixers no 5, 6, 7 & 8. Reliability indicators for each Flocculation element are given in the Table 8.

5.2.2 *Structures*

In order to provide full reliability evaluation, indicators for all technical structures were calculated. Each subsystem being separately analysed.

In this study all subsystems were analysed on the basis of the average water production. It was established that to provide the optimal filtration velocity (6.5 m/h), 8 Filters must be in operation at any one time. For this reason the analyses for the Filtration Subsystem begin with 8 Filters.

The analysis shows that 8 of 18, 9 of 18, 10 of 11, 12 of 18 and 13 of 18 are described with very long average operating times between failures and high K index. This is a result of the fact that the Filters are very rarely subject failure and what is even more important these structures have high reserve i.e. only few of elements in subsystem must be working.

Table 8. Reliability indicators for flocculation elements.

Object	Tp hr	To hr	K dimensionless
Structure of flocculation chamber no. 1	5 465.75	9.00	0.9983561
Structure of flocculation chamber no. 2	9 376.29	9.00	0.9990411
Structure of flocculation chamber no. 3	13 130.40	9.00	0.9993150
Mixer no. 1	896.17	42.84	0.9543770
Mixer no. 2	946.38	5.71	0.9940069
Mixer no. 3	946.38	5.71	0.9940069
Mixer no. 4	946.38	5.71	0.9940069
Mixer no. 5	32 843.00	2.00	0.9999391
Mixer no. 6	32 843.00	2.00	0.9999391
Mixer no. 7	32 843.00	2.00	0.9999391
Mixer no. 8	32 843.00	2.00	0.9999391
Mixer no. 9	32 843.00	2.00	0.9999391
Mixer no. 10	32 843.00	2.00	0.9999391
Mixer no. 11	925.66	12.93	0.9862266
Mixer no. 12	946.38	5.71	0.9940069

Table 9. Indicators for coagulation subsystem.

Type of structure	Tp hr	To hr	K dimensionless
1 of 3	2 410 873.17	2.08	0.9999991
2 of 3	4 114.91	4.15	0.9989919
3 of 3	141.59	13.07	0.9155180

Table 10. Indicators for sedimentation subsystem.

Type of structure	Tp hr	To hr	K dimensionless
1 of 3	113 606 197.12	5.17	1.0000000
2 of 3	199 495.22	7.91	0.9999604
3 of 3	1 454.48	16.38	0.9888623

Table 11. Indicators for filtration subsystem.

Type of structure	Tp hr	To hr	K dimensionless
8 of 18	504 221 653 219.18	0.03	1.0000000
9 of 18	5 164 410 496.92	0.04	1.0000000
10 of 18	70 647 337.54	0.05	1.0000000
11 of 18	1 318 118.90	0.06	1.0000000
12 of 18	34 851.84	0.07	0.9999979
13 of 18	1 395.58	0.10	0.9999262
14 of 18	95.07	0.16	0.9983213
15 of 18	13.19	0.30	0.9777574
16 of 18	3.05	0.48	0.8633629
17 of 18	0.87	0.68	0.5611364
18 of 18	1.74	7.81	0.1821904

6 COMBINED TECHNICAL RELIABILITY AND ECONOMICAL ANALYSIS

An analysis of the obtained results of reliability calculations indicates that for the required values of "K" indicator the following minimum structures satisfy the condition: $K_n > K$ required.

Table 12. Required K values for each subsystem.

Subsystem	K required	Required structure	Value of K for required structure
Coagulation	0.9966290	2 of 3	0.9989919
Sedimentation	0.9966290	2 of 3	0.9999604
Filtration	0.9799436	14 of 18	0.9983213

Table 13. Values of operational readiness rate (R),

Subsystem	R
Coagulation	0.5005041
Sedimentation	0.5000198
Filtration	0.5723895

During the observation period the maximum capacity of the System was 97 700 m^3/d. Taking into consideration the current trend of decreasing water consumption and the fact that the probability of a sudden increase is extremely small, it was assumed that the maximum required capacity of the system be defined as 97 700 m^3/d rather than the design value (150 000 m^3/d).

As previously stated in this paper all subsystems were analysed regarding the average and maximum observed water production.

Currently literature does not define the index linking both reliability and cost factors. The authors of this study propose to introduce the indicator of operational readiness (R), describing the probability of economic readiness of operation (Zimoch & Szymik-Gralewska 2014).

$$R = \frac{K_0 \cdot CF_0}{K_m \cdot CF_m} \tag{4}$$

where:

K_o—probability of proper operation of structure "x of y" where "x" is the number of elements necessary for average water production rate and "y" is the number of all elements necessary for max production rate,

CF_o—total cash flow related to the number of elements necessary for average water production rate,

K_m—probability of proper operation of the structure "x of y" where "x" is the number of elements necessary for max water production rate and "y" is a number of all existing elements necessary for max production rate,

CF_m—total cash flow related to the number of elements necessary for the maximum water production rate,

7 SUMMARY AND CONCLUSIONS

Most of Polish Water Companies face problems related to necessity for optimizing plants. The reason for this situation is the fact that the water demand tends to be less than the design capacity of almost all the DWTPs. Based on professional literature and minding of current trends in water management, problem of effective water supply system optimization was identified. This paper is a continuation of authors study on a new approach to reliability and LCC analysis for DWTPs and can be used as a support tool in the Operator's decision making process.

In this study a new index—operational readiness rate (R) was introduced. The index can be assumed as a first step of optimization process. The closer the value of the indicator is to 1.00, then the higher is the level of system utilization. It can be seen that all analyzed subsystems are not fully utilized. Therefore another steps of optimizing calculation should be conducted.

ACKNOWLEDGEMENT

The paper presented has been realized in frame of the research project co-financed by the European Union from the European Regional Development Fund, Sub-measure 1.3.1. "Development Projects"; project title: "IT system supporting the optimization and planning of production and distribution of water intended for human consumption in the sub-region of the central and western province of Silesia"; project ref no POIG.01.03.01-14-034/12.

Authors would like to thank dr. Ewa Szypulska and Mr. Gary Simpson for all valuable comments.

REFERENCES

Aggarwal K.K. 1977 Minimum Cost Systems with Specified Reliability *IEEE transactions on reliability* Vol.R-26.

Asiedu Y., Gu P. 1998: Product life cycle cost analysis: state of the art review. *International Journal of Production Research,* vol. 36, no. 4, pp. 883–908.

Barringer H.P., Weber D.P.: 1996 Life Cycle Cost Tutorial. Fifth *International Conference on Process Plant Realiability*, 2–4, Houston, Texas.

Dziaduch I. 2011. The life cycle cost analysis (LCCA) of technical object in dependability aspect, *Logistyka,* 2/2011.

European Commission *Guide to Cost-Benefit Analysis of Major Projects in the context of EC Regional Policy*.

European Commission *Guide to cost-benefit analysis of investment projects*.

Guikema S. Pate-Cornell 2002 Component choice for managing risk in engineered systems with generalized risk/cost functions, *Reliability Engineering and System Safety* pp. 227–238.

Jędral W. 2007 *Efektywność energetyczna pomp i instalacji pompowych* (*The energy efficiency of pumps and pump systems*), Krajowa Agencja poszanowania Energii S.A. (National Agency for Energy Conservation), Warsaw.

Kaufman R. 1970 Life cycle costing: a decision-making tool for capital equipment acquisition. *Cost and Management March/April 1970.*

Li Du L., Wang Z., Huang H. 2010 Cost-type function analysis in dynamic design under uncertainty, *Maintenance and Reliability no. 2/2010.*

Möller N. & Hansson S.O. 2008. Principles of engineering safety: Risk and uncertainty reduction. *Reliability Engineering and System Safety 93* pp. 776–783.

Niziński S. & Żółtowski B. 2002 *Zarządzanie eksploatacją obiektów technicznych za pomocą rachunku kosztów (Managing the operation of technical facilities using cost accounting)* Wydawnictwo Makar, Olsztyn—Bydgoszcz.

Polish legislation acts 2004 *Rozporządzenie Ministra Infrastruktury z dnia 18 maja 2004 r. w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Regulation of the Minister of Infrastructure of 18 May 2004 on determining the methods and bases for preparation of cost calculation, calculation of the planned costs of design and planned costs of the works specified in the functional and operational programme).*

Selech J. & Kurczewski P. 2012 Life Cycle Costing (LCC) jako nowoczesny model zarządzania kosztami cyklu życia na przykładzie obiektów technicznych (Life Cycle Costing (LCC) known as modern model of life cycle cost management based on example of technical object), *Problemy Eksploatacji tom nr 1* 2012 str. 99-108 Wydawnictwo Naukowe Instytutu Technologii Eksploatacji—Państwowego Instytutu Badawczego.

Sierpinska M. & Niedbala B. 2003. *Controlling operacyjny w przedsiebiorstwie, centra odpowiedzialnosci w teorii i praktyce, (Operational Controlling in the enterprise, responsibility centers in theory and practice)* PWN, Warsaw.

Sobczyk M. 1997 *Matematyka finansowa (Financial Mathematics*), Agencja wydawnicza Placet (Placet publishing agency), Warsaw.

Tchórzewska—Cieślak B. 2008, *Niezawodność i bezpieczeństwo systemów komunalnych na przykładzie systemu zaopatrzenia w wodę* (*Reliability and safety* of *municipal systems on the example of the water supply system)*, published by Oficyna Wydawnicza Politechniki Rzeszowskiej.

Ulatowski W. 2007 Analiza kosztów urządzeń infrastruktury tramwajowej w pełnym cyklu życia (Analysis of life cycle costs of teh tram infrastructure devices), *TTS Technika Transportu Szynowego R. 13, nr 9*, Instytut Naukowo-Wydawniczy "TTS" Sp. z o.o.

Wieczysty A. & others 2001. *Methods for assessing and improving the reliability of the municipal water supply systems,* PAN Monographs, vol. 2, Cracow.

Woodward D. 1997. Life cycle costing—theory, information acquisition and application. *International Journal of Project Management*, Vol. 15, No. 6, pp. 335–344.

Zimoch I. 2011. *Integrated method reliability and safety analysis of the water supply systems operation.* Monographs, Wydawnictwo Politechniki Śląskiej (Published by Silesian University of Technology).

Zimoch I., Szymik-Gralewska J. 2013. Application of reliability analysis in optimization of water treatment system. *Proc. of the 7th National Scientific—Technical Conference "Current issues in treatment and distribution of water"*: Szczyrk.

Zimoch I., Szymik-Gralewska J. 2014 (in press). Risk assessment methods of water supply system in terms of reliability and operation cost, Conference Urban Water 2014, 27th to 29th May 2014, Algarve, Portugal.

Zio A. 2009 Reliability engineering: Old problems and new challenges, Reliability Engineering and System Safety 94 125–141.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Methods of visualizing the risk of lack of water supply

I. Piegdoń & B. Tchórzewska-Cieślak
Department of Water Supply and Sewage Systems, Rzeszow University of Technology, Rzeszow, Poland

ABSTRACT: In the era of informatization databases and information systems are an essential source of risk analysis and risk assessment of collective water supply systems. The functioning of the water distribution system is associated with the risk of occurrence of undesirable events. The result of these events may be deterioration of the water quality parameters, reduction of water pressure in the water network or total lack of water.

The aim of the study is to present the application example of applying Geographical Information Systems (GIS), database and selected information systems helpful in mapping the risk of lack of water supply to the consumers. The study also presents the idea of the European Directive INSPIRE, which is a key in risk analyzes in the water supply.

1 INTRODUCTION

The functioning of every Water Distribution Subsystem (WDS) is related to the risk which is associated with the possibility of the occurrence of undesirable events, which may result in deterioration of water quality, lack of water, as well as reduction of water pressure in the water network. Risk associated with the operation of the entire WDS should be continuously monitored to ensure adequate safety level for water consumers. In the environmental engineering a basic definition of risk is applied. That definition presents risk as a multiplication of the probability of undesirable events occurrence, losses as a consequences of these undesirable events and the degree of system vulnerability to undesirable events (Kaplan & Garrick 1981, Rak 2009, Tchórzewska-Cieślak 2011):

$$r = P \cdot C \cdot V \tag{1}$$

where:
P—a measure of probability (frequency) of undesirable events occurrence in WDS, which can be directly felt by water consumers,
C—determines the size of losses associated with undesirable events occurrence (e.g. purchase of bottled water, medical costs after consuming poor quality water, immeasurable losses, such as loss of life or health),
V—the degree of vulnerability to undesirable events.

Risk in every technical systems belonging to the critical infrastructures is inseparably associated with risk management (Babiarz 2006, Kołowrocki 2001, Kotowski & Kaźmierczak 2013, Mays 1989, Rak 2009, Tchórzewska-Cieślak 2011).

Risk management can be defined as socio-economic decision-making process (Rak 2009). It is obvious that it is impossible to eliminate risk, but system operator can take any action to minimize it. Decision-making is the responsibility of the operator of the WDS. Therefore, to avoid the negative consequences of making wrong decisions regarding WDS operation, the operator must learn how to assess risk, inform others of its size, and know what action must be taken in critical situations (Zio 2006).

Risk analysis is a research method relying on decomposing all components creating a problem or issue and analyzing that problem. One of the methods using to minimize risk of undesirable events occurrence is the visualization of all the components that can cause risk growth using the risk maps. In this case the map of risk is understood as a graphic presentation of the areas directly exposed to the negative consequences of failures in WDS. To create the risk maps it is necessary to have a set of operational data about system, as well as detailed statistical data relating to the emergency situations. These data should also allow to identify the analyzed object, undesirable events and to make a cause-effect analysis. The complete and detailed data determine the correct risk analysis and assessment, and thus the process of risk management. Very often the problem is in information interpretation, lack of continuous recording and processing of operational data. There are many sources of operational data.

An important element in risk analysis and assessment is the possibility to use different types

of software that have significant impact on a degree of detailed calculations (Piegdoń et al. 2014, Tchórzewska-Cieślak et al. 2013).

Geographic information systems describes the spatial characteristics of the environment, underground infrastructure which is part of the critical infrastructure. GIS models and simulates the processes of the based on databases. Is developed to collect, process and display spatial data. Is applicable in many areas of life. It is used in water and sewage networks management of by water companies, in struggling with the elements of nature or in spatial, urban planning (Bahr & Vogtle 1999, Baz et al. 2009, Bernhardsen 1992, Ghinoi & Chung 2005, Rao et al. 2000, Sholten & Stillwell 1990, Williams & Shah 2000, Zeng et al. 2007).

The study presents legal regulations relating to the implementation of the directive Infrastructure for Spatial Information in the European Community (INSPIRE) (Directive 2007/2/EC 2007).

The aim of the study is to present the possibility of applying GIS and database in the process of analyzing and assessing undesirable events which may occur in WDS, and to show how determine the areas vulnerable to the negative consequences of these events.

In the example application the risk of lack of water supply using the matrix method, due to the possibility of the occurrence of the accident on the distribution network was determined. The one asset of risk—lack of water—was considered with respect to a water consumer as the main water recipient.

2 THE INSPIRE DIRECTIVE IN THE CONTEXT OF RISK ANALYSIS

In order to identify threats that accompany the WDS operation and which have a negative impact on water consumers, it has become necessary to base on the largest possible amount of data. Currently, the most popular method of data collecting became GIS applications (Filipkowski et al. 2006, Gromiec 2006, Kwietniewski 2008, Piegdoń & Tchórzewska-Cieślak 2013, Tchórzewska-Cieślak et al. 2013, Zimoch & Paciej 2013). These systems allow to collect different geo-information about topographic objects, undesirable events and processes that have significant influence on every critical infrastructure.

However, in many cases making a thorough risk analysis is not possible due to lack of complete operational database. The main reason is that searching for interesting data is a time-consuming and costly operation. In addition, there is always a need to check whether the data are current. The European Union came out to meet all these requirements establishing on March 14th 2007 the INSPIRE Directive. The INSPIRE directive aims to create the European Union (EU) spatial data infrastructure. This will enable the sharing of environmental spatial information among public sector organizations and better facilitate public access to spatial information across Europe. A European Spatial Data Infrastructure will assist in policy-making across boundaries. Therefore the spatial information considered under the directive is extensive and includes a great variety of topical and technical themes.

The main purpose of the Directive is to support Member States in the field of environmental protection and to support the activities having direct impact on environment condition. These activities are related to (inspire.ec.europa.eu):

- collecting data and keeping them where they can be maintained most effectively,
- possibility to combine seamless spatial information from different sources across Europe and sharing it with many users,
- geographic information needed for good governance at all levels should be readily and transparently available,
- easiness in finding what geographic information is available, how it can be used to meet a particular need and under which conditions it can be acquired and used.

For example, water supply companies can post information about failures of water pipes, planned renovations of the network, as well as water quality, or specific parameter values (physico-chemical, bacteriological and organoleptic) on the geoportal. Such communication between supplier and water consumer will affect their relationship as well as increase consumer trust.

3 TYPES AND SOURCES OF DATA IN RISK ANALYSIS

The availability of relevant data is the basis for reliable results obtained from the analysis of risk. These data are needed to describe the system, to identify and assess the undesirable events and mainly to minimize the potential risk. To make an analysis it is necessary to base on data with varying degrees of accuracy. The variety of databases can be considered in three categories (Hokstad et al. 2007, Hokstad et al. 2009)

- general data—data from external sources. The data may relate to the efficiency of Water Treatment Plant (WTP).
- data about system—data characterize the WDS. The data relate to the number of water consumers and local factors affecting the general knowledge about the failure of water pipes.

Table 1. Data in risk analysis.

Type of data	Data source
General data	
– data about effect of various doses of pollutants on human health.	– websites, – website of the World Health Organization (WHO), – websites of State Sanitary Inspectorates,
Data about system	
– geographic data, – possible risks in the catchment area, in water sources and water distribution subsystem, – GIS data regarding the dangers, – data about environment, – data about technology of water treatment, – data about water pipes condition, – number of water consumers, – water consumption during the day.	– maps, – water supply company, – technical drawings, – documented data, – water network exploitation, – employees knowledge, – current controls.
Event data	
– data about failures of all the subsystems forming an integral collective water supply system, – erroneous data arising from human fault, – events that had an impact on water pollution, – operational data relating to preventive and corrective measures.	– database available in water supply company about failures of water network, – active and constant exploitation of water network, – reports about undesirable events that happened in the past, – employees knowledge.

– event data—recorded and documented data about the undesirable events, system failures that occurred in the past.

Table 1 presents the data and their sources for the purposes of risk analysis.

Properly selected and prepared database can be used for many exploitation operations, such as preparing preventive schedule, renovation of critical infrastructure networks, the location of leakages from the network, in water resources management and many other tasks related to the functioning and exploitation of network systems (Applying GIS … 2000, Geographic … 1992, Glasbrook 1994, Heinonen 2000, Iglesias et al. 1997, Kane & Gough 1996, Longley et al. 1999, Lyon 2003, Otero et al. 1997, Schroeiber & Grossman 1997, Wu et al. 1997).

4 RISK AS A MEASURE OF SAFETY

4.1 *Basic concepts*

Safety in water supply is defined as a state of water management that enables to cover the current and future water demand, in a technically and economically justified way, by the requirements of environmental protection (Berg et al. 2010, Ezell et al. 2000, Kołowrocki 2001, Li et al. 2009, Mays 1989, Rak 2009, Tchórzewska-Cieślak 2011, Tchórzewska-Cieślak 2011 et al. 2012). The basic and primary entity to which the water safety concept is directed is water consumer. The secondary is water supplier—water manufacturer. That is why risk can be considered as a consumer risk and supplier risk (Rak 2009, Tchórzewska-Cieślak 2011).

Water supplier risk can be associated with the functioning of the WDS. The risk map in this aspect can be realized on the basis of:

– material of water pipes, their unreliability, age (in the sense of operating time) and pipes provided for renovation.

Figure 1 shows the options of creating the risk maps with respect to water supplier.

The second aspect is to consider risk with respect to a consumer as a major recipient. In this case the maps of risk can be created based on:

– the number of inhabitants exposed to the lack of water supply due to the undesirable events,
– the number of inhabitants exposed to consume poor quality water,
– the designation of areas vulnerable to the undesirable events occurrence.

Figure 2 shows the options of creating the risk maps with respect to a water consumer.

Risk of water supplier and water consumer should be considered separately. In the application example the risk of lack of water supply due to failure of distribution pipes in relation to the consumer of water was made.

4.2 *Research methodology*

One of the methods used for risk analysis is three parametric matrix for risk assessment



Figure 1. Possibilities of risk maps with respect to water supplier.

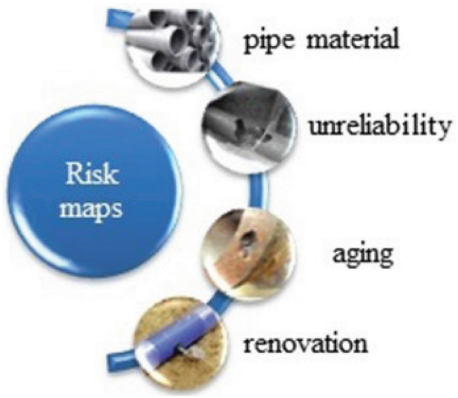


Figure 2. Possibilities of risk maps with respect to water consumer.

(Kołowrocki & Soszyńska-Budny 2012, Rak & Tchórzewska-Cieślak 2006, Tchórzewska-Cieślak & Piegdoń 2012). Risk matrix shows the dependence of the probability of the occurrence of threat from its consequences, which in the WDS are the loss of water, reduction in the level of supply reliability and consumers safety which are equivalent to the loss of water consumers health or life.

In quantitative matrix methods for all parameters of risk a point weight is assigned. In this way it is possible to make an analysis for various undesirable events.

The process of risk assessment consists of determining (estimation) its numerical value and comparing it with the accepted criteria values. The criteria values for the individual levels of scale depend on many factors, expert assessments, as well as accepted method of risk assessment, e.g. 2, 3, 4, or 5 parametric matrix method.

Using the product of the particular risk parameters according to (1) the risk matrix was obtained with numerical values within the range from 1 to 27. Three parametric risk matrix was shown in Table 2.

In quantitative matrix methods all the risk parameters have the relevant point weight assigned (depending on the adopted scale). To estimate the level of risk of the undesirable event occurrence, the criteria for the parameter showing the probability of the undesirable events occurrence (failure of water pipes) depending on the determined level of failure rate indexes, were proposed in Table 3. In Table 4 the values for parameter of losses caused by the undesirable event, depending on the value of the loss factor for the loss of water consumers safety, were proposed. The point scale and the criteria for the parameter V (vulnerability of the system to the undesirable event occurrence) were adopted according to the criteria available in the literature (Tchórzewska-Cieślak 2011).

In Table 5 the loss factor combining the type of water pipes with the degree of loss of water

Table 2. Three parametric risk matrix.

	P								
	1	2	3	1	2	3	1	2	3
C	**V** = 1			**V** = 2			**V** = 3		
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27

Table 3. Criteria for the point scale for the probability parameter with respect to the failure rate index for distribution pipes.

	Distribution pipes
P	λ [failure/km · year]
1	≤0,7
2	0,7 ÷ 1,0
3	>1,0

Table 4. Criteria for the point scale for the parameter of losses caused by the undesirable event, depending on the value of the loss factor, with respect to the loss of water consumers safety.

	Distribution pipes
C	The value of the loss factor, %, f(i)
1	20
2	60
3	80

Table 5. The values of the loss factor combing the pipe type with the degree of the loss of water consumers safety.

Type of pipe	Range of values for the failure rate index, [failure./km · year]	Calculated average value of the failure rate index, $\lambda_{śr}$ [failure./km · year]	The value of the loss factor, % f(i)
Distribution	≤0,7	0,26	20
	0,7 ÷ 1,0		60
	>1,0		85

Table 6. The three-stage scale of risk levels.

Levels of risk	Interval
Tolerable risk	$1,0 \le r \le 8,0$
Controlled risk	$9,0 \le r \le 12,0$
Unacceptable risk	$18,0 \le r \le 27$

consumers safety, was proposed. The values of the loss factor were adopted, depending on the pipe type and the values of the failure rate index.

Based on the values listed in the Tables 2–4 and according to (1), a set of possible risk values can be presented as a matrix:

$$r = \begin{bmatrix} r_{1\cdot1\cdot1} & r_{2\cdot1\cdot1} & r_{3\cdot1\cdot1} \\ r_{1\cdot2\cdot1} & r_{2\cdot2\cdot1} & r_{3\cdot2\cdot1} \\ r_{1\cdot3\cdot1} & r_{2\cdot3\cdot1} & r_{3\cdot3\cdot1} \\ r_{1\cdot1\cdot2} & r_{2\cdot1\cdot2} & r_{3\cdot1\cdot2} \\ r_{1\cdot2\cdot2} & r_{2\cdot2\cdot2} & r_{3\cdot2\cdot2} \\ r_{1\cdot3\cdot2} & r_{2\cdot3\cdot2} & r_{3\cdot3\cdot2} \\ r_{1\cdot1\cdot3} & r_{2\cdot1\cdot3} & r_{3\cdot1\cdot3} \\ r_{1\cdot2\cdot3} & r_{2\cdot2\cdot3} & r_{3\cdot2\cdot3} \\ r_{1\cdot3\cdot3} & r_{2\cdot3\cdot3} & r_{3\cdot3\cdot3} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \\ 2 & 4 & 6 \\ 4 & 8 & 12 \\ 6 & 12 & 18 \\ 3 & 6 & 9 \\ 6 & 12 & 18 \\ 9 & 18 & 27 \end{bmatrix}$$

The calculation procedure presented above concerns a general characteristics of matrix methods used for risk assessment (Rak & Tchórzewska-Cieślak 2006).

The most commonly encountered scale of risk levels is a three-stage scale: tolerated, controlled and unacceptable risk (Aven 2009, Aven 2010, Boryczko & Tchórzewska-Cieślak 2012, Ezell et al. 2000, Rak 2009, Tchórzewska-Cieślak 2011, Zio 2006).

The scale of the level of risk of lack of water is summarized in Table 6.

5 APPLICATION EXAMPLE

5.1 *Characteristics of the WDS*

Inhabitants of the city are supplied with water by boundary-chamber water intake with a capacity of 84000 m³/d. The total length of the water supply system is 894,1 km (data from 2013). The main network, 49,8 km long, is made of iron and steel pipes. The distribution pipes are made of cast iron, steel, PE and PVC, with a total length of 520,5 kilometres. The water supply connections, with a length of 323,8 km, are mainly made of steel, cast iron, PE and PVC. The water supply system in 80% is a closed system. There are two teams of water storage tanks, ZBI and ZBII, with a total capacity of 33100 m³.

Figure 3 presents water network scheme for analysed city.

5.2 *Analysis of water network failure*

For the WDS an analysis and assessment of the risk of the undesirable event occurrence (the failure of water pipes), has been made. An assessment of the failure of water pipes was made with basic characteristic, statistical parameters. The risk analysis in WDS was based on the proposed three parametric risk matrix, according to formula (1). The analysis includes an assessment of the risk for main network and distribution pipes.

In order to analyse the risk of lack of water supply in the aspect of water consumer, caused by the failures on distribution network in the first instance the analysis of the intensity of distribution network was made. In the failure analysis and assessment the failure rate index, λ, for water pipes, was used. The values of the failure rate index for distribution pipes λ_R were determined on the basis of the formulas available in the literature (Rak 2009, Tchórzewska-Cieślak 2011) and operational data. The results of the analysis and failure assessment for years 2005 to 2012 were presented in Table 7 and Figure 4.

5.3 *Results of analysis and risk assessment*

A calculation example was performed for the distribution pipes. In order to determine the risk of lack of water supply due to failure of distribution pipes the parameter values were assumed:

– parameter P (the probability of the undesirable event) was assumed to be 1 because according to Table 5 λ average ≤ 0.7 failure./km · year,

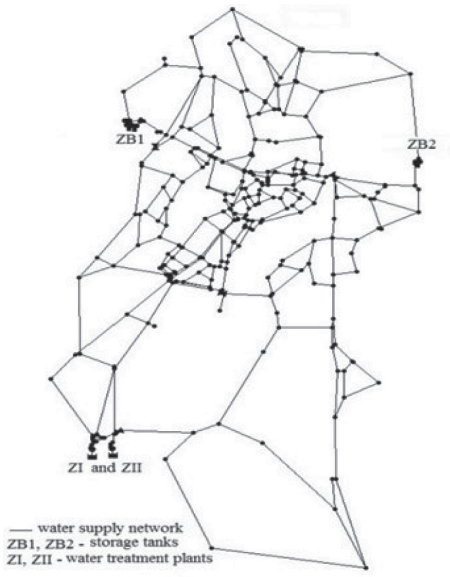


Figure 3. The scheme of water network.

Table 7. The failure rate index for the water supply network, over the years 2005–2012.

	Type of pipe		
	Distribution		
Year	length [km]	Failure	λ_R [failure./km · year]
2005	350,5	108	0,31
2006	384,4	136	0,35
2007	443,5	114	0,26
2008	447,7	106	0,24
2009	468	114	0,24
2010	490,5	114	0,23
2011	504,1	113	0,22
2012	520,5	109	0,21

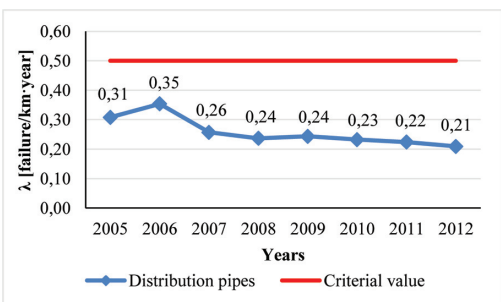


Figure 4. Failure rate indexes for water pipes over the years 2005–2012.

– parameter C (loss caused by the undesirable event) was assumed to be 1 because according to Tables 6 and 7 the undesirable event results in 20% loss of water consumer safety,
– parameter V (the degree of vulnerability to the undesirable events) was assumed to be 1 because 80% of water supply network is a closed system, with the possibility to cut-off the damaged section using gates (in order to repair the network), the network monitoring covers the whole water supply area, water supply company has the comprehensive system of warning and response in crisis situations with the full ability to use the alternative water sources.

Table 8 presents the values of P, C, and V for the risk, associated with the risk of lack of water supply with respect to water consumer and depending on the type of water pipe.

Creating a product of parameters according to the formula (1) and using the scale point for each risk parameter the value of risk of lack of water supply due to failure of distribution pipes on a tolerable level was obtained. The results were shown in Table 9.

5.4 *Risk map*

Intensive development of GIS software extends the capabilities of rational management in water distribution subsystem. An example of this phenomenon is the use of GIS as a spatial database in integrated system management for water companies. Effects of using GIS can be seen for over ten years (Applying GIS 2000, Geographic … 1992, Glasbrook 1994, Iglesias et al. 1997, Reynaert et al. 2004, Shamsi 2005, Scholten & Stillwell 1990, Seidenstat et al. 2005) and since few years also in Poland (Kotowski et al. 2007, Kwietniewski & Kłoss-Trębaczkiewicz 2007,

Table 8. Values of parameters associated with the risk of lack of water supply with respect to water consumer.

Parameter	Distribution pipes
P	1
C	1
V	1

Table 9. Value of the risk caused by failure in the distribution network.

Risk of lack of water supply	Distribution pipes
r	1
Level of risk	Tolerable

Kwietniewski et al. 2007, Kwietniewski 2008, Piechurski & Lampart 2005, Zimoch 2006). In water supply companies GIS applications are very convenient tool used in risk analysis. Using data visualization it is possible to create the risk maps based on the failure of water supply system, the age of pipes and current conditions of pipes with respect to the water supplier, taking also into account the impact of failure with respect to the water consumer. ArcMap software created by ESRI can be an important element in the process of decision making in WDS and risk analysis. ArcMap is the main tool for viewing, editing, and analysing data in a geodatabase. Is highly customizable, and it allows you to save your customization, as well as layers of data, to maps. The software has functions of acquiring and processing the data about the failure in water supply network and allows their spatial visualization.

The risk map of lack of water supply can be made taking into account the operational data, statistical analysis, and analysis of the failure rate indexes. By analysing water supply pipeline which is characterized by the highest failure rate it is possible to make for this pipeline the map of risk of lack of water supply showing the areas and buildings exposed to the long-term lack of water.

To present the results of the analysis using ArcMap it is possible to use two methods: the first method is the question about the attribute belonging to the select operation, e.g. "show water pipes with the failure rate higher than 0.2". The result of this type of analysis is to leave by the program only those sections that meet the above question. More advanced methods are buffering operations which are classified as analytical operations, e.g. "show areas being 20 m away from pipes with the failure rate higher than 0,35". The result of such an analysis are, for example, buffer areas marked above. Figure 5 presents the possibility of presenting data using the risk maps in ArcMap application.

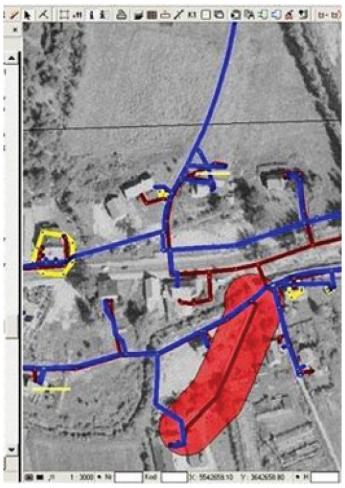


Figure 5. Graphical presentation of the results of analysis.

The map of risk of lack of water supply can be created for all types of water pipes on the basis of available data. Generated maps can be enriched by reports and charts that will clearly show the results to the water consumer. The maps in the application can be browse, edit and it is possible to analyse all kinds of data. There is also the ability to integrate data from different sources such as shape files (.shp), information layers, tables, CAD files, raster images and numerical terrain models. It is possible to browse and search interesting data and identify relationships between localized objects.

6 CONCLUSIONS

- Accurate and complete database systems are a base to perform more or less complicated risk analysis with respect to the lack of water supply to customers. Constantly updated data serve as a foundation in GIS applications. The programs allow to create GIS maps of risk due to the occurrence of undesirable events.
- The diversity of the use of simulation software enables to visualize risk analysis using models and diagrams. They can be used as a tool in decision-making process at planning a renovation of the network. The presented examples of ArcGIS application can be adapted for each water distribution subsystem, its parts or components.
- Nowadays, computer programs available on the market make it possible to fully visualize the various components of the critical infrastructure and track factors affecting the increase in risk.
- In the application example the risk of lack of water supply using matrix methods, due to failure of distribution pipes in relation to the consumer of water was made. This method allows also to determine the risk of lack of water with respect to water supplier considering all assets.
- The proposed method of determining the risk is a graphical presentation of data which clearly allows to present the analyses of conducted projects not only to the decision making body of the company but also to the general public.
- Using the risk maps it is possible to classify the pipes that have to be to replaced or renovated, taking into account the areas and buildings exposed to long-term lack of water.
- Generated risk maps can be used to increase the safety of the WDS in the context of water producer and water consumer.

– If it is not possible to obtain complete data for operational risk analysis an expert knowledge should be used. Database created in this way can be considered as a basis for risk modelling by means of fuzzy methods.
– In further work in this area with detailed simulation of the operation of water distribution subsystem should be carried out (using hydraulic network models), which is the next stage of the authors' research.

REFERENCES

Applying GIS technologies in Water Utilities: A Challenge and a Necessity, 2000. Conference Turin. "Water Supply—A Review Journal. IWA", 184.

Aven, T., 2009. Reliability and validity of risk analysis. *Reliability Engineering & System Safety* 9411: 1862–1868.

Aven, T., 2010. Conceptual framework for sik assessment and risk management. Summer Safety & Reliability Seminars *Journal of Polish Safety and Reliability Association*, 1: 15–27.

Babiarz, B. 2006. An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping*, Volume 83, Number 4/2006, p. 230–235, Elsevier, New York.

Bahr, H.P. & Vogtle, T., 1999. Gis for Environmental Monitoring. E. Schwerzerbartishe Verlagsbuchhandlung, Stuttgart.

Baz, I., Geymen, A. & Er Nogay S., 2009. Development and application of GIS-based analysis/synthesis modeling techniques for urban planning of Istanbul Metropolitan Area. *Advances in Engineering Software*, 402: 128–140. Elsevier, New York.

Bernhardsen, T., 1992. Geographic Information Systems. Viak IT, Arendal, Norway.

Berg, H.P., Gersinska, R. & Sievers, J., 2010. Procedure for probabilistic safety assessment of leaks and breaks of piping systems. International Journal of Pressure Vessels and Piping 872–3: 94–99.

Boryczko, K. & Tchórzewska-Cieślak, B., 2012. Maps of risk in water distribution subsystem. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, 2012, Curran Associates, Inc., p. 5832–5841.

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community INSPIRE 14.03.2007.

Ezell, B., Farr, J. & Wiese I., 2000 Infrastructure risk analysis of municipal water distribution system. *Journal of Infrastructure Systems*, ASCE, 63: 118–122.

Filipkowski, A., Gromiec, M., Bielobradek, P. & Witkowski, K., 2006. System informatyczny w zlewni rzecznej. [W:] Gromiec M. red. Systemy wspomagania decyzji w gospodarce wodnej. Instytut Meteorologii i Gospodarki Wodnej, Warszawa, str.63–141.

Geographic Information Systems GIS Guidelines Document, 1992 EPA, Washington.

Ghinoi, A. & Chung, Ch.-J., 2005. STARTER: a statistical GIS-based model for the prediction of snow avalanche susceptibility using terrain features—application to Alta Val Badia, Italian Dolomites. *Geomorphology*, 661–4: 305–325. Elsevier, New York.

Glasbrook, D.J., 1994. Application of GIS for Maintenance in Widespread Distribution Networks. IWSA Regional Conference, Zurich, p. 125–144.

Gromiec, M., 2006. Systemy wspomagania decyzji w gospodarce wodnej. Instytut Meteorologii i Gospodarki Wodnej, Warszawa, 2006.

Heinonen, T., 2000. Use GIS at Helsinki Water. [W:] Applying GIS technologies in Water Utilities: A Challenge and a Necessity. Conference Turin. "Water Supply—A Review Journal. IWA", 184: 1–8.

Hokstad, P., RØstum, J., Sklet, S., Rosén, L. & Linde, A., 2007. Generic Framework and Methods for Integrated Risk Management in Water Safety Plans. Publisher TECHNEAU.

Hokstad, P., RØstum, J., Sklet, S., Rosén, L., Pettersson, T.J.R., Linde, A., Sturm, S., Beuken, R., Kirchner, D. & Niewersch, C., 2009. Methods for risk analysis of drinking water systems from source to tap-Guidance report on Risk Analysis. Publisher TECHNEAU.

Iglesias, R.P., Izquierdo, S.J., Lopez, P.G. & Martinez, S.J., 1997. Geographical Information Systems GIS Applied to Water Supply Systems WSS. Proc. from the UIMP Int. Course, Valencia. Cabrera, E., Garcia-Serra J. eds. Kluwer Academic Publishers. Dordrecht-Boston-London, p. 22–51.

Kane, M.J. & Gough, A., 1996. Database to prioritize mains rehabilitation. Proc. of IWSA Spec. Conf. on New Developments in Modelling, Monitoring and Control of Water Supply Systems, Amsterdam, The Chameleon Press Ltd. London, p. 195–213.

Kaplan, S. & Garrick, B.J. 1981. On the quantative definition of risk. *Risk Analysis* 11: 11–27.

Kołowrocki, K. 2001. On limit reliability functions of large multi-state systems with ageing components. *Applied Mathematics and Computation,* 1212–3: 313–361.

Kołowrocki, K. & Soszyńska-Budny, J., 2012. Preliminary approach to safety analysis of critical infrastructures. *Journal of Polish Safety and Reliability Association* Summer Safety & Reliability Seminars, 3: 73–88.

Kotowski, A. & Kaźmierczak, B., 2013. Probabilistic Models of Maximum Precipitation for Designing Sewerage. *Journal of Hydrometeorology*, vol. 14: 1958–1965.

Kotowski, A., Pawlak, A. & Sambor, A., 2007. O możliwości budowy modeli wodociągowych w oparciu o GIS. *Forum Eksploatatora,* 128. Seidel-Przywecki. Warszawa.

Kwietniewski, M., 2008. GIS w wodociągach I kanalizacji. Wydawnictwo Naukowe PWN, Warszawa.

Kwietniewski, M. & Kłoss-Trębaczkiewicz, H., 2007. GIS, modelowanie i monitoring w zarządzaniu systemami wodociągowymi i kanalizacyjnymi. PZIiTS, Warszawa.

Kwietniewski, M., Miszta-Kruk, K. & Wróbel, K., 2007. Możliwości zastosowania GIS w wodociągach na przykładzie wybranego systemu dystrybucji wody. *Ochrona Środowiska*, 3: 73–76.

Li, H., Apostolakis, G.E., Gifun, J., Van Schalkwyk, W., Leite, S. & Barber D. 2009. Ranking the Risk from Multiple Hazards in a Small Community. *Risk Analysis* 293: 438–456.

Longley, P.A., Goodchild, M.F., Maquire, D.J. & Rhind, D.W., 1999. Geographical Information Systems: Principles, Techniques, Management and Applications. 2nd edition 2005. John Wiley & Sons Inc., New York.

Lyon, G., 2003. GIS for Water Resources and Watershed Management. CRC Press, Boca Raton, London-New York-Washington.

Mays, L.W., 1989. Reliability analysis of water distribution systems, Nowy Jork: American Society of Civil Engineers.

Otero, E., Fernandez, J., Takahashi, S., Matsushita, Versanne, D. & Godfroy, B., 1997. Interface between distribution systems and the customer: the use of management information systems to met standard of service. 4 Special Subject. Proc. IWSA, World Congress, Madrid, Blackwell Science ltd., London, p. SS4-1–SS4-12.

Piechurski, F. & Lampart, A., 2005. System ewidencjonowania sieci wodociągowej I kanalizacyjnej oraz awarii na tych sieciach. Mat. konf. GIS, modelowanie i monitoring w zarządzaniu systemami wodociągowymi i kanalizacyjnymi. PZIiTS, Warszawa, str. 89–103.

Piegdoń I. & Tchórzewska-Cieślak B., 2013. Zarządzanie ryzykiem w przedsiębiorstwach wodociągowych z wykorzystaniem nowoczesnych systemów informatycznych. *Gaz, Woda i Technika Sanitarna*. Wydawnictwo SIGMA-NOT, 10: 401–404.

Piegdoń, I., Boryczko, K. & Eid, M., 2014. Water supply systems risk analysis model by means of RENO software. *Safety, Reliability and Risk Analysis*: Beyond the Horizon. Taylor & Francis Group, London 2014, pp. 1987–1992.

Rak, J., 2009. Bezpieczna woda wodociągowa. Zarządzanie ryzykiem w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.

Rak J. & Tchórzewska-Cieślak, B., 2006. Review of matrix methods for risk assessment in water supply system. *Journal of Konbin*, 1: 67–76.

Rao, M.N., Waits D.A. & Neilsen M., 2000. A GIS-based modeling approach for implementation of sustainable farm management practices. *Environmental Modelling & Software*, 158: 745–753. Elsevier, New York.

Reynaert, B., Horemans, R. & Vercruyssen, P., 2004. ArcGIS/ArcFM 8 for water distribution network management. Case study submission in response to a call for case studies distributed by the author Shamsi U.M. for the book GIS Application for Water, Wastewater and Stormwater systems 2005.

Scholten, H.J. & Stillwell, J.C.H., 1990. Geographical Information Systems for Urban and Regional Planning. Kluver, Dortrecht.

Seidenstat, P. et al., 2005. Management Innovation in US Public Water and Wastewater Systems. John Wiley & Sons Inc., New York.

Shamsi, U.M., 2005. GIS applications for water, wastewater and stormwater systems. Taylor and Francis Group, Boca Raton, London-New York.

Tchórzewska-Cieślak, B. & Piegdoń, I., 2012. Matrix Analysis of Risk of Interruptions in Water Supply in Terms of Consumer Safety. *Journal of Konbin*, 241: 125–140.

Tchórzewska-Cieślak, B., Boryczko, K. & Eid, M. 2012. Failure scenarios in water supply system by means of fault tree analysis. In Bérenguer Ch., Grall A., Guedes Soares C. ed., *Advances in Safety, Reliability and Risk Management:* 2492–2499. London: Taylor & Francis Group.

Tchórzewska-Cieślak B., 2011. Metody analizy i oceny ryzyka awarii podsystemu dystrybucji wody. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.

Tchórzewska-Cieślak, B., Piegdoń, I. & Boryczko K., 2013. Wykorzystanie nowoczesnych technik informatycznych oraz baz danych w analizach ryzyka awarii podsystemu dystrybucji wody. *Aktualne zagadnienia w uzdatnianiu i dystrybucji wody*. Gliwice. p. 495–505.

Williams, M. & Shah, H., 2000. An Integrated IT Platform for Managing Water Distribution and Sewerage Networks. Applying GIS technologies in Water Utilities: A Challenge and a Necessity. Conference Turin. "Water Supply—A Review Journal. IWA", 184: 31–40.

Wu, W., Zhao, H., Chen, X., Markaris, A.P., Charalambous, C.N., Keleher, M. & Ulmer, J., 1997. Mapping information systems—case studies. 14 Special Subject, Part 1, Proc. IWSA, World Congress, Madrid, Blackwell Science ltd., London, p. SS14-1–SS14-12.

Zeng, H., Talkkari, A., Peltola, H & Kellomäki, S., 2007. A GIS-based decision support system for risk assessment of wind damage in forest management. *Environmental Modelling & Software*, 229: 1240–1249. Elsevier, New York.

Zimoch, I. & Paciej, J., 2013. Zastosowanie Geograficznych Systemów Informacyjnych w zarządzaniu oraz prowadzeniu kontroli jakości wody przeznaczonej do spożycia przez ludzi. *Instal*, 1: 38–41.

Zimoch, I. 2006. Application of computer techniques in reliability analysis of water supply system operation in the failure conditions. *Zaopatrzenie w wodę jakość i ochrona wód*, VII międzynarodowa konferencja, Poznań—Zakopane, 6: 679–691.

Zio, E., 2006. An introduction to the basics of reliability and risk analysis. World Scientific Publishing Co. Pte.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Concept for development of safety-related filters

O. Krini, J. Krini & J. Börcsök
Department of Computer Architecture and System Programming, Kassel, Germany

ABSTRACT: The safety standard IEC 61508 defines the requirements for safety systems in the plant safety independently of application. It is intended the basis of all safety related electrical, electronic and programmable electronic systems, in order to apply it in safety critical applications. The purpose of this paper is to describe the design and development of safety digital filters. The digital filter will be implemented on a FPGA structure. The goal of this project is to implement a safety filter which has the characteristic of a low pass filter second order. The safety concept ensures that the filter work with the predefined characteristics. In this documentation a low level safety concept will be discuss. At first an analog signals with different frequencies will be transform in the digital area to make digital signal processing on the signals. The reason of the digital signal processing is to let only some signals with certain frequencies to cross over the System. Which signals can cross over the system will be given over the transfer function of the digital filter.

1 INTRODUCTION

The reliability is one very important parameter of applications software. Hard- and Software reliability is the probability that given hard- and software will be functioning without failure in a given environment during a specified period of time. Hence, hard- and software reliability is a key factor in development process and quality. The state of the art is, that reliability models exclusively consider avoidable faults that could lead to critical failure. Furthermore, there is no possibility to predict the residual number of critical faults, since very few failure data came from the testing.

Digital filters are Systems which are changed the input signals. The changing can be happen of different modes like to steaming signals, to amplify signals or to suppress the input signals. The determining of the characteristic of the digital filter will be done with mathematical models. These mathematical models are the fundamental of the system theory. However where are here the different between the analog filters and digital filters? The different are only in the implementation. While analog filters are designed with passive components like resistors and capacitors or active components like amplifiers, the digital filters are developed with logical components. Digital filters takes an important role in this world which are most controlled by electronics. The application area of these Systems is really huge.

Like in medical technology it is important that a digital filter works with a high reliability. Information's which are converting in the medical technique can be associated with a life-threatening situation. For this reason a digital filter must be implemented safety. In this documentation will be given an abtract about the functional safety, which based on IEC 61508 and also described how a digital filter will be implemented of a FPGA structure. In addition a safety concept will be presented which can let work the filter with a higher reliability.

2 STOCHASTIC BASICS

The modeling of reliabilities, probability calculation plays a central role for the reliability and risk assessment of hardware and software systems.

The probability calculation is one of those areas of mathematics, where the connection between the real world and its mathematical description is particularly evident. However, this particular area of mathematics is one of those, in which logical thinking is so in demand than in virtually any other areas. For the assessment of reliability in software systems, it is necessary to know some basic concepts and calculations of probability theory.

The most known and must favorite probability model for the reliability analysis of safety systems is the exponential distribution. With this distribution it is possible to represent the time dependent

failure probabilities F(t) of components. For the determination of the probability of failure one needs a data of the failure frequency, number of built in components and operational time of the components. The failure probability is defined as

$$F(t) = 1 - e^{-\lambda \cdot t} \tag{1}$$

The density function is calculated from

$$f(t) = \frac{dF(t)}{dt} = \lambda \cdot e^{-\lambda \cdot t}. \tag{2}$$

The Binomial distribution, also known as Bernoulli distribution, belongs to the discrete distribution. The specific feature of the binomial distribution is that it can accept only 2 values. This means that a component failure is present $x = 0$ or is not present $X = 1$. The probability of exactly x successes is given by this formula:

$$P(X = x) = \binom{n}{x} p^x \cdot q^{n-x}, \tag{3}$$

where n is the number of experiments. The binomial distribution can be graphed as following:

The Poisson distribution is a special case of a binomial distribution, if the probability of failure p or probability of successes q is very small and the number of experiment n is very large. The conditions under which the Poisson distribution holds are the counts of rare events, all events are independent and the average rate does not change over the period of interest. The Poisson probability function is given as follows:

$$P(X = x) = \frac{\mu^x}{x!} \cdot e^{-\mu}, \tag{4}$$

the expected value $E(x)$ is

$$E(x) = \mu \cdot \sum_{x=1}^{\infty} \frac{\mu^{k-1}}{(k-1)!} \cdot e^{-\mu} = \mu. \tag{5}$$

In a Poisson distribution, only one parameter is needed to determine the probability of an event.

The Weibull distribution is one of the most commonly used distributions in reliability engineering. The Weibull distribution is a continuous distribution. The distribution makes it possible to represent the time dependent failure probabilities $F(t)$ of components. The required data are the failure frequency, number of all components and the failure times of the components. The probability of failure according to the Weibull distribution $F(t)$ is defined as

$$F(t) = W(t; \beta; t_0; T) = 1 - e^{-\left(\frac{t - t_0}{T - t_0}\right)^{\beta}} \tag{6}$$

where $\beta > 0$ is the failure slope or shape parameter and t_0 is the correction parameter. T is the characteristic lifetime or position parameter.

The Weibull distribution so known under the name "Bath tub curve" is divided into three areas. The first phase is an early phase. At the beginning, the failure rate is high. During the early phase, the failure rate decreases. The second phase is the operational use. During the operational phase, the failure rate reaches the minimum. In this phase, the failure rate is constant. The last phase is a wear out phase. During the wear out phase, the failure rate increases, because the components reach their end-off-live time. The Weibull density function is calculated as follows:

$$f\left(\tilde{t}\right) = \lambda \cdot \beta \cdot \left(\lambda \cdot \tilde{t}\right)^{\beta - 1} \cdot e^{-\left(\lambda \cdot \tilde{t}\right)^{\beta}}, \tag{7}$$

where $\tilde{t} = t - t_0$.

3 FUNCTIONAL SAFETY

The standard IEC/EN 61508 shows exemplarily the procedure for determining the probability of hardware failures. First, it specifies the principles and assumptions on which the calculations are based.

For analysing the safety integrity of safety-related systems many methods are possible. Reliability block diagrams and Markov models, however, belong to the most frequently applied. If correctly applied, both methods provide almost the same results. Nevertheless, the Markov models are still more exact (but more difficult) and provide accurate values, even for complex systems.

To determine the safety integrity of safety-related systems (i.e. consisting of several individual systems), the average probability of a failure PFD_{System} or PFH_{System}, is required for the overall system.

To determine the PFD_{System} or PFH_{System} values of a safety-related overall system (i.e. consisting of the sensor system, the logic system and the actuator system), one must add the determined average probabilities for the individual systems:

$$PFD_{System} = PFD_{Sensor} + PFD_{Logic} + PFD_{Actuator} \tag{8}$$

or

$$PFH_{System} = PFH_{Sensor} + PFH_{Logic} + PFH_{Actuator} \tag{9}$$

Table 1. Definition of safety integrity level according to IEC 61508.

SIL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$10^{-5} \leq PFD < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$
3	$10^{-4} \leq PFD < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
2	$10^{-3} \leq PFD < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
1	$10^{-2} \leq PFD < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$

To determine the average probability of failure for each subsystem, following elements must be known:

– The basic architecture
– The diagnostic cover of each channel
– The failure rate of each channel
– The factors β and β_D for common cause failures

The target is to detect common-cause failures as early as possible and to bring the system into a safe state.

The different requirements of the altered Safety Integrity Levels (SIL) are in dependent on the probability of failure and are shown in Table 1. The probability values are defined as a PFD-value (probability of failure on demand), if the system is in a low demand mode and has to execute a safety function. However, if a system is operating in a high demand mode or continuous mode and a safety function has to be executed, then the probability of failure is specified with the PFH (probability of failure per hour). Its dimension or unit is (1/h). (Carsten 2006), (Kainka 1996)

4 IMPLEMENTATION OF A SAFETY FILTERS

In this section the fundamental Basics of the implementation will be discuss.

4.1 *Design of the use FPGA-board*

A Field programmable Gate Array (FPGA) is a semiconductor chip with consists about many logical components. The User can create integrated circuits with the hardware programming languages VHDL ore Verilog. The Integrated circuits can be takes lower complexity like timers ore really higher complexity like microcontrollers. Producer of semiconductors takes this advantage to produce integrated circuits without fails to reduce the development costs. Here are the possibility to create integrated circuits and simulate this circuits until the design have no fails.

How explained in the introduction, a digital filter will be designed on a FPGA-Board. The FPGA-Board which is used here is from the company Digilent and it's known under the name BASYS2.

The operating frequency of the Board is 50 MHz. However it can be operated with higher frequency as 50 MHz. It is possible to operate the board with an extern oscillator. The Board has a base where the oscillator can be assembled. The Board takes the power supply via USB and will be programmed simultaneous via USB. The USB driver and the software tool to program the FPGA can be downloaded over the homepage of Digilent. How in Figure 1 is shown, the FPGA-Board consist other interfaces like 8 switches, 4 push buttons, 4 PMOD interfaces and a 7-Segment display. With this interfaces the user has the possibility to control input and output data. These Interfaces are direct connected with the central processing unit. The central processing unit is the Spartan-3E which is produced from the company XILINX.

4.2 *Digital filters*

Finite Impulse Response (FIR) filters are Systems where the impulse response is finite. These filter structure are non-recursive and have no feedback. The advantage of this structure is that they are always stable. That means that the system does not oscillate from self. The order of the filter is given over the number of the delays. Where X(n) stays for the discrete input samples and Y(n) stays for the discrete output samples.

These filter structures is designed always by delay blocks, additions blocks and multiplier blocks. Different filter structure with different transfer functions can be designed only by changing the filter coefficient. The following filter can be development:

– Low pass filter n-order
– High pass filter n-order
– Band pass filter n-order
– Band stop filter n-order

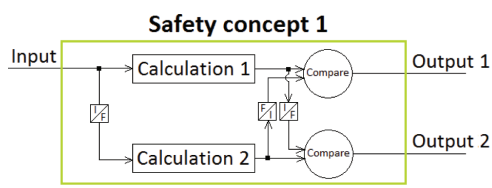


Figure 1. Safety concept 1.

4.3 *Safety concept without limitation*

In this Section a safety concept L1 of the implementation will be described. This safety concept L1 is a low level concept and is shown in Figure 1.

The safety concept will be used on the mathematical blocks. The mathematical blocks like the adder or the multiplications block are necessary for the implementation of the digital filter. The question here is how to make a mathematical function safety. For example the adder block will be designed with the safety concept (shown in Fig. 1). The adder Block has two inputs. The inputs data are represented in fix point arithmetic. The safety concept makes at first the calculation of the two inputs data in fix point arithmetic. In the same time a type converting part change the two inputs in a floating point format. After the type converting an adder makes the same calculation in floating point arithmetic. In the final way the result of the floating point block will be type converted in fix point format to compare the results in fix point arithmetic. In the same time the result of the fix point block will be converted in floating point format. After the conversion the same comparison will be executed in floating point arithmetic. Once the comparisons of both ways are in agreement, the result of the mathematical addition is correct.

5 RESULTS

In this section the results of the measurements will be discussed. For the verification of the results a comparison model will be tacked. The comparison model is the transfer function of the low pass filter which is determined with the software tool Matlab. It will be execute measurements on the low pass filter and compared with result of the theoretical values. At firs the theoretical transfer function of the low pass filter will be plotted. This will be done over the following instruction on the command window of the Matlab tool.

Instructions

- A = [0.25 0.5 0.25];
- Freqz(A);

The Instruction has to type one after another. The instruction gives the transfer function in Figure 2.

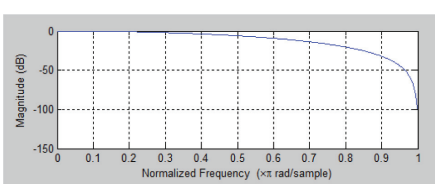


Figure 2. Theoretical transfer function.

Figure 2 shows that the frequency ache is normalized. For the comparison of the results must be considered that $\pi = J_S /$. To compare the practical results with theoretical values, different sinus signals with different frequencies are conveyed over the digital filter on the board. Consequently the attenuation of the signals on the output is measured. The logarithm output attenuation is given with the following equation.

$$A_{dB} = 20 \cdot \log\left(\frac{U_a}{U_e}\right) \tag{10}$$

The following signals will be conveyed over the system.

Input signals

- Sinusoidal signal with f1 = 5 kHz and A = 3.3V
- Sinusoidal signal with f1 = 10 kHz and A = 3.3V

The normalized frequency of 5 kHz is on the 0.21 point. The theoretical attenuation on this point is approximate 0.96 dB (see Fig. 3).

At this attenuation the output signal must be approximate 2.95V by the input signal with the amplitude 3.3V. This can be calculate by equation 11.

$$U_a = 10^{\frac{A_{dB}}{20}} \cdot U_e \tag{11}$$

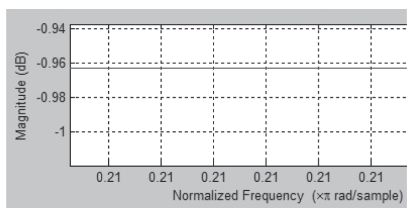


Figure 3. Theoritical tranfer function at the frequency 5 kHz.

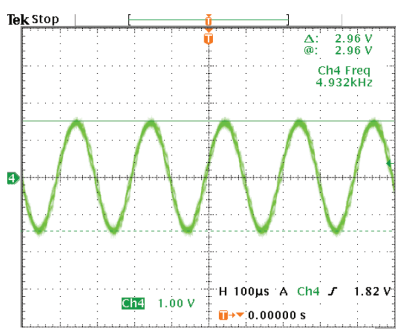


Figure 4. The practical amplitude value at the frequency 5 kHz.

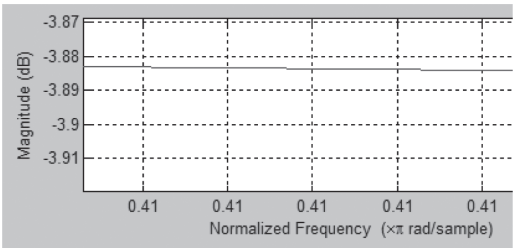


Figure 5. Theoritical tranfer function at the frequency 10 kHz.

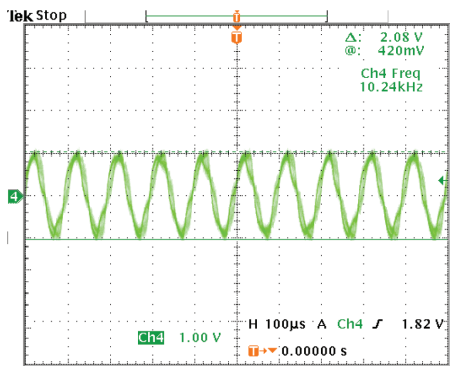


Figure 6. The practical amplitude value at the frequency 10 kHz.

The output signal is 2.95. This can be seen in Figure 4. The theoretical value is equal to the practical value.

Now the second signal with the frequency of 10 kHz is conveyed over the System. The normalized frequency of 10 kHz is on the 0.41 point. The theoretical attenuation on this point is approximate –3.88 dB (see Fig. 5).

At this attenuation the output signal must be approximate 2.11V by the input signal with the amplitude 3.3V. This can be calculating by equation 2. The output signal is approximate 2.11V. This can be seen in Figure 6. The theoretical value is equal to the practical value.

6 CONCLUSION

In this documentation an implementation of a digital filter in a FPGA structure is described. The implementation was done on a FPGA-Board from the company Diligent Inc. The FPGA-Board is known as BAYSIS 2. It was implemented a low pass filter second order. After the implementation the results was discussed. In the final section a safety concept without limitation was described. This safety concept will be a basic principle of the future work. In the future work it will be investigate more time to make the safety concept with limitation and diversity-approach witch are stable and safer. For example with a limitation it can be guaranteed the filter don't work out of range. This limitation will be designed redundant. In addition the limitation will be monitored with a diagnostics concept. This will be described in a next research work.

REFERENCES

Ansari, R.; Liu, B.: A class of low-noise computationally efficient recursive digital filters with applications to sampling rate alternations. IEEE Trans. Acoust. Speech Signal Process. 33 (1985) 90–97.

Burrus, C.S.: Block Implementation of Digital Filters. IEEE Trans. Circuit Theory, 18 (1971) 697–701.

Carsten, Roppel: Grundlagen der digitalen Kommunikationstechnik. Übertragungstechnik-Signalverarbeitung-Netze. (2006).

Fettweis, A.; Levin, H.; Sedlmeyer, A.: Wave digital lattice filters. Circuit Theory and Applications 2 (1974) 203–211.

Gaszi, L.: Explicit formulas for lattice wave digital filters. IEEE Trans. Circuits Syst. 32 (1985) 68–88.

Hering, Bressler, Gutekunst.: Elektronik für Ingenieure und Naturwissenschaftler. Springer Verlag, (1998) Auflage 5.

Hermann, Hinsch.; Elektronik. Ein Werkzeug für Naturwissenschaftler, (1996).

Kainka, B.: Häßler, M.: Straub, H.W.: Elektronik. Grundwissen Elektronik. Die Grundlagen der Elektronik für Hobby, Ausbildung und Beruf. (2004).

Martin, Werner.; Nachrichtentechnik. Eine Einführung für alle Studiengänge. (2010) 7.Auflage.

Saramäki, T.: On the design of digital filters as a sum of two all-pass filters. IEEE Trans. Circuits and Systems 32 (1985) 1191–1193.

Vaidyanathan, P.P.; Mitra, S.K.: Neuvo, Y.: A new approach to the realization of low-sensitivity IIR digital filters. IEEE Trans. Acoust. Speech Signal Process. 34 (1986) 350–361.

Wilfried, Plaßmann.; Detlef, Schulz.: Handbuch Elektrotechnik. Grundlagen und Anwendungen für Elektrotechniker, (2009) 5.Auflage.

XILIX.; KCPSM3.zip/KCPSM3_Manuell.pdf.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Heat Supply System reliability management

B. Babiarz
Rzeszow University of Technology, Rzeszow, Poland

ABSTRACT: According to the Polish energetic law act, the aim of heat engineering is to provide an uninterrupted and reliable supply of heat for consumers using commonly available services. One of the heating industry's measures of service is the reliability of this supply, determined by the following requirements, which are: the supply of heat to consumers by means of a heat-carrying agent having the necessary parameters (required quantity, temperature and pressure) in a specific location, under certain operational conditions and timeframe.

Every interruption in the heat supply to consumers indicates a decrease in the heat supply's reliability. Interruptions result in a decrease of the required parameters of a system's elements, which in consequence has an effect on users' discomfort.

Reliability management in Heat Supply System (HSS) requires consideration of their complexity and specific characters. In a heat supply system, three subsystems have been distinguished: subsystem of heat production, subsystem of heat supply and subsystem of heat distribution, which consequently consists of modules, objects and elements. The necessity and possibility of using modern techniques methods in order to improve reliability of elements, objects, subsystems and a whole system have been analysed in this work.

Presenting new methods of heat supply system operation reliability and safety management has been the main purpose of the paper. Application of methods has been showed in example of existing HSS.

1 INTRODUCTION

Heat Supply System (HSS) may be included in relatively complex technical systems. It belongs to energetic systems, being a part of the critical infrastructure, which is necessary to normal functioning of the country.

There are the following targets in the heat supply of the city:

- basic—directed for maintenance of reliability and safety in operation and commonness supply, constituting an element of all the next solutions,
- sustainable development, which follows to possible the lowest costs of energetic services considering environmental costs,
- ecological, which assumes wide scope of state environment improvement,
- social, considering the lowest share of energetic services costs in households.

The basic objective seems to be priority because of the impact on a possibility of realization other targets.

Correct operation of district heating systems gives a possibility to fulfill the requirements of users. Existing infrastructure is very various when it comes to technical and economical view. Technical effectiveness of the district heating sector has an influence on correct and optimal operation of all system.

Heat engineering like any other sector cannot exist nowadays without IT systems. Majority of system heat suppliers use it now or implement modern integrated systems, which is supportive in management enterprise and efficient customer service. Software is however only a tool assisting proper management of a system.

2 STRUCTURE AND SPECIFIC CHARACTER OF HEAT SUPPLY SYSTEM

Heat Supply System (HSS) is one the communal engineering systems consisting of technical infrastructure. At the same time it is one of the youngest and the most interdisciplinary systems connecting many technical fields such as: power engineering, civil engineering, environmental protection, transport etc. There are many features distinguishing district heating sector from of the others. HSS characterises completely local character. The locality of HSS is reflected among other in a lack of heat transfer possibility between cities, which in consequence means that it is not possible

to cover the heat requirements of the country in such a manner that it is possible in the case of electricity or natural gas.

The specific character of HSS involves changeable heat load during the year resulting from external climatic conditioning, in which is our country. The ensemble of climatic condition causes the extraction of a heating season during the whole year which is an established period in which external temperatures don't exceed +10 ^{0}C. During the heating season HSS work for the needs of heating buildings, preparing hot water, ventilation and possible technological needs, however during the after heating season it works with decreased heat load, covering the demand for heat only for hot water and technological ones according to individual production demands. Considerable differentiation of the level of HSS load and its dependence on changing external conditions as well as line functional and structural connections make them different from other technical systems.

Moreover a considerable thermal inertia in supplying the heating medium from the heat source to consumers as well as the need to foresee the sequence of weather changes create considerable difficulties in proper control of heat supply in including reliability in the operation.

Analyzing the issue of Heat Supply System (HSS) reliability requires taking into consideration their complexity and the extent of realization. In the heat supply system we can distinguish three subsystems: Subsystem of Heat Production (SbHP), Subsystem of Heat Supply (SbHS) and Subsystem of Heat Distribution (SbHD), which consequently consists of modules, objects and elements, (Babiarz 2005). There are connections between particular HSS elements and their coherent influence on operational reliability of the whole system. The structure of HSS decomposition into subsystems is presented in Figure 1.

The characteristic feature of heat-supply systems is the occurrence of many operational states of the system at various heat load and efficiency, determined by a range of random factors affecting the demand for heat. From the standpoint of reliability the states are described by a combination of damaged and undamaged elements connected with each other by means of appropriate structures.

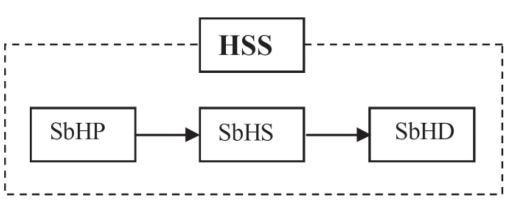


Figure 1. Decomposition of HSS into subsystems.

3 CRITERIA OF HSS RELIABILITY MANAGEMENT

3.1 *Reliability and safety*

Considering HHS as three subsystem set require distinct formulating of the management criteria.

The criteria concern meeting quantity and quality requirements, determined by external conditions. They consider variability in time (fixed variable), space (free and constrained), the nature of interaction (static, dynamic, percussion), causes of failure and above all the possibility of monitoring and control.

Reliability of HSS (REL) is its property which allows it to meet the requirements set, which are the supply of heat to consumers by means of a heat-carrying agent having necessary parameters (required quantity, temperature and pressure) in a specific location, operational conditions and duration of time, (Babiarz 2010).

What is connected with the reliability is safety as a condition of certainty, not occurring threat, the ability of the system to ensure the safety of HSS's users, other systems' users and the environment.

There are many methods using mathematic and simulative tools that can be applied in the evaluation of the reliability and safety in management of various technical systems. More detailed information about it are presented in articles: (Blokus 2006, Rak 2009, Helseth 2008, Ostrowski 2014a,b, Kołowrocki 2013, Todinow 2006, Tracz & Ostrowski 2012). The theory of reliability in heating, ventilation and air conditioning was concentrated in publications (Myrefelt 2004, Peruzzi L. et al. 2014).

Measures of Reliability (Rel) and Safety (S) can be determined according to following relations, (Rak & Babiarz 2001).

Probability of the system reliability provided the non-occurrence of the loss of safety:

$$P(REL/S) = \frac{P(REL) \cdot P(S/REL)}{P(S)} \tag{1}$$

Probability of the system reliability provided the occurrence of the Loss of Safety (LS):

$$P(REL/LS) = \frac{P(REL) \cdot P(LS/REL)}{1 - P(S)} \tag{2}$$

Probability of the system unreliability (UN) provided the non-occurrence of the loss of safety:

$$P(UN/S) = \frac{P(UN/S)}{P(S)} \quad (3)$$

Probability of the system unreliability provided the occurrence of the loss of safety:

$$P(UN/LS) = \frac{P(UN/LS)}{1 - P(S)} \quad (4)$$

3.2 *Quantity parameters*

Flow of heat-carrying agent is the quantity parameter which compliances the level of meeting requirements by the HSS. The flow rate results from thermal power demand (Φ), dependent on atmospheric conditions. Thermal power transmitted by hot water using heating network is changeable during the time (t). Typical trends of changes relative thermal power during the year presents Figure 2—the structured graph of thermal loads.

3.3 *Quality parameters*

Because the biggest influence on medium heat demands have atmospheric conditions, the regulatory graph can be determined for every type of control. Figure 3 presents dependency regulated parameters, such as: flow temperature T_f, return temperature T_r upon external temperature Te.

The regulation graphs are drawn taking into account the structure of the thermal power demand (Wojdyga K., & Niemyjski O. 2012). The example regulation graph for HSS working for heating and hot water preparation demands have been presented in the Figure 3. The correction, determined by the degree of cloudiness and wind speed contain more detailed charts.

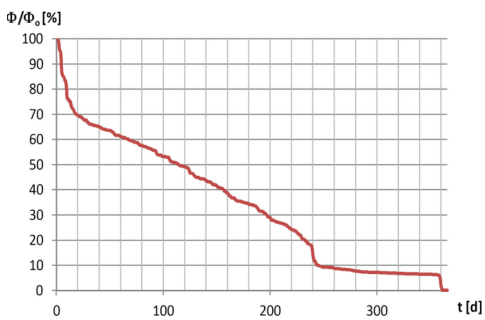


Figure 2. The structured graph of thermal loads.

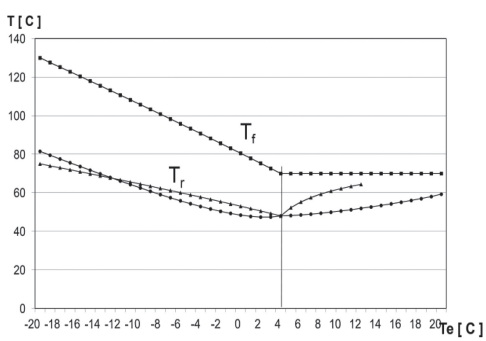


Figure 3. The regulatory graph.

4 METHODS AND TOOLS IN RELIABILITY MANAGEMENT

4.1 *Determinants of reliability management*

Reliability management means change in approach to problems of production, transmission and distribution of thermal energy, taking into account quality of performing services of heat supply. Reliability management should be treated as a complex process containing also safety, (Berg 2008, Rak J.R. 2007, Tchórzewska-Cieślak B. 2009, Tchórzewska-Cieślak B. 2012, Todinov 2006). It covers methods and tools based on experience, in order to identify potential faults or risks at an early stage in the life cycle, (Dou et al. 2011, Vališ & Zając 2010, Vališ et al. 2010).

An admission to introduction more advanced methods of reliability management should be thorough records, control and analysis of operational parameters in the system with reliability and safety evaluation. Proposed schema of reliability and safety of HSS management presents Figure 4.

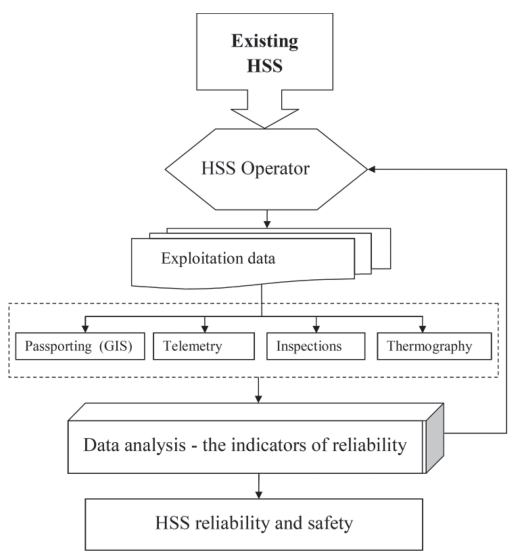


Figure 4. Scheme of HSS reliability and safety management.

In connection with growing competition incomes of enterprises generally decrease. In order to maintain or increase them, it is necessary to maintenance dependability of equipment at the proper level with the lowest costs, so the technical, operational and economical tasks appear.

Technical tasks:

– maintenance the functioning of the equipment and networks required to ensure the required level of heat supply,
– maintenance the operation of equipment to ensure their proper functioning for a long time.

Economical tasks:

– creation a plan to maintain the network and facilities providing the minimum cost of ownership over the "life";
– standardization of equipment maintenance costs;
– retaining proportionality the cost of maintaining the network and devices to the production costs, so that they are a component of variable costs;
– maintaining variable costs at the level specified as a percentage of sales volume of thermal energy;
– planning repairs of networks and devices in order to avoid additional costs associated with the aftermath of damage.

Awareness of the effectiveness of technical resources while maintaining SZC such trends significantly increases. As a result, the reliability can be treated as a commodity, so retaining appropriate level of reliability requires some costs. It should therefore strive to optimize in this area. Particular allowing active actions and decisions in this area is the availability of more and better tools that allow you to collect information about the system during operation, and then use them in the analysis of reliability and safety as well as economic analysis, (Toktasynova et al. 2014, Nowakowski & Werbińska-Wojciechowska 2009, 2010).

4.2 *Network inventory in district heating*

Network inventory of district heating (passporting) networks consisting in electronic records and technical inventory data, together with their description. Course of the network is shown in the available digital maps. Network inventory provides a database of networks for the purpose of exploitation. It helps to carry out the modernization of the network. The system includes a library of basic technical data and symbols of network devices. Network inventory system is based on GIS (Geographic Information System). GIS fulfill a role as a module, that combines other IT systems. This is due to the fact that 80% of the objects, about which information are collected, have a spatial position. Geographic Information System is not only for network inventory, but it also solves real business and technical problems. The main feature of GIS is to provide a mechanism for entering, gathering and storing spatial data, management, providing their integrity and consistency and allowing for their initial verification.

On the basis of the data collected in the system, it is possible to carry out specific analyzes based, among others, on the spatial relationships between objects. The results of spatial analysis and operations characteristic of the programs of base-set may be presented in the descriptive (tabular) or graphic (map, we diagrams, graphs, drawings) form, hence the visualization and sharing of spatial information in the desired form are features of the system.

GIS is a system composed of four inseparable and equivalent elements:

- spatially oriented data;
- hardware and software;
- problems or tasks to be solved;
- people making system and using results of analyzes.

This system provides the following capabilities:

- networks and devices records;
- prediction of heat consumption and thermal power ordered by customers;
- support disaster recovery;
- inventory of assets;
- analysis and statement related to business;
- hydraulic and thermodynamic calculations;
- monitoring of investment and repair activities;
- assist the work of disposal and registration of the network;
- supporting the process of connecting a new recipient;
- integration of the systems in heating enterprise.

4.3 *Telemetry system*

Telemetry system is part of the monitoring, which is used for remote monitoring and controlling district heat network devices. It enables observation of individual elements and objects district heating network in on-line mode. Heat sources, heat exchanger stations and heat chamber are connected to the system. The system allows to control parameters at every point of the city and control of operations carried out currently in the network. It sends periodic inquiries about their status to the devices in the node. It also accepts alarm messages and collects historical information about the node work. Connection of nodes provides transmission equipment through a wired network and the GSM

system. Specialists can watch work of sources and heat networks through a visual representation of the network and its current parameters on monitors. Incoming information are collected in a database server telemetry. This allows to perform detailed analyzes, as well as the aggregation of the data to more general comparisons.

4.4 *Direct maintenance*

Direct inspections are important from the point of view of heat supply security to customers. They require usage of specialized equipment to the location of network failures, leaks and control of a district heating networks. Infrared cameras and other devices, which are part of the resistive pulse or alarm systems, are used to analyze the quality of the insulation of heating networks. They enable ongoing monitoring of the state of the system components to prevent the occurrence of major accidents.

One of the most important system functions for the district heating sector is possibility of remote, automatic reading of heat meters, combined with the collection of measurement results in the so-called repository. Modern IT systems for heat engineering collect information about each device heating infrastructure and also connection between elements of the heating system. The system supports the settlement process with clients, by continuously collecting and analyzing data. It facilitates monitoring of district heating network and also reduces the risk of failure.

4.5 *Remote thermography*

Remote thermography is the analysis of the district heating network by performing "thermal maps of the city"—risk maps. Remote inspection of heat distribution networks is made by overheat path using infrared technology and is a constant element in the palette of mobile procedures for locating leaks. Through remote and comprehensive analysis of the state heating networks with the use of infrared sensors, image data of geometric and thermal high-resolution can be obtained in a short time of measurement and in identical, predefined measurement conditions. This strategy of collecting the data allows to perform comparative analysis of the entire network on the inspected thermal heat supply area. The aim of the investigation is not primarily to locate individual leaks, but large-area assessment of all elements of the heating network and to register and to differentiate all its weak points. This method's target is to direct funds to the priority network failures and to check workmanship on the route sections after repairing or carrying out new project managements. In this way the analysis of the state of the HSS elements is an objective mean of decision-making about planning repairs and inspections.

5 EXAMPLE OF APPROACH TO THE RELIABILITY MANAGEMENT

Reliability management in the existing heat supply system requires continuous improvement and expanding tools of monitoring and control. On the basis of the exploitation data provided by the Municipal Heating Company in Rzeszow city an approach to the management of the reliability in the existing heat supply system have been illustrated. Schema of Rzeszow HSS using the Inventory system is shown in Figure 5.

Inventory system in the HSS of Rzeszow city enables a comprehensive solution to the problem of management of spatial resources. It is based on a foundation consisting of two products:

- *Smallworld*—a universal geographical information system of General Electric company, being the mean of creating specialized GIS systems for asset management, particularly in network industries;
- *EC.GIS*—specialized GIS system for enterprises of thermal energy distribution of Globema company, based on *Smallworld*, composed of a number of functional modules.



Figure 5. Scheme of Rzeszow HSS using the inventory.

Such built system is configured and integrated with other IT systems in Municipal Heating Company in Rzeszow city.

The main functional modules of the system is the *Main Module*, which is used by the following modules:

- *EC.GIS Dispatcher* module—for switching the stroke and analyzes the state of the network;
- *EC.GIS Operation* module—support exploitation activities on the network;
- *EC.GIS Failures* module—to register of failure and failure analysis;
- *EC.GIS Calculations* module—for the hydraulic and thermodynamic calculations;
- *EC.GIS Investments* module—to support investment planning processes;
- *EC.GIS Net* module—to share data on the web/intranet.
- *Smallworld Spatial Intelligence* module—for business analysis and reporting.

In addition, distinguished interfaces for integration with: Komadres and Telemetry system.

Telemetry system in the HSS of Rzeszow city has 39 points on the network. The current system is a telemetry monitoring system only allows observation of individual objects on—line. Current synoptic image of investigated HSS is shown in Figure 6.

All information read on the premises is sent to disposable centers, where it is converted into a user-friendly visualization program WIZCON by 8.20.

The dispatching centers DC-1, DC-2, DC-3 system user (dispatcher) has the ability to:

- control the operating parameters of a heat source (Fig. 7);

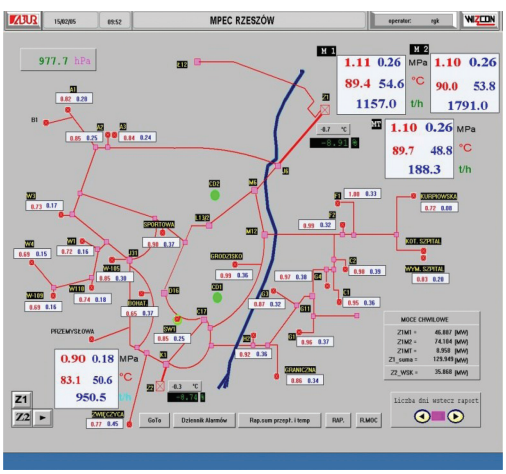


Figure 6. Synoptic image of HSS city of Rzeszow.

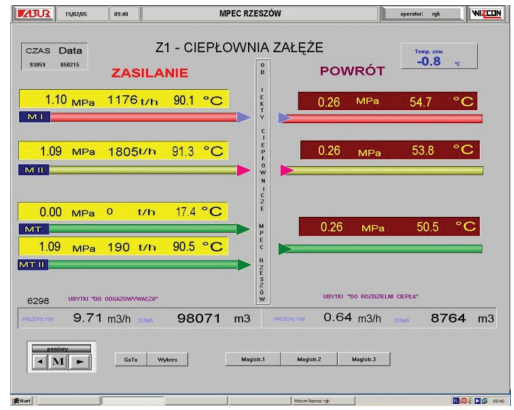


Figure 7. Control of parameters in the heat source.

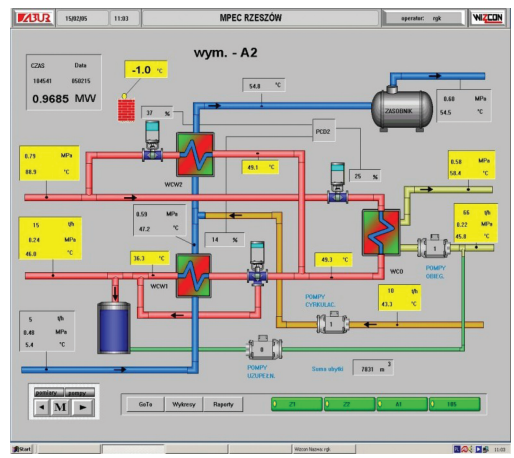


Figure 8. Control of parameters in the heat exchanger station.

- control the operating parameters of the heat exchanger stations and the individual components: pumps, valves (Figs. 8–9);
- control of the level of thermal power usage;
- monitor the carrier losses in heat sources and heat nodes which allows to detect and locate failure in the short-time (Fig. 10);
- control the work and read the level of heat and water meters;
- response immediately to emergency conditions that are reported by the system;
- compile reports concerning operation of individual objects;
- data archive;
- create graphical images of work for performing analysis.

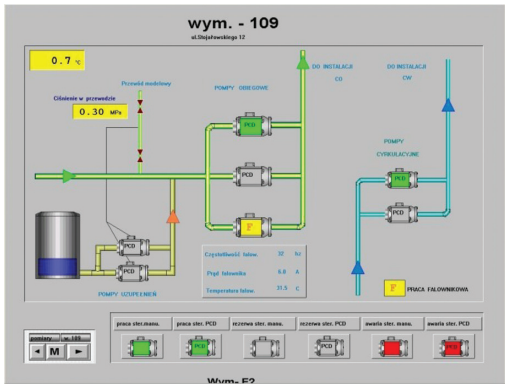


Figure 9. Synoptic image of the pumps control in a heat exchanger station.



Figure 10. Control of water losses in the heating network.

The parameters collected by the system in the form of HTML files, synoptic images, charts, the reports are made available through a network of computers to other users for further analysis.

One of the effects of the use of the possibilities offered by HSS telemetry is to reduce the heat losses and the heat transfer losses to a minimum.

There are many benefits from using Telemetry system, such as:

- conscious management of heat source operation, district heating network and thermal nodes through a solid, all-day control parameters of objects' work;
- disciplining operation of heat sources—enforcement of necessary parameters, the control of the heat carrier losses;
- raising the quality standards of the delivered heat to the customers—supplying adequate thermal power at the right time;
- optimization of nodes' work (number of pumps, pressure, flow—inverters, the level of thermal power usage, thermal comfort recipient);
- rapid detection and minimizing the effects of network's and nodes' failures;
- control of the indication of the measurement systems in heat exchanger and monitored stations;
- continuous monitoring of the heat carrier losses in heat sources and district heating substations;
- possibility of data archiving with the aim of pursuing analysis: daily, monthly, annual, triennial and different ones;
- the ability to verify and adjust the theoretical hydraulic calculations with real data.

Currently telemetry system is still being modernized and developed as well as new facilities are being connected.

6 SUMMARY

Optimal exploitation of HSS, directed to the proper reliability management, determines its proper operation. The variety of devices operating under extensive district heating system requires the support from modern IT systems. In order to maintain the reliability and security of heat supply to the customers, it is necessary to continuously improve and develop of monitoring and control tools, together with application of operating costs optimization.

Consideration of the indicated monitoring and control systems of operating parameters HSS together with reliable records of operational data is required for the proper management of reliability and security of the system. It allows to minimize or completely eliminate the risk of failure to supply heat to the customers.

REFERENCES

Babiarz B. 2005. An introduction to the assessment of reliability of the heat supply systems. Proceedings of the European Safety and Reliability Conference (ESREL 2005),115–121, *International Journal of Pressure Vessels and Piping,* Volume 83, Number 4/2006: 230–235, Elsevier.

Babiarz B. 2010. Reliability assessment of heat supply systems in their operational process. *Electronic Journal Reliability & Risk Analysis: Theory & Applications,* Vol. 1 No. 1, issue of March: 7–1.

Berg H.P. 2008. Risk and safety management—procedures, methods, experiences. *Summer Safety and Reliability Seminars,* Gdansk, Poland: 65–75.

Blokus A. 2006. Reliability analysis of large systems with dependent components, *International Journal of Reliability, Quality and Safety Engineering,* Vol. 13: 1–14.

Dou J., Chen W., Zhong Z. 2011. Operational reliability evaluation of ship-to-air missile weapon system. Systems Engineering and Electronics, Vol. 33, No. 4: 954–957.

Helseth A. 2008. Modelling Reliability of Supply and Infrastructural Dependency in Energy Distribution Systems *Doctoral theses at NTNU*: 1–72.

Kołowrocki K. 2013. On safety of critical infrastructures. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars,* Volume 4, Number 1: 51–72.

Myrefelt S. 2004 The reliability and availability of heating, ventilation and air conditioning systems, *Energy and Buildings* 36: 1035–1048.

Nowakowski T., Werbinska-Wojciechowska S. 2009. On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing,* vol. 6, nr 4: 364–378.

Nowakowski T., Werbinska-Wojciechowska S. 2010. Maintenance models—role of logistic support review. *Scientific Problems of Machines Operation and Maintenance*, 3(163): 45–64.

Ostrowski K. 2014a (in prep.) Operational reliability modeling at signalized intersection, Article accepted for *Journal of KONBIN* 2014.

Ostrowski K. 2014b (in prep.) Practical application of the reliability theory to the assessment of a signalised traffic lane, Article accepted for *European Safety and Reliability Conference ESREL*, Wroclaw 2014.

Peruzzi L., Salata F. Vollaro A. d L, Vollaro R. de Lieto. 2014. The reliability of technological systems with high energy efficiency in residential buildings. *Energy & Buildings* 68, Part A: 19–24.

Rak J., Babiarz B. 2001. Wstęp do symulacyjnej metody wyznaczania wskaźników niezawodności funkcjonowania i bezpieczeństwa systemów komunalnych *II Ogólnopolska Konferencja Naukowo-Techniczna.* Zakopane—Kościelisko, Poland: 311–320.

Rak J. 2007. Some aspects of risk management waterworks. *Ochrona Środowiska,* Vol. 29 Issue: 4: 61–64.

Rak J. 2009. Selected problems of water supply safety. *Environmental Protection Engineering,* Vol. 35, No. 2: 23–28.

Tchórzewska-Cieślak B. 2009. Risk management system in water-pipe network functioning. Proceedings of the European Safety and Reliability Conference ESREL, *Reliability and Risk Analysis: Theory Methods and Applications,* Vols. 1–4: 2463–2471.

Tchórzewska-Cieślak B. 2012. Urban Water Safety Management. *Chemical Engineering Transactions*. Vol. 26: 201–206.

Todinov M.T. 2006. Reliability analysis of complex systems based on the losses from failures, *International Journal of Reliability, Quality and Safety Engineering* 13 (2): 127–148.

Toktasynova N., Bazil G., Adilova S. 2014. Quality management system in heat supply operation. *Informatics Control Measurement in Economy and Environment Protection* 1/2014: 36–38.

Tracz M., Ostrowski K. Impact of capacity variability in different weather conditions on reliability of signalised intersections, *Proceedings* of *The 5th International Symposium on Transportation Network Reliability*, Hong Kong 2012: 901–916.

Valis D., Pietrucha-Urbanik K. 2014. Utilization of diffusion processes and fuzzy logic for vulnerability assessment. *Eksploatacja i Niezawodnosc—Maintenance and Reliability*, Vol. 16, no. 1: 48–55.

Valis D., Vintr Z., Koucky, M. 2010. Contribution to highly reliable items' reliability assessment. Proceedings of the European Safety and Reliability Conference ESREL, Prague, Czech Republic. Reliability, Risk and Safety: Theory and Applications. Taylor & Francis 1–3: 1321–1326.

Wojdyga K., Niemyjski O. 2012. Hydraulic analysis for a district heating system supplied from two CHP plants. *Energy & Buildings* Vol. 54: 83–86.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Uncertainty in the regulation systems of temporary organizations: A challenge for improving the organizational reliability

F. Mazzorana-Kremer, C. Martin & J.L. Wybo
Mines Paristech/CRC, Sophia-Antipolis, France

ABSTRACT: Mainstream economic and sociological theories tend to analyse organizations as permanent entities. However, industry provides many examples of organizations that are not permanent: construction projects, maintenance tasks, crisis management units, the decommissioning of nuclear plants, etc. In addition, classical theories that argue organizations should be long-lasting are inherited from the industrial revolution. Today, many organizations are becoming less rigid and are moving towards more flexible structures oriented to the short-term.

Temporary organizations differ from permanent organizations in that they are designed to have a short lifespan. They are generally created with a specific goal in mind and dissolved once this goal is reached. Different market players interact in these structures: they include distinct legal entities, freelancers or consultants who coordinate their work on a single site or from different geographic areas. Typically the temporary organization is linked to a permanent organization. In other cases, it is fully independent and those involved do not expect to work together once their objectives have been achieved. The unsustainable dimension of these organizations raises many issues in terms of risk and uncertainty.

This paper provides a better understanding of temporary organizations, their coordination, their regulatory systems and their links with the permanent parent organization (if there is one). The research described in this paper is based on a literature review. It provides a typology of temporary organizations and analyses their coordination, regulatory systems and reliability issues.

1 INTRODUCTION

The literature shows that a new trend has emerged in recent years: the increasingly widespread phenomenon of using temporary projects or organizations to perform some tasks or implement new services (Turner and Keegan, 2001; Lundin et al., 2003; Roy and Audet, 2002; Lundin and Söderholm, 1994; Whitley, 2006; Turner and Müller, 2003). This led to an increasing number of new, so-called temporary forms of organization. At the same time, most organizations have been subject to permanent and constant change (Bahrami, 1992; Lundin et al., 2003) which increased their reliance on ad-hoc temporary structures.

There are various kinds of temporary organizations in the industry (e.g. construction sites, periodic maintenance projects and crisis management units). They are defined by their ephemeral nature and modes of cooperation between actors which are different from the usual relationships found in traditional organizations. Often embedded into permanent organizations (particularly for large construction projects and periodic maintenance in complex socio-technical systems), these organizations show a high degree of autonomy and are subject to forms of internal and external regulation that are currently poorly understood.

With respect to safety culture, the autonomy and regulation modes found in temporary organizations can lead to divergence from the objectives of the parent organization.

Risk prevention research has so far shown little interest in the parent/temporary organization relationship (Bourrier, 1999) and in the impact of these relationships on organizational reliability. The purpose of this article is to present a typology of temporary organizations, based on a literature review, and to characterize the relationships between their organizational characteristics and the reliability of socio-technical systems.

In the first part of this article we define the temporary organization. In the second part we present the principal characteristics of this type of organization. Finally, we present an initial attempt to link these characteristics and organizational reliability.

2 UNDERSTANDING TEMPORARY ORGANIZATIONS

This section begins with a sample of definitions of temporary and project-based organizations.

Then we propose a definition of the temporary organization and summarize its main characteristics with respect to permanent structures.

2.1 *Definition*

Before discussing safety concerns and organizational characteristics, it is essential to first define what a temporary organization is.

Temporary organizations are, as the wording suggests, organizations that have the particular characteristic of being "temporary". Organizations are more commonly seen as social entities that have a collective goal; they often are characterized by actors, tasks, formal and informal governance rules, regulations and their environment. In this context, temporary organizations can be seen as collective structures, focused on a specific goal—like any other organization—but with a "temporary" dimension. This temporary dimension can be related to its ephemeral nature or because their duration appears to be much shorter than the average lifetime of traditional organizations. Their temporary nature means that they are set up to meet a specific goal and are dissolved once this goal is achieved.

Compared to research on traditional organizations, there is little current literature on temporary organizations. However, a certain degree of consensus exists on the characteristics of projects, which can be seen as a particular form of temporary organization. Therefore, in order to refine and improve our definition of the temporary organization, our review included articles related to projects.

Some definitions of temporary organizations and projects are presented in the Table 1.

Most of these definitions are global and implicit. We consider the Goodman definition as one of the most explicit. In practice, most researchers have explored the characteristics of temporary organizations rather than provided simple definitions.

From these definitions, we argue that a temporary organization is a collective and social entity set up for a limited period of time, in order to achieve a specific goal, and dissolved when the goal is reached.

In the next section, we review a selection of relevant articles in order to determine the main characteristics of temporary organizations with respect to permanent structures.

2.2 *Main characteristics of project-based and temporary organizations*

Turner and Müller (2003) offer some insight into the definition of a project as a temporary

Table 1. Definitions.

Reference	Definition of project/temporary organization
Goodman and Goodman (1976)	Temporary organizations involve "a set of diversely skilled people working together on a complex task over a limited period of time."
Keith (1978)	"Temporary systems are structures of limited duration that operate within and between permanent organizations."
Cleland and Kerzner (1985)	A project is "a combination of human and non-human resources pulled together into a temporary organization to achieve a specified purpose."
Turner (1990)	A project is "an endeavor in which human, material and financial resources are organized in a novel way, to undertake a unique scope of work, of given specification, within constraints of cost and time, so as to achieve beneficial change defined by quantitative and qualitative objectives."
Lundin and Söderholm (1994)	"Temporary organizations are almost always motivated by a need to perform specific actions in order to achieve immediate goals."
Packendorff (1995)	A project is "a given, plannable and unique task, limited in time, complex in its implementation and subject to evaluation."
Lundin et al. (2003)	"A project has a beginning and an end, and has none of the aspired continuity of the ordinary organization." "A project tends to pass through a series of phases during its lifetime." "Projects generally have two very characteristic features: they have been designed for a purpose so their existence is delimited in time from the moment of their creation, and they are focused on one primary task."
Turner and Müller (2003)	"A project is a temporary organization to which resources are assigned to undertake a unique, novel and transient endeavour managing the inherent uncertainty and need for integration in order to deliver beneficial objectives of change."
Janowicz-Panjaitan et al. (2009)	Projects are "one of many tangible manifestations of temporary organizations." According to the authors, "despite the great diversity of forms and activities temporary organizations undertake (…) temporariness is the only factor that is unique to TOs, while others are simply consequences or correlates thereof."

organization. They argue that projects are unique, special forms of organization, found in businesses that use innovative and transient processes. They view the project as an organization with a production function, a temporary organization and as an agency created to guide change, use resources and manage uncertainty.

In 1994, Lundin and Söderholm, in their theory of temporary organizations, presented action as the main concept of temporary organizations. They argue that temporary organizations are almost always "motivated by the need to perform specific actions to achieve immediate goals". They defined the temporary organization in terms of the contrast with permanent organizations and highlighted the following characteristics:

– it has a limited lifespan, which is established at the outset;
– typically, the creation of a temporary organization is motivated by a task that must be accomplished;
– it consists of a team that is put in place for a known, limited period. The skills and expectations of team members provide the commitment and motivation that will enable the organization to function and accomplish its task;
– it enables transition, a change.

These characteristics highlight that the temporary organization, or an internal project, is defined by its temporality and a task to be accomplished.

However, if the temporary organization is completely assimilated to the project, there is a risk of overlooking the collective dimension of the organization. In practice, 'organization' usually refers to a set of individuals and resources that are coordinated in order to meet a shared goal (Simon, 1983). The organization is therefore often characterized by resources, individuals, the rules governing their relationships and their behaviour in order to maximize the chances of achieving the collective goal.

From this point of view, the concept of the temporary organization refers to the collective nature of action. Here, the approach put forward by Packendorff (2002) differs significantly from others and is a useful addition to our argument. The author reminds us that the literature usually defines the project as focused on a given task, which is unique, follows a set timetable, is time limited, complex to implement and evaluated. Packendorff argues that projects are often seen as tools. Little attention is given to the motivation of the individuals who participate in them; although in practice they suffer from the same dysfunctions as other organizations. He therefore suggests that "Projects should be researched in terms of culture, conceptions, relations to the environment, longitudinal processes, etc., rather than simply as goal-fulfilling

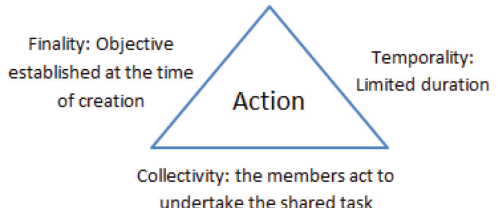


Figure 1. The key dimensions of temporary organizations.

subsystems whose *raison d'être* is provided by a decisive and strategically aware super-system."

According to Packendorff (2002), the project is a temporary organization. However, while a project is generally seen as a "tool" and only implies a user perspective, a temporary organization is constantly embodied by individuals who are continually learning from their experience and who expect to learn more. This suggests that research into temporary organizations should focus more on the actors, their expectations, their actions and what they learn.

This last point underlines the need to understand the collective dimension of this type of organization. We argue that the context for the temporary organization is unstable and that its existence coincides with the achievement of an action. Specifically, it is defined by three fundamental characteristics that distinguish it from the permanent organization or project: its temporality, its predetermined time-sensitive objectives and the collective nature of the action.

The analysis of a temporary organization as an organization and not as a project invites us to also examine its actors, their expectations, and the problems of leadership, control and coordination.

In the next section we focus on the relationship that a temporary organization has with a permanent organization that is responsible for its creation.

2.3 *The relationship between temporary organizations and the permanent parent organization*

It is reasonable to ask what motivates the creation of a temporary organization. Some researchers, such as Modig (2007), highlight the stronger or weaker relationships that may exist between a temporary organization and the permanent organization responsible for its creation. Others (Turner and Keegan, 2001; Turner and Müller, 2003) analyse the temporary organization in terms of a project and see it as a way for a permanent organization to assume a production function while managing the

uncertainty of change. It can also be the genesis of an organization (Lundin and Söderholm, 1994); for example the result of an entrepreneurial effort.

In the case where a permanent organization is responsible for creating a temporary organization, the latter generally pursues objectives that are in the interests of, and in line with those of the parent company.

In the case where a temporary organization fully independant is created, typically in response to an identified need, one or more individuals form its nucleus. In this case, the time-limited nature of the organization is more dependent on the positive motivation of its instigators. This is particularly the case with start-ups and organizations that are designed to make a short-term capital gain or profit.

We note that if a temporary organization is linked to a permanent parent organization, its collective objectives are likely to be linked to the interests of the parent organization. If this is not the case, collective objectives will have been set by one or more individuals before the temporary organisation was created and will correspond to their expectations or interests (financial added value, sporting or artistic events, humanitarian commitments, etc.).

In the next section we analyse its modes of operation as an organization.

3 THE CHARACTERISTICS OF THE TEMPORARY ORGANIZATION

As the temporary organization is a form of organization, it is interesting to analyse how it implements collective action and what issues arise related to decision-making, control, coordination and conflicts.

In this section, we look at how the temporary organization operates (particularly collectively) and we aim at highlighting the characteristics that make it different from the permanent organization, in order to understand the risks and uncertainties specific to this type of structure.

The temporary organization is, as an organization, in part defined by its objectives and the tasks to be accomplished to meet these objectives, which are assigned to people at different levels of the hierarchy (Simon, 1983). Many conditions are necessary to achieve these collective goals. Here we look in more detail at the following:

- The bond of individuals with the organization. The activities of a group of people are only organized to the extent that they allow their bond with the organization to control their decisions and behaviour (Simon, 1983, p.99): this bond is possible only when "directly or indirectly their activity within it contributes to achieving their own goals."
- The definition and coordination of tasks, which makes it possible to centralise decisions, define the roles of members of the organization and achieve the collective goal.
- The exercise and respect for authority, which ensures the necessary coordination between actors and tasks.
- Communication, which enables the transmission and processing of the information necessary for decision-making and for the execution of tasks within the organization.

In the following sections, we analyse to what extent these conditions are met in a temporary organization.

3.1 *Individual bonds with the organization*

For an organization to function according to its initial objectives, these objectives must be compatible with those of the individuals and the objectives of the individuals must also be compatible with the organization's limited timeframe.

In practice, when members of a temporary organization are linked to or employed by its parent organization(s), they are likely to support the project if it improves their remuneration or promotion prospects. A permanent organization that prospers and grows rapidly can offer greater prestige and promotion opportunities (Simon, 1983, p.105). This means that an individual seconded by the permanent organization is likely to value the positive impact it may have on its career, once the collective goal has been met.

However, in cases where individuals working in the temporary organization are not seconded by a permanent structure, their commitment to the goals of the organization will probably depend on the potential beneficial effect on their future career, once the structure has been dissolved. In this case, their motivation may be shaped by substantial financial benefits related to the achievement of collective goals or the hope of better employability in future structures. This is only possible if their work has had high visibility *vis-à-vis* external actors. This idea has been put forward by Modig (2007) and Packendorff (2002) in particular, who argue that the duration of the involvement of actors and their relationship with a permanent parent organization, if any, will influence their behaviour. People who are hired for a limited time by a temporary structure will be more loyal to their network or other potential professional partners than members of the organization. This is explained by the fact that they seek to secure future employment or contracts. "There is a risk that employees whose future work opportunities or position in an organization are dependent on their visibility in earlier projects […], will act opportunistically" (Modig, 2007, p. 810).

In this section we have shown that the bond that individuals form with a temporary organization is not the same as that found in a permanent organization. We also have seen that the members of the organization have a different motivation when they are employed by a permanent parent structure than when they are completely independent; the latter case can present a risk of opportunism and departure from collective goals.

We now examine issues related to the definition and coordination of tasks in temporary organizations.

3.2 *The definition and coordination of tasks*

According to Simon (1983, p. 124), the purpose of coordination is that all members of the group adopt the same decision or, more specifically, take consistent decisions, which when combined, achieve the intended goal. According to the same author, there are two types of organizational coordination: "form", which defines the domain of competence and the limits of the authority of each worker and "substance", which specifies the nature of the task for the individual (e.g. drawing up strategy).

According to some authors (Modig, 2007; Oerlemans et al., 2009), the definition of rules and tasks in a temporary organization depends on the role and involvement of the parent company(s) that it is linked to. In particular, research carried out by Modig (2007), although conducted on a small sample, suggests that, "the more involved a stationary 'parent' organization is in a project, the more guidelines are given as to how the temporary organization is to perform its task." However, according to the author, "Temporary organizations that are 'pure' or virtually 'pure' instead have to develop routines and procedures internally."

Modig adds that, "If work roles, relations and required skills and competencies are well defined, this can reduce the risk for rivalry and conflicts in temporary organizations and facilitate the training of new employees." It also allows the transfer of accumulated knowledge from one project to another, with the advantage of making organizations more competitive and mistakes more easily avoidable. The counterpart is that when rules are predefined, then an element of flexibility and creativity in the organization is lost. In this case, "members of temporary organizations might be more restrained than helped in their work by predefined work processes, as these can hinder them from using their knowledge and skills to develop work routines that match the unique project conditions." Modig (2007).

Oerlemans et al. (2009, p. 36) looked at collaborative temporary organizations in several German Small- and Medium-sized Enterprises (SMEs). Based on a survey of 1,500 SMEs having participated in collaborative programs, the analysis focused on the management style chosen by the organization and founded, on the basis of four case studies, that they were managed in different ways (Table 2).

Other work (Janowicz-Panjaitan et al., 2007) focuses on the literature concerning project coordination or temporary organizations. The authors argue that temporary organizations are generally less formal and normative than permanent organizations. In addition, they have fewer hierarchical processes and bureaucracy and make greater use of interpersonal coordination. However, one example of interpersonal coordination is trust, and it can be difficult to build trust in a context where

Table 2. Characteristics of temporary organizations highlighted by Oerlermans et al. (2009).

	No further collaboration once the project has ended	Ongoing collaboration between companies once the project has ended
Collaborative project under 36 months (average)	Case 1: film production Coordination is provided by a specific role such as a "director" or "general contractor". Hierarchical roles Work takes places in a specific timeframe with contractual deadlines that are fixed according to the phases of the project Personal relationships are only important for a few key players	Case 3: network alliances Coordination is provided by the lead company that provides products and services Deadlines and roles contractually defined Work takes place according to the phases of the project Relationships between partners continue from one project to another
Collaborative project over 36 months (average)	Case 2: crisis management Coordination is provided by a third party Hierarchical roles Working patterns are learned and respond to the needs of the crisis Little priority is given to personal relationships	Case 4: major construcion project Coordination is handled by the lead company or the government agency Work takes place according to the phases of the project

time is limited. To explain this, the authors refer to the work of Ness and Haugland (2005), which shows that even in a short-term collaboration, relational norms and trust develop. According to the authors, "while hierarchical control mechanisms can supply the necessary confidence level, the trust that is necessary to assure sufficient information sharing for problem solving does evolve despite the temporary nature of a project".

The examples cited above lead us to the following conclusions:

The definition of the roles and tasks in a temporary organization is often carried out upstream by the permanent parent organization(s) if there is one, and when there are strong links with it (Modig, 2007). However, if this is not the case, it is carried internally, by the temporary organization itself;

When a collaboration implemented by the temporary organization must be renewed after its dissolution, the lead parent company usually coordinates tasks and actors (Oerlemans et al., 2009). On the other hand, in cases where it is unlikely that the collaboration will be renewed, coordination is undertaken by a dedicated person or group belonging to the temporary organization.

Finally, temporary organizations generally have fewer formal coordination and bureaucratic processes and rely more on the interpersonal skills of their members. These informal processes require a minimum level of trust to ensure collaboration and the resolution of problems.

In the next section, we analyse the different management styles that are implemented, which make it possible for this type of organization to successfully meet its objectives.

3.3 *The managerial dimension of the temporary organization*

In an organization, management and authority are necessary to ensure respect and the coordination of tasks. Authority, according to Simon (1983, p. 119) is the relationship that coordinates the behaviour of a group by subordinating the decisions of an individual to those that are communicated by others. Individuals particularly respect authority under the following conditions: when the person who gives the orders (typically the project manager or the director of the temporary organization) is recognized as competent by peers and subordinates; when the individuals who receive the orders are responsible and naturally accept authority; when the person giving the orders has the power to sanction; when authority does not come from several persons giving contradictory orders; when the given tasks are consistent with the personal goals of the individual.

These criteria raise the question of the coexistence of several management teams. If the temporary organization does not have its own management structure, including a command unit, there is a risk of conflicts or problems with authority.

Research by Oerlemans et al. (2009) highlighted three management configurations in temporary collaborative organizations in German SMEs: co-management by several parent organizations, management by one of the parent organizations, or management by a dedicated, project-specific team. In general, each of the three cases occurs equally often. The exception is collaborative projects with few parent organizations, in which case co-management by parent organizations is found more often.

According to Turner and Keegan (2001), uncertainty about the product and process is greater in the project context than in a classical organization or business. Simple routine management by the permanent parent organization, when there is one, may not be sufficient for the project; it may prove unsuitable and raise the risk of error, opportunism and lack of customer satisfaction.

Turner and Keegan highlight that such projects need a governance interface between them and routine operations, beyond the normal hierarchy. They argue that, in addition to the project manager who manages the project's processes, the governance structure is based on two key roles: the broker and the steward. The role of the broker is to maintain and monitor the relationship(s) with the client(s): they ensure that deliverables and products meet the expectations and needs of customers. The steward "puts together the network of resources to deliver the project, ensuring that the right people are in the right place at the right time to ensure it happens."

For the authors, depending on the type of project organization (if they manage one or multiple projects, or one or many clients), the roles of the broker and the steward will be more or less important and may be partially assumed, or not, by the project manager. In all cases, the authors note that these roles should be separate and this is what is seen in practice. There is a psychological explanation, "the broker must align with the culture of the client, whereas the steward must align with the culture of the competence pools." "The broker is essentially an extrovert, entrepreneurial role, whereas the steward is essentially an introvert, intrapreneurial[1] role."

The examples cited above lead us to the following conclusions concerning the management and governance of temporary organizations or projects:

- There are three types of management in temporary organizations: co-management by many

[1] a person who while remaining within a larger organization uses entrepreneurial skills to develop a new product or line of business as a subsidiary of the organization.

permanent parent organizations, management by one of the parent organizations, or management by a dedicated, project-specific team. (Oerlemans et al., 2009). When there are parent organizations, there is no real trend; the exception is where there are few of them, in which case it is more often that case that management is exercised by the parent organization(s).

- Whatever type of management is in place, authority must not emanate from several hierarchical superiors who manage the same tasks and may give contradictory orders.
- When there is a permanent parent organization there should be an interface between the governance of the parent organization and that of the temporary organization (Turner and Keegan, 2001). Three key roles make this possible:
  - Theprojectmanager, who manages all of the project's processes.
  - The broker, who checks that the services or products meet the client's expectations and constraints.
  - The steward, who organizes and mobilizes the human and technical resources necessary to obtain the services and products defined or re-defined by the broker.

The latter two roles make it possible to manage on the one hand the bilateral dependency between the client (which may be the parent organization) and the project team and, on the other hand, uncertainty surrounding the product or service undertaken.

The question of authority and management is therefore important in a temporary organization as, very often, several independent individuals or structures coexist. When different control structures are shared, it is essential that they ensure the efficient coordination of tasks within the timeframe and budget constraints initially set. The next section is dedicated to another key parameter for the proper functioning of the organization: communication.

3.4 *Communication in the temporary organization*

Communication is another key element in the organization as it enables it to carry out its objectives collectively. In particular, it enables the transmission and processing of information necessary for decision-making and the execution of tasks within the organization.

According to Simon (1983), there are two types of communication in an organization: formal and informal. The formal communication system is implemented notably by discussions, letters, circulars, reports and should, according to the author, be sufficiently well organized and robust to ensure that actors and their personal interests cannot weaken the organization. The informal communication system "is built around the social relations of the organization's employees." This latter type of relationship is created spontaneously by individuals to advance their personal goals or collectively to establish their power within the organization, "it could be said that the weakness of the formal system of communication and the ensuing lack of coordination appears to encourage the formation of cliques" (Simon, 1983, p. 143). Here, cliques mean a group of individuals united by a common interest that differs or even goes against the collective interest of the organization.

Therefore, the question that arises in a temporary organization concerns the robustness of the formal communication system, which is necessary to avoid the formation of cliques that may divert the organization from its objectives. However, the limited duration of such an organization is likely to make it difficult to set up a formal communication system if it is not inherited from a permanent parent organization.

Some of the research mentioned above sheds light on the functioning of communication and the exchange of information in temporary organizations. According to Modig (2007), "All organizations need a variety of resources to perform their activities. Thus, easy access to key resources such as skilled professionals, vehicles, tools and suppliers facilitates project work considerably." The author also points out that in a temporary organization there is insufficient time and above all, a shared history to be able to implement channels for the dissemination of knowledge and information. Generally, a permanent parent organization that has a strong influence on the temporary organization will ensure that its actors have access to the resources and information necessary to meet their objectives.

For Turner and Keegan (2001), communication issues are closely related to issues of governance, which defines and provides the means to achieve a project's objectives (Müller, 2009; Turner, 2009). Communication is thus one of the problems of governance. Turner and Keegan (2001) argue that communication within a project structure is made possible and efficient through the roles of the broker and steward defined above. In order to analyse the internal and external communication needs of projects, the authors define four types of project-oriented organization: multiple small projects with a few large clients; multiple projects with multiple clients; major projects with a few large clients; and finally the start-up (comparable, according to the authors to a project associated with multiple clients).

The authors conclude that in the case of organizations managing multiple small projects with a few large clients, the role of the broker is extremely

significant. In this scenario project teams are often relatively independent and it is important that communication is maintained at the interface between them and clients to ensure that the product and the service develop according to the needs of the client. In the case of a multiple projects with multiple clients, the role of the broker is as important as in the previous case but must be complemented by a strong steward who works with the broker to ensure that project teams receive the right resources in order to deliver the expected service or product. In the case of major projects with a few large clients, they note that the project manager has a direct relationship with the client and plays the role of broker. However, in the start-up case they suggest the opposite: the director (who is usually the originator of their product) plays the role of steward and ensures both internal communication and communication with suppliers in order to carry out tasks and deploy resources, while they rely on a broker for external communication.

This research suggests that communication is a key element in the temporary organization due to uncertainty about its services or products; the behaviour of actors makes it increasingly necessary to put in place functions that ensure communication between the permanent parent organization, the client (or the recipient of the goods or services), and the organization's actors.

There is less risk of cliques being created in organizations if actors' roles are defined and there is (for example through the permanent parent organization) a formal structure to ensure communication at the interface between external actors (the client) and organizational resources (suppliers and employees).

3.5 *Conclusions concerning the characteristics of temporary organizations and their regulatory systems*

Our review of the literature shows that various authors (Whitley, 2006, p.79; Lundin and Söderholm, 1994; Turner and Cochrane, 1993; Oerlemans et al., 2009, p.36; Turner and Keegan, 2001; Modig, 2007) have drawn up typologies of temporary organizations, showing that they can be distinguished from each other based on their proximity to the parent organization, the repetitive nature of their objectives, their intra or inter-organizational nature, or the tasks performed (a project to be developed, a new product or market, etc.).

A temporary organization thus appears to be a complex system composed of individuals that are independent or dependent of permanent structures and who interact with each other (whether they are employees of the same company or not), external actors, their network, clients and other businesses.

In these organizations, coordination and communication will naturally orient the behaviour of actors. However, we have seen that these measures, because of the temporary nature of the organization, are often informal and different to the relationships usually found in permanent organizations.

Returning to the work of Turner and Keegan (2001), temporary organizations operate through the action of a few key players: the project manager, the broker and steward, who are responsible for integration and coordination. Other studies (Modig 2007; Oerlemans et al., 2009; Turner et Cochrane, 1993) show that coordination, authority and communication, which contribute to the regulation of these atypical systems, are also conditioned by external systems such as the permanent parent organization, which is linked to the temporary organization.

Therefore, there is a great uncertainty with respect to the ways in which the actors and subsystems of these organizations regulate themselves in order to reconcile interests, individual behaviours and collective goals.

4 TEMPORARY ORGANIZATIONS AND RELIABILITY ISSUES

In this section, we examine two types of risk: risks created when the temporary organization is conceived and risks associated with the temporary nature of this type of organization.

4.1 *Risks insufficiently taken into account in the design phase*

The analysis of the characteristics of temporary organizations has shown that tasks can be organized upstream, by the permanent organization or the temporary organization itself (if it is semi-independent). However, most of the time, as is the case for temporary organizations established for infrastructure projects (power plants, construction sites) or decommissioning (end-of-life oil fields, nuclear power plant decommissioning or waste treatment installations, etc.), operating budgets are often set in advance. This predetermined factor makes it difficult to assess the technical and financial risks once the temporary organization has been established and its tasks have been defined. Safety issues often appear after the design of a project has been fixed and its budgets determined by the various companies involved (Koppenjan, 2001), "Since finding a balance between various interests is a delicate matter, such a disturbance may even jeopardize the realization of the project." This issue raises two fundamental problems: first, when the temporary organization is initiated, there is a need to define and anticipate risk upstream so that

the project's budget and its capacity are correctly assessed; second, the interests of key individuals in the organization must not be an obstacle to the communication of any difficulties encountered as the project progresses—even if this jeopardises the entire project and raises questions about the personal interests of individual stakeholders.

Similarly, the flexibility of temporary organizations, which is based on good interpersonal communication (that is more informal than formal) raises ethical issues. In particular, how is it possible to ensure that project managers and other key individuals will communicate with each other and disclose safety issues that appear once the structure is in place, if their personal interest is limited to their role in the temporary structure and the achievement of objectives? We argue that there is currently insufficient research into the methods and formal systems (both in terms of communication and governance), which should be implemented upstream in temporary organizations to ensure that technical and human risks and divergences from objectives are given sufficient weight. Serious care should be taken to the control modes of actors, which take into account the risks incurred during and after the lifespan of the temporary organization.

4.2 *Risks related to the temporary nature of the organization*

As we have shown, definitions of temporary organizations highlight their limited duration, task orientation and uncertainty. We argue that these criteria lead to specific risks.

First, one of the most important features of temporary organizations is their limited duration. This short lifetime, according Janowicz-Panjaitan et al. (2009) leads to several problems including: lack of time to develop a relevant shared knowledge base, to plan organisational change and to develop trusting long-term interpersonal relations. Furthermore, the author refers to the work of Weick (1993, p. 644) to highlight the fact that the organization, when viewed in the short term, prevents its members from developing goals that transcend their personal interests.

On the other hand, Janowicz-Panjaitan et al. (2009) suggest that when time limitations and the date or the conditions for the dissolution of the organization are known by its members from the beginning, they will feel under greater time pressure than in classical organizations. The work may become more pressurised and is therefore more likely to lead to deviations or errors than in conventional organizations.

Similarly, the uncertainty inherent to temporary organizations may pose more problems than in permanent organizations. Team members have less shared task knowledge; collective learning is lacking and the uncertainties faced by members of the organization must be managed, starting from their ability to communicate and identify problems.

The task-oriented character of temporary organisations makes their members more focused on getting the work done, which can lead to improved performance. On the other hand, they will be less influenced by other factors; the environment and potential risks are not likely to be priorities, due notably to the "emergency" requirement to achieve objectives.

Finally, the time-limited and task-oriented nature of the temporary organization raises issues of psychosocial risk and organizational reliability. Individuals in these organizations are likely to be under more pressure; in addition they are less likely to be loyal to an organization that is doomed to be quickly dissolved than a permanent organization.

5 DISCUSSION

Based on a literature review, our research consisted in describing temporary organizations that we first defined as "collective and social entities set up for a limited period of time, in order to achieve a specific goal". It appears to us that key features of such organizations are their temporariness, their set-in-advance objectives as well as their collective nature. They also are often linked to permanent parent structures and such link can naturally impact the nature of their tasks and goals.

We have highlighted some of the characteristics of temporary organizations: they generally have fewer formal coordination and bureaucratic processes; they rely more on the interpersonal skills of their members; they need specific roles—between their working staff and their external environment—in order to ensure an efficient communication and a proper completion of their tasks.

Thus, our analysis leads us to see them as atypical and complex structures. Such complexity, associated with a high level of autonomy, seem to raise many issues in terms of risk and reliability. First of all, it is obvious that the limited duration of temporary organizations can represent a stressful environment for individuals. It also let little time for the creation of a common knowledge necessary for the successful completion of the collective tasks and goals. Secondly, because the tasks, objectives and financial budgets of such organizations are often determined in advance, an afterwards emerging risk might endanger their survival much more than in a permanent organization. For these reasons, when they are linked to a permanent parent company, project managers, or some other key players, may be reluctant to communicate problems if

these ones endanger the survival of the temporary organization they are involved in.

Therefore, the issue of the reliability of temporary organizations with respect to the parent organization needs more research founded in organizational theory and oriented towards the energy sector where this type of organizations is widespread and the safety stakes are high.

REFERENCES

Bahrami, H., 1992. *The Emerging flexible organization: perspectives from Silicon Valley*. California Management Review, Summer 1992, 33–52.

Bourrier, M., 1999. Le nucléaire à l'épreuve de l'organisation. Le travail humain, Paris, Presses universitaires de France, 294p.

Cleland, D.I. and Kerzner, H.A., 1985. *Project management dictionary of term*s. New York: Van Nostrand Reinhold.

Goodman, R.A. and Goodman, L.P., 1976. Some management issues in temporary systems: a study of professional development and manpower—the theatre case, *Administrative Science Quaterly*, 21, 494–501.

Janowicz-Panjaitan, M., Bakker, R.M. and Kenis, P., 2009. Research on temporary organizations: the state of the art and distinct approaches toward temporariness. In Kenis, P., Janowicz-Panjaitan, M., and Cambre, B. (Eds.). *Temporary Organizations: Prevalence, logic and effectiveness.* Northampton, MA: Edward Elgar.

Keith, P.M., 1978. Individual and organizational correlates of a temporary system, *The Journal of Applied Behavorial Science*, 14 (2), 195–203.

Koppenjan, J., 2001. Project development in complex environments: assessing safety in design and decision-making. *Journal of contingencies and crisis management*, Vol. 9 (3), 121–130.

Lundin, R.A., Runólfur, S., Steinhórsson, R. and Audet, M., 2003. Studying organizations as temporary. *Scandinavia Journal of Management*, 19, 233–250.

Lundin, R.A. and Söderholm, A., 1994. A theory of the temporary organization. *Scandinavia Journal of Management*, 11, 437–455.

Miles, M.B., 1964. On temporary systems, in M.B. Miles (ed.), *Innovation in education*. New York, NY: Teachers, College, Columbia University, pp. 437–490.

Modig, N., 2007. A continuum of organizations to carry out projects. *International Journal of Project Management*, 25, 807–814.

Müller, R., 2009. *Project governance. Fundamentals of Project Management Series*, Gower Publishing: Aldershot, UK.

Ness, H. and Haugland, S.A., 2005. The evolution of governance mechanisms and negotiation strategies in fixed-duration interfirm relationships, *Journal of Business Research,* 58, 1226–1239.

Oerlemans, L., de Kok, J. and de Jong, J., 2009. The prevalence and characteristics of interorganizational temporary collaborations of Dutch small and medium sized firms (SMEs). In Kenis, P., Janowicz-Panjaitan, M., and Cambre, B. (Eds.). *Temporary Organizations: Prevalence, logic and effectiveness.* Northampton, MA: Edward Elgar.

Packendorff, J., 1995. Inquiring into the temporary organization: new directions for project management research. *ScamL Journal of Management*, Vol. 11 (4), 319–333.

Packendorff, J., 2002. The temporary society and its enemies. Projects from an individual perspective. In: Sahlin-Andersson, K. and Söderholms, A., editors. *Beyond project management: New perspectives on the temporary—permanent dilemm*a. Malmö: Liber ekonomi, p. 348.

Roy, M. and Audet, M., 2002. La transformation vers de nouvelles formes d'organisation plus flexible: un cadre de référence. HEC Montreal. Gestion, Vol. 27, p. 43–49.

Simon, H.A., 1983. Administration et processus de décision. *Economica*, French translation.

Turner, J.R. and Cochrane, R.A., 1993. Goals-and-methods matrix: coping with projects with ill defined goals and/or methods of achieving them, *International Journal of Management,* 11 (2), 93–102.

Turner, J.R., 1990. *What are projects and project management?* Henley Working Paper 9002. Henley-on-Thames: Henley Management College.

Turner, J.R. and Keegan, A., 2001. Mechanisms of governance in project-based organization: Roles of the Broker and Steward. *European Management Journal*, Vol. 19 (3), 254–267.

Turner, J.R. and Müller, R., 2003. On the nature of the project as a temporary organization. *International Journal of Project Management*, 21, 1–8.

Turner, J.R., 2009. *The handbook of project-based management* (3rd ed.). New York, NY: McGraw-Hill.

Weick, K.E., 1993. The collapse of sensemaking in organizations: The Mann Gulch disaster, *Administrative Science Quarterly,* 38, 628–652.

Whitley, R., 2006. Project-based firms: New organizational form or variation on a theme? *Industrial and Corporate Change*, 15 (1), 77–99.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Solutions and safety barriers: The holistic approach to risk-reducing measures

A. Sevcik & O.T. Gudmestad
University of Stavanger, Norway

ABSTRACT: Currently in the offshore industry on the Norwegian Continental Shelf (NCS), there is much discussion about barriers and the interactions between them. This discussion is fostered to a large extent by the Norwegian Petroleum Safety Authority's (PSA) emphasis on safety barriers. The term 'safety barriers' refers to the measures used to reduce the likelihood and limit the consequences of major accidents. However, the question is whether safety barriers are the only measures for risk reduction. This paper will describe the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the Petroleum Safety Authority Norway (PSA). Two main groups of risk-reducing measures are distinguished: (1) technical, operational and organizational solutions applied to the critical systems and (2) safety barriers. The main focus in this paper is the demand from the Norwegian offshore industry for clarification of the term 'safety barrier'.

1 INTRODUCTION

Generally, risk treatment may be seen as a process which ensures that an acceptable risk level is achieved and maintained. To align with the Norwegian Petroleum Safety Authority regulations, Sections 4 & 5 of the Management Regulations are followed (PSA 2014a & PSA 2014b):

- In reducing risk […] the responsible party shall select technical, operational and organizational solutions that reduce the probability that harm, errors and hazard and accident situations occur.
- Furthermore, barriers as mentioned in Section 5 shall be established. The solutions and barriers that have the greatest risk-reducing effect shall be chosen […].
- Barriers shall be established that:
  - reduce the probability of failures and hazard and accident situations developing,
  - limit possible harm and disadvantages.

Two main groups of risk-reducing measures are named: risk-reducing solutions and safety barriers (Sevcik & Gudmestad 2014).

On further assessment of the definitions provided, it may be stated that risk-reducing solutions are the measures to reduce the likelihood of errors, hazards and accident situations occurring, i.e. preventing hazards (potential source of harm) from being realized. In other words, the solutions are used to reduce the likelihood of such deviations which could initiate (trigger) an unwanted chain of events. Systems that are primary targets of these solutions may be seen as Safety Critical Systems (SCS) and will be discussed further in the paper.

Safety barriers are the measures which are selected after the risk-reducing solutions have been established, with the purpose of reducing the likelihood of failures and hazards, preventing accident situations from developing and limiting the possible harm caused by an unwanted chain of events. Safety barriers are established to reduce the likelihood of the development of an unwanted chain of events when an initiating (triggering) event has already occurred, i.e. a hazard scenario has already started. The main and only function of a barrier is a safety function that is required on demand.

While we make a distinction between the risk-reducing solutions and safety barriers, it is important to see both of them as one entity designed to reduce the risk within performed activities.

2 RISK-REDUCING MEASURES IN AN ACCIDENT MODEL

2.1 *Generic accident model*

In line with ISO 17776 (2000) and its general hierarchy of risk-reducing measures, this work will propose the following risk-reducing phases as generic safety functions: Prevention, Detection, Control, Mitigation and Emergency Response. These functionalities act in the same sequence when placed on the chain of accident development (Fig. 1).

The term 'prevention' can be used with several meanings. In line with ISO 13702 (1999), prevention means a reduction of the likelihood of a

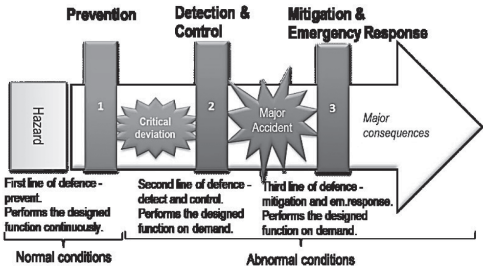


Figure 1. General accident model with safety functions.

hazardous event, and a further specified definition is used in this paper: to prevent means *to reduce the likelihood that a critical deviation occurs,* where critical deviation is seen as an initiating event of an unwanted chain of events.

While the term 'detection function' is commonly understood, the term 'control function' has several different interpretations. ISO 13702 defines control as the limitation of the extent and/or duration of a hazardous event. In this paper we further specify the term and state that control means *to reduce the likelihood that a critical deviation will develop into a major accident once it occurs*, i.e. to stop the unwanted chain of events when critical deviation occurs.

A major accident is the result of the failure of the safety-related solutions (prevention) and detecting/controlling barrier systems. In order to limit or reduce the consequences of an accident, mitigating barrier systems are established together with emergency response measures. The successful functioning of these systems will ensure the lowest feasible harm by stopping the accident escalation as soon as possible. If the mitigation and emergency response barrier systems function poorly, the accident may develop to its full potential and cause maximal damage.

2.2 *Risk reducing measures as systems*

Currently the industry uses the term 'Safety Critical Element (SCE)' to define all the elements that are "such parts of the installation […] which could cause and contribute substantially to a major accident or a purpose of which is to prevent or limit the effect of a major accident" (Dhar 2011). According to the concept presented in this paper, the boundaries of the SCE would embrace parts of the installation which could cause or contribute to a major accident (Fig. 2).

A Safety Critical System (SCS) is described as a system with applied technical, operational and organizational solutions designed to prevent the realization of a potential source of harm inherent

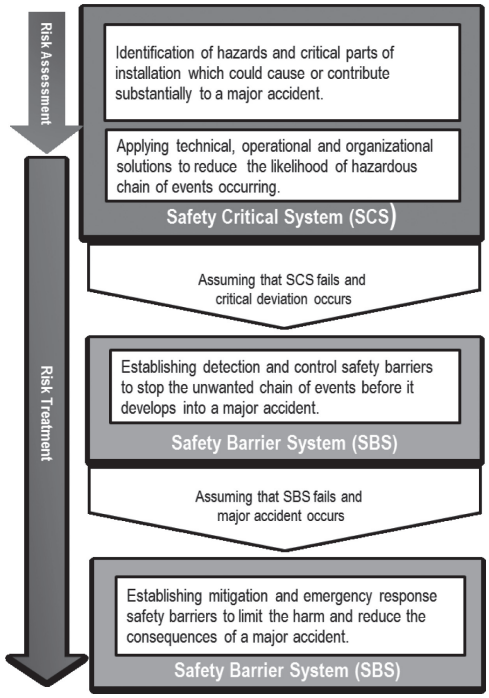


Figure 2. Establishing SCS and SBS of an installation.

in the activities. The requirement to perform is constant. In the case of a system failure, a critical deviation will occur and start the development of an unwanted chain of events (Fig. 3).

The Safety Barrier System—SBS—will embrace the elements of independent safety systems that are installed only for the safety function and in the case of failure will stop the accident's development or limit the effect of an accident (Figs. 4–5).

It is important to see a barrier as an actually established measure that is able to prevent or stop the unwanted chain of events once the initiating event is triggered. Safety principles for nuclear power plants distinguish barriers as physical measures only, while other types of protection are recognized but not defined as barriers (IAEA 1999). Organizational safety measures, such as procedures, strategies, guidelines, requirements, etc., can be seen as part of a regulatory basis that is used to establish the barriers, but they are not barriers in themselves. There is considerable eagerness are a lot of intentions to name them as organizational barriers; however, they cannot be seen as actual barriers that would be able to perform in the case of need. Either physical equipment—a technical barrier—or human actions—an operational barrier—can actually stop the unwanted chain of events that has already started due to the specific

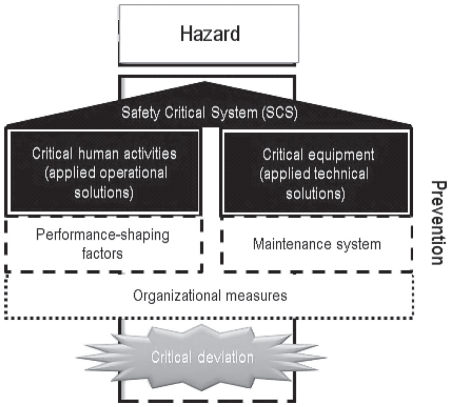


Figure 3. SCS for prevention.

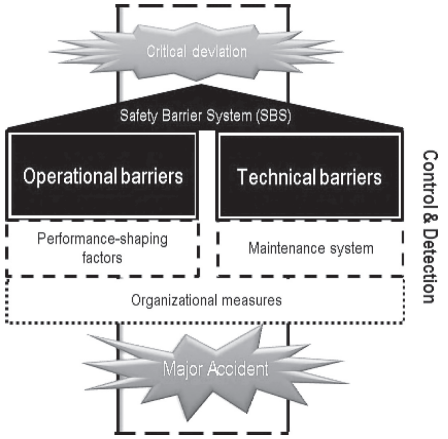


Figure 4. SBS for detection and control.

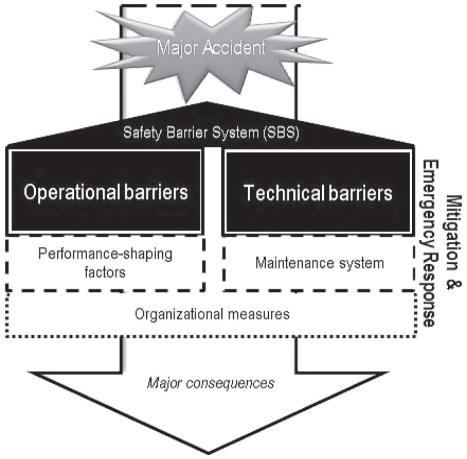


Figure 5. SBS for mitigation and emergency response.

Table 1. SCS and SBS comparison.

Safety Critical System (SCS)	Safety Barrier System (SBS)
Technical, operational and org. solutions applied to process, utilities, structural, etc. elements to reduce risk.	Independent system designed only for risk-reducing functions.
Reduces the likelihood of critical conditions occurring.	Reduces the likelihood of critical conditions developing and limits the harm.
Requirement to perform—constant (normal conditions).	Requirement to perform—on demand (abnormal conditions).
Cannot be removed without affecting process.	Can be removed without affecting process.

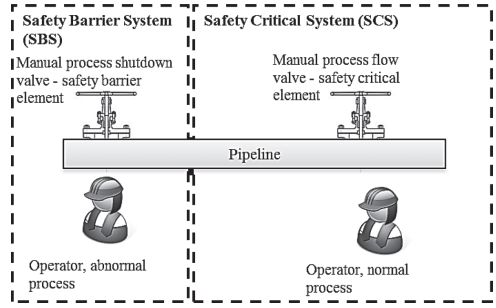


Figure 6. SCS and SBS comparison—generic example.

critical deviation or mitigate the consequences of it.

The differences between SCS and SBS are summarized in Table 1 and Figure 6.

3 SAFETY-RELATED ORGANIZATIONAL MEASURES

Safety-related organizational measures embrace the application of principles that ensure inherent Health, Safety and Environment (HSE) qualities related to the design and technical basis of the facility. The examples of such principles could be the principle of an Inherently Safer Design (ISD) (Mannan 2014), that involves the concept of reducing (avoiding, eliminating) rather than preventing or controlling hazards. The ISD principles should be applied during the general design and layout of the facility. Best Available Techniques (BAT) is another principle, which states that technology and the way it is used in the installations should be "most effective in achieving a high general level of protection of the environment as a whole" (EU Directive 1996); it

is similar to the As Low As Reasonably Practicable (ALARP) principle that adapts a best common practice for judgment of the balance of risk and benefit (HSE 2014). Furthermore, Samarakoon and Gudmestad (2011) have extended the BAT principle to include Qualification: Best Available Qualified Technology (BAQT).

In general, safety-related organizational measures may be seen as a foundational basis for safety-related systems including the design, technology and operational activities.

4 TECHNICAL SOLUTIONS AND BARRIERS

4.1 *Technical solutions*

Technical solutions are applied to the main process and related auxiliary equipment as a derivation of the safety-related principles mentioned in the third section above. The purpose of these solutions is to prevent a critical deviation from occurring and to sustain the normal designed conditions. For example, the thickness of a particular pipeline could be 10 mm if process-needs alone (i.e. pressure or flow rate) are taken into the account, but for safety reasons (i.e. estimated corrosion allowance, etc.) the pipeline is designed with 15 mm walls. Another example could be the selection of process control equipment, preferring modern technology to an obsolete version. The idea of technical safety-related solutions is to decrease the risk within the associated equipment and so it differs from the general design of the facility, which is focused on the process needs. Once applied, technical solutions cannot be removed from the installation without interrupting the functions of the facility for which the solutions were designed.

4.2 *Technical barriers*

A technical barrier is a physical element that is established to perform safety functions related to stopping the unwanted chain of events once it has started: detection, control, mitigation or emergency response. It is designed to perform once prevention fails and abnormal conditions occur and to stop the development of a chain of unwanted events, or to limit the harm of these unwanted events. Examples of technical barriers are: a firewall that is designed to perform if fire breaks out; an Emergency Shutdown (ESD) system that is activated if process control is lost; the fire detection and deluge systems installed to fight the fire. Technical barriers do not perform constantly and may be removed from the installation without interrupting the main process functions for which the facility was designed.

4.3 *Maintenance system*

To ensure the required functionality of critical equipment and technical barriers, maintenance and follow-up activities should be performed by establishing a maintenance system (PSA 2014c). For example, the automatic safety system is one of the main technical barriers; therefore function testing and demand monitoring should be established (IEC:61511-1 2004). Technical barriers should be analyzed, the criticality and failure/fault modes of their elements determined and appropriate maintenance activities undertaken. All critical equipment and technical barrier elements should be tagged and marked accordingly in the general maintenance system of the facilities. In addition, the maintenance system should incorporate an analysis of the human factors and the performance-shaping factors of the operational maintenance activities. Industry examples show that a maintenance system may be enabled through the creation of performance standards—the functional requirement list of each barrier system (Firing *et al.* 2011). The performance standards may serve as a link between technical safety and maintenance disciplines (Fig. 7).

The importance of a well-performing maintenance system is recognized, but industry examples show that implementation often struggles in practice. For example, the accident report on the *Deepwater Horizon* case concludes that "maintenance was inadequate", work orders issued by the maintenance system were "disorganized, erroneous, or irrelevant to individual rig crews" and the "maintenance system was not understood by the crew" (Chief Counsels Report 2011). The challenges facing the maintenance management are indicated in the report on trends in risk level in the petroleum activity (RNNP) process prepared by the Petroleum Safety Authority (PSA) Norway (PSA 2012), which describes the existing difficulties fulfilling regulatory requirements for maintenance management: "tagging and classification of equipment, backlogs of preventive maintenance and outstanding corrective maintenance, including HSE-critical maintenance".

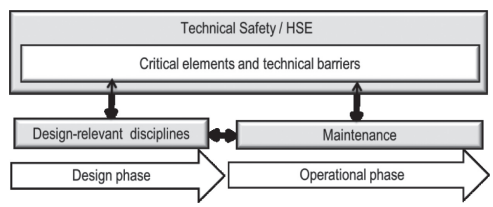


Figure 7. Links between design-relevant disciplines and maintenance.

The authors of this paper believe that one of the main reasons for such a situation is the missing links between the maintenance discipline and other disciplines, especially technical safety. The various analyses done by safety and maintenance engineers often do not have clear linkage and can hardly be implemented in the practical sense. Moreover, a general inconsistency in Computerized Maintenance Management Systems (CMMS) may often be observed due to the overlapping data of maintenance criticality analysis and technical safety analysis.

5 OPERATIONAL SOLUTIONS AND BARRIERS

5.1 *Operational solutions*

Similarly to technical solutions, operational solutions are derived from safety-related organizational principles and are applied to the main operational activities. For example, an operator could do his job in a very cost-efficient way, but, after a risk analysis is performed, a safety-related operational solution—the way the technology is used—will be applied to the job in order to reduce the risk. A safety checklist before an activity may also be seen as an operational solution, as it is an additional activity with a focus on preventing any abnormalities during the operation. The safety checklist may be seen as a part of safety-critical activities, but it is not a barrier by itself.

5.2 *Operational barriers*

An operational barrier can be seen as a determined specific action that shall be carried out in the case of critical deviation to prevent or to stop the development of an unwanted chain of events. A manual shutdown valve is often treated as a technical barrier element; however, it will not perform the barrier function unless somebody activates it on demand. This action is an operational barrier element.

Operational barriers are the part of the Safety Barrier System (SBS) that involves specific human actions related to the barrier function: detection, control, mitigation or emergency shutdown. Examples of operational barriers could be a manual activation of emergency shutdown systems, firefighting and evacuation. A specific lookout or visual check of an operator that is performed only for safety reasons may be seen as an operational detecting barrier.

5.3 *Performance-Shaping Factors (PSF)*

The UK Health and Safety Executive defines human factors as "environmental, organizational and job factors, and human and individual characteristics which influence behavior at work in a way which can affect health and safety" (HSG48 2009). Explicitly defined, human factors may be seen as Performance-Shaping Factors (PSF) and are used to model human behavior as the underlying causes of abnormal performance (El-Ladan and Turan 2012). It must be noted that PSF are explicitly used to describe the influence on human performance (Musharraf *et al.* 2013) and should not be directly referred to as the performance of technical equipment. Technical equipment is affected by maintenance actions which are again influenced by PSF (Toriizuka 2001). However, the PSF of maintenance activities should be seen as an integral part of the maintenance system, and maintenance activities should be distinguished from the operational safety barrier concept that embraces specified safety actions in the case of abnormal situations.

PSF may be characterized as internal and external (Boring *et al.* 2007). Internal PSF influence individual attributes such as mood, fitness, stress level, etc. External PSF exert influence in the situation or environment that affects the individual, such as temperature, noise, work practices, etc. The performance of operational activities is directly affected by PSF, so they must be taken into consideration when SCS or SBS are designed.

6 MANAGEMENT SYSTEM

6.1 *Workflow*

The general steps for establishing the management system for risk-reducing measures is shown in Figure 8. It may be seen as an interpretation of ISO31000 (2009) and the PSA regulations, Section 17 of the Management Regulations (PSA 2014a).

The context is seen directly or indirectly as acting factors that may be important in the risk-reduction process. It includes not only requirements, standards, guidelines, acting regulations and policies, but also general experience, expert knowledge, engineering judgment, etc. The risk analysis is intended to identify, analyze and evaluate the hazards in the activities performed. By understanding the nature of the hazard, the possible scenarios can be laid out and the corresponding safety measures can be discussed accordingly. The required safety-related solutions and barrier functions should be derived as a result of this process. Further steps are the actual identification of system functions and corresponding systems up to the equipment tag level to include them into the maintenance system. Finally, visualization and monitoring tool should be created specifically for SCS & SBS.

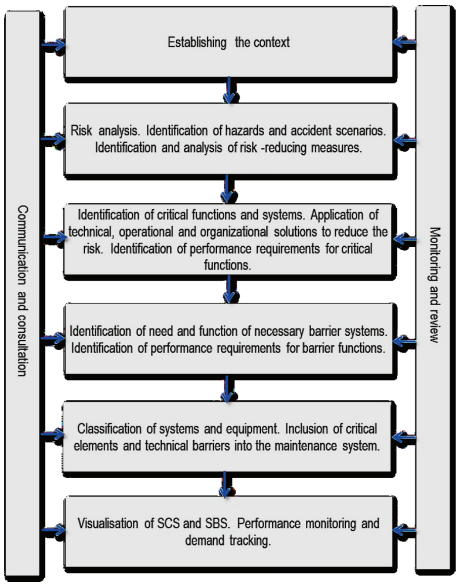


Figure 8. Managing the risk-reducing measures.

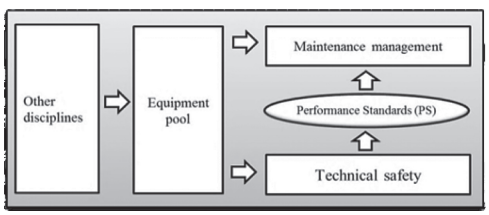


Figure 9. PS as a link between technical safety and maintenance.

6.2 *Challenges facing maintenance management*

The audit activities often find deficiencies in the completion of maintenance activities and missing links between equipment and the safety barriers (Ratnayake *et al.* 2012). It is essential to know the links and interconnections between maintenance and technical safety disciplines. The safety analyses and identification of safety functions should be transferred to the maintenance engineers in order to classify specific equipment accordingly. Results of safety-related analyses performed by technical safety engineers should be prioritized over results of maintenance criticality analyses. Clear links should be established in order to ensure that one discipline's output can be used as input for other disciplines. The mandatory Performance Standards (PS) required by the PSA may be seen as a potential major link between safety and maintenance disciplines (Fig. 9).

For example, the equipment tags of the Safety Instrumented Systems (SIS) should be specified in the Safety Requirement Specification (SRS), a live document made specifically for every installation (GL-070 2004 & IEC:61508 2010). The PS should contain links to such relevant documentation. In addition to specific requirements for safety critical and barrier functions, the PS should have a clear description of equipment groups that are considered as part of the SCS/SBS. A properly created PS will allow the correct identification of critical equipment tags and the implementation of data into the CMMS.

6.3 *Visualization of system*

The integrity status of SCS/SBS should be visualized. From the point of view of ergonomics and human factors, it is important that only the required data and information should be provided; it should not overflow, but be sufficient, unambiguous and non-misleading (Wong and Ceng 2002). Industry examples show how the visualization of safety systems is being implemented (Johansen and Toennessen 2002 & Firing *et al.* 2011). The purpose of this paper is not to evaluate the current achievement but to provide additional insights to the discussions and further development of these systems.

The visualization system should not only show the integrity status of technical parts of the SCE/SBS, but contain the names and duties of responsible personnel in the case of abnormal process conditions. Specific human activities are seen as operational barriers and as an integral part of the safety system. Automatic systems such as Safety Instrumented Systems (SIS) are an exception and may be seen as an SBS without an operational barrier element. The proposed concept of the visualization system is based on the generic accident model shown in Figure 1 and separates SCS and SBS (Fig. 10).

A status color code can be used as an indication of the general status. There may be various selections, for example, three levels of status: green, yellow, and red. The green would indicate that SCS/SBS integrity meets performance requirements, the yellow would demand attention and possible actions to be taken, while a red status would mean that the SCS/SBS is not performing and the risk is increased. The integrity status may be derived from the results of a system function test, preventive/corrective maintenance reports, etc.

By visualizing the status of the safety-related systems, an overview of the integrity status can be made available for operators and managers. This information is essential when evaluating work permits, the bypass of safety systems for maintenance,

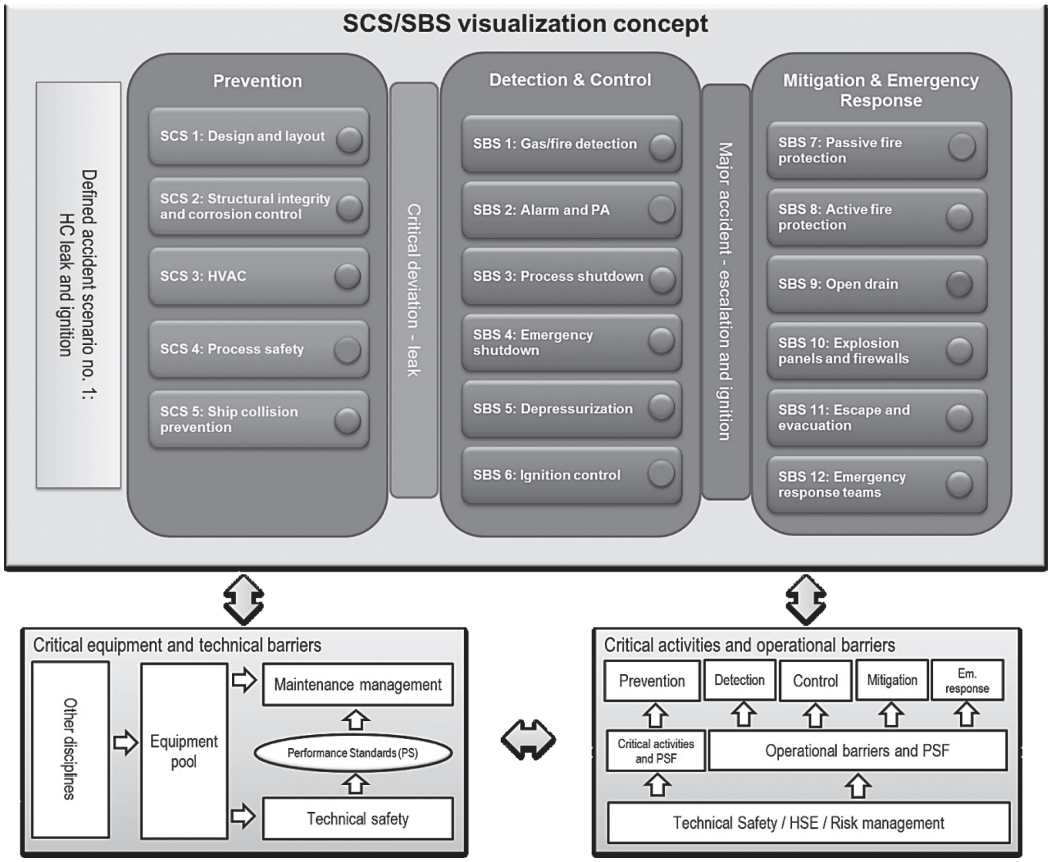


Figure 10. Generic example of visualization of SCS/SBS.

and increased levels of activities. Easy and user-friendly access to the information would facilitate good practices of safety management (Johansen and Toennessen 2002).

7 SUMMARY

Based on the synthesis of ISO 17776, the PSA regulations and common features of the terms found in the scientific literature, the concepts of Safety-Critical Systems (SCS) and Safety Barrier Systems (SBS) are proposed as a basis for further discussion of risk-reducing measures in industrial activities.

Correspondingly, prevention, detection/control, and mitigation/emergency response systems have been introduced and described. Aligning with the PSA regulations, safety-related solutions and corresponding critical systems have been separated from safety barriers and described. Links between technical, operational and organizational elements have been suggested, incorporating maintenance activities and performance-shaping factors. The presented accident chain model (Fig. 1) may be used as a tool for a broader communication about the safety barriers and their role in arresting the accident's escalation.

This may be valuable in risk communication, where the model's simplicity could be well-accepted by non-technical safety personnel.

Furthermore, some important issues regarding the management of safety systems have been discussed with a focus on maintenance and its links with other disciplines. Generic examples of conceptual workflow and system visualization have been proposed and described.

Today the industry has a challenge to link technical and operational elements into a united system. A conceptual framework of systems consisting of technical and operational elements has been discussed in the manuscript.

Further studies are required to enable a synergy of separate work processes that would ensure

adequate maintenance and follow-up of risk-reducing measures during their lifecycle.

REFERENCES

Boring, R.L., Griffith, C.D. & Joe, J.C. 2007. The Measure of Human Error: Direct and Indirect Performance Shaping Factors (ed.). In *Human Factors and Power Plants and HPRCT 13th Annual Meeting.* IEEE, 170–176.

Chief Counsels Report: Chapter 4.10: Maintenance. 2011. http://cybercemetery.unt.edu/archive/oilspill/20121210200431/http://www.oilspillcommission.gov/final-report, p. 221–224. [Accessed 2014].

Dhar, R. 2011. Performance Standards For Safety Critical Elements—Are We Doing Enough! In *SPE European Health Safety and Environmental Conference in Oil and Gas Exploration and Production.* Society of Petroleum Engineers.

El-Ladan, S.B. & Turan, O. 2012. Human reliability analysis—Taxonomy and praxes of human entropy boundary conditions for marine and offshore applications. In *Reliability Engineering & System Safety*, 98, 43–54.

EU Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control. 1996. http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996 L0061:en:HTML. [Accessed 2014].

Firing, F.L., Ostby, E., Ingvarson, J. & Strom, O. 2011. TTS-The Systematic and Efficient Approach to Define Maintain and Demonstrate Safety Performance on Complex Hydrocarbon Processing Facilities (ed.). In *Offshore Technology Conference*.

GL-070. 2004. "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry", rev. 2. The Norwegian Oil Industry Association.

HSE. 2014. UK Health and Safety Executive. http://www.hse.gov.uk/risk. [Accessed 2014].

HSG48. 2009. "Reducing error and influencing behaviour". UK Health and Safety Executive.

IAEA. 1999. "Basic safety principles for nuclear power plants: 75-INSAG-3", rev. 1. Vienna: The International Atomic Energy Agency.

IEC:61508. 2010. "Part 1–7 Functional safety of electrical/electronic/programmable electronic safety-related systems". Geneva: International Electrotechnical Commission.

IEC:61511-1. 2004. "Functional safety—Safety instrumented systems for the process industry sector—Part 1: Framework, definitions, system, hardware and software requirements". Geneva: International Electrotechnical Commission.

ISO:13702. 1999. "Petroleum and natural gas industries—Control and mitigation of fires and explosions on offshore production installations". Geneva: International Organization for Standardization.

ISO:17776. 2000. "Petroleum and natural gas industries. Offshore production installations. Guidance on tools and techniques for hazard identification and risk assessment". Geneva: International Organization for Standardization.

ISO:31000. 2009. "Risk management. Principles and guidelines on implementation". Geneva: International Organization for Standardization.

Johansen, J.A. & Toennessen, N. 2002. Maintenance Management of Essential Safety Systems (ed.). In *SPE International Conference on Health Safety and Environment in Oil and Gas Exploration and Production*. Society of Petroleum Engineers.

Mannan, S. 2014. Chapter 21—Inherently Safer Design. In S. Mannan (ed.), *Lees' Process Safety Essentials.* Oxford: Butterworth-Heinemann, 403–407.

Musharraf, M., Hassan, J., Khan, F., Veitch, B., Mackinnon, S. & Imtiaz, S. 2013. Human reliability assessment during offshore emergency conditions. *Safety Science*, 59, 19–27.

PSA. 2012. "The trends in risk level in the petroleum activity (RNNP)". Norway, Stavanger: Petroleum Safety Authority.

PSA. 2014a. "Regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.

PSA. 2014b. "Guidelines to regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.

PSA. 2014c. "Regulations relating to conducting petroleum activities (The Activities Regulations)". Norway, Stavanger: Petroleum Safety Authority.

Ratnayake, R.M.C., Singh, S.P. & Raza, J. 2012. Development of a Barrier Management System for Continuous Monitoring and Maintenance of Safety Barriers (ed). In *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management.* IEEE.

Samarakoon, S.M.S.M.K & Gudmestad, O.T. 2011. Qualification of offshore facilities prior to application in a new field. *Journal of Cleaner Production*, 19, 13–20.

Sevcik, A. & Gudmestad, O.T. 2014. Systematic Approach to Risk Reduction Measures in the Norwegian Offshore Oil and Gas Industry. Accepted for publication in *9th International Conference on Risk Analysis and Hazard Mitigation, Wessex Institute*, *4–6 June.* New Forest, UK.

Toriizuka, T. 2001. Application of Performance Shaping Factor (PSF) for work improvement in industrial plant maintenance tasks. *International Journal of Industrial Ergonomics*, 28, 225–236.

Wong, W. & Ceng, F. 2002. *How did that happen?: engineering safety and reliability*. Professional Engineering.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A multi-criteria decision model to mitigate the operational risks of offshore wind infrastructures

Mahmood Shafiee
Institute for Energy and Resource Technology, School of Applied Sciences, Cranfield University, Bedfordshire, UK

Athanasios Kolios
Energy and Power Division, School of Engineering, Cranfield University, Bedfordshire, UK

ABSTRACT: For many power generation systems, it is extremely important to control the likelihood as well as the consequences of potential risks during actual operation. Operational risks may result in substantial costs of repair or replacement, significant losses of power production, and catastrophic safety hazards to personnel or infrastructure. The selection of an appropriate strategy to mitigate the operational risks is a very complex and critical task for the offshore wind energy sector. In recent years, Multi-Criteria Decision Making (MCDM) approaches have gained momentum in this field. The aim of this paper is to propose a decision model based on Analytic Network Process (ANP) technique in order to select the best "risk mitigation strategy" for offshore wind infrastructures. The proposed model consists of a number of alternatives (e.g., variation of offshore site layout, improvement of maintenance services, upgrading the control and monitoring systems, and modification in design of wind turbine sub-assemblies) among which the decision maker has to select, on the basis of a finite set of criteria (e.g., safety, added value, cost, and feasibility). The model developed is applied to an offshore wind farm consisting of 30 wind turbines of 2 MW. Our findings indicate that "improving the repair and maintenance services" is chosen to be the most cost-effective approach for mitigating the operational risks of offshore wind infrastructures.

1 INTRODUCTION

Offshore wind energy industry has grown very rapidly over the last years. The cumulative installed capacity of offshore wind power in the EU has increased from 532 MW in the year 2003 to 6.6 GW in the end of 2013, which represents an annual growth of about 29% (European 2014). Along with the growth of the market for offshore wind energy, particular attention should be focused on Operation and Maintenance (O&M) as well as reliability and availability of the installed wind power systems.

Analyses of field failure data collected from various databases like Elforsk in Sweden (Elforsk.se) show that the availability of onshore wind power plants is typically between 95% to 99%, while it is evaluated to be in the range of 60% to 70% for offshore plants. Moreover, offshore wind turbines suffer from a higher failure rate compared to the wind turbines located onshore (Tavner 2012). The main reason might be that offshore wind power generation systems are typically subject to a wider range of *operational* risks, hazards, or damages.

In general, the operational risks within offshore wind farms involve two major categories: (i) the risks of system failures (e.g., asset breakdowns) and (ii) the environmental risks (e.g., natural catastrophes, ship collisions) (Wilson 2013). The former is generally caused by system/component degradation, whereas the latter results from extreme weather conditions and harsh marine environments (see Fig. 1).

Any of the mentioned hazards can potentially have a negative impact on plant profitability if it is not prevented in an efficient way. Random failures result in substantial costs of repair or replacement, and significant losses of power production, and

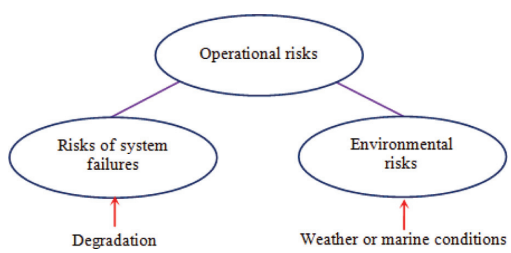


Figure 1. Operational risks within offshore wind power plants.

nature events lead to catastrophic safety hazards to personnel or infrastructure (e.g., grid disconnection). Therefore, there is a critical need to control the likelihood as well as consequences of potential risks during actual operation. For this purpose, a risk management plan should be developed and implemented for the existing offshore wind power plants.

Risk management is a process focusing on the identification and elimination of hazards that could adversely affect asset performance. This process normally includes several steps like identification, assessment, evaluation, control and monitoring, and mitigation of risks resulting from a certain hazard (Aven 2007). Among them, the risk identification and assessment area has received a reasonable attention in the wind energy sector. To this end, the following studies are identified:

Tavner *et al.* (Tavner 2010) and Arabian-Hoseynabadi *et al.* (Hoseynabadi 2010) propose a Failure Mode and Effects Analysis (FMEA) methodology for prioritization of failure modes in a 2-MW wind turbine system. Kahrobaee and Asgarpoor (Kahrobaee 2011) develop a risk-based FMEA approach for wind turbine systems, in which the criticality of a failure is determined on the basis of failure probability and the incurred costs. Das *et al.* (Das 2011) implement the tarditional FMEA methodology on a 2-MW variable speed wind turbine system. Dinmohammadi and Shafiee (Dinmohammadi 2013) develop a fuzzy-FMEA approach for risk and failure mode analysis in offshore wind turbines when the failure data is unavailable or unreliable. Sunder and Kesavan (Sunder 2013) studied the implementation of an FMEA methodology for wind turbines located in uncertain wind environments. Shafiee and Dinmohammadi (Shafiee 2014) propose a mathematical tool for risk and failure mode analysis of wind turbine systems (both onshore and offshore). The proposed tool combines the aspects of the FMEA methodology in (Hoseynabadi 2010) with some economic considerations like power production losses and the costs of logistics and transportation.

In spite of the vast research on risk identification and assessment, only a few methods exist in the literature for mitigating the operational risks within offshore wind farms. A recently published report by the U.S. Department of Energy (The U.S. Department of Energy 2008) recommends enhancing the wind turbine reliability (through prototype testing of components before deployment) to mitigate the failure risks in offshore wind power plants. Sjodin *et al.* (Griffin 2012) and Griffin (Griffin 2014) introduce the variation of offshore site placement/layout as a way of reducing the weather-related risks. Even though this strategy might be non-practical or even not feasible for many offshore farms, it can be cost-effective for some small projects.

In this paper, we propose a Multi Criteria Decision Making (MCDM) approach based on the Analytic Network Process (ANP) technique to select the best risk mitigation strategy for offshore wind infrastructures. The proposed model consists of a number of alternatives (e.g., variation of offshore site layout, improvement of maintenance services, upgrading the control and monitoring systems, and modification in design of wind turbine sub-assemblies) among which the decision maker has to select or rank, on the basis of a finite set of criteria (e.g., safety, added value, cost, and feasibility). Our findings indicate that improving the repair and maintenance services is chosen to be the most cost-effective approach for mitigating the operational risks of offshore wind infrastructures.

This paper is organized as follows: (i) first, a brief overview of the risk mitigation strategy selection and ANP technique is given so as to set the background for the main contribution of the paper, (ii) second, a decision model is proposed for risk mitigation strategy selection in offshore wind farms, and (iii) finally, the implementation of proposed model is presented and the results are discussed.

2 RESEARCH BACKGROUND

2.1 *Risk mitigation strategy selection as a complex MCDM problem*

The selection of a suitable risk mitigation strategy is a very complex and critical task. An appropriate risk mitigation strategy not only reduces the probability of failure occurrence but also improves the assets' operating conditions, which eventually result in higher Operating expenses (Opex). On the other side, an improper selection of strategies may adversely affect the operating budget and thereby reducing productivity as well as profitability.

Risk mitigation strategy selection is considered as a typical MCDM problem. In this problem, the decision-maker (i.e., plant managers or stakeholders) must decide on the best strategy among a set of possible alternatives to mitigate operational risks. Moreover, in the decision making process, many goals or comparing criteria must be taken into consideration (e.g. the investment required, safety aspects, environmental issues). These criteria cannot fulfilled simultaneously, i.e., according to a criterion, a given alternative is the best one, while according to another criterion, other alternatives score higher. Thus, each alternative is evaluated with respect to each criterion and then, the evaluation ratings are aggregated to obtain a global evaluation. Last, the alternatives are prioritized from the best (optimal) to the worst.

In recent years, the MCDM approach has gained momentum in selection of the best risk mitigation strategy within a wide range of industries including oil and gas, construction, and transport. In contrast, to the best of the author's knowledge, there is no presented work dealing with the problem for wind farms.

2.2 *Analytic Network Process (ANP)*

Among the several existing MCDM techniques, the Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP) are the most widely used in solving decision-making problems. In AHP technique, the problem is modeled in a hierarchical structure showing the relationships between various components, namely, goal, criteria (and any sub-criteria) and alternatives [16]. So, the components of decision problem are connected top-to-bottom in a way that the upper level node does not depend on the lower levels, and the elements presented in a node are independent of each other. This one-sided network fails to capture the complex interactions and feedbacks which might be present in the system. To overcome this limitation, the ANP technique was introduced by Saaty in 1996 (Saaty 1994).

In ANP, the goal, criteria and alternatives are modelled in the form of clusters, and all possible interactions between the clusters and elements within a cluster are considered. In fact, the ANP technique provides a general framework to deal with decisions without making assumptions about the independence of higher level elements from lower level elements and about the independence of the elements within a level. So, ANP is a coupling of two parts: the first part consists of a control hierarchy or network of criteria and sub-criteria that control the interactions, and the second part is a network of influences among the elements and clusters.

A brief review of the literature shows that ANP technique has been applied to various fields including economics, engineering, education, health, political and social science, and technology management. Readers can refer to a recently published book by Saaty and Vargas (Saaty 2013) for a thorough review on ANP applications.

3 PROPOSED METHODOLOGY

In this Section, we propose a methodology for selecting an appropriate risk mitigation strategy in offshore wind farms. The eight main steps of our methodology are described as follows.

3.1 *Step 1. Form a group of decision makers*

First, a project team must be established to determine and examine the operational hazards and their potential impact on the wind farm operation. The team is often composed of key plant managers (i.e., power generation manager, head of safety and risk, and project finance director) as well as some practitioners in operation and maintenance.

3.2 *Step 2. Determine the alternative risk mitigation strategies*

Several alternatives can be taken into account in selection of the best risk mitigation strategy, but some of them might be non-applicable to offshore wind industry. In this paper, four alternative risk mitigation strategies are considered: variation of offshore site layout, improvement of maintenance services, upgrading the control and monitoring systems, and modification in design of wind turbine sub-assemblies. These alternatives are briefly described below.

3.2.1 *A.1. Variation of offshore site layout*

The 'layout' of an offshore wind farm is one of the critical elements influencing the risks associated with natural events (i.e., environmental risks) [19]. It is expected that, in general, the potential risks become more likely to happen for wind farms located in ultra deep waters far offshore compared to installation in shallow waters near shore. Therefore, any improvement in offshore site layout will have a substantial impact on likelihood as well as consequences of environmental risks on offshore wind infrastructures.

3.2.2 *A.2. Improvement of maintenance services*

Current practice in offshore wind farms for maintenance is reactive response (or failure-based). Under this policy, the maintenance actions are undertaken when a failure is detected. According to various studies (see, e.g., (Musial 2006)), using the reactive response policy in offshore farms results in high repair costs, frequent unplanned outages, lengthy waiting and maintenance times, and trouble shooting problems. For this reason, Preventive Maintenance (PM) policies (including periodic inspections, risk-based, condition-based, and predictive) are extensively used to control the rate of asset degradation and avoid costly failures (Andrawus 2008). A well-planned and optimized maintenance policy can effectively reduce the costs associated with operating and repairing wind turbines.

3.2.3 *A.3. Upgrading the control and monitoring systems*

One effective way to reduce the likelihood of operational risks in offshore wind farms is improving the fault detection capability. This improvement can be achieved by installing a number of

high quality and technically advanced sensors at specified locations as well as using new monitoring techniques (such as acoustic emission, ultrasonic testing, strain measurement, radiographic inspection, thermography, and signal processing methods) (Yang 2012).

3.2.4 *A.4. Modification in design of wind turbine sub-assemblies*

The operational risks in offshore wind farms can be reduced by enhancing the reliability of wind turbines through design modification. The aim of design modification is to minimise the number of failure experienced in wind turbines, which results in enormous savings in maintenance and energy costs. The modifications could involve reliability growth testing, or adding redundancy to critical components in order to increase the Mean Time Between Failures (MTBF).

3.3 *Step 3. Determine the decision criteria*

In order to evaluate and prioritize the mitigation actions, the project team must specify a set of criteria. Different decision-makers may have different objectives. In this paper, the criteria for risk mitigation strategy selection are determined based on the review of literature and semi-structured interviews undertaken with key managers. The criteria considered can be divided into four categories as follows.

3.3.1 *C.1. Safety*

A high safety level is required for many offshore wind power plants, especially for the ones which are connected to the grid in series. The relevant factors describing safety are:

- *Technicians safety*: A failure of a wind turbine and/or an environment event may lead to serious damages to personnel/technicians working on site.
- *Power grid safety*: A failure of a wind turbine and/or an environment event has a negative impact to the grid-connection equipment and thereby disconnects the power plant from electric grid.

3.3.2 *C.2. Added value*

The added-value criterion deals with the benefits that may be gained from implementing a particular risk mitigation strategy. This criterion includes the improvements in terms of power production and fault detection.

- *Power production*: A failure of a wind turbine and/or an environment event often leads to a substantial production loss. Selecting a suitable strategy for risk mitigation can potentially enhance the power produced by offshore wind farms.
- *Fault detection*: Fault diagnostic and prognostic techniques aim to quickly alert the maintenance engineers where and why faults occur. As a result, the maintenance lead-times are shortened, and the availability of wind farms will be improved.

3.3.3 *C.3. Cost*

Different risk mitigation actions have different expenditure of hardware, software, and personnel training.

- *Hardware cost*: For implementation of risk mitigation strategies, a number of service vessels, support facilities, maintenance tools, monitoring and prognostic sensors should be acquired.
- *Software cost*: More expensive and advanced software are needed if decided to upgrade the control and monitoring systems or modify the design of sub-assemblies.
- *Training cost*: Risk mitigation actions in offshore wind farms should be initiated only after sufficient training.

3.3.4 *C.4. Feasibility*

The feasibility of risk mitigation strategies is divided into acceptance by stakeholders and acceptance by plant managers.

- *Acceptance by stakeholders:* Successful implementation of a risk mitigation action needs the support and participation of wind farm stakeholders (i.e., financial institutions, insurance companies, owners, and regulatory authorities).
- *Acceptance by plant managers:* Plant managers often prefer the strategies that yield more Return On Investment (ROI) and are easier to implement. So, the variation of plant layout and modification of the design of wind turbines might be suitable alternatives for long-term investments.

3.4 *Step 4. Construct a network model*

Using criteria, sub-criteria and alternatives, a network model is constructed. The relationship among criteria and sub-criteria are also determined and reflected in the network model.

Figure 2 shows a network model for the decision problem of risk mitigation strategy selection in offshore wind farms. As can be seen, the proposed network includes three clusters. The first cluster represents the ultimate goal of the problem (i.e., selection of the best risk mitigation strategy). The second cluster consists of four main criteria, namely, safety, added value, cost, and feasibility.

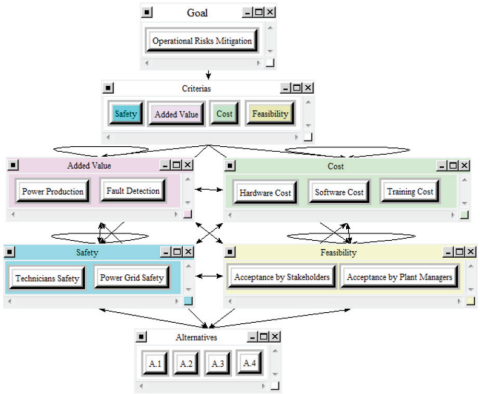


Figure 2. A network model for risk mitigation strategy selection in offshore wind power plants.

Table 1. Pair-wise comparison scheme [16].

Value of rating judgments	Verbal judgments
$a_{ij} = 1$	The tow parameters are equally important
3	Parameter *i* is weakly more important than parameter *j*
5	Parameter *i* is strongly more important than parameter *j*
7	Parameter *i* is very strongly more important than parameter *j*
9	Parameter *i* is absolutely more important than parameter *j*
2, 4, 6, 8	Interval values between two adjacent choices

The criteria are decomposed into various sub-criteria as discussed. Finally, the third cluster of the network represents the alternative strategies.

3.5 *Step 5. Pair wise comparison among criteria and sub-criteria*

Pair wise comparisons are done among related criteria and sub-criteria following the scale suggested by Saaty [16] in Table 1. A questionnaire form is used to complete the pair-wise comparison matrix.

3.6 *Step 6. Calculating local priority vector and testing the consistency*

Once the pairwise comparisons are completed, the local priority vector is computed as the unique solution to:

$$Aw = \lambda_{\max} w, \tag{1}$$

where A is the matrix of pairwise comparison, w is the eigenvector, and $\lambda_{\max}$ is the largest eigenvalue of A. The Consistency Index (CI) and Consistency Ratio (CR) are used to measure the consistency of the pair-wise comparison matrix. The CI and CR values are defined as follows:

$$CI = \frac{\lambda_{\max} - n}{n-1}, \tag{2}$$

$$CR = \frac{CI}{RI}, \tag{3}$$

where n is the number of elements and RI denotes the average consistency index for numerous random entries of same order reciprocal matrices. If $CR \leq 0.1$, then the pairwise comparison matrix is consistent; otherwise, a new comparison matrix is solicited until $CR \leq 0.1$.

3.7 *Step 7. Super-matrix and limit super matrix formation*

The impact of the elements in network on the other elements can be represented in a super-matrix. The super-matrix is actually a partitioned matrix where each matrix segment represents a relationship between two clusters in the network. The local priority vectors, obtained in Step 6, are grouped and placed in proper columns of the super-matrix based on the flow of influence from one cluster to another, or from a cluster to itself, as in the loop.

Since there is usually dependency among clusters in a network, the aggregate of the column vectors of a super matrix may sum to more than one. In this case, the super matrix must be modified so that each column of the matrix sums to unity. To achieve a convergence on a long-term stable set of weights, the weighted super matrix is raised to the power of $2k + 1$, where k is an arbitrarily large number, and the new matrix is called the limit super matrix.

3.8 *Step 8. Selection of the best strategy*

Desirability index (D_i) is used to determine the best alternative. The equation for D_i is defined by (Saaty 1994):

$$D_i = \sum C_i M_i A_i, \tag{4}$$

where C_i is the relative importance of each category metric, M_i is the relative importance of each measure, and A_i is the relative importance of an alternative for a measure. The alternative with the largest desirability index is selected as the best strategy.

4 APPLICATION AND RESULTS

In this Section, the proposed methodology is applied to an offshore wind farm located approximately 5 miles off the coast, and consist of 30 wind turbines of 2 MW (see Fig. 3). The wind plant generates on average 200 GW of electricity per year hours, which it provides about 40,000 households' electricity needs.

Computer software based on the ANP technique, 'Super Decisions' has been utilized for the evaluation and analyses (for more see (Super Decision)). First of all, the priority weights of four criteria with respect to the overall goal are obtained using a pairwise comparison matrix. The exact ratios of the obtained weights of four main criteria are given as follows:



Figure 3. Offshore wind farm considered for this study.

$w_1 = 0.345$ (Safety); $w_2 = 0.202$ (Added value); $w_3 = 0.329$ (Cost); $w_4 = 0.124$ (Feasibility).

As can be seen, in evaluation of the risk mitigation strategies for offshore wind power plants, the greatest weight is given to the safety criterion. This is perhaps in due consideration of the huge impact of operational hazards on grid safety.

Next, all sub-criteria are compared at the second level in terms of corresponding main criteria, and the related comparison matrixes are constructed. The priority weights for sub-criteria with respect to the main criterion are given as follows:

$w_{11} = 0.207$ (Technicians safety); $w_{12} = 0.138$ (Grid safety); $w_{21} = 0.155$ (Power production); $w_{22} = 0.047$ (Fault detection); $w_{31} = 0.149$ (Hardware cost); $w_{32} = 0.107$ (Software cost); $w_{33} = 0.073$ (Training cost); $w_{41} = 0.086$ (Acceptance by stakeholders); $w_{42} = 0.038$ (Acceptance by plant managers).

In addition, the amount of interdependency among sub-criteria or in fact the amount of sub-criteria impacts on each other is measured from the

Table 2. Importance weights among sub-criteria.

	Sub-criteria								
	11	12	21	22	31	32	33	41	42
11	0.000	0.000	0.500	0.500	0.500	0.400	0.800	0.500	0.500
12	0.000	0.000	0.500	0.500	0.500	0.600	0.200	0.500	0.500
21	0.500	0.500	0.000	0.000	0.800	0.200	0.400	0.500	0.602
22	0.500	0.500	0.000	0.000	0.200	0.800	0.600	0.500	0.398
31	0.334	0.334	0.334	0.334	0.000	0.000	0.000	0.333	0.333
32	0.333	0.333	0.333	0.333	0.000	0.000	0.000	0.333	0.333
33	0.333	0.333	0.333	0.333	0.000	0.000	0.000	0.333	0.333
41	0.500	0.500	0.500	0.500	0.800	0.714	0.588	0.000	0.000
42	0.500	0.500	0.500	0.500	0.200	0.286	0.412	0.000	0.000

Table 3. Importance weights of alternative strategies with respect to sub-criteria.

	Sub-criteria								
	11	12	21	22	31	32	33	41	42
A1	0.100	0.025	0.100	0.010	0.080	0.300	0.333	0.010	0.100
A2	0.300	0.300	0.400	0.200	0.500	0.350	0.286	0.700	0.400
A3	0.350	0.350	0.300	0.700	0.120	0.150	0.238	0.200	0.300
A4	0.250	0.100	0.200	0.100	0.300	0.200	0.143	0.090	0.200

answers to questionnaire. The priority weights of sub-criteria against each other are addressed in Table 2.

Afterwards, the priority weights for the alternative risk mitigation strategies with respect to sub-criteria are obtained. These estimated priority weights are shown in Table 3.

Finally, the priority weights for the sub-criteria regarding maintenance alternatives are determined. Table 4 represents the estimated priority weights of each sub-criterion against four risk mitigation strategies.

The priority vectors obtained through paired comparisons are placed in the appropriate columns to form the super-matrix. The zero elements in the super-matrix show the independency among the variables in the rows and columns. The global weights of sub-criteria against the overall goal (determining the appropriate maintenance strategy) were obtained by multiplying the weight of main criterion with the local weight of sub-criteria, and are entered in to column 'goal'.

Later, the super-matrix is transformed into a weighted matrix. The transformation process involves multiplying the super-matrix by the cluster matrix, so that the priorities of the clusters can be taken into account in the decision making process. Finally, the weighted super-matrix is transformed into the limit super-matrix to make the distribution of the vector values meaningful to decision makers. The limit super-matrix is shown in Table 5.

The final priority of the four risk mitigation alternatives is represented in Table 6.

As shown, "improvement of maintenance services" is chosen as the best risk mitigation strategy within the offshore wind power plant.

Table 4. Importance weights of sub-criteria with respect to alternative strategies.

Sub-criteria	Alternative strategies			
	A1	A2	A3	A4
11	0.500	0.500	0.500	0.500
12	0.500	0.500	0.500	0.500
21	0.800	0.800	0.200	0.800
22	0.200	0.200	0.800	0.200
31	0.800	0.520	0.500	0.200
32	0.150	0.320	0.300	0.500
33	0.050	0.160	0.200	0.300
41	0.901	0.500	0.602	0.700
42	0.099	0.500	0.398	0.300

Table 5. Limit super-matrix for the risk mitigation strategy selection.

Cluster node level	Alternatives				Criteria									
					C1		C2		C3			C4		
	A1	A2	A3	A4	11	12	21	22	31	32	33	41	42	Goal
Alternatives														
A1	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026	0.026
A2	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067
A3	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055	0.055
A4	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032
Criteria														
C1														
11	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137	0.137
12	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126	0.126
C2														
21	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094	0.094
22	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0.086	0 086	0.086
C3														
31	0.950	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095	0.095
32	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084	0.084
33	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076	0.076
C4														
41	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070
42	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049	0.049
Goal	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 6. Priority scores of the four risk mitigation strategies.

Risk mitigation strategy	Normalized limiting values
Improvement of maintenance services	0.371
Upgrading the control and monitoring systems	0.305
Modification in design of wind turbine sub-assemblies	0.178
Variation of offshore site layout	0.145

5 CONCLUSIONS AND TOPICS FOR FUTURE RESEARCH

Selection of an appropriate strategy to mitigate the operational risks is a very complex and critical task. In this paper, an MCDM approach was proposed based on the ANP technique to select the best risk mitigation strategy for offshore wind farms. The reason that ANP technique has been used is to overcome the limitation of AHP to take into account the possible dependencies among various components. For instance, the relationship between two criteria 'safety' and 'cost' could be such that an alternative with low risks to technicians as well as power grid would probably be expensive. So, compared to AHP, the proposed methodology is better able to deal with real world problems. The model was applied to an offshore wind farm consisting of 30 wind turbines of 2 MW, and finally, 'improvement of maintenance services' was found to be the most effective alternative for risk mitigation.

There is a wide scope for future research in the area of risk mitigation strategy selection within wind power sector (either onshore or offshore). In this study, we confined the analysis to only four alternatives. However, other alternatives such as outsourcing the operation and repair services of plants could be involved. Also, some other MCDM techniques (such as ANP-TOPSIS) could be applied to study this problem.

REFERENCES

Andrawus, J.A., 2008. Maintenance optimization for wind turbines. PhD thesis, Robert Gordon University, Aberdeen, UK.

Arabian-Hoseynabadi, H., Oraee, H., Tavner, P.J., 2010. Failure modes and effects analysis (FMEA) for wind turbines. *International Journal of Electrical Power & Energy Systems*, 32, 817–824.

Aven, T. and Vinnem, J-E., 2007. Risk management with applications from the offshore petroleum industry, *Springer Series in Reliability Engineering*. Springer, London. ISBN 978-1-84628-653-7.

Das, M.K., Panja, S.C., Chowdhury, S., Chowdhury S.P. and Elombo, A.I., 2011. Expert-Based FMEA of Wind Turbine System. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, December 6–9, pp. 1585–1589.

Dinmohammadi, F. and Shafiee, M., 2013. A fuzzy-FMEA risk assessment approach for offshore wind turbines. *International Journal of Prognostics and Health Management*, 4, pp. 1–10.

European Wind Energy Association. Wind in Power, 2013 European Statistics; Published in February 2014. Available online: http://www.ewea.org/statistics/.

Griffin, D.A., 2014. Mitigating project risks for offshore wind. Offshore wind China Conference & Exhibition, Shanghai, China, June 4–6.

http://www.elforsk.se.

Kahrobaee, S. and Asgarpoor, S., 2011. Risk-based failure mode and effect analysis for wind turbines (RB-FMEA). In *Proceedings of the North American Power Symposium* (NAPS), Boston, USA, August 4–6, pp. 1–7.

Musial, W. and Butterfield, S., 2006. Energy from offshore wind. In Proceedings of the Offshore Technology Conference, *National Renewable Energy Laboratory* (NREL), Houston, Texas, U.S., May 1–4.

Saaty, T.L. and Vargas, L.G., 2013. Decision making with the analytic network process: Economic, political, social, and technological applications with benefits, opportunities, costs, and risks. Second edition, Springer, New York.

Saaty, T.L., 1994. Fundamentals of decision making and priority theory with the analytic hierarchy process. Pittsburgh, PA: RWS.

Saaty, T.L., 1996. Decision making with dependence and feedback: The analytic network process. Pittsburgh, PA: RWS.

Shafiee, M. and Dinmohammadi, F., 2014. An FMEA-based risk assessment approach for wind turbine systems: a comparative study of onshore and offshore. *Energies* 7(2): 619–642.

Sjodin, E., Gayme, D.F. and Topcu, U., 2012. Risk-mitigated optimal power flow for wind powered grids. *American Control Conference* (ACC), Montreal, Canada, June 27–29, pp. 4431–4437.

Sunder, T.S. and Kesavan, R., 2013. Failure modes and effects analysis system deployment in a wind turbine at high uncertain wind environment. Advanced Science Letters, 19(8): 2166–2169.

Super Decision Software for Decision Making, http://www.superdecisions.com.

Tavner, P., 2012. Offshore wind turbines: Reliability, availability and maintenance. *The Institution of Engineering and Technology*, London. ISBN: 978-1-84919-229-3.

Tavner, P.J., Higgins, A., Arabian-Hoseynabadi, H., Long, H. and Feng, Y., 2010. Using an FMEA method to compare prospective wind turbine design reliabilities. *In Proceedings of the European Wind Energy Conference*, Warsaw, Poland, April 20–23, pp. 1–7.

The U.S. Department of Energy, 2008. 20% wind energy by 2030: increasing wind energy's contribution to U.S. electricity supply. Chapter 2: Wind turbine technology. pp. 23–60.

Tiusanen, P., Jännes, J. and Liyanage, J.P., 2011. Framework to assess system risks associated with offshore wind farms in northern context. *In Proceedings of the 21st International Offshore and Polar Engineering Conference*, Maui, Hawaii, U.S. June 19–24.

Wilson, G. and McMillan, D., 2013. Modeling the relationship between wind turbine failure modes and the environment. In Proceedings of the European Safety, Reliability and Risk Management (ESREL), Amsterdam, the Netherlands, 30 September–2 October; pp. 801–809.

Yang, W., Tavner, P.J., Crabtree, C.J., Feng, Y. and Qiu, Y., 2012. Wind turbine condition monitoring: technical and commercial challenges. Wind Energy, doi:10.1002/we.1508.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Evaluation of operational reliability of the supply chain in terms of the control and management of logistics processes

I. Jacyna-Gołda
Institute of Organization of Production Systems, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: The paper presents an approach reliability of the supply chain in terms of the control and management of logistics processes. Determination of reliability of complex systems of this type should take into account wide range of issues. The article poses the thesis that based on studies of supply chain model concerning speed and reliability it is possible to determine whether the relationships in the supply chain have a high enough reliability factor or not. In order to investigate the supply chain for a company was used the SCOR model. This model is a useful tool for analyzing supply chains and allows you to measure, control and manage processes throughout the supply chain, including all participants (producers, transport companies, distributors, consumers).

1 INTRODUCTION

Modern logistics is primarily a method of managing the flow of goods from suppliers to customers in such a way that the flow proceeds without interference. Logistics, which is engaged in thempumpkins activities related to supplying customers with products and services is defined as the distribution logistics (Barnes et al. 2003, Brzeziński 2006, Ghazanfari & Fatholla 2006, Korzeń 2001, Pfohl 1998, Witkowski 2000). In contrast, supply logistics is a system of managing the flow of materials from suppliers to production areas at the right price, in the right quantity, at the right time, quality and location.

Purchase the product by the end user causes a whole string of earlier events in the supply network, resulting from orders placed to suppliers (Sołtysik 2000). Re-stocking distributor, in turn, affects the supply from the manufacturer, therefore, affect the implementation of production processes, and thus supplies. Logistics supply chain manufacturing company is becoming more complex as companies expand their economic cooperation.

According to Barnes et al. (2003) structure containing a supply warehouse at production (Fig. 1), allows for the delivery of material requirements for a manufacturing plant in Just-In-Time (JIT).

Presented supply chain includes all activities related to the processing of materials and replacement goods from the raw material stage to the stage of delivery to the end user, as well as information and financial processes associated with them, as well as coordinated and integrated management (Shafia et al. 2008).

In a broader sense, the supply chain consists of two or more organizations, which may be the production company parts, components and final products or may also include the supply and distribute service providers or end-customer (SCC 2008). The most important determinant of effective supply chain management is the credibility and confidence in the relationship between partners in the chain. Therefore, in the development of any integrated supply chain, increase trust among partners and creating for them reliability are key factors to achieve sustained success (Ghazanfari & Fatholla 2006). One of the measures of confidence assessment for the project is its reliability.

Numerous studies on the problems of reliability of supply chains (Ball 1979, Barnes et al. 2003, Brzeziński 2006), treat primarily on the reduction of system performance and load changes in

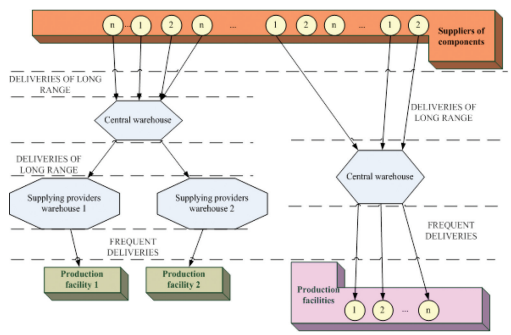


Figure 1. The concept of supply chain with and without considering the providers warehouses.

the network of transport routes (Rutkowski 2009, Seidler 1994). Analyzing the literature, reliability modeling of the logistics system or performance degradation is rarely undertaken topics.

Earlier studies (Chen et al. 1999 Dandamudi & Lu 1994) concerning the reliability of the network connections are addressed primarily to the connectivity and reliability during the trip. Logistics systems described by the authors include the transport of goods, energy, water and information on places of origin to the final consumer in terms of economic prosperity of each country. This approach, however, has limited use in planning at the level of the whole system, such as logistics network design to satisfy the requirements of reliability and supply chain costs and time rating decision.

Pierskalla & Voelker (1976) in their work took care of the problems of reliability theory of technical objects. Authors investigated discrete time vs. continuous time maintenance models, later updated by Valdez-Flores & Feldman (1989).

Improved approach propose Magott, Nowakowski, Skrobanek i Werbińska (2007), where has been taken also a problem of the influence of a spare provisioning policy on the maintenance policy. The authors have attempted to clarify the problem of providing an adequate and efficient supply of spare parts, in support of maintenance and repair of operational systems.

Werbińska-Wojciechowska (2010) in her work analized reliability of complex transportation systems. Author compared the models of systems, on the one hand, integrated, where all the components should be considered in a single model, on the other hand models, in which maintenance, replacement and inventory decisions should be considered separately.

Another approach in terms of reliability of supply chains is a Fault Trees Analysis (FTA) (1990), which is probabilistic approach to safety, reliability, and risk analysis. Traditional fault trees contain Boolean gates to represent how component failures combine to produce system failures. These fault trees are now called static. Dugan et al. (1992, 1993) in their papers presented Dynamic Fault Trees (DFTs). They suggested that Gates of DFTs can express the following features:

– dynamic replacement of failed components from pools of spares,
– failures can occur only in a predefined order.

Bobbio & Codetta (1994), extended DFTs by repair boxes. These boxes can express a repair time of components. In this paper, transformations of different gates and repair boxes into Stochastic High Level Colored Petri Net are given.

In the literature (Bobbio & Codetta 1994, Dugan et al. 1992, 1993, Magott et al. 2008, Montani 2008) can be found a number of issues dealing with the reliability of the network associated with the gates of dynamic fault trees. In most of them in calculation of probabilistic characteristics of systems using DFTs, the following formalisms are used: Markov models, Petri nets and Bayesian networks.

Magott et al. (2008), Montani et al. (2009), Mazuruk & Rzepka (2006) have modified the previous gate of dynamic fault trees. In the analyzed transportation system beyond repair and lead time, also taken into account time consuming replacement process and time resource. Through such a modification the DFT method become increasingly constrained in the expression of the time dependence in a quantitative way. Therefore, the method now as a Fault Tree with Time Dependencies method (FTTD) are not sufficient to represent the transportation system, but provides an interesting solution for non-deterministic models.

Another approach was proposed by Bobyr et al. (2008). Authors in their work in contrast to the analytic approaches they used Monte Carlo simulation. However, Monte Carlo simulation is time-consuming because of the intensive computations. This is because an extremely large number of simulated samples may be needed to estimate the reliability parameters at a high level of confidence

In summary, the available literature for the study on the reliability of supply chains can be classified according to various criteria, such as:

– relationship between the availability of information and object states (Nowakowski 2000, Seidler 1994),
– range of variability of the data relating to the subject (Du et al. 2010, Green 1995, Nowakowski 2000),
– theory (general informations) (Bukowski 2006).

2 RELIABILITY IN SUPPLY CHAINS

Term supply network exists in the literature in terms of the subject, logistical and institutional level and in terms of functional and organizational management view. In the first case, the material flows between suppliers and production companies and products between producers and final consumers (Sołtysik 2000). In the second, as a set of cooperating with each other entities (companies, firms or institutions) (Pfohl 1998, Rutkowski 2009, Witkowski 2000). However, in functional terms as a string of successive links (companies, institutions), which are involved in the shipment of products (Brzeziński 2006), and in terms of organizational managerial processes as integrated management of the flow of materials from suppliers up to final customers (Stephens 2001).

Supply network includes all activities associated with the flow of goods (Fig. 2), from sourcing of basic raw materials and ending with the sale the final product to the final customer and dispose what becomes of this product after use (Beier & Rutkowski 2000, Brzeziński 2006, Daganzo 1996, Ghazanfari & Fatholla 2006, Korzeń 2001). At every stage movement may appear phrases, or materials rejected by the next company in the chain or wastes that require disposal.

Modern supply chains are becoming more complex, increasing thus their exposure to noise and danger. Growing importance of risk management in this type of logistics structures. The supply chain is cooperating in various functional areas of mining companies, manufacturers, retailers, service providers and their customers, between which streams flow of products, information and funds. The interpretation of the structural—the personal supply chain can be (Fig. 2):

– single companies (internal supply chain);
– pair or chain of companies that are in relationships: supplier—customer;
– network, or a group of cooperating and/or competing companies.

An enterprise may be a link several supply chains at the same time; then belongs to the so-called logistics network, and one of the effects of such membership may be conflicts between the requirements of the logistics chains of adjacent cells, and the possibilities of the company.

It seems that the decomposition of the chain-link joint logistics system and logistics tasks are appropriate "levels" in reliability and risk modeling supply chains. Therefore, one should speak about the reliability of cells logistics and logistics task risk, where the insufficient reliability of the results

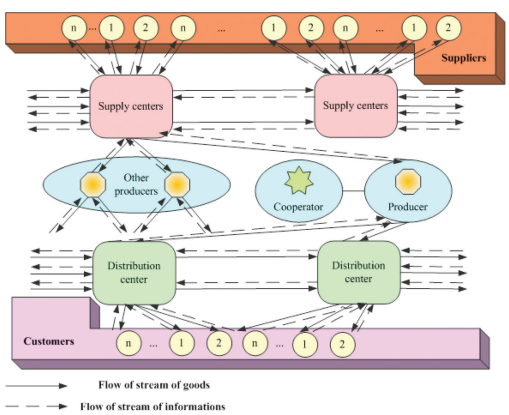


Figure 2. The general model of an integrated management of logistics network.

in a loss, you have to analyze both characteristics. As you know, determinants of reliability and risk in supply chains are "weak links"; therefore simplified reliability analysis and risk supply chains boiled down to, in particular, the analysis of these cells and logistical tasks that have been identified to as the "weak points" chain or logistics system.

According to the standards PN-82/N-04001 & PN-93/N-50191, the reliability of the system (technical object) is defined as a set of properties that describe the object and the willingness affecting it reliability, maintainability and maintenance support. Term dependability is used only for general not numerical technical description of the properties of the object.

To clarify the definition of the reliability should first introduce the importance of availability, which in accordance with the technical recognition PN-82/N-04001 means the ability of an object to remain in condition for fulfilling the required function under given conditions at a given moment or in a given time interval, assuming that there are delivered required external resources. Furthermore Villemeur (1992) assume that external funds other than funds service do not affect the availability of the object. The basic measure of availability is the availability function $Kg\ (t)$ - the probability that the i-th object is able to be in working condition (state of belonging to the set of states S^+), in given conditions, at a given time t, assuming that were delivered required external funds, the form of:

$$Kg(t) = \sum_{i \in S^+} P_i(t) \tag{1}$$

Availability is defined as a measure of the degree of the object reside in the state of functional worthiness and possibility of commencement of operation, which start time is a random variable. From the point of view of the user, the availability is a function of the frequency of occurrence of damage and related necessity to perform a repairs, the frequency of preventive handlings, time period of preventive handlings and the time period of logistics delays affecting the object.

Reliability is understood as the ability of an object to the correct operation is not interrupted with damage. Therefore means the ability of the i-th object to fulfill the required function under given conditions, in a given time interval [0, t]. Distinction is made between operational reliability (missionary) and logistics. It is assumed that at the beginning of time interval object is the state of worthiness—can properly function. Most often reliability is expressed by the probability:

$$R(t) = \sum_{i \in S^+} P_i[0,t] \tag{2}$$

Maintainability, it is the ability of an object to maintain or restore the given conditions in the state in which it can fulfill the required functions, with the assumption that the service is carried out while maintaining accepted conditions and procedures determined for each level of service.

The basic measure of the maintainability is the probability of service $M(t)$—the probability of making within a fixed time interval $[0, t]$ active service of the object exploited under certain conditions, with the assumption that the service is carried out under specified conditions with the use of specific methods and instrumentalities (Nowakowski 1999).

$$M(t) = P_t[0,t] \tag{3}$$

Referring to the logistics system there is no unambiguous definition of system reliability. According to the authors (Magott et al. 2007, Nowakowski 2000) reliability is one of the unquantifiable factors taken into account while designing logistics systems and:

- measure of the operational reliability are the interferences or the degree of performance degradation,
- is taken into account the flexibility of the system (the ability to adapt and change the area of operation) and expandability—extending the area.

The term reliability of the supply chain mostly is limited to the delivery process. Delivery service, as the output of the logistics system consists of elements such as delivery time, delivery reliability, readiness to provide the supply, quality and flexibility of supply. Delivery cycle determines the period between the filing of the order by the customer and the receipt of the goods. It consists of various components of time (time of transport, development time of the order, order-picking and preparation time), which should be taken into account.

Reliability of supply (Twaróg 2003) is determined by the ratio of orders delivered on time to the total number of demands. Quality of supply can be measured by the ratio of the number of complaints and the total number of demands. Flexibility of supply (the ability to adapt to the specific needs of customers) may be specified by the ratio of the number of fulfilled wishes to the number of these special wishes. Readiness to provide supplies may be expressed by the ratio of the number of demands realized from the warehouse to the total number of demands.

The reliability of the supply chain in discussed article will therefore mean among others (Nowakowski 2004):

- term undertake the task
- complete execution of the order,
- receipt and delivery of the goods without any damage.

Thus, an important aspect is the designation of the probability of faultless operation of the system will be the implementation of the service according with the expectation of the members of a supply chain.

3 MAPPING OF THE SUPPLY CHAIN STRUCTURE

Assume, that the structure of supply chain $\boldsymbol{S}$ can be defined as:

$$S = \langle \boldsymbol{V}, \boldsymbol{L} \rangle \tag{4}$$

where $\boldsymbol{V}$—set of numbers of elements of the supply chain of interpretation as suppliers, production companies as customers and storage facilities, $\boldsymbol{L}$—set of transport links occured between elements of the supply chain.

According to the interpretation of the supply chain, the set of its elements are the suppliers (other companies production or extraction), storage facilities and production companies. The model assumes that only the storage facilities are place of transformations performed on streams of loads.

Relationship between the elements (relations) will be transport links existing in the actual transport network.

Considering the above, the structure of the supply chain, understood as a set of elements and a set of relationships between network elements can be represented as a graph. For the purposes of the logistics network model, we assume that the network elements will be numbered with index of v. Thus $\boldsymbol{V}$ will be a set of numbers of elements of the supply chain as a:

$$V = \{v : v = 1,2, \ldots, v', \ldots, V\} \tag{5}$$

wherein V is cardinality of $\boldsymbol{V}$ set.

We assume that, in the set $\boldsymbol{V}$, distinguishes three types of subsets, i.e. set $\boldsymbol{A}$ of numbers of suppliers, which are sources of streams of goods (origin point), set $\boldsymbol{B}$ of numbers of production companies, which are the mouths of streams of goods (collection points) and a set of $\boldsymbol{M}$ of numbers of points in which material flow transformation is done (storage facilities).

Finally, the symbol $\boldsymbol{V}$ indicates a set of numbers of elements of the supply chain, i.e. the set of numbers of sources, outlets and intermediate points, which are involved in the movement of stream of loads, wherein:

$$\boldsymbol{V} = \boldsymbol{A} \cup \boldsymbol{M} \cup \boldsymbol{B} \tag{6}$$

where $\boldsymbol{V}$—set of numbers of elements of the supply chain, $\boldsymbol{V} = \{1,2, a, \ldots, m, \ldots, v, v', \ldots, b, \ldots, V\}$,

$\boldsymbol{A}$—set of numbers of sources of goods, $\boldsymbol{A} = \{v: \alpha(v) = 0,\ v \in \boldsymbol{V}\}$, $\boldsymbol{B}$—set of numbers of collection points, $\boldsymbol{B} = \{v: \alpha(v) = 1,\ v \in \boldsymbol{V}\}$, $\boldsymbol{M}$—set of numbers in which material flow transformation is done, $\boldsymbol{M} = \{v: \alpha(v) = 2,\ v \in \boldsymbol{V}\}$.

The symbol $\alpha(v)$ represents the elements of assigning functions to disjoint subsets $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{M}$ of set $\boldsymbol{V}$, $v \in \boldsymbol{V}$, wherein $\alpha(v) = 0$ when the element is the point of origin, $\alpha(v) = 1$ when the element is the point of reception, and $\alpha(v) = 2$ when the element is the point at which there is a stream of loads transforming.

Geographically elements $v \in \boldsymbol{A}$ and $v' \in \boldsymbol{B}$ in a particular case may overlap but they differ in the role they perform in the supply chain, so they are different. We assume that the division of the logistics network nodes into sets $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{M}$ is exhaustive and disjoint, i.e.:

$$\boldsymbol{A} \cap \boldsymbol{B} = \varnothing; \quad \boldsymbol{A} \cap \boldsymbol{M} = \varnothing; \quad \boldsymbol{B} \cap \boldsymbol{M} = \varnothing$$
$$\text{and } \boldsymbol{A} = \boldsymbol{V} \setminus (\boldsymbol{B} \cup \boldsymbol{M}); \quad \boldsymbol{B} = \boldsymbol{V} \setminus (\boldsymbol{A} \cup \boldsymbol{M});$$
$$\boldsymbol{M} = \boldsymbol{V} \setminus (\boldsymbol{A} \cup \boldsymbol{B}).$$

Furthermore, we assume the following assumption regarding the interpretation of logistics service providers, i.e.:

- services in the area of transport of goods are realized with the use of arcs (v, v') $v \in \boldsymbol{A}$, $v' \in \boldsymbol{B}$ of the supply chain,
- suppliers who are mapped of intermediate nodes of the logistics network $v \in \boldsymbol{M}$ realize services in the form of admission, demoulding, storage, formation and preparation of loads.

In addition, it is assumed that are possible direct transport links between the different elements of the chain, i.e. links that exist between:

- points of sources of goods and points in which material flow transformation is done;
- points of sources of goods and collection points;
- different points in which material flow transformation is done;
- points in which material flow transformation is done and collection points.

It was also assumed, that on Cartesian ratio $\boldsymbol{V} \times \boldsymbol{V}$ mapping is done ϕ conducting elements of the product in the set $\{0, 1\}$, i.e.:

$$\phi: \boldsymbol{V} \times \boldsymbol{V} \to \{0,1\} \tag{7}$$

wherein if $\phi(v,v') = 1$, then between nodes v and $v' \neq v$ there is a direct transport link, otherwise $\phi(v,v') = 0$.

We assume that $\boldsymbol{L}$ would be a set of transport links, tj.:

$$\boldsymbol{L} = \{(v,v'): \phi(v,v') = 1, \text{ for } v \neq v' \wedge v,v' \in \boldsymbol{V}\} \tag{8}$$

whose elements have the interpretation of direct transport links existing in the actual transport network.

It was assumed that set $\boldsymbol{L}$ can be decomposed into four pair wise disjoint sets. Considering the above assumptions, we assume therefore that $\boldsymbol{L}^{A,M}$ is a set of direct transport links between points of sources of goods and points in which material flow transformation is done, i.e.:

$$\boldsymbol{L}^{A,M} \subset \boldsymbol{L} \text{ and } \boldsymbol{L}^{A,M} = \{(v,v'): v \in \boldsymbol{A} \wedge v' \in \boldsymbol{M}\} \tag{9}$$

We assume that $\boldsymbol{L}^{A,B}$ is a set of direct transport links between points of sources of goods and collection points, i.e, tj.:

$$\boldsymbol{L}^{A,B} \subset \boldsymbol{L} \text{ and } \boldsymbol{L}^{A,B} = \{(v,v'): v \in \boldsymbol{A} \wedge v' \in \boldsymbol{B}\} \tag{10}$$

We assume that $\boldsymbol{L}^{M,M}$ is a set of direct transport links between different points in which material flow transformation is done, i.e.:

$$\boldsymbol{L}^{M,M} \subset \boldsymbol{L} \text{ and } \boldsymbol{L}^{M,M} = \{(v,v'): v \neq v' \wedge v,\ v' \in \boldsymbol{M}\} \tag{11}$$

We assume that $\boldsymbol{L}^{M,B}$ is a set of direct transport links between points in which material flow transformation is done and collection points, i.e.:

$$\boldsymbol{L}^{M,B} \subset \boldsymbol{L} \text{ and } \boldsymbol{L}^{M,B} = \{(v,v'): v \in \boldsymbol{M} \wedge v' \in \boldsymbol{B}\} \tag{12}$$

Considering above assumptions, it can be assumed that the supply chain network can be described by a pair $\langle \boldsymbol{V}, \boldsymbol{L} \rangle$, where $\boldsymbol{V}$ and $\boldsymbol{L}$ are respectively the non-empty sets of nodes and arcs. In order to describe the reliability of the network as a model of supply chain with regard to its independence can be used the following nomenclature:

- network consists of $\boldsymbol{V}$ nodes and $\boldsymbol{L}$ arcs,
- each element v represents respectively element of the set $\boldsymbol{V}$ (i.e. $v \in \boldsymbol{A}$, $v \in \boldsymbol{M}$ or $v \in \boldsymbol{B}$),
- each element (v, v') represents arc of the set $\boldsymbol{L}$ (wherein (v, v') belongs to the set $\boldsymbol{L}^{A,M}$, $\boldsymbol{L}^{A,B}$, $\boldsymbol{L}^{M,M}$ or $\boldsymbol{L}^{M,B}$),
- with each node v and the arc (v,v') are related the reliability of the probabilities respectively of the node $r(v)$ and the arc $r(v,v')$.

4 CRITERIA FOR EVALUATION OF OPERATIONAL EFFECTIVENESS OF THE SUPPLY CHAIN

As is apparent from the research all elements of the supply chain must fulfill their own separate performance expectations. This means that the elements in the chain may be considered as whole series of system reliability. The unreliability of one or more elements translates into a failure

of the whole chain. Conversely, the reliability of individual elements of the supply chain, makes it can meet the performance expectations in all markets in their environment. Hence, for the entire system, according to Nahmias (1989) reliability of the chain can be represented as:

$$R(\boldsymbol{V}, \boldsymbol{L}) = \prod_{v \in V:\,(v,v') \in L} \left(r(v) - r(v,v') \right) \tag{13}$$

Taking into account the above to assess the effective functioning of the entire supply chain can be a criterion of the degree of utilization of both its components and the whole system. The degree of use of the whole supply chain can be assessed as the ratio of the total time required for the transition of ordered materials for production through the supply chain in relation supplier-company to a maximum total duration of stay of vehicles in the chain.

Assuming we know moments $\theta\rho_v^{pk_n} : \theta\rho_v^{pk_n} \in \boldsymbol{T}$ of the appearance of the n-th vehicle of class pk ($pk \in \boldsymbol{S}$, $\boldsymbol{S}$-set of classes of vehicles, $pk_n \in \boldsymbol{N}(pk)$, $\boldsymbol{N}(pk)$-a set of vehicles of the class pk) in the nodes $v \in \boldsymbol{V}$ of the supply chain and exit times $\theta\kappa_v^{pk_n} : \theta\kappa_v^{pk_n} \in \boldsymbol{T}$ of the chain is the total time required to move the ordered raw production and supplied by the vehicles through the supply chain in relation supplier-company we write in the form of:

$$\sum_{v \in \boldsymbol{V}} \sum_{pk \in \boldsymbol{S}} \sum_{pk_n \in \boldsymbol{N}(pk)} \left(\begin{array}{l} \left(\theta\kappa_v^{pk_n} - \theta\rho_v^{pk_n} \right) \\ + \sum\limits_{v':\,(v,v') \in \boldsymbol{L}} \left(\theta\rho_{v'}^{pk_n} - \theta\kappa_v^{pk_n} \right) \end{array} \right) \tag{14}$$

With knowledge of the maximum capacity (number of vehicles) $\zeta^{max}(v)$ for each v-th element of the supply chain and the maximum capacity (number of vehicles) $\eta^{max}(v,v')$ of each (v,v')-th arc of the network, and assuming that we know the expected value $E(TO(v, (v,\tau), nk(v,\tau), pk))$ of service time of pk-th class of vehicle to the service station number of $nk(v,\tau)$ (charging device, discharging, etc.) in the time interval τ and the expected value $E(TO(v, v', \tau, pk))$ of service time of pk-class of vehicle to the service station number $nk(v,\tau)$ (charging device, discharging, etc.) passing the arc of the supply networks to fix a maximum total period of stay of vehicles in the supply chain by using the equation:

$$\sum_{pk \in \boldsymbol{S}} \sum_{pk_n \in \boldsymbol{N}(pk)} \left(\begin{array}{l} \sum\limits_{v \in V} \zeta^{max}(v) \mathrm{E}(c) \\ + \sum\limits_{v \in \boldsymbol{V}} \sum\limits_{v':(v,v') \in \boldsymbol{L}} \eta^{max}(v,v') \mathrm{E}(d) \end{array} \right) \tag{15}$$

where $c = \mathrm{TO}(v,(v,\tau),nk(v,\tau),pk)$, $d = \mathrm{TO}(v, v', \tau, pk)$.

Thus, the criterion of maximizing the average use of all elements of the chain can be saved the following relation, i.e.:

$$F1(\boldsymbol{\theta P}, \boldsymbol{\theta K}) = \left(\begin{array}{l} \dfrac{\sum\limits_{v \in V} \sum\limits_{pk \in \boldsymbol{S}} \sum\limits_{pk_n \in \boldsymbol{N}(pk)} \left(\theta\kappa_v^{pk_n} - \theta\rho_v^{pk_n} \right)}{\sum\limits_{pk \in \boldsymbol{S}} \sum\limits_{pk_n \in \boldsymbol{N}(pk)} \sum\limits_{v \in \boldsymbol{V}} \left(\begin{array}{l} \zeta^{max}(v) \mathrm{E}(c) + \\ \sum\limits_{v':(v,v') \in \boldsymbol{L}} \eta^{max}(v,v') \mathrm{E}(d) \end{array} \right)} \\ + \dfrac{\sum\limits_{v \in \boldsymbol{V}} \sum\limits_{pk \in \boldsymbol{S}} \sum\limits_{pk_n \in \boldsymbol{N}(pk)} \sum\limits_{v':(v,v') \in \boldsymbol{L}} \left(\theta\rho_{v'}^{pk_n} - \theta\kappa_v^{pk_n} \right)}{\sum\limits_{pk \in \boldsymbol{S}} \sum\limits_{pk_n \in \boldsymbol{N}(pk)} \sum\limits_{v \in \boldsymbol{V}} \left(\begin{array}{l} \zeta^{max}(v) \mathrm{E}(c) + \\ \sum\limits_{v':(v,v') \in \boldsymbol{L}} \eta^{max}(v,v') \mathrm{E}(d) \end{array} \right)} \end{array} \right) \to \max \tag{16}$$

where $c = \mathrm{TO}(v,(v,\tau),nk(v,\tau),pk)$, $d = \mathrm{TO}(v, v', \tau, pk)$.

A very important from the point of view of the effectiveness to the functioning degree of utilization of all elements of the supply chain. Decision variables take the form of $z_{v,nk(v,\tau)}^{t,pk_n} \in \{0,1\}$ defining assignment of vehicles pk-th class at the service station with the number $nk(v,\tau)$ in the v-th element of the chain, we can evaluate effectiveness to the functioning of the supply chain from the point of view of average use of all elements of the point of the supply chain, i.e.:

$$F2(\mathrm{Z}) = \frac{\sum\limits_{v \in V} \sum\limits_{pk \in \boldsymbol{S}} \sum\limits_{pk_n \in \boldsymbol{N}(pk)} \left(\begin{array}{l} \mathrm{E}(c) \\ \mathrm{sgn} \sum\limits_{t \in \boldsymbol{T}} z_{v,nk(v,\tau)}^{t,pk_n} \end{array} \right)}{\sum\limits_{v \in V} \zeta^{max}(v) \left(\theta\kappa_v^{pk_n} - \theta\rho_v^{pk_n} \right)} \to \min \tag{17}$$

where $c = \mathrm{TO}(v,(v,\tau),nk(v,\tau),pk)$.

Another indicator that can be used to assess effectiveness to the functioning of the supply chain is to minimize time loss occurring during logistical processes. It can be determined as the difference between the total length of stay of load in the supply chain (raw materials for production or finished goods to customers in the supply chain) and the expectation time, namely:

$$F3(\mathbf{Y},\boldsymbol{\theta}\mathbf{P},\boldsymbol{\theta}\mathbf{K})$$

$$= \left(\begin{array}{l} \left(\sum\limits_{v\in V}\sum\limits_{pk\in S}\sum\limits_{pk_n\in N(pk)} \left(\theta\kappa_v^{pk_n} - \theta\rho_v^{pk_n}\right) \right. \\ + \sum\limits_{v\in V}\sum\limits_{v':(v,v')\in L}\sum\limits_{pk\in S}\sum\limits_{pk_n\in N(pk)} \left(\theta\rho_v^{pk_n} - \theta\kappa_v^{pk_n}\right) \\ - \sum\limits_{v\in V}\sum\limits_{nk(v,\tau)\in NK(v,\tau)}\sum\limits_{(v,\tau)\in T(v)}\sum\limits_{pk\in S}\sum\limits_{pk_n\in N(pk)} \\ \left(\begin{array}{l} \mathrm{E}(c) \\ \max\limits_{t\in\left[t_\tau^v,\ t_{\tau+1}^v\right]} \left\{ z_{v,\mathrm{nk}(v,\tau)}^{t,\ pk_n} \right\} \end{array} \right) \\ - \sum\limits_{v\in V}\sum\limits_{v':(v,v')\in L(v,\tau)\in T(v)}\sum\limits_{pk\in S}\sum\limits_{pk_n\in N(pk)} \\ \left. \left(\begin{array}{l} \mathrm{E}(d) \\ \max\limits_{t\in\left[t_\tau^v,\ t_{\tau+1}^v\right]} \left\{ y_{v,v'}^{t,\ pk_n} \right\} \end{array} \right) \right) \end{array} \right) \rightarrow \min \tag{18}$$

where $c = \mathrm{TO}(v,(v,\tau),nk(v,\tau),pk)$, $d = \mathrm{TO}\ (v,\ v',\ \tau,\ pk)$.

The proposed approach to the research of the logistics process in the supply chain allows the assessment of operational reliability of the supply chain under different boundary conditions and constraints defining the equipment of the chain and for various tasks i.e. different stream of notifications of orders into the system.

5 SUPPLY CHAIN OPERATION REFERENCE MODEL AS A TOOL FOR CONTROLLING AND MANAGEMENT OF THE PROCESSES IN THE SUPPLY CHAIN

Analyzed in the article discussion concerns the supply chain model whose objective is to study the reaction speed and reliability of the chain elements to determine whether the relationships in the supply chain have a high reliability factor or not. In order to investigate the supply chain enterprises use the SCOR model (reference model of the supply chain, called Supply Chain Operation Reference-model), published by the SCC (Supply-Chain Council), which is used to describe and comprehensive analysis of the supply chain (Haj 2002, Mazuruk & Rzepka 2006, Stephens 2001, Stephan & Badr 2007). This model is a valuable tool for the analysis of the supply chain, have been used.

SCOR model allows for measurement, control and management processes throughout the supply chain-pond, covering all participants (manufacturers, transport companies, distributors, consumers). It is based on five main by processes SCM (Supply Chain Management) (Haj 2002, Stephens 2001, Stephan & Badr 2007):

- "Plan"—covers the planning and allocation of resources, capacity and trade rules along the supply chain and aims to streamline procurement processes, production and supply in terms of resources and demand,
- "Source"—includes the processes of sourcing, purchasing goods and services and the management of the sources of supply,
- "Make"—includes the planning and implementation of the transformation processes that convert the available goods and services in the ordered goods,
- "Deliver"—includes the management of the orders, storage, transportation and installation of goods or commercial goods,
- "Return"—these processes include the organization and execution of shipments of returnable defective products cases, warranty and unnecessary resources to suppliers or customers,

SCOR model supports the operating indicators for the evaluation on four levels (Haj 2002, Stephens 2001).

- "Top Level": by assigning the main processes allows a clear view of the supply chain.
- "Configuration Level": at this level, there is a total of 21 categories of processes for the processes of the first level, by means of which the supply chain can be configured. For each executive process Source, Make, Deliver shared is a variant-oriented warehouse (MTS), in order (MTO) and structure (ECA).
- "Process Element Level": here distributes selected at level 2 categories on the process chains processes and individual elements of the transaction. These elements are closer to the process defined on the basis of input and Output documentation, good examples, support systems and process indicators.
- "Implementation Level": this level is specific to the company and is not part of the reference model. Using the SCOR model processes must be transferred at least to the fourth level, to be able to introduction standardized waveforms in the company.

SCOR model, through the defined process components, allows for modeling, measuring of the description and evaluation of the entire supply chain. It can also serve the restructuring process

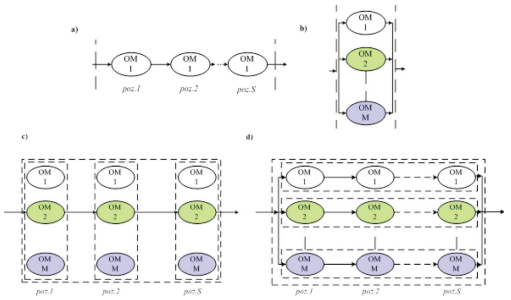


Figure 3. Reliability structures on the example of of supply chains storage facilities (OM) in the system: a) series, b) parallel, c) series-parallel, d) parallel-series.

or construction of a new business area or product line (Mazuruk & Rzepka 2006, Stephens 2001, Stephan & Badr 2007).

Measures from the first level approach to supply chain management in order to assess, and the relevant parameters from the second and third contain more specific and detailed criteria for the categories and components processes. Indicators of the level of the first SSC (2006) divided into five operational criteria, of which three, reliability, flexibility and speed of response, are directed to the attributes of the client, and the other two, expenses and assets are used to measure inside the company. Each of these measures is further divided into small ratios at lower levels.

According to sources in the literature (Stephan & Badr 2007) the level of reliability of the supply chain of the first level can be assessed and measured by SCOR metrics superior orders, and at the other by a metric superior orders, deliveries in a timely manner, with appropriate documentation and excellent quality delivered the goods to the customers.

On the third and fourth level supply chain by SCOR model can be seen small, but more detailed metrics for the evaluation of these measures. It is possible to calculate the level of reliability in each loop chain wide variety of pre-selected time periods. In order to measure the speed of the reliability of the entire supply chain in a certain period of time (Haj 2002) proposes that the first step is to determine the type of supply chain, which can be placed in one of five possible structures of reliability (Fig. 3), i.e., serial, parallel, series-parallel or a parallel—serial, and then, on the basis of a formula related reliability of the system, it is possible to calculate the reliability of the whole system during that period.

6 CONCLUSIONS

The proper functioning of all elements of the supply chain significantly affect the quality of the final product, and hence on:

– meeting customer requirements, which translates into the realization of business objectives,
– greater chance of further contracts, and thus the development of the entire supply chain,
– enhancing ties customer-supplier-subcontractor throughout the life cycle of the product.

The efficiency of the supply chain is a cumulative characteristics of quality of functioning of the entire supply chain, which can be expressed by means of specific characteristics. It determines the effectiveness of expenditure incurred for the useful effects, such as reducing time loss of implementation of a logistics process in the supply chain.

Thus, the proposed indicators to assess effectiveness to the functioning of the chain can be a feature of the system, measurable and useful when comparing supply chains of the same class, expressing different aspects of the different compartments depending on their purpose and conditions of use.

The effective functioning of supply chains is very important not only for companies but also for logistics operators and transport companies, largely because it affects the level of service provided by these companies.

The supply chain will be effective when provided implementation of the agreed tasks at the required level of quality at a reasonable use of the equipment of the whole chain. Thus, analysis of supply chain efficiency should be based on its graduation from global ratings to the partial assessments concerning overall resource efficiency of the chain and the cost of tasks realization.

REFERENCES

Ball M.O. (1979). Computing Network Reliability. *Operations Research*, 27: 823–838.

Barnes, E., Dai, J., Deng, S., Down, D., Goh, M., Lau, H.C., Sharafali, M. (2003). On the Strategy of Shupply Hubs for Cost Reduction and Responsiveness. *White Paper, The Logistics Institute—Asia Pacific*, National University of Singapore, Singapore.

Beier F.J., Rutkowski K. (2000). *Logistyka*. OW SGH, Warszawa.

Besag J., York J., Mollie A. (1991). Bayesian Image Restoration with Two Applications In Spatial Statistics. *Annals of the Institute of Statistical Mathematics*, 43, 1–59.

Bobbio A., Codetta D. (2004). Parametric fault trees with dynamic gates and repair boxes, in: *Proc. Annual Symposium on Reliability and Maintainability*: 459–465.

Bobyr M., Yakhno B., Rusinski E., Harnatkiewicz P. (2008). Damage in the complex low-cycle fatigue. *Archives of Civil and Mechanical Engineering*, Vol. VIII, no. 3: 23–31.

Box, G.E.P., and Tiao, G.C. (1973). *Bayesian Inference in Statistical Analysis*. London: Addison-Wesley.

Bramel, J., and D. Simchi-Levi (1997), The Logic of Logistics: Theory, Algorithms and Applications for Logistics Management. New York: Springer-Verlag.

Brzeziński M. (2006). Logistyka w przedsiębiorstwie, Dom Wydawniczy Bellona, Warszawa.
Bukowski L., Majewska K. (2006). Evaluation of uncertainty of logistic systems, (in Polish), *Wybrane Zagadnienia Logistyki Stosowanej*, Oficyna Wydaw. TEXT, Kraków, No. 3, pp. 9–22.
Chen, A., Yang, H., Lo, H., and Tang, W.H. (1999). A Capacity Related Reliability for Transportation Networks. *Journal of Advanced Transportation*, 33(2), 183–200.
Daley, D.J., and Vere-Jones, D. (1988), Introduction to the Theory of Point Processes. New York: Springer.
Daganzo, C.F. (1996). *Logisitcs Systems Analysis*, New York: Springer Verlag.
Dandamudi, S., and Lu, J.-C. (2004). Competition Driving Logistics Design with Continuous Approximation Methods. *Technical Report of the School of Industrial and Systems Engineering*, Georgia Tech, http://www.isye.gatech.edu/apps/research-papers/.
Diebolt, J., and Robert, C.P. (1994). Estimation of Finite Mixture Distributions through Bayesian Sampling. *Journal of the Royal Statistical Society*, Series B, 56, 363–375.
Diggle, P.J. (1990). A Point Process Modelling Approach to Raised Incidence of a Rare Phenomenon in the Vicinity of a Pre-specifed Point. *Journal of the Royal Statistical Society*, Series A, 153, 349–362.
Du L., Wang Z., Wang H-Z. (2010). Cost-type function analysis in dynamic design under uncertainty, *Maintenance and Reliability*, Vol. 46, No. 2, pp. 17–20.
Dugan J.B., Bavuso B., Boyd M. (1992). Dynamic fault tree models for fault tolerant computer systems. *IEEE Trans. Reliability*, Vol. 41, 363–377.
Dugan J.B., Bavuso B., Boyd M. (1993). Fault trees and Markov models for reliability analysis of fault tolerant systems. *Reliability Engineering and System Safety*, Vol. 39, 291–307.
Fault Tree Analysis (1990), International Technical Commission, *IEC Standard*, Publication 1025.
Ghazanfari M., Fatholla M. (2006). *A comprehensive look at supply chain management*, 1st edn. Iran Science and Technology University Publications, Tehran.
Gołembska E. (1994). *Logistyka jako zarządzanie łańcuchem dostaw*. AE, Poznań.
Green, P.J. (1995). Reversible Jump Markov Chain Monte Carlo Computation and Bayesian Model Determination. *Biometrika*, 82, 711–732.
Haj Shirmohammadi A. (2002). Programming maintenance and repair. *Technical management in industry*, 8th edn. Ghazal Publishers, Esfahan.
Huang C.H., Sheoran S.K., Keskar H. (2005). Computer-assisted supply chain configuration based on supply chain operations reference (SCOR) model. *Computers & Industrial Engineering*, vol. 48, Issue 2.
Klir G.J. (2004). Generalized information theory: aims, results and open problems, *Reliability Engineering & System Safety*, Vol. 85, pp. 21–38.
Korzeń Z.: Logistyczne systemy transportu bliskiego i magazynowania. t. 1, 2, ILiM, Poznań 2001.
Langevin, A., Mbaraga, P., and Campbell, J. (1996), "Continuous Approximation Models in Freight Distribution: An Overview," Transportation Research B, 30, 163–188.
Magott J., Nowakowski T., 12. Skrobanek P., Werbińska S. (2007). Analysis of logistic support system using Fault Trees with Time Dependencies. *Archives of Transport*,No. 4.
Magott J., Nowakowski T., Skrobanek P., Werbińska S. (2008): Analysis of possibilities of timing dependencies modelling—example of logistic support system. *European Safety and Reliability Association Conference*, ESREL, Valencia, Spain, Leiden: Taylor and Francis, 1055–10.
Magott J., Nowakowski T., Skrobanek P., Werbińska S. (2009). Logistic system modelling using Fault Trees with Time Dependencies—example of tram network. *European Safety and Reliability Association Conference*, ESREL, Praha, Czech Republic, Leiden: Taylor and Francis, 2293–2300.
Magott, J., Skrobanek, P. (2000). A method of analysis of fault trees with time dependencies. In Proc. *SAFECOMP'2000*, Rotterdam, The Netherlands, LNCS, Vol. 1943, Springer-Verlag, 176–186.
Montani S., Portinale L., Bobbio A., Codetta-Raiteri D. (2008). RADYBAN: a tool for reliability analysis of dynamic fault trees throughconversion into dynamic Bayesian networks. *Reliability Engineering and System Safety*, Vol. 93, 922–932.
Mazuruk M., Rzepka M. (2006). Przegląd łańcucha dostaw według SCOR. Jak skutecznie kontrolować przepływ materiałów? *EuroLogistics*, nr3.
Nahmias S. (1989). *Production and Operations Analysis*. Homewood, IL: Richard D. Irwin, Inc.
Nowakowski T. (1999). *Metodyka prognozowania niezawodności obiektów mechanicznych*. 14. PW, Wrocław.
Nowakowski T. (2000). Models of uncertainty of operation and maintenance information, *Zagadnienia Eksploatacji Maszyn*, Vol. 35, No. 2, pp. 143–150.
Nowakowski T. (2004). Problemy niezawodności funkcjonowania systemów logistycznych. *Inżynieria Maszyn*, vol. 9, zeszyt 1.
Pate-Cornel M.E. (1996). Uncertainty in risk analysis: six levels of treatment. *Reliability Engineering & System Safety*, Vol. 54, pp. 95–111.
Pfohl H. (1998). Logistyka w systemie przedsiębiorstw zintegrowanych. Łańcuch, cykl zamknięty, sieć. *Materiały Międzynarodowej konferencji Logistics '98* ILiM i PTL Katowice.
Pierskalla W.P., Voelker J.A. (1976). A survey of maintenance models: the control and surveillance of deteriorating systems. *Naval Research Logistics Quarterly*, 23, 353–388.
PN-82/N-04001, Eksploatacja obiektów technicznych. Terminologia ogólna.
PN-93/N-50191, Słownik terminologiczny elektryki. Niezawodność, jakość usługi.
Reilly, C., Schacker,T., Haase, A.T., Wietgrefe, S., and Krason, D. (2002), "The Clustering of Infected SIV Cells in Lymphatic Tissue," Journal of the American Statistical Association, 97, 943–954.
Rutkowski K. (2009). *Logistyka dystrybucji*. Wydawnictwa SGH, Warszawa.
Sanso, B. and Soumis, F. (1991). Communication and Transportation network reliability using routing models. *IEEE Transaction on Reliability*, 40: 29–37.
Seidler J.A. (1994): Fundamental concepts of intelligent info system theory, *Information Systems Architecture and Technology ISAT '94*, Proceedings of 16th Scientific School, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław.

Shafia M.A., Jabal Ameli M.S., Fathollah M. (2008). A study of the effect of sharing costs in the supply chains based on SCOR. *The International Journal of Industrial Management and Production Management*, Iran Science and Technology University.

Shi, V. (2004), Evaluating the Performability of Tactical Communications Network. *IEEE Transaction On Vehicular Technology*, 53, 253–260.

Sołtysik M. (2000). *Zarządzanie logistyczne*. AE, Katowice.

Stephens S. (2001). Supply Chain Council & Supply Chain Operations Reference (SCOR). Model Overview. *Supply Chain Management An International Journal*.

Stephan J, Badr Y. (2007). A quantitative and qualitative approach to manage risks in the supply chain operations reference. *2nd International Conference on Digital Information Management* 1:410–417.

Stewart G. (1997). Supply-chain operations reference model (SCOR): the first cross-industry framework for integrated supply-chain management. *Logistics Information Management*, Vol. 10 Iss: 2.

Supply Chain Council (2006). Supply chain operations reference (SCOR) model version 8.0. http://www.scribd.com/doc/2939600/.SCOR-Model-Version-8. Dostępne 16.08.2012.

Supply Chain Council (2008). *Supply chain operations reference (SCOR) model version 10.0: overview*. http://supply-chain.org/f/SCOR-Overview-Web.pdf Dostępne 16.08.2012.

Szymanowski W. (2008). *Zarządzanie łańcuchem dostaw żywności w Polsce. Kierunki zmian*. Difin, Warszawa.

Taniguchi, E., Thompson, R.G., Yamada, T., and Duin, R.V. (2001), *City Logistics*. New York: Elsevier Science Ltd.

Twaróg J. (2003). *Mierniki i wskaźniki logistyczne*, wyd.1. Instytut Logistyki i Magazynowania, Poznań.

Valdez-Flores C., Feldman, R. (1989). A survey of preventive maintenance models for stochastically deteriorating single-unit systems. *Naval Research Logistics*, Vol. 36, 419–446.

Villemeur A. (1992). *Reliability, Availability, Maintainability and Safety Assessment*. Wiley.

Werbińska-Wojciechowska S. (2010). Time Dependencies in Supply Chain Perfomance Process, *Logistics and Transport*. No 1(10)/2010.

Witkowski J. (2000). Logistyka w organizacjach sieciowych, *Gospodarka materiałowa i logistyka*, nr 7–8.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Effectiveness of national transport system according to costs of emission of pollutants

M. Jacyna, K. Lewczuk, E. Szczepański, P. Gołębiowski, R. Jachimowski, M. Kłodawski, D. Pyza, O. Sivets, M. Wasiak & J. Żak
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

I. Jacyna-Gołda
Faculty of Production Engineering, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: The paper presents the problem of the effectiveness of the national transport system in terms of the cost of emissions. It sets out the general principles of research methodology, taking into account actual emissions from vehicles. The paper formalized effectiveness indicators for road transport modeling of such systems. Transport effectiveness is characterized by significant difficulties in the study due to the large scale of the system as well as many of the entities involved and the need to take into account their interests. Transport is a very important sector of the economy contributing to its development and the development of societies. In view of the above, the paper also presents an example of research on the identification of Polish areas with increased emissions in a macro scale. This article is the result of works done in the project EMITRANSYS funded by the National Centre for Research and Development in Poland.

1 INTRODUCTION

1.1 *General assumptions*

Road transport is the dominant mode of transport in the European Union and is responsible for environmental pollution (Przybyłowski 2011). In turn rail transport is the second most popular mode of transport, but it involves other environmental threats than road. Both modes are included in the national transport systems. The European Union is taking actions to reduce harmful effects of transport through the integration of transport policy with environmental policy, which is to lead to the formation of environmentally friendly transport system (Ambroziak et al. 2013).

Road transport pollution spreads in close proximity to human settlements at high concentrations at low altitudes (Danklefsen 2011) and depends on many factors such as fuel composition, engine type, vehicle maintenance, type and basic characteristics of the vehicle, deployment of infrastructure, speed patterns, routing, congestion, etc. Research on the analysis of emissions under real conditions indicate that certain toxic components of exhaust gases are as much as several hundred percent larger than from non-transport sources for both gaseous compounds (see Engeljerhinger 2011, Merkisz et al. 2014a,b, Merkisz & Pielecha 2014) and particle matter (see Merkisz & Pielecha 2014, Steiningier 2009). Harmful components of exhaust gases are divided into: harmful for living creatures and regulated by Euro standards (carbon monoxide, hydrocarbons, nitrogen oxides, nitrogen oxides) and non-regulated (nitrogen dioxide, sulfur oxide, non-methane HC) and harmful for environment i.e. carbon dioxide, CO_2 equivalent, ammonia, nitrous oxide, methane (REGULATION EC No 715/2007).

National transport system embraces all transport infrastructures and supports all types of vehicles and all types of loading forms. It is based mostly on road transport network—a source of pollutants, which closely cooperates with railway transport, so effect of comodality can be a significant factor creating total pollution patterns on national level.

National transport system should be constantly designed and controlled with regard to different aspects of its activity including environment degradation, economic and social needs. Proper designing and controlling mean right usage of resources reflected in relation between expenditures and

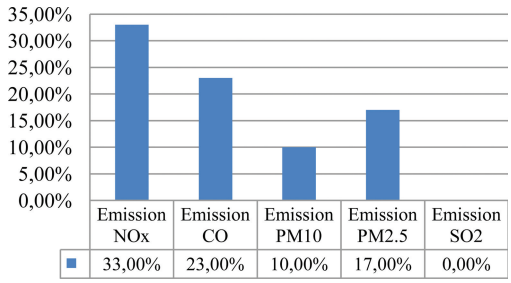


Figure 1. Share of air pollutants from road transport in Poland in 2011. Source: based on KOBiZE 2013.

effects. The effect of particular importance is environment degradation expressed by costs of emission correlated to means of transport, especially road transport.

Effectiveness of transport system embraces different aspects. Individual users perceive differently advantages and costs of transport. In the assessment process it is essential to have possibility of selection of options of infrastructure adjustment to perform transport tasks. The complexes of decisions affect the effectiveness of integrated transport systems (Leontiadis et al. 2011).

1.2 *Road transport emission*

In addition to road transport the sources of air pollutions are (KOBiZE 2013): production processes, energy transformation (coal to electricity), non-industry combustion processes, waste management, agriculture. Figure 1 presents emission levels of basic pollutants from road transport in Poland in 2011.

Against the background of the national emissions, road transport produces 33.18% of nitrogen oxides (NO_x), 23.15% of carbon monoxide (CO), 10.36% and 17.18% of particulate matter (respectively PM10 and $PM_{2,5}$). Emission of sulfur dioxide (SO_2) is 0.15%, and nowadays is not considered as important pollutant. The road infrastructure in Poland is around 3% of the country, but within the direct impact of transport pollution is about 50% of the Poland (Ambroziak et al. 2013).

2 ROAD TRANSPORT EFFECTIVENESS

Efficiency of large scale transport systems is difficult to define and measure because of system complexity and range. According to definition, efficiency is a result of undertaken actions, described by relation of gained effects to expenditures (Leontiadism et al. 2011). Efficiency is correlated to: performance; taking right actions, and efficacy; assessment of fairness of method adopted to the planned goals.

Most commonly the inputs for effectiveness calculation are the costs of actions, and the effects in the form of mass of transported goods and number of conveyed passengers or the transport performance measurements like tonne-km and passenger-km.

Effectiveness of transport system in terms of sustainable economy means minimization of external costs at the least possible increase in direct costs of transport. Presented paper limits discussion to the external cost resulting from emission.

The basic measures of effectiveness of national transport system are economic and ecological (Delucchi & McCubbin 2011). If the emission is considered as effect of transport activity, then following economic measures are used:

– Difference between the costs incurred by society for treatment of diseases and saving the natural environment arising due to air pollution and expenditures greening of the transport system:

$$\sum_{s\in S} kz(s) - \sum_{r\in R} n(r) \tag{1}$$

where:

$kz(s)$—costs of prevention of harmful effects of s-th compound of exhaust gases; $n(r)$—expenditures to increase environmental friendliness of r-th mode of transport.

– Quotient of the costs incurred by society for treatment of diseases and saving the environment due to the expenditures increasing environmental performance of the transport system.

$$\sum_{s\in S} kz(s) \Big/ \sum_{r\in R} n(r) \tag{2}$$

– The quotient of the difference between the costs incurred by society for treatment of diseases and saving the environment in the following two years and expenditures increasing environmental performance of the transport system.

$$\left(\sum_{s\in S} kz(s,t) - \sum_{s\in S} kz(s,t-1)\right) \Big/ \sum_{r\in R} n(r,t) \tag{3}$$

The ecological measures are then:

– The quotient of the number of vehicles with the highest EURO standard to the total number of vehicles in the country:

$$\exists neu \quad \sum_{st\in ST} l(st,neu) \Big/ \sum_{neu\in Neu} \sum_{st\in ST} l(st,neu) \tag{4}$$

where: $l(st,neu)$—numer of st-th type vehicles keeping neu-th EURO standard.

– The quotient of volume of transport done by low-emission modes (eg. inland, rail) to transport volume done by all modes of transport.

$$\sum_{r\in R_e} q(r) \Big/ \sum_{r\in R} q(r) \tag{5}$$

where: $q(r)$—transport volume done by r-th mode, R_e—set of low emission modes $R_e \subset R$.

From an economic point of view, the criterion of the transport system performance evaluation is the direct cost of transportation (Mashayekh et al. 2011). Taking into account previously formulated markings; criterion can be given as follows:

$$\sum_{neu\in Neu}\sum_{st\in ST} l(st,neu)\cdot c(st)\cdot d(st) \longrightarrow \min \tag{6}$$

where: $c(st)$—unit costs of transport by st-th type of vehicle; $d(st)$—the average distance covered by st-th type of vehicle.

3 EFFECTIVENESS FORMALIZATION

3.1 *General remarks*

Estimation of ecological efficiency of national transport system requires formal model of this system to represent its complexity and its features significant for the purpose of research (Jacyna 2012).

Considering tasks realized by national transport system, the model developed to estimate emission and ecological interactions must include following elements:

– Structure of the system representing real transport connections between its elements,
– Characteristics mapping real features of system structural elements important for proper flows distribution that minimize emission of harmful compounds, including technical, organizational and economical characteristics,
– Transport tasks defined as material and passenger streams between points of origin and destinations,
– Organization of flows in the system representing the ways of usage of elements of transport infrastructure.

The model of proecological transport system (MEST) is then given as follows (Jacyna et al. 2013, Jachimowski et al. 2013):

$$\mathbf{MEST} = <\boldsymbol{GE}, \boldsymbol{FE}, \boldsymbol{QE}, \boldsymbol{OE}, \boldsymbol{IE}> \tag{7}$$

where: $\boldsymbol{GE}$—graph of system structure; $\boldsymbol{FE}$—set of characteristics representing real features of system elements; $\boldsymbol{QE}$—transportation tasks performed by system representing all material and passenger flows given as origin-destination matrixes; $\boldsymbol{OE}$—organization—the way of realizing transportation tasks by system with regard to emission of harmful compounds—apportion of material and passenger flows on transportation network; $\boldsymbol{IE}$—databases and information systems.

Organization of material flow determines desired way of transport tasks realization by transport system. So, the load of transport links by vehicles of different types according to different segments of demand for freight and passenger transport is sought. The load of elements of transport network results from directing means of transport to the routes identified in particular transport relations (Farmer 2013, Sivilevičius 2011).

3.2 *Structure and characteristics of the model*

The infrastructure has basic meaning for realization of transport tasks:

– Line; existing transport links (road, rail),
– Point; logistics infrastructure for material handling and passenger servicing;
– Information; processing data, security.

as well as superstructure embracing means of transport fitted to different tasks and types of infrastructure.

In formal way the structure of national transport system is modelled by a graph $\boldsymbol{GE} = <\boldsymbol{WE}, \boldsymbol{LE}>$ where $\boldsymbol{WE} = \{1, \ldots, a, \ldots, b, \ldots, i, \ldots, i', \ldots, WE\}$ is a set of transport nodes including origin and destination points, $\boldsymbol{LE}$ is a set of transport links between nodes of transport representing different modes of transport and different possibilities of movement.

The set $\boldsymbol{WE}$ is divided into three subsets: the set of origins of material and passenger flows $\boldsymbol{N}$, the set of destinations of material and passenger flows $\boldsymbol{O}$, and set of intermediate (transition) points $\boldsymbol{P}$.

For each pair of nodes $(a,b)\in \boldsymbol{E}$, $a\in \boldsymbol{N}$, $b\in \boldsymbol{O}$ the transport relation can be set. For each relation, a set of potential transport paths $\boldsymbol{P}^{ab}$ is known. A single path in a given relation (a, b) is numbered with index p, where $p\in \boldsymbol{P}^{ab}$ so $\forall(a,b)\in \boldsymbol{E} \quad \exists p \in \boldsymbol{P}^{ab}$. Moreover $\boldsymbol{P}_{ii'}^{ab}$ is a set of paths in relation (a, b) passing the (i, i')-th transport link.

Numbers of nodes in set $\boldsymbol{P}$ represent real transport nodes of different types like crossroads, stops, stations, airports, terminals, and other points where characteristics of infrastructure change. Nodes in sets $\boldsymbol{N}$ and $\boldsymbol{O}$ represent areas generating demand for transportation.

Transport links are characterized by assigned types of vehicles to move on $\boldsymbol{ST}'(i, i')$, assigned

EURO standards to enter $\boldsymbol{NEU}(i, i')$, lengths $l(i, i')$, entering costs $k_d(i, i')$, speed limits $v^{max}(i, i')$, capacity $d(i, i')$, loading capacity $DMC(i, i')$, axle load limits $Qosi(i, i')$, horizontal gauge $B(i, i')$ vertical gauge $H(i, i')$, area type $\boldsymbol{OB}(i, i')$, as well as relevant for estimating the dispersion: longitudinal inclination, the occurrence of road noise barriers or plantings, most frequent wind direction and the location of the section in the plan (its direction).

Due to the purpose of the research significant characteristics of means of transport related to the capacity and utilization, operating costs and function of emission according to speed and mileage (the effect of heating up the engine) are noted. For the purpose of research it was assumed that $\boldsymbol{S} = \{1, \ldots, s, \ldots, S\}$ is a set of harmful compounds of exhaust gases. Then characteristics of means of transport are as follows:

- maximal loading capacity of $n(st)$-th vehicle of st-tego type, $q_{max}(n(st), st)$,
- permissible load of $n(st)$-th vehicle of st-th type, $q_{dop}(n(st), st)$,
- cubic capacity of number of passengers of $n(st)$-th vehicle of st-th type, $p(n(st), st)$,
- permissible weight of $n(st)$-th vehicle of st-th type, $DMC(n(st), st)$,
- permissible axle loads of $n(st)$-th vehicle of st-th type, $qosi(n(st), st)$,
- emission standard kept by $n(st)$-th vehicle of st-th type, $nes(n(st), st)$,
- height of $n(st)$-th vehicle of st-th type, $h(n(st), st)$,
- width of $n(st)$-th vehicle of st-th type, $b(n(st), st)$,
- coefficient of average fulfilment of st-th type of vehicle when conveying materials of spt-th demand segment, $Ct(st, spt)$,
- average capacity utilization coefficient of st-th type of vehicle when conveying passengers of spp-th segment of demand, $Cp(st, spp)$,
- average exploitation cost of st-th type vehicle dependent on mileage, $k_l(st)$,
- average exploitation cost of st-th type vehicle dependent on work time, $k_h(st)$,
- level of unit emission of s-th compound identified for st-th type of vehicle, driven by engine of $rsp(st)$-th type, keeping $neu(st)$-th emission standard and moving on (i, i')-th segment of transport network, $em(s, st, neu(st), rsp(st), i, i')$,
- the rate of the effect of the route mileage on unit emission of s-th compound identified for st-th type of vehicle, driven by engine of $rsp(st)$-th type, keeping $neu(st)$-th emission standard and moving on relation (a, b) on p-th route, $\psi(s, st, neu(st), rsp(st), p, a, b)$,
- the number of available st-th type vehicles with $rsp(st)$-th type of engine and keeping $neu(st)$-th EURO standard, $lp^{max}(st, neu(st), rsp(st))$.

Above characteristics are necessary because particular vehicles are different according to usage, type of engine, fuel, capacity etc.

3.3 *Selected criteria for emission estimation*

The problem is reduced to seting values of decision variables:

- number of freight vehicles $xt(p,a,b,st)$ of st-th type moving through p-th path in relation (a,b),
- number of passenger vehicles $xp(p,a,b,st)$ of st-th type moving through p-th path in relation (a,b),

to extremize values of criteria of effectiveness of national transport system in relation to emission of harmful compounds. According to the nature of the problem criteria functions describe the level of emission of different compounds while the transportation process is performed (Kok et al. 2011). For optimal solution these criteria will take possibli lowest values. Criterion describing level of emission is as follows $\forall s \in \boldsymbol{S}$:

$$\sum_{st\in\boldsymbol{ST}}\sum_{(i,i')\in\boldsymbol{LE}}\sum_{(a,b)\in\boldsymbol{E}}\sum_{p\in\boldsymbol{P}^{ab}_{i,i'}}\left[xt(p,a,b,st)+xp(p,a,b,st)\right]\cdot l(i,i')\cdot ema(s,st,i,i')\cdot\psi a(s,st,p,a,b)\longrightarrow\min \tag{8}$$

where coefficients of unit emission $ema(s,st,i,i')$ and $\psi a(s,st,p,a,b)$ are set by formulas (9) i (10):

$$\forall s\in\boldsymbol{S}\ \ \forall st\in\boldsymbol{ST}\ \ \forall(i,i')\in\boldsymbol{LE}^{\boldsymbol{PP}}\quad ema(s,st,i,i) = \frac{\sum\limits_{\substack{rsp(st)\\ \in\mathbf{RSP}(st)}}\ \sum\limits_{\substack{neu(st)\\ \in\mathbf{NEU}(st)\\ \cap\mathbf{NEU}(i,i')}} \begin{pmatrix} em(s,st,neu(st),rsp(st),i,i') \\ \cdot lp^{max}(st,neu(st),rsp(st)) \end{pmatrix}}{\sum\limits_{\substack{rsp(st)\\ \in\mathbf{RSP}(st)}}\ \sum\limits_{\substack{neu(st)\\ \in\mathbf{NEU}(st)\\ \cap\mathbf{NEU}(i,i')}} lp^{max}(st,neu(st),rsp(st))} \tag{9}$$

$$\forall s\in\boldsymbol{S}\ \ \forall st\in\boldsymbol{ST}\ \ \forall(a,b)\in\boldsymbol{E}\ \ \forall p\in\boldsymbol{P}^{\mathbf{ab}}\quad \psi a(s,st,p,a,b) = \frac{\sum\limits_{\substack{neu(st)\\ \in\mathbf{NEU}(st)}}\ \sum\limits_{\substack{rsp(st)\\ \in\mathbf{RSP}(st)}} \begin{pmatrix} \psi(s,st,neu(st),rsp(st),p,a,b) \\ \cdot lp^{max}(st,neu(st),rsp(st)) \end{pmatrix}}{\sum\limits_{\substack{neu(st)\\ \in\mathbf{NEU}(st)}}\ \sum\limits_{\substack{rsp(st)\\ \in\mathbf{RSP}(st)}} lp^{max}(st,neu(st),rsp(st))} \tag{10}$$

From an economic point of view, the criterion of performance evaluation of the transport system

is the direct cost of transportation. Taking into account previously formulated markings, criterion can be ascribed as follows:

$$\sum_{\substack{st \\ \in \boldsymbol{ST}}} \sum_{\substack{(i,i') \\ \in \boldsymbol{LE}}} \sum_{\substack{(a,b) \\ \in \boldsymbol{E}}} \sum_{\substack{p \\ \in \boldsymbol{P}_{i,i'}^{ab}}} \left[\begin{matrix} xt(p,a,b,st) \\ + xp(p,a,b,st) \end{matrix} \right] \cdot c(st,i,i') \longrightarrow \min \tag{11}$$

where: costs $c(st,i,i')$ of entering particular types of transport links by means of transport are set from formula (12):

$$\forall st \in \boldsymbol{ST} \;\; \forall (i,i') \in LE^{\boldsymbol{PP}}$$
$$c(st,i,i') = k_l(st) \cdot l(i,i') + \frac{k_h(st) \cdot l(i,i')}{v(i,i',\mathbf{X}^*)} + k_d(i,i') \tag{12}$$

where: ($k_l(st)$ and $kh(st)$) are cost characteristic of means of transport, $v(i,i',\mathbf{X}^*)$—average velocity of traffic on given transport link dependent on cargo and passenger distribution $\mathbf{X}^*$.

Of course solutions are sought under appropriate conditions and restrictions touching among others; range of variability, exceeding capacity, or limiting acsess to certain areas or sections of roads, etc (Sen et al. 2010).

4 EXEMPLARY AREAS OF POLAND WITH HIGHER CONCENTRATION OF SELECTED COMPOUNDS

Considerations presented below have been compiled basis on the researches included in Ambroziak et al. 2013 that have been conducted for the EMITRANSYS project. Chief Inspectorate of Environmental Protection in Poland on the basis of regional data provides an annual assessment of air quality in specific areas of Poland (GIOŚ 2011, GIOŚ 2012). Assessment has been carried out taking into account two criteria: protection of human health (criterion f_1), protection of plants (criterion f_2). Effectiveness of national transport system according to pollution can be presented on examples of areas contaminated by harmful compounds of fumes arising from road transport. Railway transport is not included because its indirect air pollution share.

The first criterion bases on sulfur dioxide, nitrogen dioxide, carbon monoxide, benzene, ozone, particulate matter PM10, lead, arsenic, cadmium, nickel and benzo(a)pyrene contained in PM10, particulate matter PM2,5. Second criterion uses: sulfur dioxide, nitrogen oxides and ozone. Highlighted substances are emitted by means of transport and measurements are performed in relation to areas (zones), comprising:

- agglomerations with a population of over 250 thousand inhabitants,
- cities (non-urban area) with a population of over 100 thousand inhabitants,
- remaining areas of the voivodships, not forming part of the agglomeration and city with over 100 thousand inhabitants.

The area can be assigned to one of the classes depending on concentration level of harmful compounds: A—concentrations not exceeding the permissible level, B—concentration above the permissible level, but not exceeding the permissible level plus the margin of tolerance, C—concentration above the permissible level plus the margin of tolerance, D1—concentrations not exceeding the level of the long-term target, D2—concentration above the level of long-term target.

Figures 2 and 3 show the areas contaminated by nitrogen oxides (NO_x) emitted by means of transport too.

Assessing areas for safety of human health the level above the permissible for nitrogen dioxide was recorded in five areas: in the agglomeration of Warsaw and Krakow and in the Silesian conurbation and in Czestochowa and Wroclaw. Due to the criterion of plant protection in the whole country the level of concentrations of nitrogen oxides did not exceed permissible level. The share of road transport in total emissions of nitrogen dioxide is high and is at the level 33.18%. Based on the preliminary analysis carried out and the data available

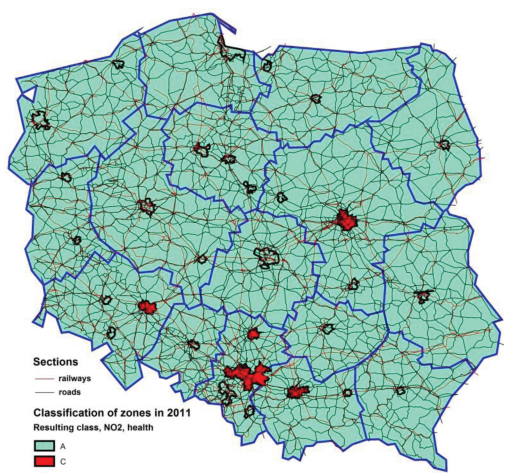


Figure 2. Classification of areas in Poland according to NO_2 emission in 2011 (criterion f_1). Source: own research based on GIOŚ 2011, GIOŚ 2012.

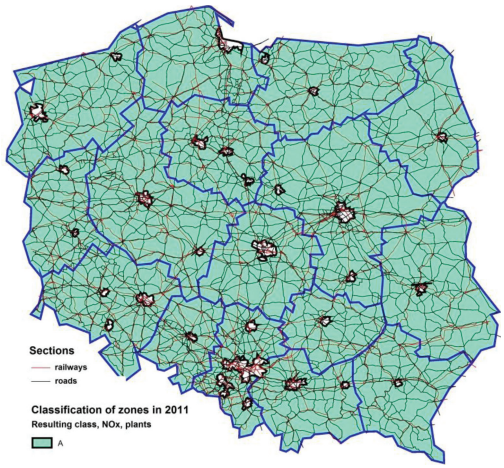


Figure 3. Classification of areas in Poland according to NO_x emission in 2011 (criterion f_2). Source: own research based on GIOŚ 2011, GIOŚ 2012.

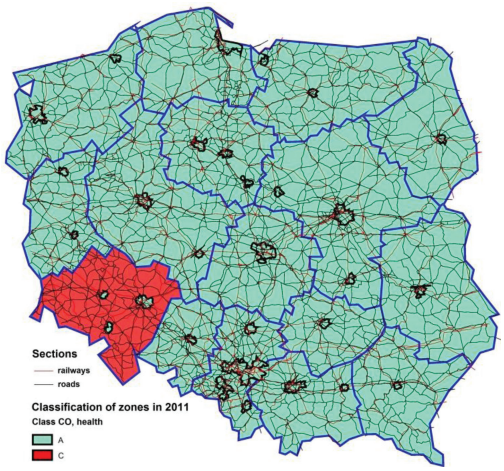


Figure 4. Classification of areas in Poland according to CO emission in 2011 (criterion f_1). Source: own research based on GIOŚ 2011, GIOŚ 2012.

in the study (GIOŚ 2011) it can be concluded that one of the reasons for exceeding the allowable concentration is intense traffic in city centres and in the agglomeration. The analysis shows that it should be included in the model national transport system restrictions on movement of vehicles in these area.

Figure 4 shows the classification of the areas due to air pollution by carbon monoxide (CO), and Figure 5 due to contamination with lead. Both substances were analysed only by the criterion of human health protection.

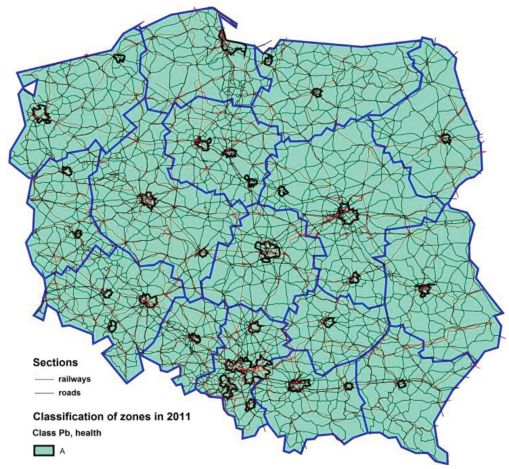


Figure 5. Classification of areas in Poland according to Pb emission in 2011 (criterion f_1). Source: own research based on GIOŚ 2011, GIOŚ 2012.

Maximum concentration of carbon monoxide has been exceeded in one area (Lower Silesia), due to the excess concentration in the health-resort Cieplice-Zdroj (near the Jelenia Gora). It should be noted that the concentrations of the standards for health resorts are much more stringent than for other areas. As can be seen from the data shown in Figure 1 the share of road transport in total emissions of this compound is high and the value is at the level 23.15%. Due to the location of the health resort area in the neighbourhood of major road transport routes with heavy traffic the sphere of road transport can cause excess of the limit.

Figure 6 presents the classification of areas for air pollution by particulates matter classified into a fraction PM_{10}, and $PM_{2,5}$ (Fig. 7). Both substances were analysed only by the criterion of human health protection.

From the point of view of criterion f_1 (human health) for PM_{10} air pollution in only four areas the acceptable level of concentration has not been exceeded (cities of Elblag, Koszalin, Olsztyn and Zielona Góra). In other cities, and in all voivodships permissible concentration has been exceeded. As can be seen from the data shown in Figure 2 share of road transport in total emissions of particulate matter PM_{10} fraction is at the level 10.36%. It can be concluded that one of the reasons for exceeding the limit value can thus be heavy traffic, especially in cities and towns over 100 thousand inhabitants. This reason is not dominant because the engines of new cars must comply with ever higher emission standards Euro.

Air pollution by particulates matter $PM_{2,5}$ fraction has qualified for three classes: A, B and C.

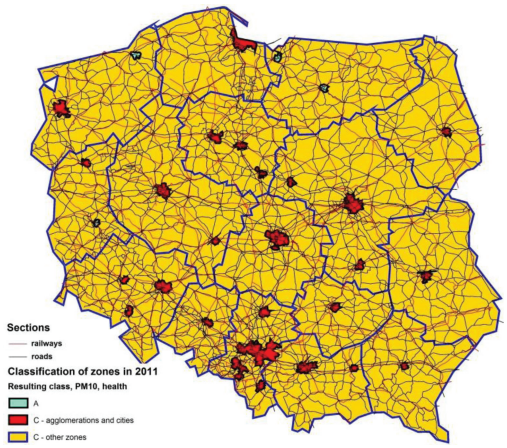


Figure 6. Classification of areas in Poland according to PM_{10} emission in 2011 (criterion f_1). Source: own research based on GIOŚ 2011, GIOŚ 2012.

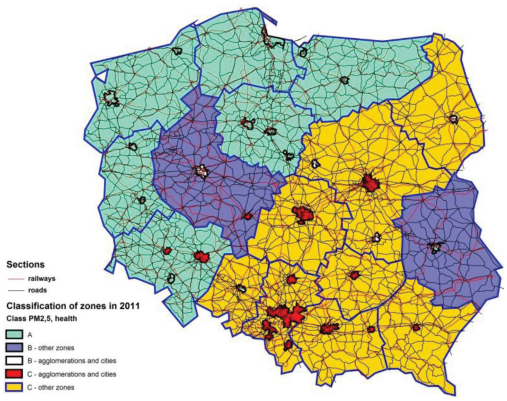


Figure 7. Classification of areas in Poland according to $PM_{2,5}$ emission in 2011 (criterion f_1). Source: own research based on GIOŚ 2011, GIOŚ 2012.

To the class A, where does not exceed the limits, classified North-western area of the Poland and the city Lublin. In five voivodships all areas classified into the class A (Pomorskie, Warminsko Mazurskie, Zachodniopomorskie, Kujawsko-Pomorskie and Lubuskie). To the class B, which has been exceeded a limit value for particulate matter $PM_{2,5}$, but within the limits of tolerance, qualified six zones: Lubelskie and the Wielkopolskie voivodships and the cities Bialystok, Plock, Radom and Poznan. Southeastern Voivodships are an areas where the permissible parameter value has been greatly exceeded. To the class C classified all areas in the voivodships: Lodzkie

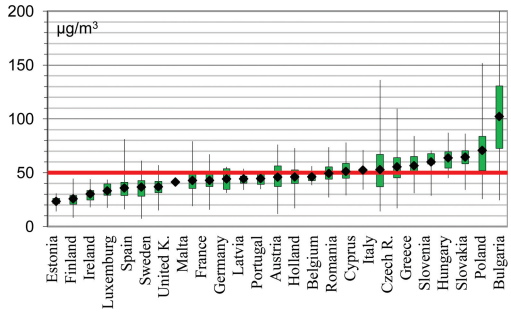


Figure 8. Daily limits of PM_{10} in 2011 in European countries. Source: EEA 2013.

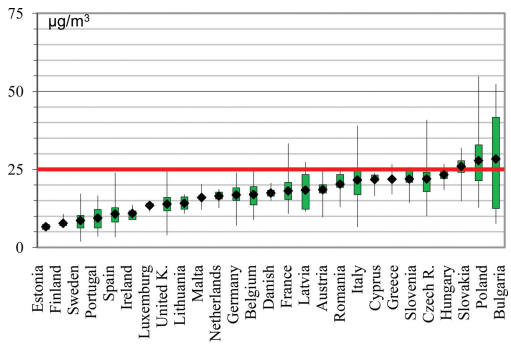


Figure 9. Daily limits of $PM_{2,5}$ in 2011 in European countries. Source: EEA 2013.

Malopolskie, Podkarpackie, Silesian and Swietokrzyskie. The share of road transport in total emissions particulate matter $PM_{2,5}$ is at the level 17,18%.

Basing on EEA data at Figures 8 and 9 daily limits for PM_{10} and $PM_{2,5}$ in 2011 are presented.

5 CONCLUSIONS

The article presents selected issues of effectiveness of transport system in terms of costs of the functioning. Presented research is based on economic and environmental criteria relating to the community and pollution problems. Presented mathematical model takes into account criteria of efficiency in terms of emission and costs as a discriminants of proecological transport system.

The effectiveness of the functioning in terms of ecology is made on the basis of quantitative and qualitative indicators. For the study, it was assumed that both quantitative and qualitative indicators are measurable and only those were analyzed.

Implementation of the work indicates that the designing environmentally friendly transport system should take into account:

- reducing emissions of nitrogen dioxide (NO_2) in large towns and cities by minimizing the movement of vehicles on the road/in the fields;
- reducing emissions of carbon monoxide (CO) in the spa areas by reducing the traffic around and in the zone,
- reducing emissions of particulate matter (PM_{10}) throughout the country, especially in urban areas and agglomerations,
- reducing emissions of particulate matter ($PM_{2,5}$) in the central and south-west areas of Poland, which is quite complicated, as the share of road transport in total emissions is significant, and one of the factors affecting the emission of the terrain.

Therefore, in these areas, it is proposed to introduce the low emission zones or areas which it is possible to enter only by vehicles that meet certain emission standards or charging for entry depending on EURO standards.

The introduction of such zones will serve the improvement of air quality and increasing motivation to buy more environmentally friendly vehicles. The good test area for such a restriction could be established in spa town of Teplice—Zdroj in Lower Silesia because of exceeded allowable concentration of carbon monoxide (CO).

Category of effectiveness embraces many different issues characteristic for transport systems, especially of large scale systems. This also applies to decision making in transport enterprises. Decision-makers in transport enterprises by analyzing the current solutions in the area of transport organization, must consider possible impact of their actions on the environment.

Proposed mathematical model implemented into PTV Visum environment bases on representation of full railway and road transport network of Poland with appropriate transition points. Model uses complete ODO matrixes for segments of demand for freight transport and uses full structure of vehicles for both modes. These elements allow for testing efficiency of transport system of Poland according to different aspects, like environmentally friendliness resulting from emission patterns. Emission levels are implemented into the model as functional dependences gained from on-board surveys (Merkisz et al. 2014, Mierkish & Pielecha 2014).

Above research allows for the development of guidelines to design proecological transport systems. This will lead to long-wave effects allow for reducing pollutant emissions.

ACKNOWLEDGEMENTS

Article was prepared as a part of research project "Proecological transport system designing" (EMITRANSYS), funded by the National Centre for Research and Development in Poland.

REFERENCES

Ambroziak, T., Gołębiowski, P., Pyza, D., Jacyna-Gołda, I. & Merkisz-Guranowska, A. 2013. Identification and analysis of parameters for the areas of the highest harmful exhaust emissions in the model EMITRANSYS, *Journal of KONES Powertrain and Transport* 20(3): 9–22.

Danklefsen, N. 2009. The calculation of external costs in the transport sector, European Parliament, Brussels.

Delucchi, M., & McCubbin, D. 2011. External costs of transport in the United States. In De Palma, A., Lindsey, R., Quinet, E., & Vickerman, R. (eds.), *A handbook of Transport Economics*. Cheltenham: Edward Elgar Publishing.

EEA. 2013.*Air quality in Europe—2013 report* (9/2013). European Environment Agency.

Engeljerhinger, K. 2011. Automotive emission testing certification, past, present and future. *2nd International Exhaust Emissions Symposium*, Bielsko-Biała.

Farmer, A. 2013. *Managing environmental pollution.* Routledge.

GIOŚ. 2011, *Ocena jakości powietrza w strefach w Polsce za rok 2011*. Główny Inspektorat Ochrony Środowiska: Warszawa.

Gioś. 2012. *Europejska Agencja Środowiska W Roku 2012 Udział Polski w realizacji zadań—sprawozdanie.* Główny Inspektorat Ochrony Środowiska: Warszawa.

Jachimowski, R., Kłodawski, M., Lewczuk, K., Szczepański, E., & Wasiak, M. 2013. Implementation of the model of proecological transport system, *Journal of KONES Powertrain and Transport* 20(4): 129–139.

Jacyna, M. 2012. *System logistyczny Polski: uwarunkowania techniczno-technologiczne komodalności transportu.* Publishing House of Warsaw University of Technology, Warsaw 2012.

Jacyna, M., Żak, J., Jacyna-Gołda, I., Merkisz, J., Merkisz-Guranowska, A., & Pielecha, J. 2013. Selected aspects of the model of proecological transport system, *Journal of KONES Powertrain and Transport* 20 (3): 193–202.

KOBiZE. 2013. Krajowy bilans emisji SO2, NOx, CO, NH3, NMLZO, pyłów, metali ciężkich i TZO za lata 2010–2011 w układzie klasyfikacji SNAP. Raport syntetyczny. http://www.kobize.pl/materialy/Inwentaryzacje_krajowe/2013/Bilans_emisji-raport_syntetyczny_%202011.pdf.

Kok, R., Annema, J.A., & van Wee, B. 2011. Cost-effectiveness of greenhouse gas mitigation in transport: A review of methodological approaches and their impact, *Energy Policy* 39(12): 7776–7793.

Leontiadis, I., Marfia, G., Mack, D., Pau, G., Mascolo, C., & Gerla, M. 2011. On the effectiveness of an opportunistic traffic management system for vehicular networks, *IEEE Transactions on Intelligent Transportation Systems* 12(4): 1537–1548.

Mashayekh, Y., Jaramillo, P., Chester, M., Hendrickson, C.T., & Weber, C.L. 2011. Costs of automobile air emissions in US metropolitan areas, *Transportation Research Record: Journal of the Transportation Research Board* 2233(1): 120–127.

Merkisz, J. & Pielecha, J. 2014. *Emisja cząstek stałych ze źródeł motoryzacyjnych*. Poznań: Publishing House of Poznan University of Technology.

Merkisz, J., Jacyna, M., Merkisz-Guranowska, A. & Pielecha, J. 2014a. Exchaust emissions from models of transport under actual traffic conditions. In Brebbia, C.A., Magaril, E.R. & Khodorovsky, M.Y. (eds.), *Energy production and management in the 21st Century* 190, Southampon: WIT Press.

Merkisz, J., Pielecha, J., & Radzimirski, S. 2014b. *New Trends in Emission Control in the European Union*. Dordrecht: Springer.

Przybyłowski, A., 2011. Strategia zrównoważonego rozwoju transportu w polityce Unii Europejskiej, *Ekonomia i Środowisko* 1(39): 81–91.

Regulation EC No 715/2007. 2007. 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information.

Sen, A.K., Tiwari, G., & Upadhyay, V. 2010. Estimating marginal external costs of transport in Delhi. *Transport Policy* 17(1): 27–37.

Sivilevičius, H. 2011. Modelling the interaction of transport system elements, *Transport* 26(1): 20–34.

Steiningier, N. 2009. Automotive particulate emissions in European legislation: state of the art and developments to come, *13th ETH Conference on Combustion Generated Particles*. Zurich.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Experiments for PHM: Needs, developments and challenges

Xiao-Yang Li, Le Liu, Rui Kang, Dan Xu & Fuqiang Sun
Science and Technology on Reliability and Environmental Engineering Laboratory, Beihang University, Beijing, China
School of Reliability and Systems Engineering, Beihang University, Beijing, China

Jay Lee
NSF I/UCR Center for Intelligent Maintenance Systems, Department of Mechanical Engineering, University of Cincinnati, OH, USA

ABSTRACT: Currently, the focus of reliability engineering has been extended from product design quality to product service, which drives the research on Prognostics and Health Management (PHM) methodology to provide timely and reliable service information about the health status of product. However, traditional PHM technique mainly concentrates on usage information which leads to the shortcomings of prediction modelling problems, especially for high-reliability and long-life products. This paper proposed an experiment-based PHM life cycle framework, aiming to integrate information from the in-field development phase to provide usage-oriented life prediction model set. When the on-line monitoring data is available, model set can be updated to acquire accurate prediction results and ensure effectively maintenance activity. In this paper, the life cycle is divided into seven stages and related modelling processes are given with specific case studies.

1 INTRODUCTION

Prognostics and Health Management (PHM) technique is to manage product health status through utilizing monitor information, do decision-making before failure happens and avoid catastrophe events, while reducing life cycle cost. The development of PHM represents that the focus of current reliability engineering has come into a new stage extended from quality-centered to service-centered, which can provide customers timely and reliable health information about their products and manage them properly. Among the service indexes, customers are mainly concerned about the Remaining Useful Life (RUL) which is to answer how much time is left for products to perform well. This demand promotes the deeper research on RUL prediction during the past decades, which is widely used in prognostics and maintenance scheduling for machinery, electronics and other products. The core of RUL research is to set up life prediction model whose accuracy will definitely affect the follow-up maintenance activity.

Traditional PHM extracts performance degradation pattern from real-time monitoring signal data or acquire degradation parameter data directly. Based on that information, life prediction model can be given according to the nature of data or the generalization capability of the selected models to capture the time-varying performance. However, it is difficult to verify whether the model itself is reasonable accuracy which will definitely increase the potential risk of product operation. Meanwhile, the advanced technology promotes the emergence of high-reliability and long-life products, which make it even harder to collect sufficient data for capturing the degradation process of such products in a limited time, especially for newly ones. Thus, traditional PHM technique faces the problem of life prediction modelling for the new generations which is high risky and less cost effective.

This paper at first reviews the existing research of traditional PHM in life prediction aspect and proposes an experiment-based PHM framework to overcome the abovementioned shortcomings. The usage-oriented life prediction model set is given at the in-field development phase and integrated with operational data to do health evaluation and maintenance decision-making. The rest of this paper is organized as follows. In Section 2, the research status of life prediction methods is analyzed and the existing problems are pointed out. The new framework is presented in Section 3 and three stages are mainly introduces, i.e. pre-design, after-design and field use, with related research contents for life prediction modelling. The flexibility of the framework is verified by case studies in Section 4. Section 5 concludes this paper.

2 REVIEW OF LIFE PREDICTION METHODS FOR PHM METHODOLOGY

RUL represents the length of time when product performance degrades below failure threshold or cannot meet the requirements, which is the key research of Condition Based Maintenance (CBM) and PHM (Jardine et al. 2006, Si et al. 2011). The RUL prediction methods can be divided into three categories: model-based (also called physical-based), data-driven and hybrid modelling (Heng et al. 2009, Zhou et al. 2013). Nevertheless, model-based methods require that the failure mechanism is known or degradation process can be analytical expressed, which cannot be applied for complex products, while data-driven methods is widely used since there is no need to know about the physical property. However, the prediction accuracy highly depends on the generalization capability of the selected models. The hybrid models integrate the strengths of both model-based and data-driven methods, which still cannot ensure the prediction accuracy.

The present research of RUL prediction in PHM technique mainly concentrates on product usage information. For the high-reliability and long-life products, the existing prediction methods have the following two problems:

- *Data:* How to collect sufficient monitoring data for the purpose of capturing the degradation process in a limited time?
- *Model:* How to establish reasonable life prediction models and simultaneously verify them for new products?

For the data problem, some research integrates expert knowledge or historical information with monitoring usage data. Zio & Di Maio (2010) proposed a similarity-based RUL prediction approach which utilizes the fuzzy similarity between system measurements with the reference failure trajectory patterns by giving related weights. Similar research refers to Wang (2011). Vaidya & Rausand (2011) studied the life extension problems of the equipment in offshore oil and gas industry which considers the influence of expert judgment, operational and environmental conditions, initial system state, etc. on RUL prediction. Chen & Tsui (2013) proposed a two-phase modelling method based on degradation signals which combines historical data with real-time monitor data to improve the RUL prediction results through Bayes theorem. Considering that in-field experiments, like Accelerated Testing, can shorten the test time effectively and gather performance degradation information rapidly for life prediction. Liao & Tian (2013) researched degradation modelling based on drift Brownian Motion and used Accelerated Degradation Testing (ADT) data to do model validation and parameters' evaluation, then the results are used as prior information for product RUL prediction under time-varying operational conditions. Similarly, Li et al. (2013) proposed an approach to build life prediction model based on degradation data under accelerated stress levels and the evaluated parameter results are used as prior information for RUL prediction in normal stress level. The case study shows that the proposed approach has a satisfactory prediction results even under the condition that field monitoring data is insufficient.

As for the model problem, researchers mainly do model comparison or combination to get the applicable prediction model. Saha et al. (2009a) compared several typical algorithms for battery RUL prediction, like Autoregressive Integrated Moving Average (ARIMA), Support Vector Machine (SVM), Relevance Vector Machine (RVM), etc. and results shows that integrated Bayesian regression and estimation methods, like SVM-PF, has significant prognostic advantage than traditional ARIMA and Extended Kalman Filter (EKF) methods. Then, Saha et al. (2009b) furthered this study. Caesarendra et al. (2010) studied the prognosis of complex devices based on sequential Mento Carlo method which shows a potential capability to predict trend data. Zio & Peloni (2011) proposed a RUL prediction method for non-linear component based on particle filtering (PF). Liu et al. (2012) proposed a data-model-fusion framework to improve the accuracy of long-term system state prediction results. Similarly, Zhao et al. (2013) offered a reliability prediction method which integrates PF and Support Vector Regression (SVR). Details about the hybrid prognosis algorithms in engineered system, readers are referred to Liao & Kottig (2014).

The above research papers partially answer the questions on both data and model for life prediction of high-reliability and long-life products. However, as described in Lee et al. (2014), explanation documents about the reason why select some specific prognosis algorithms still lack, which constrain the RUL prediction research into practical applications. Meanwhile, if we choose them blindly without reasonable basis, future life prediction activities will be extremely dangerous.

In order to solve those problems, we transfer the line of sight to the process before product put into market which is called the in-field development phase. In this phase, many experiments are conducted to ensure the requirement of high reliable and long life, among which reliability tests are the most important part. Through repeating the process of test-failure-fix, product life and reliability levels can be guaranteed to meet the design requirements (Collins et al. 2013). Meanwhile, this phase

will accumulate a wealth of important information, such as failure mechanism, key components, accelerated testing data, etc. If those information can be properly utilized to build usage-oriented prediction model set, the life prediction problems for current PHM technique will be solved. Hence, an experiment-based PHM framework is proposed to make up the shortcomings for high-reliability and long-life products. The usage-oriented model set will also be verified at the in-field phase. When field monitoring data is available, the model will be updated and improved correspondingly to ensure the accuracy of life prediction results and maintenance activities.

3 THE EXPERIMENT-BASED PHM LIFE CYCLE FRAMEWORK

For the purpose of solving existing life prediction problems in PHM, the experiment-based life cycle framework is proposed by integrating testing techniques at the in-field develop phase, including seven different stages which are pre-design, final-design, trial, manufacturing, field use, re-manufacturing and cycling, as shown in Figure 1. It should be mentioned that not all products experience these stages.

With the main line of life cycle stages, we introduce the interdependent relationship of the data and model under this framework, and provide their support for life prediction modelling.

In pre-design stage, which is also called concept demonstration phase, the feasible way is to carry out simulation test. According to the historical or similar product information and user requirements, we can acquire the material, geometric and other attributes. Then, product degradation behavior simulation can be undertaken based on Physics of Failure (PoF) model. This process covers from the determination of the degradation mechanism in component level to the degradation behavior modelling in system level, producing the weakest link of the design and assessing the life and reliability of products. Therefore, the design will be improved

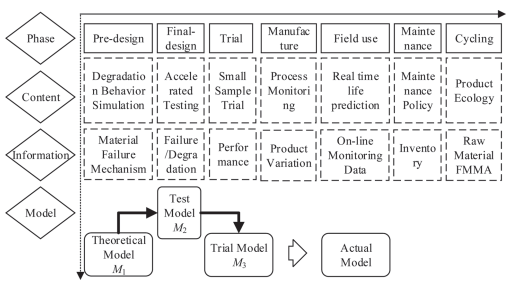


Figure 1. The experiment-based PHM life cycle framework.

until the specific requirements are satisfied. Hence, this stage will set up the relationship among performance parameters, time and the stresses which is the theoretical life prediction model M_1.

$$M_1 : \begin{cases} P = f(t, M, S_{sim}) \\ T = g(P, S_{sim}, D) \end{cases} \tag{1}$$

where M represents product material information; S_{sim} represents the specific operational conditions; D is the failure threshold. f represents the relationship among stresses, material and performance parameters, i.e. P, with time t, while g for stresses, performance parameters, threshold and product life T.

This relationship can be either analytical expression or data-driven models in accordance with the system complexity.

In final-design stage, in order to assess and verify the life and reliability level of product in a limited time, life prediction modelling based on accelerated testing will be carried out. With the input accelerated model M_1 from simulation test, ADT or ALT (Accelerated Life Testing) will be conducted to acquire accelerated data of product. When modelling the degradation data, both the models from M_1 and newly algorithms can be used and the most suitable model set, i.e. M_2, will be chosen for life prediction.

$$M_2 : \begin{bmatrix} M_{1\to 2} \\ M_{0\to 2} \end{bmatrix} \tag{2}$$

where $M_{1\to 2}$ represents the models inherited from M_1, while $M_{0\to 2}$ for the new ones.

Field trial can be arranged into different stages according to different purpose. For example, the trial is normally arranged into the middle of the development phase to reveal the early defect of product design, while after the final-design to assess if the reliability indexes satisfy the general requirements. No matter which stage that is, the field trial can appraise the actual performance level of product although that is not exactly the same one for future use. In this stage, initial PHM prediction module can be set up based on model set $[M_1, M_2]^T$, including sensor layout, data acquisition system and life prediction algorithms, etc. With the data from typical operational conditions, the most suitable prediction sets for field use are selected, M_3, which is the usage-oriented model set.

$$M_3 : \begin{bmatrix} M_1' & M_2' \end{bmatrix}^T = \begin{bmatrix} M_{11}', M_{12}', \ldots, M_{21}', M_{22}', \ldots \end{bmatrix}^T \tag{3}$$

where the symbol $'$ represents model updating.

In manufacturing, the consistency of production quality will be controlled by process monitoring, random sampling, etc. However, it is inevitable to introduce product variation which should be taken into consideration in future life prediction activity.

The above all stages is called the in-field development phase which utilizes the sub-stage data and models to provide usage-oriented prediction model set M_3. The contained models are verified through simulation, testing and trial. Therefore, the prediction results can be reasonable and accurate to avoid the prediction modelling problems in field actual use.

In field use, the monitoring data, like performance degradation, life and failure data, etc. is under actual operational and environmental conditions. Thus, the best prediction models or model combination, M_4, can be selected by ranking or assigning weights according to the prediction accuracy of M_3. Apparently, M_4 is a subset of M_3 but not a null set since the modelling process integrates all the information related to product.

$$M_4 : \left\{ \left(M_4 \in M_3 \right) \cap \left(M_4 \neq \varnothing \right) \right\} \tag{4}$$

At the end of field use, the product performance degrades nearly to the threshold and maintenance policy based on RUL should be carried out, like keep use after repair, replacement, etc. which can effectively prolong its life cycle and enhance system safety (You & Meng 2013). Just take battery as an example. The maintenance policy can provide battery manufacturing scheme, inventory and other information. If the battery completely scrap, it will be into the cycling stage to collect the raw materials and do Failure Mode and Mechanism Analysis (FMMA), which can be compared with the results of simulation test to adjust model set M_1. This improvement will be feedback to the battery design of next generation, thus to achieve the ecological life cycle management.

Overall, the proposed experiment-based PHM framework can utilize all the information from the in-field development phase to provide usage-oriented life prediction set and verify it simultaneously, specifically the life and reliability tests before products are put into use. This overcomes the shortcomings of traditional PHM technique on model selection and data acquisition in the aspect of life prediction. The framework is applicable to the new products which have high-reliability and long-life properties, providing technical support for the new reliability engineering area which centers in intelligent service. Therefore, it has practical engineering value and broad development prospects for the implement of PHM system in engineering applications.

The specific modelling process for several typical stages are given below.

3.1 *Product degradation behavior simulation based on PoF models*

The goal of product degradation behavior simulation is to acquire performance data varying with time under specific conditions and find out the weakest link of product design.

This process uses historical and similar product information, and expert knowledge as inputs. The output is the theoretical life prediction model set M_1 (Fig. 2).

Conventional layer classification is the first step for product analysis. Then, the related failure mode and mechanism, environmental and load conditions, and other information should be determined to conduct performance simulation in component level. Through the transfer function between system and component levels, performance simulation in system level can be carried out, collecting simulated performance data varying with time under specific conditions. Finally, modelling the degradation process with consideration of the failure threshold is to produce the model set M_1. Noting that theoretically physical model can be established for product with simple failure mechanism, while modern engineering tools should be used for complicated products. Thus, the model set M_1 can be analytical functions or data-driven models.

The selected models are applicable to describe the properties of product performance which, however, are under many assumptions, like boundary conditions, etc. which may not be suitable for real applications. Therefore, more test data is needed to verify the feasibility of M_1.

3.2 *Life prediction modelling based on accelerated testing*

For high-reliability and long-life products, accelerated tests are normally used to evaluate its life

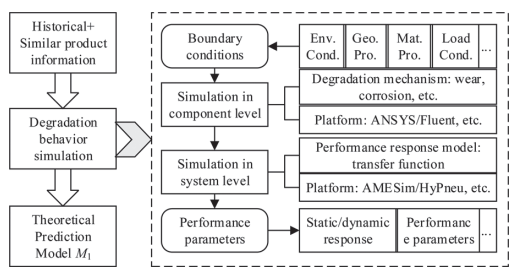


Figure 2. Degradation behavior simulation based on PoF models.

and reliability by experiencing severe stress levels than that in normal conditions to accelerate product failure or degradation process. Thus, sufficient data will be obtained in a short period of time and used for life prediction modelling. This process is dependent on the basis of accelerated model from simulation test, i.e. M_1, and the sensitive stress to conduct accelerated test. Then, suitable models will be selected from M_2 based on the test data, see Figure 3.

This stage is usually first carry out the qualitative accelerated tests, such as High Accelerated Life Test (HALT), etc. to obtain the stress limit where product can still function well. Then, with the input from simulation test, quantitative accelerated tests will be carried out, such as ALT, ADT, etc. including test plan design (Tseng et al. 2009, Liu & Tang 2010) and data proceeding (Meeker et al. 1998, Escobar & Meeker 2006). For the proceeding of accelerated test data, the models from M_1 should be verified and eliminated the unreasonable ones, while new models can be introduced. Therefore, the new level prediction model set is achieved, i.e. M_2.

Being similar to the selected procedure in simulation stage, the models in this stage still need further screening process since there are still exist many assumptions, like stress simplification, ignoring multi-degradation mechanism, etc.

3.3 *On-line predictive maintenance through PHM*

Traditional PHM technique mainly focus on field use information by which to evaluate product health status and offer maintenance policy, i.e. CBM (Niu et al. 2010, Meng & You 2011). However, this technique has its limitations when applying to high-reliability and long-life products. On the contrary, the experiment-based PHM framework provides alternative prediction model sets M_1, M_2 and (or) M_3 at the in-field development phase, which can be used for field life prediction. Figure 4 illustrates this process.

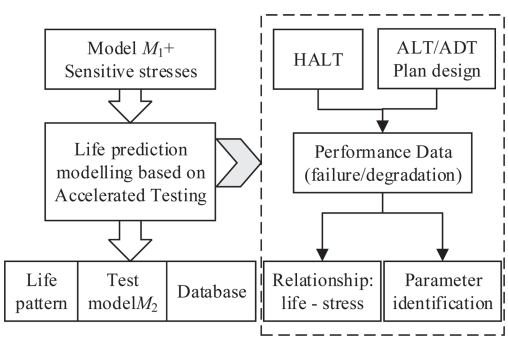


Figure 3. Life prediction modelling based on accelerated tests.

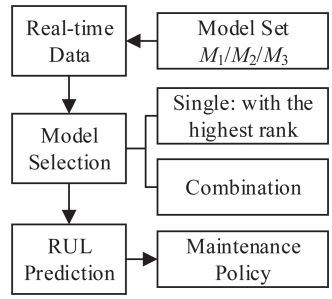


Figure 4. On-line Life predictive maintenance through PHM.

When field monitoring data is available, life prediction can be accomplished by either single model with the highest rank or combined models with their weights according to the prediction accuracy. Its procedure is significant different from the traditional selection method without criteria and it can achieve reasonable RUL prediction results and ensure the effectiveness of maintenance decision-making.

4 CASE STUDIES

The below several cases are used for describing the field RUL prediction modelling based on the information from each life cycle stage under the experiment-based framework. It should be noted that partially tests are carried out for the specific applications at some stages, but all the information collected from this tests do help modelling the RUL prediction for field use.

4.1 *Life prediction modelling for Double nozzle flapper electro-hydraulic servo valve*

Electro-hydraulic servo valve is a key control unit widely used in modern aircraft. In practical application, servo valve is susceptible to the effect of the oil particle pollution which affects its performance, causing the wear of the valve core and sleeve edge. The influence mainly includes pressure gain, inner leakage, etc.

For the purpose of evaluating the life and reliability indexes of servo valve, both simulation test and accelerated test are conducted before that is put into use. The information obtained from the two tests are used for life prediction modelling according to the procedure in Section 3.1 and 3.2. The results are shown in Figure 5. At first, the wear of nozzle flapper and sliding valve under the influence of oil pollution is simulated through

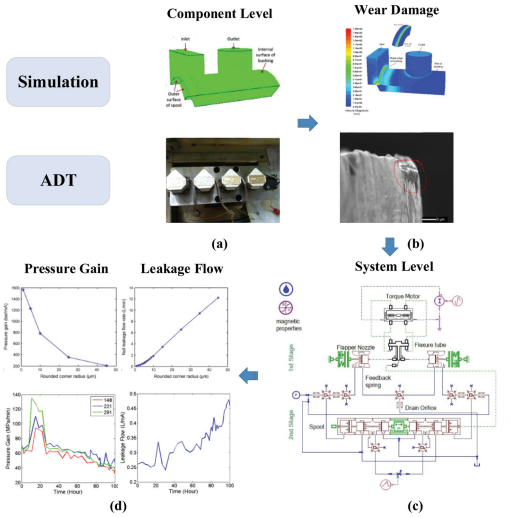


Figure 5. Life prediction modelling for Double nozzle flapper electro-hydraulic servo valve.

FLUENT software in component level, acquiring the wear degradation process of structure parameters varying with time (Fig. 5a, 5b). Then, the data is used as input for system level simulation through transfer function which shows the link between components and system (Fig. 5c) using AMEsim software. Finally, the degradation behavior of system performance is obtained which shows that the pressure gain reduces with time, while leakage flow increases. After the simulation test, the collected data is also used for designing accelerated plan. The optimal plan is Step Stress ADT (SSADT) with 5 stress levels (oil pollution degree) and 3 samples. The monitor interval is 2 hours and the performance parameters are pressure gain and leakage flow, see Figure 5d. After the test, the edges of valve core wear severely.

Based on the degradation data from simulation and accelerated tests, the life prediction models M_1 (Quadratic or linear function) and M_2 (drift Brownian Motion) can be given by integrating with the failure thresholds (25% initial pressure gain and 10% rated flow-rate). Details are referred to Zhang et al. (2014) and Wang et al. (2014). The model set then will be used for field life prediction. This modelling procedure is also applicable to other products by building usage-oriented prediction models and being verified for field use, which can definitely guarantee the accuracy of prediction results.

4.2 *Life prediction modelling and on-line updating for super luminescent diode*

Super Luminescent Diode (SLD) is a kind of one-way light amplification devices which has excellent properties, like wide spectrum, high power. Light SLD is one of the key functional modules of fiber optic gyroscope, experiencing temperature stress in practical use. The inner components degrade with time and that decrease the output optical power.

SLD belongs to high-reliability and long-life product which should be in use for several years. If the life prediction modelling only rely on field use data, sufficient data is needed to capture the degradation process which, however, is hard to acquire even for a long time. Thus, the models based on this data cannot ensure the prediction results. Before SLD is put into market, ADT was carried out at the in-field phase. According the procedure from Section 3.2, eight samples and four temperature stress levels were used in the SSADT (Fig. 6a, 6b). The monitoring parameter is the output optical power which is shown in Figure 6c. Therefore, the life prediction model M_2 (drift Brownian Motion, etc.) can be built based on the ADT data. When on-line data is available (Fig. 6d), the model is updating with time through Bayesian approach. The prediction results show that this method has higher accuracy than the traditional regression method which only uses the field data. Meanwhile, monitoring data in a limited time is enough for modelling the degradation process for this kind of product (Li et al. 2013).

4.3 *Life prediction based on combined algorithms*

This case is to describe how to use the usage-oriented model sets to conduct field RUL prediction. Commonly used method is single prediction model or combined models with associated weights according to their prediction accuracy. Here, we only consider the combined model for life prediction.

As shown in Section 3.3, the input is the model sets, M_1, M_2 and (or) M_3 which are BP neural

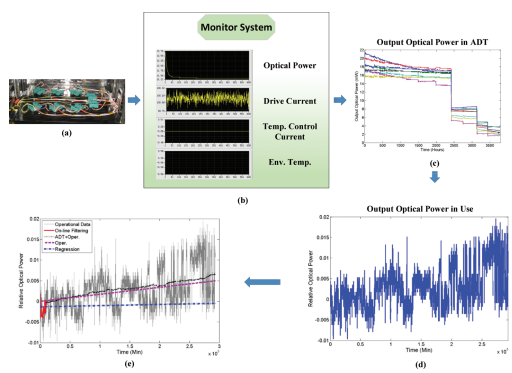


Figure 6. Life prediction modelling based on ADT data and on-line updating through Bayesian approach for super luminescent diode.

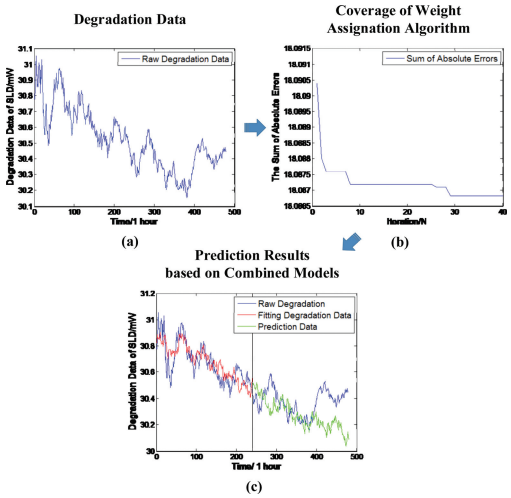


Figure 7. Life prediction based on combined algorithms.

network (f_1), drift Brownian Motion (f_2), time series model (f_3) and particle filtering model (f_4). Degradation data for the particular optical device was collected in field use for 480 hours (Fig. 7a). The first half is used for model training, while the rest for validation. Then, training data is fitted by each single model and encompassment test is conducted to do model selection. The ranking result based on their prediction accuracy is $f_3 > f_2 > f_1 > f_4$ and the encompassment test rejects model f1. Thus, the other three models are combined for RUL prediction in the following process. Combinatorial optimization algorithm, like the Particle Swarm Optimization with Immunity Algorithms (IA-PSO), is used to assign weights for the three models (Fig. 7b) which are 0.288, 0.712 and 0, respectively. Finally, we use the rest data to verify the prediction accuracy and the result is $f_{com} > f_3 > f_2$. Hence, the combined model perform better than the single forecasting models (Fig. 7c). Details are referred to Feng et al. (2014).

The experiment-based PHM framework can provide usage-oriented prediction model at the in-field development phase for field RUL prediction, which is superior to the traditional methods that mainly rely on field monitoring data.

5 CONCLUSIONS

Nowadays, the PHM technique has been applied in rotating machinery, batteries and other complicated equipment, providing on-line health evaluation results of the product to users and saving maintenance cost (Sikorska et al. 2011, Zhang et al. 2011, Lee et al. 2014). However, traditional PHM technique mainly focus on the monitoring data from field use to undertake RUL prediction modelling, which has shortcomings on both data and model for high-reliability and long-life products. Therefore, this paper proposed the experiment-based framework to integrate all the information from in-field phase to do life prediction modelling from the perspective of total life cycle. The prediction model sets keep updating with the information accumulating to ensure the effeteness of prediction activity. At the viewpoint of reliability engineering, this is also a new development of reliability growth program. The usage-oriented life prediction model set is given and verified at the in-field development phase, which definitely ensure the accuracy of prediction results.

The values of the experiment-based PHM technique are on:

- Integrating the idea of prognosis and acceleration to enrich the connotation of reliability engineering.
- Supporting the total life cycle management of product with the further development of reliability platform, which can be widely used in aerospace, automotive, energy and other fields.
- Shortening the product development time by improving product reliability and life expectancy, realizing intelligent maintenance to ensure its safety and economy, achieving green product ecology.

The development of high-reliability and long-life products promotes new requirements for current reliability engineering systems. The proposed experiment-based framework integrates diagnostics, prognosis and health management with reliability testing methods, providing a feasible idea to achieve total life cycle management.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Kun Zhang, Dr. Jin-Yong Yao and Dr. Xiao-Hong Wang for their contribution to this paper. The authors would also like to express their gratitude to the anonymous reviewers for their valuable suggestions. This work was partially supported by the National Natural Science Foundation of China under Grant NSFC 61104182.

REFERENCES

Caesarendra, W., Niu, G. & Yang, B.S. 2010. Machine condition prognosis based on sequential Monte Carlo method. *Expert Systems with Applications* 37(3): 2412–2420.

Chen, N. & Tsui, K.L. 2013. Condition monitoring and remaining useful life prediction using degradation signals: revisited. *IIE Transactions* 45(9): 939–952.

Collins, D.H., Freels, J.K., Huzurbazar, A.V., Warr, R.L. & Weaver, B.P. 2013. Accelerated Test Methods for Reliability Prediction. *Journal of Quality Technology* 45(3): 244–259.

Escobar, L.A. & Meeker, W.Q. 2006. A review of accelerated test models. *Statistical Science* 21(4): 552–577.

Feng, L., Li, X.-Y., Jiang, T.-M. & Dang, X.-J. 2014. A Combined Prediction Method for the Life of Product Based on PSO with Immunity Algorithms. Reliability & Maintainability Symposium (RAMS) 1–6.

Heng, A., Zhang, S., Tan, A.C.C. & Mathew, J. 2009. Rotating machinery prognostics: State of the art, challenges and opportunities. *Mechanical Systems and Signal Processing* 23(3): 724–739.

Jardine, A.K.S., Lin, D.M. & Banjevic, D. 2006. A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing* 20(7): 1483–1510.

Lee, J., Wu, F., Zhao, W., Ghaffari, M., Liao, L. & Siegel, D. 2014. Prognostics and health management design for rotary machinery systems—Reviews, methodology and applications. *Mechanical Systems and Signal Processing* 42(1): 314–334.

Li, X.-Y., Liu, L., He, B. & Jiang, T.-M. 2013. Accelerated Degradation Test and Particle Filter Based Remaining Useful Life Prediction. *Chemical Engineering Transactions* 33: 343–348.

Liao, H. & Tian, Z. 2013. A framework for predicting the remaining useful life of a single unit under time-varying operating conditions. *IIE Transactions* 45(9): 964–980.

Liao, L. & Kottig, F. 2014. Review of Hybrid Prognostics Approaches for Remaining Useful Life Prediction of Engineered Systems, and an Application to Battery Life Prediction. *IEEE Transactions on Reliability* 63(1): 191–207.

Liu, J., Wang, W., Ma, F., Yang, Y.B. & Yang, C.S. 2012. A data-model-fusion prognostic framework for dynamic system state forecasting. *Engineering Applications of Artificial Intelligence* 25(4): 814–823.

Liu, X. & Tang, L.C. 2010. A Bayesian optimal design for accelerated degradation tests. *Quality and Reliability Engineering International* 26(8): 863–875.

Meeker, W.Q., Escobar, L.A. & Lu, C.J. 1998. Accelerated degradation tests: modeling and analysis. *Technometrics* 40(2): 89–99.

Meng, G. & You, M.-Y. 2011. Review on condition-based equipment residual life prediction and preventive maintenance scheduling (In chinese). *Journal of Vibration and Shock* 30(8): 1–11.

Niu, G., Yang, B.S. & Pecht, M. 2010. Development of an optimized condition-based maintenance system by data fusion and reliability-centered maintenance. *Reliability Engineering & System Safety* 95(7): 786–796.

Saha, B., Goebel, K. & Christophersen, J. 2009a. Comparison of prognostic algorithms for estimating remaining useful life of batteries. *Transactions of the Institute of Measurement and Control* 31(3–4): 293–308.

Saha, B., Goebel, K., Poll, S. & Christophersen, J. 2009b. Prognostics Methods for Battery Health Monitoring Using a Bayesian Framework. *IEEE Transactions on Instrumentation and Measurement* 58(2): 291–296.

Si, X.-S., Wang, W., Hu, C.-H. & Zhou, D.-H. 2011. Remaining useful life estimation—A review on the statistical data driven approaches. *European Journal of Operational Research* 213(1): 1–14.

Sikorska, J.Z., Hodkiewicz, M. & Ma, L. 2011. Prognostic modelling options for remaining useful life estimation by industry. *Mechanical Systems and Signal Processing* 25(5): 1803–1836.

Tseng, S.T., Balakrishnan, N. & Tsai, C.C. 2009. Optimal Step-Stress Accelerated Degradation Test Plan for Gamma Degradation Processes. *IEEE Transactions on Reliability* 58(4): 611–618.

Vaidya, P. & Rausand, M. 2011. Remaining useful life, technical health, and life extension. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 225(2): 219–231.

Wang, T. 2011. *Trajectory similarity based prediction for remaining useful life estimation*. PhD, University of Cincinnati.

Wang, X.-H., Li, Q.-X. & Feng, Y.-L. 2014. Research of Double Nozzle Flapper Valve Accelerated Degradation Test. *Applied Mechanics and Materials* 532: 18–21.

You, M.-Y. & Meng, G. 2013. A predictive maintenance scheduling framework utilizing residual life prediction information. *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering* 227(3): 185–197.

Zhang, K., Yao, J. & Jiang, T. 2014. Degradation assessment and life prediction of electro-hydraulic servo valve under erosion wear. *Engineering Failure Analysis* 36: 284–300.

Zhang, X., Chen, X., Li, B. & He, Z. 2011. Review of Life Prediction for Mechanical Major Equipments (In chinese). *Journal of Mechanical Engineering* 47(11): 100–116.

Zhao, W., Tao, T., Ding, Z. & Zio, E. 2013. A dynamic particle filter-support vector regression method for reliability prediction. *Reliability Engineering & System Safety* 119: 109–116.

Zhou, D.-H., Wei, M.-H. & Si, X.-S. 2013. A Survey on Anomaly Detection, Life Prediction and Maintenance Decision for Industrial Processes (In chinese). *Acta Automatica Sinica* 39(6): 711–722.

Zio, E. & Di Maio, F. 2010. A data-driven fuzzy approach for predicting the remaining useful life in dynamic failure scenarios of a nuclear system. *Reliability Engineering & System Safety* 95(1): 49–57.

Zio, E. & Peloni, G. 2011. Particle filtering prognostic estimation of the remaining useful life of nonlinear components. *Reliability Engineering & System Safety* 96(3): 403–409.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Effects of external audits on safety management systems: A case study of the Norwegian-managed maritime industry

J.F. Aae, A.K. Sydnes & C. Heggøy
University of Tromsø—The Arctic University of Norway, Norway

ABSTRACT: The maritime industry is subject to an enforced self-regulation regime based on the 1993 international code for the safe operations of ships and for pollution prevention. Companies in the maritime industry are required to establish Safety Management Systems (SMS) that are subject to external audits. This study examines the effects of external audits on vessel SMS, based on a series of interviews from the Norwegian-managed offshore supply vessel and dry bulk segments. First, it outlines how external audits are conducted, as mandatory and as industry-driven. Second, it finds that companies largely perceive the incentives for complying with regulations and external audits to be based on the threat of sanctions. Third, external audits are associated with both positive and negative effects on a vessel's SMS. This depends on the type of audit, where the flag state is seen as most beneficial for promoting safety.

1 INTRODUCTION

This paper examines how external audits affect the Safety Management Systems (SMS) of merchant vessels: specifically, Norwegian-managed Offshore Supply Vessels (OSV) and dry bulk vessels. Vessels in these segments operate under the 1993 International Code for the Safe Operations of Ships and for Pollution Prevention (ISM Code) established by the International Maritime Organization (IMO). The ISM Code requires companies to develop, implement and maintain SMS (IMO 2002: 7). However, it is largely left to the companies to design cost-effective SMS to meet their specific circumstances (Anderson 2003). To ensure that companies and their vessels comply with the ISM Code and other relevant rules and standards, the ISM Code, Part B, requires the use of internal and external audits, to be conducted by flag or port states, classification societies, and other safety or technical audits (IMO 2002: 7). Thus, the regime is based on 'enforced self-regulation' (Kristiansen 2005). We explore how the 'enforced' component, as represented by various external audits, affects the 'self-regulation' component, as represented by the company SMS. We do so through a series of more specific research questions: First, what practices have been established for the Norwegian OSV and dry bulk segments regarding external vessel audits? Second, how do companies perceive the need or incentives for complying with external vessel audits? Third, how do external vessel audits affect the SMS on board the vessels?

2 METHODS AND DATA

Our main data source is a series of semi-structured interviews conducted during the first half of 2013 (Heggøy & Aae 2013). We have selected two somewhat different maritime segments as cases for exploring the research topics in this study. The first is the offshore supply segment specialized in offshore supply vessels, aimed at the offshore petroleum industry. The second is shipping companies that operate deep-sea dry bulk carriers. These are vessels that carry homogeneous cargo worldwide in bulk, such as grain and minerals, stored in large cargo holds. Vessels from these two segments have different operational patterns, designs and technologies, but both are subject to the ISM Code and the regime it establishes for safety management. The companies included in the study are all well-established in the Norwegian shipping industry, varying in size from relatively small to large global companies. In total, six Health, Safety, Environment and Quality (HSEQ) managers and five vessel captains were interviewed (Table 1). Informants were selected on the basis of their involvement in on-board vessel audits. All interviews have been anonymized as regards both personal and company information. Interviews with HSEQ managers and captains from the two segments were conducted in person or by telephone. The data were then transcribed and categorized analytically.

Table 1. Informants, by company code and position.

Code	A OSV	B OSV	C OSV	D DB	E DB	F DB	G DB
HSEQ	A1	B1	C1	D1	E1	F1	
Captain	A2, A3	B2		D2			G1

3 MARITIME SAFETY REGULATIONS

3.1 *Safety regulation*

In recent decades, safety regulation has shifted from the use of detailed prescriptive regulations towards the use of functional requirements and self-regulation (Power 2000). This transfers greater responsibility to the company for establishing and maintaining an SMS that complies with established safety objectives (Reason 1997). The role of the regulator is, on the one hand, to establish the overall levels of safety or other goals to be achieved, and, on the other, to audit whether the company's safety management system complies with current safety legislation (Baldwin et al. 2010).

Enforced self-regulation implies that companies are required to establish a management system that takes into account all identified risks, and to continuously evaluate and improve the system (Gilad 2010). State agencies (or other mandated actors) then conduct systematic checks of the organization's activities and arrangements, to determine whether it is complying with the required standards (Blewett & O'Keffe 2011). These systematic checks are referred to as audits, defined as *"systematic, independent and documented process for obtaining audit evidence, and evaluating it objectively to determine the extent to which the audit criteria are fulfilled"* (ISO 2011).

The ISM Code was introduced in response to a series of serious accidents in the 1980s and early 1990s (Anderson 2003). In contrast to earlier safety measures, the ISM Code is based on an enforced self-regulating strategy, taking a step away from more traditional descriptive legislations (Kristiansen 2005). Despite the intentions of promoting a safer shipping industry, the effects of the ISM Code have been debated, within the industry, in the academic literature and by policy-makers (Anderson 2005; Batalden & Sydnes 2014).

The ISM Code has been made mandatory through the IMO convention SOLAS, but legal enforcement is delegated to the flag state—the state where the vessel is registered (Kristiansen 2005; Oltedal 2010). Additionally, safety audits are also conducted by many other actors within the shipping industry (Kristiansen 2005; Vorbach 2010). According to Gunningham et al. (1999) professional industry bodies, industry associations, trading partners and supply chains can provide an external pressure on companies to comply with market-based or branch requirements. Such audits complement traditional flag- or port state sanctions—such as fines, detentions and certificate withdrawal (Anderson 2005). Commercial and reputational concerns are particularly prevalent (Van Erp 2008).

3.2 *Safety management systems*

A safety management system can be seen as a systematic process for achieving and maintaining a safety level in accordance with the organization's goals (Aven & Vinnhem 2004). The ISM Code defines a safety management system as "*a structured and documented system enabling Company personnel to implement effectively the Company safety and environmental protection policy*" (Section 1.1.4). Adherence to functional requirements is to be developed, implemented and maintained by the company's SMS as defined above; a safety and environmental-protection policy; instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation; defined levels of authority and lines of communication between and among shore and shipboard personnel; procedures for reporting accidents and non-conformities with the provisions of the Code; procedures for preparing for and responding to emergency situations; and procedures for internal audits and management reviews (ISM Code, Section 1.4). As Anderson (2003) points out, these requirements represent the *minimum* features of an acceptable safety management system.

We consider SMS as a process that can be divided analytically into four stages which in sum meet the functional requirements presented above: 1) *safety target and policy,* 2) *risk management,* 3) *internal audit,* and 4) *monitoring and learning* (Stolzer et al. 2008). This can be considered as an action-cycle, based on Deming's Plan–Do–Check–Act model (Reason 1997). In the first stage the overall safety and environmental policy is established, determining which objectives will be met. The second stage involves risk identification, management and execution of the scheduled tasks. In the third stage the company should conduct regular internal audits to ensure that the safety objectives have

been met. Stage four, monitoring and learning, requires the company to follow up on the information from the previous stages, and implement corrective measures if necessary (Stolzer et al. 2008; Reason 1997). In this fourth stage, the company can also draw on results from external vessel audits as a source of information (Stolzer 2008). Further, SMS is a circular process which demands continuous holistic improvements to the system (Aven & Vinnem 2007).

4 EXTERNAL VESSEL AUDITS

Here we present the main external audits that are conducted on board vessels within the two segments of our study (see Table 2). We will also present our findings as to how informants perceive the relative importance of complying with requirements of external audits.

The ISM Code establishes a series of mandatory audits to be conducted by the flag state (or classification society on its behalf) in addition to internal audits. In order to operate a vessel, the owner or operator must initially have a Document of Compliance. This is a document issued on the basis of flag state audits, verifying that an SMS consistent with the ISM Code is in place (IMO 2010). A vessel must also carry a Safety Management Certificate, verifying that the key elements of the ISM Code are in place (Anderson 2003). Further, external audits are conducted to ensure the effectiveness of the SMS in meeting the objectives of the ISM Code (IMO 2010). When a vessel enters port, it can also be subjected to port state control. The port state does not have the authority to suspend or withdraw the document of compliance for vessels issued by the flag state. However, it has the right to impose sanctions, for example by fines or detaining a vessel in port (Anderson 2005).

In addition to the mandatory audits established by the ISM Code, various non-mandatory, or industry-driven, audits are conducted (Knapp 2007). Importantly, industry-driven audits serve as databases where cargo owners and charterers can get information about a vessel's safety standard. Results from the audits, or vettings (as these types of audits often are called), are made available in online databases, where vessels also are given safety rankings (Knapp 2007). In the Norwegian OSV segment, two industry-driven audits have predominated. First, the Common Marine Inspection Document (CMID), aimed at improving technical standards and reducing the number of inspections, by providing a common industry format (IMCA 2009). Second, the Offshore Vessel Inspection Database (OVID), which aims to establish an internationally accepted assessment tool to be applied as a basis for selection during vetting and assurance of OSVs (OCIMF 2010). In addition come other industry-driven audits, or "spot audits," generally more limited in scope. An example of such audits can be "falls from heights audit" (A2). However, as our informants saw these as less important to the main research topics addressed here, they are not addressed in detail. From the sample of cases from the Norwegian OSV segment, it is clear that industry-driven audits play an important role as an addition to the mandatory audits established by the ISM Code. All three companies are subject to OVID and CMID audits on a regular basis. In addition, there are spot audits initiated by contractors or the vessel-companies themselves.

Table 2. External audits, OSV and dry bulk segments.

Audit segment type	OSV	Dry bulk
Mandatory	Flag state	Flag state
	Port state	Port state
Industry-driven	CMID	Rightship
	OVID	Spot audit
	Spot audit	

In the dry bulk segment, Rightship has been established as an international, industry-driven audit and ranking system. Rightship combines information from various sources, such as vetting inspections, port state controls, casualties and owner information (Knapp 2007). Based on this, it provides an information system where vessels are ranked from 1 to 5. Rightship inspections primarily concern dry bulk carriers (Rightship 2014). Industry-driven audits have a less prominent role in the dry bulk segment. Only company D has Rightship auditing its vessels. As one HSEQ manager noted regarding Rightship, "*The oil companies have practiced this vetting form for a while now, and seem to have benefited a lot from it, so now we also have started. Earlier we just had to show our papers, now we have to show that we actually work according to the papers*" (D1). Vessels from company D, E and F are occasionally subject to spot audits from cargo owners, but none of the informants indicated that this occurs regularly. According to one informant, "*The customers do not really have any concerns regarding safety on board the vessel*" (F). Though only company D is currently audited by Rightship, all companies are aware of its existence. It is not unlikely that industry-driven auditing will become more prevalent in the Norwegian dry bulk segment over time.

4.1 *Complying with external audits*

In general the informants in this study, within both the dry bulk and OSV segments, noted the need

for external audits to be conducted, and felt that these audits have a positive effect on safety management. However, we wish to understand what kind of external pressure external audits put to bear on companies to comply with regulations and standards as part of their safety management on board vessels. Being audited provides external pressure on companies in the dry bulk and OSV segments in several ways, two of which will be examined here. First, vessels need to meet the formal requirements established by the ISM Code and other regulations through mandatory audits. Second, the maritime industry is known for being driven by international competition (Vorbach 2010). Safety management is an important aspect in this regard as well. As explained by one captain, and one HSEQ manager, from the OSV segment: *"One side is more of a commercial importance, while the other side is important for simply being a shipping company"* (B2). Also, *"When we submit an offer for a job, safety is a big part of the competition"* (A2). Compliance and scoring during audits are commercially important for gaining commercial contracts. For example, results from the industry-driven CMID and OVID audits are used as a basis for decision-making and risk management when negotiating contracts in the offshore supply segment. While several informants in the OSV segment (A2, B2, C1) considered the audits themselves to be a burden due to the time and resources required, they nevertheless recognized the importance of performing well during audits.

In the dry bulk segment, industry-driven Rightship audits have a more limited role. The mandatory flag- and port state controls seem to be of greater concern, as regards both the costs of being detained or getting non-conformities, and the commercial consequences of negative publicity and loss of reputation (D2, G1, E1, F1). However, several informants saw limited safety benefits of port state controls (D1, D2, E1, F1). The main challenge concerns the varying interpretations of legislation applied by port states; *"The worst thing about port state control is that they don't even have similar interpretations of the law. What can be accepted in England you might risk to get a deficiency on in the Netherlands"* (E1).

In summary, within both the dry bulk and the OSV segments, compliance is primarily related to sanction costs that may follow as a consequence of poor audit results. This leads to a more limited focus on auditing and compliance as measures for improving the safe management of operations.

5 EFFECTS OF EXTERNAL AUDITS ON VESSELS SMS

Here we present our findings regarding the effects of external audits on the SMS on board the vessels in the study. The results are arranged according to the four stages of a SMS: safety policy, risk management, internal audit, and monitoring and learning (Reason 1997; Stolzer et al. 2008).

The overall objective of an SMS is defined in a safety and environmental protection policy, and is a mandatory part of the system according to the ISM Code (Section 1.4.1). However, auditing safety policy, though important for companies and vessels SMS, is part of the onshore company audit, not the vessel audits. Consequently it lies beyond the scope of this study and the data we have gathered.

5.1 *Risk management*

Risk management includes risk identification, assessment and the conduct of shipboard operations (Stolzer 2009; Reason 1997). Informants gave statements concerning both positive and negative impacts on risk management on board dry bulk and offshore supply vessels. The results of vessel audits can be considered as a source of proactive information (Anderson 2005), or a type of information that enables companies to implement measures before accidents occur (Rausand & Utne 2009). In general all informants from both segments saw external vessel audits as a proactive measure (A1, A2, A3, B2, C1, D2, G1, E1, F2). External audits provide an independent view of the system on board (A1, A3, B2, G1, F1). As one captain in the OSV explained, *"Working on board a vessel is like living in a small closed community; when you're audited you get an independent view on how you work"* (A3). However, one captain from the OSV notes, *"External audits must not turn in to a false sense of safety, you still have to exercise caution constantly"* (B2).

High-quality information can enable a company to predict an accident (Turner 1976). There are differences in the value of information the various types of audits provide about the SMS. In the OSV segment, industry-driven audits were seen as being less relevant (A1, A2, B2, C1). Informants from the dry bulk segment felt that port state controls did not always provide information useful for improving vessel SMS (D1, E1, F2, G1). As one informant from the dry bulk segment explained, *"During audits we get a good discussion and dialog, where they provide suggestions, and thereby help to improve our system, but this is mainly the [flag state audits], port state control doesn't make such a contribution"* (F1). Port state audits are seen as less useful due to the diverging interpretations of legislation and requirements between different port states (D1, D2, E1, F1, G1). One captain noted, *"Sometimes I get quite astonished when I see some of the vessels that certain port states let pass, but maybe they are*

better than they look from the outside. I don't know, but sometimes is seems that the threshold for detaining a vessel is quite high" (G1).

In the OSV segment, concerns relate mainly to the industry-driven audits OVID and CMID. Here our informants shared a common concern regarding what one informant referred to as *"audit overkill"* (C1). External vessel audits from OVID and CMID seem to be conducted very frequently, which leads to considerable time being spent on satisfying the auditors (A1, A2, A3, B2, C1). A shared consideration among our informants was that the OVID system does not function as intended (A1, A3, B2, C1). As one captain explained, *"The idea was that you were supposed to have one OVID every 12 months. The charterer then could see the results in a database, but what happens is that every charterer requires their own OVID audit. The regime that was supposed to make things easier does not work"* (B2). Moreover a HSEQ manager noted: *"OVID was supposed to replace CMID, nevertheless they exist in parallel"* (A1).

Vessel audits require involvement from the crew on board. This is identified as a common challenge as informants from both segments expressed concerns regarding how external audits consume time when the vessel is in port, where time already is short (A1, A2, A3, B2, C1, D2, E1, F1). Two captains, one from the OSV and one from the dry bulk segment, said that the extra work external audits entail can come the expense of rest-hour regulations (B2, D2). As one captain said, *"To operate a vessel you have to be sharp. But when I've been busy all day with an audit, in addition to all the other things we have to do in port, then I am not fit to maneuver the vessel, and accidents may happen"* (D2).

These findings show that our informants are generally positive to the effects of external audits on risk management. However, the effects depend on the audit. Here, flag state audit was regarded most positively. The OSV and dry bulk segments consider industry-driven and port state audits, respectively, to have more limited positive effects. A common challenge noted was the time required for conducting external audits.

5.2 *Internal audits*

Internal audits are a measure for the company to evaluate the effectiveness of the SMS in accordance with established procedures (ISM Code, Section 12.2). All informants from both segments say that internal audits of their vessels' SMS are performed at least once a year, as per the ISM Code, Section 12.1. As required in Section 12.4, internal vessel audits are conducted by HSEQ personnel who are working on the companies' onshore staff. All informants felt that these internal vessel audits were important, and that, due to the presence of external audits, the internal audits become even more important (A1, A2, A3, B1, B2, C1, D2, E1, F1, G1). It was commonly held that it is better to discover deficiencies internally than have them found by external auditors. This triggers a self-critical view on the system when internal audits are conducted. This was a consideration shared by all informants in our study. One captain from the dry bulk segment explained, *"I bring my biggest magnifying glass and tell the crew that it's better that I find something than someone else does. We probably could be better, but I clamp down on every little thing I find"* (D2).

A prominent view among informants was that internal audits are a tool for ensuring good results on external audits (A1, A2, A3, B1, B2, C1, D2, E1, F1, G1). As one HSEQ manager said, *"For us it means that we have to be ahead of those who audit us, there are small margins in the industry today, and we have to be out in front and proactive regarding the regulations"* (E1).

The OSV segment appears to be subject to extensive industry initiated auditing compared to the dry bulk segment, and informants were preoccupied with scoring high on these audits. This is because the results also are associated with commercial aspects (A1, A2, A3, B1, B2, C1). *"It is a lot better to find things internally, because than it does not lead to any economic consequences"* (A1). Another informant said, *"Results from an OVID are available for the whole industry in 12 months. If you have several deficiencies, you've shot yourself in the foot"* (B2). The same motivation for conducting industry-driven audits was, naturally enough, not expressed by informants from the dry bulk segment. This being said, one company had the commercial actor Rightship auditing their vessels, which added commercial interests to having good scores on these audits, as we saw in the OSV segment (D1, D2). *"Rightship is a big actor in the dry bulk segment, you can compare them with BP and Shell, and so they have a lot of influence. Even when we are in line with international requirements, Rightship can tell us that we still aren't good enough"* (D2).

In general, internal audits are seen as an important measure for evaluating and improving vessel SMS. A main motivation for internal auditing is to avoid non-conformities during external audits.

5.3 *Monitoring and learning*

We have seen how external audits contribute to monitoring the vessels' SMS to varying degrees. Below we focus on how external audits contribute to system learning. According to our informants, find-

ings from external audits can sometimes contribute to learning and development on board vessels. All companies represented in this study have systems for transfer of experience, enabling all vessels in the fleet to benefit from the results of an external audit.

Findings from external audits do not always serve as a source of learning. Informants raised concerns as to the port state controls performed in the dry bulk segment and industry-driven audits in the OSV segment (A1, A2, B2, C1, D1, E1, F2, G1). They said that the following factors affect the learning value from information generated from external vessel audits: type of audit, experience and knowledge of the auditor, and the auditor's intentions.

Most informants felt that flag state audits bring the most learning value about the system, mainly because the auditors are familiar with the vessel and often are experienced (A1, B2, C1, D2, E1, F1, G1). In contrast, informants from the dry bulk segment all held that port state controls were too unpredictable, making it difficult to update the system in accordance with various auditors' interpretations of the regulations (D1, E1, F2, G1). One HSEQ manager put it like this: *"Port state is very unpredictable, you cannot update the vessels according to all deficiencies"* (E1).

In the OSV segment, customer-initiated audits as a whole were subject to criticism regarding learning value, but the examples provided by informants mainly concerned the OVID audit. We were given various examples that indicated that OVID was less beneficial as a source of learning. As one captain remarked, *"They search for errors just so that they can write something. Once on an OVID vetting we got a deficiency because the chef's hat was the wrong color"* (B2). Another point made was that the OVID audit is not fully adapted the OSV segment. *"They seem to have copied and pasted a lot from the tanker segment and this does not necessarily fit a supply vessel"* (A3). A third criticism was that the OVID audit is too superficial, *"It's based on yes/no questions, so you actually end up not gaining any more knowledge"* (A1).

To summarize, there seems to be a clear connection between how informants consider the relevance and quality of the external audit and to what extent they perceive it as providing a basis for learning. Again flag state-audits are considered to have the greatest learning effect as regards SMS. In the dry bulk segment, the port state audits score lower, while for the OSV segment OVID in particular was regarded as having a more limited effect on learning.

6 DISCUSSION

In this study we have examined how external safety audits affect the SMS on board OSVs and dry bulk vessels. In 1998 the ISM Code became mandatory for all vessels, and required companies to establish a SMS on their vessels. The ISM Code is implemented through the use of enforced self-regulation, which makes the company responsible for establishing a system that ensures safety at sea (ISM Code 1.2.1), including both human life and damage to the environment. The performance of this system is then audited through external mandatory and industry driven audits, in addition to internal audits.

The Norwegian dry bulk and OSV segments are both subject to mandatory audits established by the ISM Code and international requirements. Our focus here has been on flag- and port state audits. These audits are frequently conducted by classification societies acting on behalf of the states as "recognized organizations" (IMO 2010). In addition come established, industry-driven audits within both segments, albeit far more prevalent in the OSV segment, where CMID and OVID, in addition to various spot audits, are well established. In the dry bulk segment Rightship has been established to perform a similar function as CMID and OVID, but has not yet achieved the same widespread recognition and use. According to Lindøe et al. (2011), these differences may be explained partly on the basis of the regulators associated with the offshore petroleum industry and maritime bulk transport. The Norwegian petroleum industry aims to be a world leader in safety. This pervades the whole industry, including shipping companies (Lindøe et al. 2011). As opposed to bulk transport, the petroleum industry has close connections between contractors and suppliers, often resulting in strong industrial relations (Oltedal & Engen 2010). This is also evident in our study. Rightship is a fairly new actor in the Norwegian setting, but informants note that it is becoming more prevalent in the dry bulk segment and may contribute to strengthened industry-driven auditing practice over time.

Stronger industry involvement may also entail challenges. As Baldwin et al. (2012) emphasize, with a multitude of audits and regulators, coordination is necessary. Our data from the OSV segment indicate that audits, especially industry-driven ones, are not well-coordinated. While the intention was to reduce the number of audits, CMID and OVID audits are conducted in parallel and more frequently than expected. This has also been found in studies of other industries (Blewett & O'Keffe 2011). Therefore, greater industry involvement in auditing may not always lead to safer practices.

Our study also found that compliance is generally driven by the costs related to potential sanctions. In the dry bulk segment, port state audits were seen as most 'risky' in terms of the sanctions that could be imposed and their consequences. The OSV segment focused more on the financial costs of poor scores or ratings on publicly available industry-driven audits. These were considered to have implications

on the tendering process. Thus, both legal and non-legal sanctions prove to have an effect on compliance (Van Erp 2008). At present their relative effect depends largely on the characteristics of the audits and the industry (Oltedal & Engen 2010). As Vorbach (2010) notes, audits need to be coordinated, to increase the desired effects on safety management.

6.1 *Effects on SMS*

The final question raised in this paper was how informants assessed the effect of external audits on a vessel's SMS. External audits seem to have two main effects on a vessel's SMS. The first is related to the tangible feedback that an external audit provides about the SMS. The second concerns the external pressure the audits place on companies to establish and maintain their vessels' SMS. We find that external vessel audits have both positive and negative effect on a vessel's SMS. In particular flag state audits are seen as making positive contributions to a vessel's SMS, in contrast to industry-initiated audits in the OSV segment and port state controls in the dry bulk segment. In the following we discuss our findings regarding the stages of the SMS: risk management, internal audit, and monitoring and learning (Reason 1997; Stolzer et al. 2008).

In general, accidents occur when hazards accumulate unnoticed in the system (Turner 1976; Reason 1997). Detecting these and acting accordingly is therefore crucial for a vessel's SMS. As a contribution to risk management, external audits stimulate companies to be more proactive, and the audits provide a fresh view of the system on board. In this regard we can argue that external vessel audits provide a positive contribution to a vessel's SMS. However, according to our informants, this is mainly the case for flag state audits.

We also found that external audits are often seen as more of a burden than a measure for promoting safety. In both segments, external audits place an extra workload on the crew on board, especially in the OSV segment, where industry-driven audits seem to be conducted quite frequently. In consequence, the crew has less time for conducting other shipboard operations. Moreover, as also indicated by Knapp (2007), rest-hour regulations may suffer. This is disturbing, stress and fatigue are known to increase the risk of accidents (Sneddon et al. 2013).

All companies are required to establish procedures for internal audits, according to Section 1.4.6 of the ISM Code. Our informants consider this arrangement to be of great importance, noting in particular that internal audits provide an opportunity to discover non-conformities and deviations ahead of the external audits. This is an incentive for companies to conduct internal audits, to ensure compliance with established requirements and positive results on external audits. On the other hand, internal audits risk having a stronger focus on scoring on external audits and complying with established standards, than focusing on work-safety on board (Bhattacharya 2009). This is a well-known pitfall from internal auditing in enforced self-regulatory regimes (Blewett & O'Keffe 2011; Hohnen & Hasle 2011). Focusing on external requirements and audits rather than applying a risk-based approach based on the vessels may lead to a false sense of security (Batalden & Sydnes 2014b forthcoming). Disasters like the Longford explosion (1998) and the Piper Alpha (1988) have showed that external audits may be of little value in detecting hazards and avoiding accidents (Hopkins 2000). This underscores the need for thorough internal audits and risk management.

Monitoring and learning is the last stage of the SMS as defined in this paper. Our informants mentioned that external audits often provide inputs that fail to result in improved SMS. This is primarily related to industry-driven audits in the OSV segment and port state audits in the dry bulk segment. Again this has been shown in other studies of auditing (Blewett & O'Keffe 2011). Both the scope of the audits and the competence of auditors are important for understanding the extent to which audits may provide valuable inputs to SMS (Bhattacharya 2009; Batalden & Sydnes 2014b forthcoming). Also our informants highlighted these factors to explain why flag state audits are seen as providing positive inputs as sources of learning.

7 CONCLUDING REMARKS

This study first outlined how the OSV and dry bulk segments are subject to a series of mandatory and industry-driven external audits. What effects these audits have will depend largely on the characteristics of the individual audits and the maritime segments. However, we find that, in both cases, compliance is driven by the costs of sanctions, legal and commercial, related to the different audits.

We have also seen that external audits are important for the continuous focus on SMS on board both dry bulk and OSV vessels. However, not all external audits contribute equally to enhancing safety on board vessels. Here we find the flag state audits to be of greatest importance. They are regarded as having the most competent auditors and most relevant scope. Other audits discussed here, such as industry-driven and port state audits, do not have the same positive effect in promoting safe practices and learning in the SMS.

Internal audits seem to be a tool for ensuring good results on external audits and avoiding sanctions. However, that also entails the risk of losing the focus on a risk-based and self-regulatory approach to SMS.

In sum, our study has shown that the maritime industry still faces challenges in achieving the aims of the ISM Code. Nevertheless, external audits do put pressure on companies to comply with established requirements, and are thus part of the solution in addressing these challenges.

Our findings largely echo those of previous studies of auditing in the maritime industry. However, there is need for more extensive studies covering a broader range of cases sampled. There is also a need for further in-depth studies of how the characteristics of audits (design, conduct and sanctions) affect how companies respond to them. This would contribute to our knowledge on the effects of external audits on safety management.

REFERENCES

Anderson, P., 2003. *Cracking the Code. The relevance of the ISM Code and its impact on shipping practices*. London: The Nautical Institute.

Anderson, P., 2005. *ISM Code, A practical guide to the legal and insurance implications*. London: Informa Professional.

Aven, T. & Vinnem, J.E., 2007. *Risk Management*. London: Springer Verlag London Limited.

Baldwin, R., Cave, M & Lodge, M., 2010. *Understanding Regulation*. Oxford: Oxford University Press.

Baldwin R., Cave, M. & Lodge, M., 2012. *The Oxford Handbook of Regulation*. Oxford: Oxford University Press.

Batalden, B.M. & Sydnes A.K., 2014. Risk assessment, Key Shipboard Operations and soft barriers in offshore opertions. *Safety, Reliability and Risk Analysis: Beyond the Horizon*. London: CRC Press, 1611–1618.

Batalden, B.M. & Sydnes A.K., 2014b. Auditing the maritime industry: A case study of the offshore support vessel management. Forthcoming. Arctic University of Norway.

Bhattacharay, S., 2009. The Impact of the ISM Code on the Management of Occupational Health and Safety in Maritime Industry. Cardiff: Cardiff University.

Blewett, V. & O'Keeffe, V., 2011. Weighing the pig never made it heavier: Auditing OHS, social auditing as verification of process in Australia. *Safety Science* 49: 10141021.

Gilad, S., 2010. It runs in the family: Meta-regulation and its siblings. *Regulations & Governance*, 4: 485–506.

Gunningham, N., Grabosky, P. & Phillipson, M., 1999. Harnessing Third Parties as Surrogate Regulators: Achieving environmental outcomes by alternative means. *Business Strategy and the Environment*.

Heggøy, C. & Aae, J., 2013. Betydningen av ekstern kontroll i en selv-regulert maritim næring. Master thesis. Tromsø: Arctic University of Norway.

Hohnen, P. & Hasle, P., 2011. Making work environment aditable: A "critical case" study of certified occupational health and safety management systems in Denmark. *Safety Science*, 49: 1022–1029.

Hopkins, A., 2000. Lessons from Longford: The Esso Gas Plant Explosion. Australian National University.

IMCA, 2009. Common Marine Inspection Document. International Marine Contractors Association. London.

IMCA, 2013. Guidance on Using the eCMID and the CMID Inspection Report Database. London: International Marine Contractors Association.

IMO, 2002. International Safety Management Code & Revised Guidelines on Implementation of the ISM Code by Administrations. London: International Maritime Organization.

IMO, 2010. ISM Code: International Safety Management Code and Guidelines on Implementation of the ISM Code. London: International Maritime Organization.

ISO IOfS, 2011. Guidelines for Auditing Management Systems ISO 1901: 2011. Geneva: International Organization for Standardization.

King, A.A. & Lenox M.J., 2000. Industry Self-Regulation Without Sanctions: the Chemical Industry's Responsible Care Program. *Academy of Management,* Journal 4(4): 698–716.

Knapp, S., 2007. *The Econometrics of Maritime Safety*. Erasmus University Rotterdam.

Kristiansen, S., 2005. Maritime Transportation: *Safety Management and Risk Analysis*. Burlington: Elsevier Butter worth Heinemann.

Lindø, H. P., Engen, O.A. & Olsen, O. E., 2011. Responses to accidenst in different industrial sectors. *Safety Science*, 49: 90–97.

NOU, 2008. NOU 200:8 Bourbon Dolphins forlis den 12. april 2007. Oslo: Ministry of Justice and Public Security.

OCIMF, 2010. Offshore Vessel Inspection Database-OVID. http://www.ocimf-ovid.com/Welcome.aspx. Accessed 5. February 2014.

Oltedal, H.A., 2010. Safety Culture and safety management within the Norwegian-controlled shipping industry. Stavanger: University of Stavanger.

Oltedal, H.A. & Engen, O.A., 2010. Tanker versus dry cargo: The use of safety management systems within Norwegian dry cargo shipping. *Reliability, Risk and Safety*, 2118–2125.

Power, M., 2000. The Audit Society: Second Thoughts. *International Journal of Auditing*, 4: 111–119.

Rausand, M. & Utne, I.B., 2009. *Risikoanalyse teori og metode*. Trondheim: Tapir.

Reason, J., 1997. *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.

Rightship, 2014. About Rightship. http://site.rightship.com/about/who-we-are/. Accessed 20 February 2014.

Sneddon, A., Mearns, K. & Flin, R., 2013. Stress, fatigue, situational awareness and safety in offshore drilling crew. *Safety Science*, 56: 80–88.

Stolzer, A., Halford, C.D. & Goglia, J.J., 2008. *Safety management systems in aviation*. Aldershot: Ashgate.

Turner, B., 1976. The Organizational and Inter Organizatio al Development of Disasters. *Administrative Science Quartely*, 21: 378–396.

Van Erp, J., 2008. Reputational Sanctions in Private and Public Regulation. *Erasmus Law Review*, 1(5): 145–161.

Vorbach, J.E., 2010. The Vital Role of Non-flag State Actors in the Pursuit of Safer Shipping. *Ocean Development & International Law*, 32: 27–42.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Review of acceptable risk levels of bridge collapse in respect of ships collisions

L. Gucma
Maritime University of Szczecin, Poland

ABSTRACT: The bridge collapse due to ship collision is supposed to be the cause of almost half of the bridge catastrophes. The paper intention is to gather the existing methods of risk acceptable level and compare them. The paper presents also selected problems of accident probability assessment in respect of ship collisions with bridges. Accident statistics in Poland and around the world are presented. Wide discussion on bridge collapse risk acceptance criteria have been carried out. Finally to different case studies of probability assessment taking into account both horizontal and vertical clearances. Two case studies partly covering discussed aspects are presented.

1 THE ACCIDENT STATISTICS AND THE PROBLEMS OF SHIPS COLLISIONS WITH BRIDGES

Bridges situated on sea and inland waterway areas belong is the particularly sensitive infrastructure from three the major causes:

1. create restrictions of not only in the vertical water area but also in horizontal;
2. they create the threat to its users in the case of ship-bridge collision and bridge collapse,
3. the cost of the bridge is usually considerably larger then the cost of the ship itself.

He the ground analyses of the literature [Scheer, 2010; Radomski, 2011] it is clear that the collisions with ship is they of the major causes of bridges disasters and they can be even 30% of all reasons of whole bridge catastrophes. In years 2003–2013 the scientific the team of the marine traffic engineering of Maritime University of Szczecin executed the row of analyses of the safety of bridges in this [Gucma L., 2013]:

– the railway bridge in Szczecin (2003),
– two locations of foot bridges in Elbląg (2008),
– foot bridges to the Ołowianka Island in Gdańsk (2009),
– two bridges on the Motława in Gdańsk (2009),
– the bridge to the Ostrów Brdowski Island in Szczecin (2013).

The problems of ships collisions with bridges comes from years 60, when is in the result of the height of the intensity of the traffic and dimensions of ships followed the scale of events and disasters. First, sizable studies were done in the year 1980 after the allision of the ship Summit Venture with the bridge Sunshine Skyway. In monograph [Gucma L., 2013] it is presented the composition of several collisions of ships with bridges since the year 1980 together with results and reasons of collisions, the death rate and the name of the ship. One can notice (Fig. 1) that averagely in the world it appear 2 serious collisions of ships with bridges per year, and every 2 years it appears the event with catastrophic results causing the destruction of the bridge, the loss of the ship or the fatalities.

American statistics [USCG, 2003] brought to light that the large part of collisions of ships with bridges caused however comparatively not large scale losses. In years 1992–2001 one noted together 2692 collisions. Only 61 from them (2,2%) caused greater losses then 0,5 millions USD. The 1702 events (63%) of them was incidents in which the damage were not significant and the repairs of the bridge was not necessary. In the inland area administered by RZGW in Szczecin there was average one collision of the inland unit with the bridge per year. Most destructive was the collision

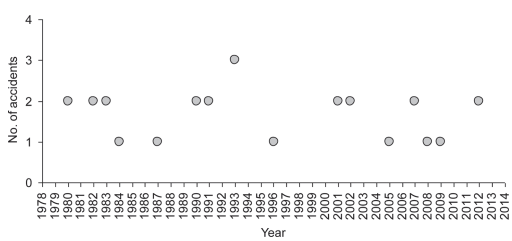


Figure 1. The yearly number of ships collisions with bridges serious in results in the world.

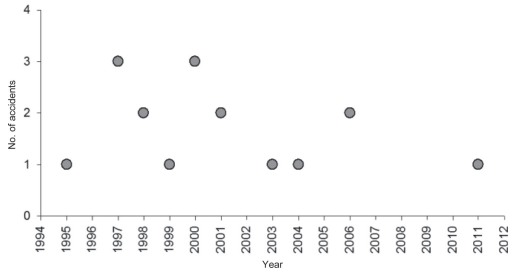


Figure 2. The number of events with bridges in the region administered by RZGW in Szczecin [Gucma L., 2013].

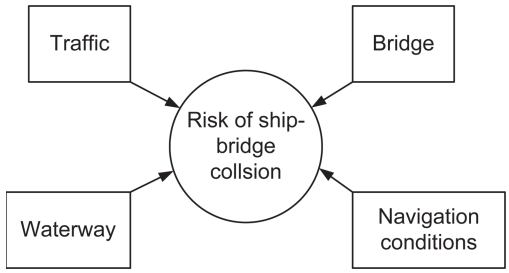


Figure 3. Factors of the risk of collisions of ships with bridges.

in 2001 when the guides of the railway bridge in Szczecin was destroyed, what caused the necessity of their exchange. In the region administered by RZGW all cases of collisions of inland units with bridges Szczecin are presented in Figure 2. It was recorded 17 cases within analysed of 16 years. Happily, it never arrived to fatalities in people. Events due to error of the navigator dominates, they happens with the frequency approx. 90%, what confirm world statistics. Alarming is also the large participation of collisions with bridge spans which amounts around 65%. The part from them ended with bulky damages of the ship. Such collisions result most often due errors in the planning phase of navigational passage under the bridge, mostly from the ignorance about the current clearance of the bridge or the height of the air-draught of ship.

2 THE RISK MANAGEMENT IN THE ASPECT OF THE COLLISION WITH SHIPS IN THE BRIDGES AREA

The creation of the rational risk management system before the delivery of engineering construction, especially, when such object could attract possible fatalities, are nowadays the standard in many countries. In this chapter some theoretical and practical aspects of the risk management are presented. The important are the measures of the risk assessment what ties in with the settlement of levels of its acceptance. Figure 3 presents the four main factors influent on collisions of ships with bridges. To navigational conditions need to be also considered.

The risk of the collision of ships with bridges one can divide on five main categories:

1. the risk for the owner of the bridge connected with necessity of its repair or the loss of profits after the break of the bridge passage;
2. the risk for users of the bridge connected with the possibility of the loss life, health's or the monetary values during the passage;

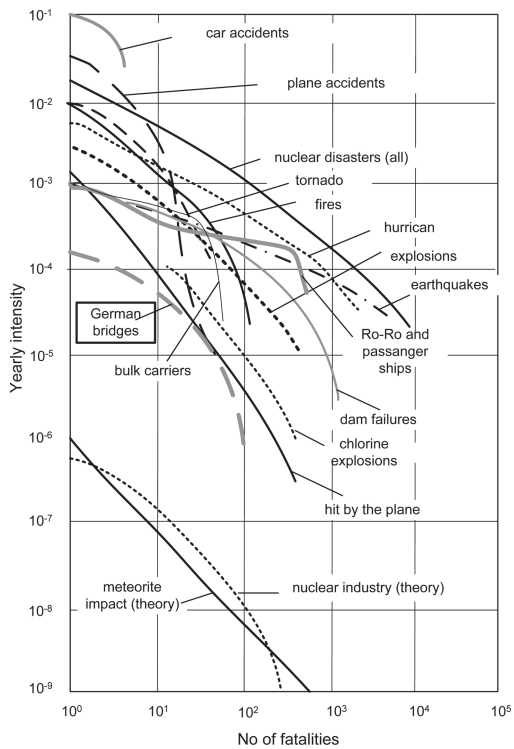


Figure 4. Example FN curves for different activities together with FN estimated for German historical bridges [Gucma L., 2013].

3. the risk for third parties which do not draw any advantages from the bridge. It refers also ships, in case, when the bridge causes the threat with relation to of the state before construction of the bridge;
4. the risk concerning of results socioeconomic because of the break of the passage;
5. the risk environmentally as result of pollution with the overflow or with the liberation of toxic gases.

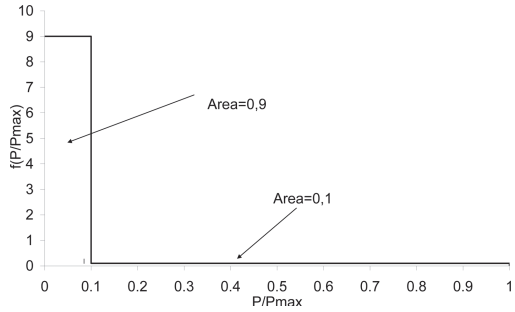


Figure 5. Density function of bridge collapse due to ship collision (AASHTO [1991]).

The procedure of the risk management is the multistage rational method, targeting increasing of the safety of the shipping throughout the protection of lives and health's of people, environments and properties [Gucma L., 2009]. The procedure consists of the risk analysis (estimation), the assessment of the risk which requires of the decision about his acceptability and his temporary inspection. It consists of four following stages:

1. The identification of hazards.
2. Risk analyses (the estimation of the risk on the basis of data possessed without taking into account of changes in analysed area) which consists of assessing of the probabilities of the threats (probability assessment) and the qualification of consequences (consequence analysis).
3. Evaluation of the risks (the comparison of the risk with criteria values, to meet the acceptable level).
4. Risk managements (with the regard of methods of the risk reduction and its temporal control).

It is the risk analysis of ship-bridge collisions the measures of the societal risk described by FN (frequency—number) are widely used (Fig. 5).

3 ACCEPTABLE LEVELS OF BRIDGE COLLAPSE AS RESULT OF THE SHIPS COLLISION—COMPARISON OF CRITERIA VALUES

Acceptability criteria of break of the bridge connection risk is set up due to following factors:

– possible number of fatalities in the case of the traffic on the bridge,
– the degree of the importance of the bridge for the society or/and defence of the country,
– costs of the restoration and costs of the operation as result of the break of the bridge passage, qualified most often by means of CBA analyses.

Taking into account international and local regulations, the acceptability of the risk of the critical bridge by trespassing ships are varied in different designs of the bridge in the world. When risk acceptability criteria does not exists it is necessary to perform wide relations to the existing projects or to natural threats in the investigated region.

The probability applied for bridge failure in codes and international standards differs from 0,0001 to 0,001 for 100 year (10^{-6} to 10^{-5} per year). Analysing the accessible literature shown in [Gucma L. 2013] within the range of the risk acceptability of the bridge destruction as result of the collision with ship, following conclusions could be drawn:

1. For the project of the bridge through Great Belt the criterion of the bridge serious collision with ship was 1 per 10 000 years, that gives the probability of the bridge collapse 0.02 on 100 years (2.0 10^{-4} per year).
2. Given in 1985 the recommendation of the Louisiana State divide bridges on 2 categories. For deep water bridges (ships up to 13 m of the draught) the admissible probability of the destruction of the bridge as result of the ship is 0,01 on 100 years (10^{-4} a year).
3. The ISO standard puts limit probabilities of the destruction of the bridge as result of the collision with ship on level of 0.01 per 50 years, what gives value of 0.02 per 100 years (2.0 10^{-4} a year).
4. J.B. Menzies proposes to apply the acceptable risk of bridges destruction on level 2.0 10^{-6} which then the value seems to be nearing to norms quoted in Eurocode 1 EN1990:2002. It is worth of notice that this author ascertains, that in the past above the half of all destructions of bridges was due to event relied with the ship collision or the erosion the bottom at the pier as result of the flood.
5. Recommendations of the American Association of State Highway and Transportation Officials (AASHTO) assumes the probabilities of the bridge destructions on level from 0.1 and 0.01 per 100 years (10^{-3} and 10^{-4} a year) consecutively for standard- and critical bridges.
6. According to L.J. Vincentsena and S. Spangenberga in changed project of the bridge and the tunnel through Great Belt the accepted levels of the bridge road- and of railway link break simultaneously is set to 0.02 on 100 years, and bridge or railway alternatively as 0.1 per 100 years.
7. According to the report 63 of Construction Industry Research and Information Association the risk of the destruction of the construction can be definite as $P_z = (10^{-4}/n_r)K_s n_d$, where

P_z is a probability of the destruction of the construction due to any reason within a period of its operation n_d, n_r is a number of persons threatened in the accident and K_s is the coefficient dependent of values related with class of the building: places of public meetings, dams—0.005; the household activity, the office, the trade or the industry—0.05; bridges—0.5; towers, masts and sea-constructions—5. This criterion has became put-upon to the designing of the second bridge trough Severn river and brought the acceptability level to value of less than 4,0 10^{-7} per a year.

8. *Nordic Committee for Safety of Structures* gives legitimate values of the probability of the one year's damage as 10^{-3} to 10^{-7} for serious results or very serious.
9. JCSS gives criteria values on level 10^{-3} to 10^{-6} for damages with serious results.
10. AASHTO use the so called return periods. For the erosion the bottom at the pier as result of the flood it apply 100 and 500 years return-period adequately for regular and critical bridges (0,01 and 0.02 in the year), for earthquakes 475- and 2500-the years return-period (0.02 and 0.004) period and for the collision with ships 1000- and 10 000-years (0.001 and 0.0001 per year).

It should be noticed that criteria of the risk acceptance in Europe are created usually for cumulative all possibly events such as: seismic, fires, the bottom erosion at piers and the influence of ice etc. US criteria are built rather for single events. The above-analysis shows that the lack is generally accepted acceptability criteria of the risk. Guidelines have a considerable spread of the criteria values. The probability of the break of the bridge connection varies widely from 10^{-3} to 10^{-6}, can be accepted as the enter average value to further analyses.

The US analysis of ship—bridge collisions [USCG, 2003] reveals that only 2% events ends with events of considerable consequences, which could be the reason of high resistances of bridge supports for collisions and the fact that these studies embraced majority of inland units. AASHTO [1991] proposed method of density function creation of the bridge collapse probability composed of two uniform distributions (Fig. 6):

$$f(P/P_{\max}) = \begin{cases} 0,9 & for\ \ 0 \le P/P_{\max} < 0,1 \\ 0,1 & for\ \ 0,1 \le P/P_{\max} \le 1 \end{cases}$$

where:

P/P_{max}—the relation of the load from the ship collision (P) to the peak load (P_{max}), which can be transferred to the bridge pier.

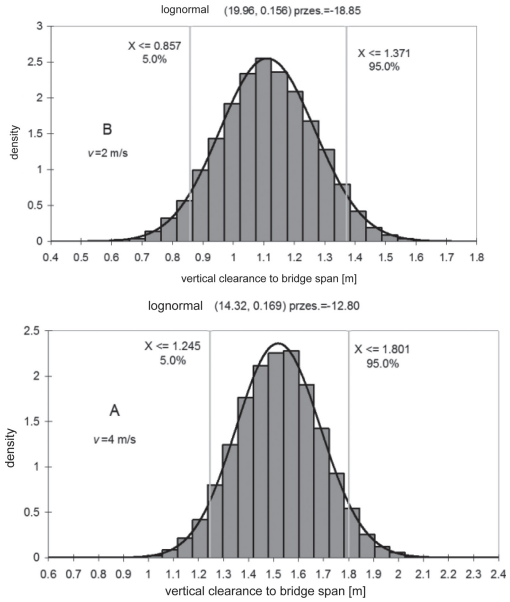


Figure 6. The distribution of the vertical clearance of the height over the ship to the span for two speeds of ships: A—8 kn (abt. 4 m/s) and B—4 kn (abt. 2 m/s).

4 SELECTED CASE STUDIES OF THE SAFETY ANALYSIS WITH ACCIDENT PROBABILITY ESTIMATION OF THE SHIPS PASSAGE UNDER THE BRIDGES

Two example analyses concerning the quantifying of the risk of the ship passages under bridges thet restricts water area both concerning the horizontal and vertical area.

4.1 *The collision with the span: Qualifying of horizontal clearance with the methods of the statistical simulation*

The Monte Carlo based model was built of the clearance between ships and the span. The random variables and their parameters were estimated he the base results obtained in the project: "The creation of the method of dynamic and probabilistic underkeel clearance estimation" [L. Gucma, 2008d]. To build example solution the example bridge on the fairway Szczecin–Świnoujście with the height above water level of H = 36 m have been chosen. The maximum ship, which can enter to Szczecin now is ship with following parameters: L = 160 m, T = 9,15 m, and A = 35 m. The horizontal clearance have been calculated for two ship speeds 8 and 4 kn. Input data to the model one are presented in the Table 1. Monte Carlo simulations

Table 1. The random distributions of variables accepted to the Monte Carlo simulation of horizontal clearance to the bridge and their parameters.

Variable	Symbol	The accepted average value	Distribution of errors	Parameters of given distribution
Bridge height [m]	H	36	Uniform	(0; –0,05)
Draught [m]	T	9, 15	Normal cut	(0; 0,1; 0,2)
Ships air draught [m]	A	35	Based on T	a.a.
Squat [m]	O	4 models	*Bootstrap*	
Water level [m]	p_{wa}	0	Normal cut	(0; 0,1, 0,15)
Breadth [m]	B	35	Uniform	(35; 40)
Speed of the ship [in]	v	8 and 4	Normal	(0, 0,5)

were executed by means of the @Risk software, the number of samples equals 100 000, what gave the suitable statistical convergence of obtained results. The best fit of the clearance of the height to the span of the bridge gives the log-normal distribution with relatively low asymmetry. In further step it is possible to qualify the probability of the collision of the ship into the span of the bridge. From graphs presented in Figure 6 it is apparently visible that 5% ships will keep a smaller than: 1,24 m and 0,86 m for investigated speeds 4 and 2 m/s It was confirmed also the argument about the relationship of the reserve of the height over by ship to the span with her speed, what results from the squat phenomenon.

4.2 *The collision with pier: The bridge Great Belt—the traffic analysis of ships by means of AIS*

The AIS system could be a very useful tool to the traffic analysis of ships and their safeties also in the bridges area. It should be noted that the possibility exists of the GPS satellites signal reception difficulties and consecutive loss of ships position during the passage under bridge due to its shadowing effect. The traffic analyses of ships during the passage under the greatest European bridge Great Belt Western is presented. The traffic under the bridge is two-way. As an input data unprocessed signal from the AIS Baltic countries exchange network (AIS HELCOM) was applied. The number of registered passages was about 6500 ships per year in one direction. Research embraced the year 2011. Registered chosen passages of ships are showed in Figure 7. It is visible that some ships passed vary close to the pier of the bridge.

In the next step the distributions of density probability of the position of registered positions of ships during the passage under the bridge have been analysed. The CDF of ships positions moving north is presented in Figure 8. The logistic

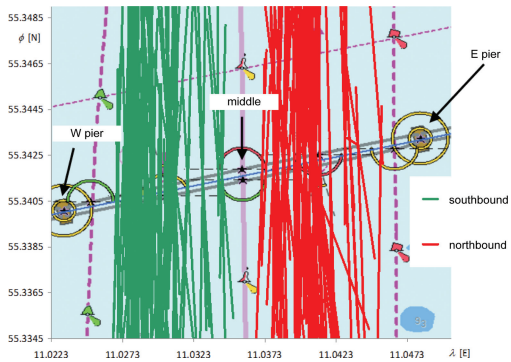


Figure 7. Registered routes of ships in the region of the Bridge Great Belt Eastern.

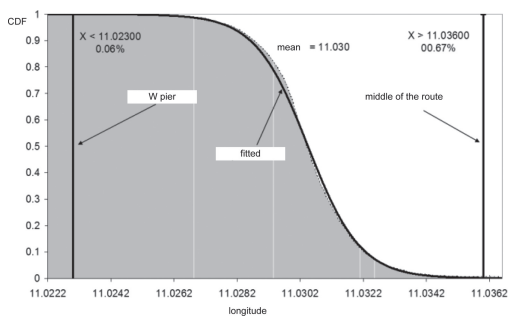


Figure 8. Cumulative distribution function of positions of ships under the bridge (the western route).

distribution with parameters of a = 11,03 and b = 8,32 showed good fit to given empirical (the Kołmogorowv–Smirnow tests was applied). It is visible that the probability of the collision with the western pier of the bridge lead to values of $6 \cdot 10^{-4}$, so shows the large agreement with the values meet in the literature. The probability of the exit outside the given route and intrusion to opposite traffic lane is higher and quails: $6{,}4 \cdot 10^{-3}$.

5 CONCLUSIONS

It was shown that the problem of collisions of ships with bridges in Poland and in around the world is serious, also on inland waterways. Additionally the fact of the considerable degradation of the infrastructure contributes to his deepening. There exists the row of methods of the valuation of the risk from which two were described.

The designing of new locations of bridges should be supported by individual risk analyses, because as it was showed norms and guidelines are sometimes inconsistent and not always assure optimum-foundations to their designing.

It is necessary to carry out of the deeper discussion in the matter of the safety of the location of bridges in the respect of collisions with ships in Poland especially that possible disasters can entail deadly sacrifices.

REFERENCES

AASHTO (1991): Guide specification and commentary for vessel collision design of highway bridges. Volume I: Final report. American Association of State Highway and Transportation Officials (AASHTO). Washington, D.C.

Gucma L. (2009): Wytyczne do zarządzania ryzykiem morskim (in polish: Guidelines for maritime risk assessment). Wydawnictwo Akademii Morskiej w Szczecinie. Szczecin.

Gucma L. (2013): Zarządzanie ryzykiem w rejonie mostów usytuowanych nad drogami wodnymi w aspekcie uderzenia jednostek pływających (in polish: Risk management in the areas of bridges located above waterways in respect to ships collisions). Wydawnictwo Akademii Morskiej w Szczecinie. Szczecin.

Radomski W. (2011): Katastrofy i awarie mostów a rozwój wiedzy budowlanej. (in polish: Bridge catastrophes and accidents in scope of development of construction knowledge) Konferencja Naukowo-Techniczna—Awarie Budowlane. Międzyzdroje.

Scheer J. (2010): Failed Bridges—Case Studies, Causes and Consequences, Ernst&Sohn, 2010.

USCG (2003): Report of U.S. Coast Guard and American Waterways Operators. Bridge Allision Work Group. A Product of the Coast Guard—AWO Safety Partnership May.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A new approach for evaluating the disruption risks of a seaport system

A. John, R. Riahi, D. Paraskevadakis, A. Bury, Z. Yang & J. Wang
Liverpool John Moores University, UK

ABSTRACT: Much of the available data associated with seaport operations is uncertain and ambiguous, requiring an approach capable of handling both quantitative and qualitative information. Conventional risk modelling approaches are considered to be inadequate in many circumstances due to the lack of flexibility and an inappropriate structure for addressing the system's risks. This paper proposes a flexible risk assessment approach to facilitating the treatment of uncertainties in seaport operations in a systematic manner. The methodology consists of a fuzzy analytical hierarchy process, an Evidential Reasoning (ER) approach, and fuzzy set theory. The fuzzy analytical hierarchy process is used to analyse the complex structure of seaport operations and determine the weights of significant risk factors while ER is used to synthesise them. The methodology provides a framework for collaborative modelling of the system and allows for a step by step analysis. It could provide managers and infrastructure analysts with a flexible tool in order to enhance the resilience of the seaport system.

1 INTRODUCTION

Safety Critical Maritime Infrastructure (SCMI) systems, which are defined as ports, waterways, vessels and their intermodal connections, are the foundation of world economic growth. Due to the interaction and interdependence among their components and subcomponents, the systems are vulnerable to various risks in their field of operations.

As a result of multiplicity of stakeholders and the operational complexity in SCMI systems, high levels of operational uncertainty exist in the systems (Mansouri *et al.*, 2010). Given that the world's trade is mainly carried out by sea transportation, the global economy is heavily dependent on the effective operation of these systems, disruptions at any point could potentially result in catastrophic and disastrous consequences.

Building resilience in maritime operations requires creating capabilities and a sustained engagement from the stakeholders involved in these operations. In order to optimise the protective capability of the system, it is essential to constantly revise and update the risks that are associated with the system in such a way that it would recover to a desired level of functionality when facing adverse operational constraints. The complexity of a SCMI system is caused by the integration of technical, organisational, operational and security issues into its routine operations.

Conventional techniques such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode, Effects and Criticality Analysis (FMECA) and Bow-Tie (BT) have been widely used in analysis of critical systems and have contributed greatly to the literature of risk analysis. The aforementioned approaches have some drawbacks which affect their applications. The use of traditional risk assessment approaches to deal with newly arising hazards and threats (e.g. potential terrorist attacks) to maritime infrastructure reveals two major challenges: i) the lack of capability to process diverse data suitable for input into a risk inference mechanism, and ii) the lack of capability to analyse the interactive dependence between risk factors (Yang *et al.*, 2009).

One realistic way to analyse a system with unavailable data is to employ subjective assessment using the combination of fuzzy logic and Evidential Reasoning (ER). Compared to the traditional fuzzy inference mechanism (i.e. max-min fuzzy operations), an ER approach has the advantage of avoiding the loss of useful information in its inference processes; hence, it can be suitable for modelling complex systems.

The insufficiency of quantitative risk assessment in the maritime-related literature together with the vision to establish a secure and resilient SCMI system has resulted in a need for an integrated risk assessment methodology capable of tackling the uncertainties associated with a system's operation (John, 2013).

This paper is organised as follows. Section 2 reviews the existing literature on SCMI systems, and discusses the major risk factors associated with seaport operations. Sections 3 and 4 highlight the decision making techniques that are used for

the analysis. Section 5 presents the methodology of the study. Section 6 provides a numerical example to demonstrate the applicability of the proposed methodology. Section 7 concludes the study.

2 LITERATURE REVIEW

SCMI systems are complex due to the dynamic interactions among their interrelated components. The level of interdependences and complexity of the system's operations can be acknowledged through its description by the US Department of Homeland Security "as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterways, including all maritime related activities, infrastructure, people, cargo, vessels and other conveyances" (Moteff and Parfomak, 2004). Analysing the disruption risks of a CMI system's operation will: i) improve security, ii) increase the resilience of the system, and iii) reduce its susceptibility to hazards.

Modern seaports as an important component of SCMI systems focus their operations on continuous handling of flows and efficient transport. Experience has shown that operation of a seaport has progressed from performing cargo handling, stacking and distribution functions to a complex transportation hub in a logistic chain. Comprehensive analysis of maritime infrastructure revealed that a seaport system is entailed with: i) the infrastructure (i.e. assets that are capable of an intended service delivery, such as access channels, turning basins, quay walls, jetties, navigational aids, breakwaters, pilots, tugs and stacking areas), ii) the superstructure (i.e. logistics, ICT, handling equipment, warehouses, *etc*.), iii) the operating procedures, iv) management practices, v) complex interactions with the society to facilitate trade, and vi) the transfer of goods and services for economic development (Taneja *et al.*, 2010).

The flexibility in the flows of vessels and large amounts of bulk cargoes has created a huge amount of concerns about the integrity of the infrastructure because of the numerous opportunities for them to be tampered with for terrorism-related acts and sabotage. Additionally, their operations can be hampered by several organisational and environmental risks that range from natural to man-made disasters, with disruption likelihood that can potentially result in a large amount of direct and indirect financial losses (Hultin *et al.*, 2004; Nilchiani and Mostashari 2008).

When studying the safety aspects of a seaport system, a logical approach is to break down the system into its functional entities comprising components and subcomponents. Safety modelling of these functional entities can be carried out to fit such a logical structure, then the interrelationships can be examined and a system safety model can be formulated for risk-based decision making in all phases of the system's activity, from its conception and design to its operation, maintenance and decommission.

The risks associated with seaport operations are multifaceted. Risk factors are presented in Table 1 (Nair *et al.*, 2010; Handley-Schachler and Navare, 2010; Moktari *et al.*, 2011; Slatter and Force, 1999).

Each main risk factor, as shown in Table 1, is broken down to its associated root causes. These causes are chosen because they are regarded as the most significant ones associated with major disruption of seaport activities. The selection of such disruption risks and causes is conducted based on extensive discussions with experts and a robust literature review (John, 2013).

2.1 *Operational risk factors*

The evolution of large vessels for maritime transportations has necessitated the need to optimise terminal infrastructures to systematise the management of risk in loading and unloading operations in ports and maximise the possibility of controlling incident/accident cases effectively.

Table 1. Causes of seaport disruption.

Main risk type	Associated cause
Operational risk factors (R1)	Port equipment failures
	Vessel accident/grounding
	Cargo spillage
	Human errors
	Sabotage
Security risk factors (R2)	Terrorism attacks
	Surveillance system failures
	Arson
Technical risk factors (R3)	Lack of equipment maintenance
	Lack of navigational aid maintenance
	Lack of IT system maintenance
	Lack of dredging maintenance
	Labour unrest
	Dispute with regulatory bodies
Organisational risk factors (R4)	Berth congestion
	Gate congestion
	Storage area congestion
Natural risk factors (R5)	Geologic/seismic
	Hydrologic
	Atmospheric

The operational risk factors that cause disruption of maritime activities are due to port equipment failures, vessels accident/grounding, human error and cargo spillage (John, 2013).

2.2 *Security risk factors*

Since the 9/11 attacks, security experts have shown serious concerns over the efficiency and robustness of SCMI systems, with regard to their possible exploitation by terrorists, who could cause a disaster in the system either through the sinking of a large vessel in a port channel or by attacking a port's physical infrastructure facilities (Bichou, 2008 and Fritelli, 2005).

Experience has shown that decision makers have invested significant resources on sophisticated security measures in order to ensure smooth flows of trade. The effective performance of security systems or measures can be built based on a robust modelling of the system (John, 2013).

2.3 *Technical risk factors*

SCMI systems can be categorised as: i) marine constructions, ii) port maintenance, iii) port operations, and iv) logistics. Because ports are open facilities with multiple means of access by both land and sea routes, they involve multiple modes and each is managed by a different entity within the system. For smooth operations of maritime systems, events such as the lack of equipment, navigational aid, IT systems and dredging maintenance are identified as significant issues leading to disruption of the systems with long-term financial consequences (Moktari *et al.*, 2011).

2.4 *Organisational risk factors*

Events such as labour unrest, dispute with regulatory bodies, breakdown in organisational communications leading to berth congestion, incompatible management goals leading to gate congestion, and poor management procedures leading to storage-area congestion are major factors mentioned in the current literature which lead to the disruption of seaport operations (John, 2013; Mansouri *et al.*, 2010). There is a widespread agreement among safety researchers that the key means of tackling the human element contribution to disruptions will be via the incorporation of resilience into the operations of the system (Mostashari *et al.,* 2011).

2.5 *Natural risk factors*

The dynamics of the natural environment affect the entirety of seaports' operations. The most important hazards due to natural factors are hydrological, atmospheric and geological ones (Kroger, 2008). The impacts of these hazards have consistently added more cost to management of seaports in the form of maintenance, reconstruction and preparedness.

Heavy rainfall, flooding and snow are important examples of hydrological hazards; tsunamis and earthquakes are categorised as geological or seismic hazards; hurricanes and cyclones are classed as atmospheric hazards.

3 EVIDENTIAL REASONING ALGORITHM

The theory of evidence was first generated by Dempster (1968) and further developed by Shafer (1976). It is often referred to as the Dempster-Shafer theory of evidence or D-S theory. The D-S theory was originally used for information aggregation in expert systems as an approximate reasoning tool (Mantaras, 1990). Subsequently, it has been used in decision making under uncertainty (Yager, 2004).

Due to the ever-changing environment and the multiple criteria decision-making problems having a degree of uncertainty, the ER algorithm was developed (Yang and Xu, 2002).

The major advantages of ER are listed as follows:

- It is capable of handling incomplete, uncertain and vague as well as complete and precise data.
- It is capable of providing its users with a greater flexibility by allowing them to express their judgements both subjectively and quantitatively.
- It is capable of accommodating or representing the uncertainty and risk that is inherent in decision analysis.
- As a hierarchical evaluation process, it is capable of offering a rational and reproducible methodology to aggregate the data assessed.
- It is capable of obtaining the assessment output using mature computing software, Intelligent Decision System (IDS) (Yang and Xu, 2002).

4 THE EXPECTED UTILITY

The concept of expected utility is utilised to generate numerical values equivalent to the distributed assessment of the top-level criterion or goal of each alternative for ranking in order to obtain the probable risk level of disruption for decision making.

In light of the above, let the utility value of an evaluation grade H_n be denoted as $u(H_n)$ and $u(H_{n+1}) > u(H_n)$ if H_{n+1} is preferred to H_n (Yang, 2001). It is worth mentioning that $u(H_n)$ represents

utility values of each linguistic term and can be determined using the decision makers' preference. If there is no preference information available, it could be presumed that the utilities of the evaluation grades are equidistantly distributed in a normalised utility space. The utilities of evaluation grades that are equidistantly distributed in a normalised utility space are calculated as follows:

$$u(H_n) = \frac{V_n - V_{\min}}{V_{\max} - V_{\min}} \quad (1)$$

V_n stands for the ranking value of the linguistic term that has been considered (H_n), V_{max} is the ranking value of the most preferred linguistic term (H_N), and V_{min} is the ranking value of the least preferred linguistic term (H_1). The utility of the top-level or general criterion $S(E)$ is denoted by $u(S(E))$. If $\beta_H \neq 0$ (i.e. the assessment is incomplete, $\beta_H = 1 - \sum_{n=1}^{N} \beta_n$ where β_n is a belief degree to which $S(E)$ is assessed to H_n) there is a belief interval $[\beta_n, (\beta_n + \beta_H)]$, which provides the likelihood that $S(E)$ is assessed to H_n.

Without loss of generality, suppose the least preferred linguistic term having the lowest utility is denoted by $\mu(H_1)$ and the most preferred linguistic term having the highest utility is denoted by $\mu(H_N)$. Then the minimum, maximum and average utilities of $S(E)$ are defined as follows (Yang, 2001):

$$u_{\min}(S(E)) = \sum_{n=2}^{N} \beta_n u(H_n) + (\beta_1 + \beta_H) u(H_1)$$
$$u_{\max}(S(E)) = \sum_{n=1}^{N-1} \beta_n u(H_n) + (\beta_N + \beta_H) u(H_N) \quad (2)$$
$$u_{average}(S(E)) = \frac{u_{\min}(S(E)) + u_{\max}(S(E))}{2}$$

Obviously, if all the assessments are complete, then $\beta_H = 0$ and the maximum, minimum and average utilities of $S(E)$ will be the same. Therefore, $u(S(E))$ can be calculated as follows:

$$u(S(E)) = \sum_{n=1}^{N} \beta_n u(H_n) \quad (3)$$

5 METHODOLOGY

The aim of this paper is to develop a decision-making model for evaluating the diverse risks of a seaport system in a systematic manner. The methodology in a stepwise order is explained as follows:

1. Identifying the risk factors associated with seaport operations.
2. Developing a model with a hierarchical structure for evaluating the risk of disruption to seaport operations.
3. Assigning a weight to each different criterion by using Fuzzy Analytical Hierarchy Process (FAHP).
4. Assessing the risk level of a hazardous event using triangular fuzzy numbers.
5. Aggregating the input data using an evidential reasoning algorithm.
6. Determining a crisp value for a risk level in terms of expected utilities.

6 A NUMERICAL EXAMPLE

A numerical example is used in this section to show how the proposed approach can be implemented for the assessment of the various risk factors and their impact on the smooth operations of a seaport.

6.1 *Identification of risk factors associated with disruption of a seaport operation* (*step 1*)

Based on the literature review, risk factors associated with disruption of a seaport's activities are identified and presented in Table 1. Each risk factor is investigated based on its associated causes. These causes are chosen because they are regarded as the most significant factors associated with major disruption of a seaport activity.

6.2 *Development of a model for evaluating the risk of disruption to seaport operations* (*step 2*)

Based on the risk factors identified in Section 2, as shown in Figure 1, a model with hierarchical structure is developed. Following a review of Wang *et al*. (1995) for effective information processing of a safety expression, linguistic terms need to be in the range of four to seven. As a result, within this paper five linguistic terms are defined to evaluate the likelihood and consequence of each identified risk factor, as shown in Table 2.

6.3 *Assigning a weight to each different criterion by using FAHP (step 3)*

Questionnaires were designed and possible values were assigned through meetings with experts. Weights were assigned to all criteria by using FAHP (An *et al*., 2007). These weights are presented in Table 3.

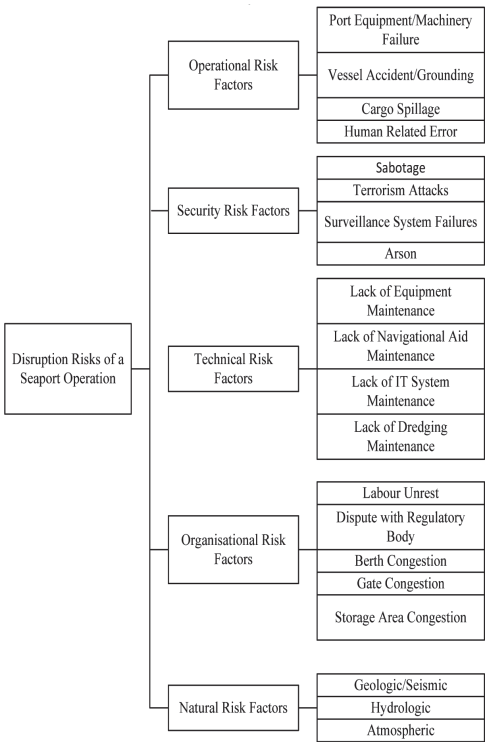


Figure 1. Model for disruption of a seaport system.

Table 2. Triangular fuzzy numbers for likelihood and severity.

Grade	Occurrence likelihood (L)	Consequence severity (S)	Triangular fuzzy numbers
1	Very low	Negligible	(0, 0, 0.25)
2	Low	Moderate	(0, 0.25, 0.5)
3	Medium	Serious	(0.25, 0.5, 0.75)
4	High	Very serious	(0.5, 0.75, 1.0)
5	Very high	Disastrous	(0.75, 1.0, 1.0)

6.4 *Assessing the risk level of a hazardous event using triangular fuzzy number (step 4)*

When the occurrence Likelihood (L) of a hazard and its consequence Severity (S) are assumed to be mutually independent, their combination is equal to the product of the two. Hence, under the same assumption, the product of the two triangular fuzzy numbers denoted by $TFN_L = (a_L, b_L, c_L)$ and $TFN_s = (a_s, b_s, c_s)$ as presented in Equation 4 is equal to the risk level of a hazardous event under investigation.

$$TFN_{LS} = TFN_L \otimes TFN_S = (a_L \otimes a_S, b_L \otimes b_S, c_L \otimes c_S) \quad (4)$$

Table 3. Weights of risk parameters.

Risk parameters	Abbreviation	Weights
Port equipment failures	R11	0.510
Vessels collision/grounding	R12	0.083
Cargoes spillage	R13	0.258
Human related error	R14	0.149
Sabotage	R21	0.481
Terrorism attacks	R22	0.306
Surveillance system failure	R23	0.124
Arson	R24	0.089
Lack of equipment maintenance	R31	0.490
Lack of navigational maintenance	R32	0.076
Lack of IT system maintenance	R33	0.283
Lack of dredging maintenance	R34	0.150
Labour unrest	R41	0.475
Dispute with regulatory bodies	R42	0.054
Berth congestion	R43	0.081
Gate congestion	R44	0.114
Storage area congestion	R45	0.275
Geologic	R51	0.35
Hydrologic	R52	0.325
Atmospheric	R53	0.325
Operational risk factors	R1	0.246
Security risk factors	R2	0.291
Technical risk factors	R3	0.188
Organisational risk factors	R4	0.153
Natural risk factors	R5	0.122

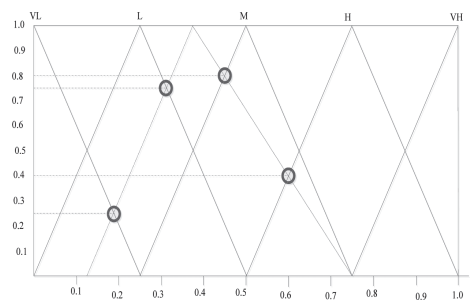


Figure 2. Converting a triangular fuzzy number to a set with five linguistic grades.

TFN_L stands for the triangular fuzzy number for likelihood and TFN_S stands for the triangular fuzzy number for severity and TFN_{LS} stands for the triangular fuzzy number for the risk level of a hazardous event under investigation.

As an example and based on Table 3, if a risk has an occurrence Likelihood (L) of Medium (0.25, 0.5, 0.75) and consequence Severity (S) of Very Serious

(0.5, 0.75, 1), based on the Equation 4, the corresponding triangular fuzzy number for the risk level of a hazardous event under investigation (i.e. TFN_{LS}) is evaluated as (0.125, 0.375, 0.75). To obtain a risk set with five linguistic terms, as shown in Figure 2, TFN_{LS} is mapped over the membership functions of a risk with five uniformly distributed grades (Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH)) (Moktari *et al.*, 2011).

As shown in Figure 2, a point where the TFN_{LS} intersects a linguistic term is circled and the corresponding degree of membership (i.e. Z_P) is presented in Table 4. As illustrated in Table 4, Z_P is normalised to obtain Z (i.e. linguistic variables; linguistic terms with their membership degrees).

Based on Equation 4, the risk level of a hazardous event can be evaluated as follows:

$$\begin{aligned} TFN_{LS(VeryLow)} &= TFN_{L(VeryLow)} \otimes TFN_{S(Negligible)} \\ TFN_{LS(Low)} &= TFN_{L(Low)} \otimes TFN_{S(Moderate)} \\ TFN_{LS(Medium)} &= TFN_{L(Medium)} \otimes TFN_{S(Serious)} \\ TFN_{LS(High)} &= TFN_{L(High)} \otimes TFN_{S(VerySerious)} \\ TFN_{LS(VeryHigh)} &= TFN_{L(VeryHigh)} \otimes TFN_{S(Disastrous)} \end{aligned} \quad (5)$$

Table 5 presents the triangular fuzzy numbers for the risk levels based on Equation 5. K is the risk level value used for the grouping of a triangular number (a_1, a_2 and a_3) and is obtained as follows:

$$K = \frac{1}{2(a_1 + a_2 + a_3)} \quad (6)$$

Table 4. Example of mapping FTN_{LS} into five grades.

FTN_{LS}	0.125, 0.375, 0.75
Grade	VL L M H VH
Z_P	0.25, 0.75, 0.80, 0.40 0
Z	0.10, 0.34, 0.36, 0.20 0

6.5 *Aggregation of input data using evidential reasoning algorithm (step 5)*

Based on the demonstrated techniques in Section 6.4 the linguistic variables (Z) for all risk factors, as shown in Table 6, are evaluated. By using the evidential reasoning algorithm the risk factors are aggregated and the linguistic variables for main criteria, as shown in Table 7, are assessed.

By using the ER algorithm the linguistic variables for main criteria are aggregated and the linguistic variables for disruption risks of a seaport operation (DR) are assessed (Table 7).

6.6 *Evaluation of a crisp value for a risk level using the expected utility approach (step 6)*

Quantitative assessment based on a single value is much easier and is a more realistic tool for a decision maker to rank the risk factors. In view of the fact that the linguistic variables for the disruption risks of a seaport operation (DR) was characterised by five linguistic terms, the highest preference is given to the "Very High" linguistic term and the lowest preference is given to the "Very Low" linguistic term.

By using Equations 1–3, the DR value was evaluated as: = (0.2349 × 0) + (0.461 × 0.25) + (0.2348 × 0.5) + (0.0693 × 0.75) + (0 × 1) = 0.285 or 25.8%. This value represents the disruption risks of a seaport operation under investigation.

Based on Table 5, it is close to the class of significant risk category. This value means that the risk must be reduced if practicable. It can be used to benchmark the safety performance among different ports or in the same port at different periods of time.

Such a result can be used to help port safety analysts to carry out formal safety assessment of a port, and to initiate safety audit and review of key performance indicators of various port departments for enhanced operation. The result of the analysis could also help analysts to propose various

Table 5. Definition of linguistic variables used for risk evaluation and risk levels based on TFNs.

Risk level	Description of risk evaluation variables	Triangular fuzzy numbers	Centroid values (Risk levels) K
Very low: Risk is acceptable	If likelihood is very low and severity is negligible	(0, 0, 0.0625)	0.020
Low: Risk is tolerable but should be reduced if it is cost effective	If likelihood is low and severity is moderate	(0, 0.0625, 0.25)	0.104
Medium or significant: Risk must be reduced if it is practicable	If likelihood is medium and severity is serious	(0.0625, 0.25, 0.5625)	0.292
High: Risk must be reduced	If likelihood is high and severity is very serious	(0.25, 0.5625, 1.0)	0.604
Very High: Risk must be reduced and controlled	If likelihood is very high and severity is disastrous	(0.5625, 1.0, 1.0)	0.854

Table 6. Linguistic terms with their membership degrees (Z) for risk factors.

Risks factors	Z				
	VL	L	M	H	VH
R11	0.29	0.47	0.24	0	0
R12	0.40	0.45	0.15	0	0
R13	0.40	0.45	0.15	0	0
R14	0.15	0.35	0.34	0.16	0
R21	0.10	0.48	0.42	0	0
R22	0	0.17	0.46	0.37	0
R23	0.15	0.35	0.34	0.16	0
R24	0.23	0.46	0.26	0.05	0
R31	0.40	0.45	0.15	0	0
R32	0.15	0.35	0.34	0.16	0
R33	0.29	0.47	0.24	0	0
R34	0.23	0.46	0.26	0.05	0
R41	0.58	0.42	0	0	0
R42	0.40	0.45	0.15	0	0
R43	0.40	0.45	0.15	0	0
R44	0.40	0.45	0.15	0	0
R45	0.40	0.45	0.15	0	0
R51	0.26	0.48	0.26	0	0
R53	0.26	0.48	0.26	0	0
R53	0.40	0.45	0.15	0	0

Table 7. Aggregation of main criteria.

Main criteria	Very low	Low	Medium	High	Very high
R1	0.3074	0.4566	0.2223	0.0137	0.0000
R2	0.0754	0.3884	0.4195	0.1167	0.0000
R3	0.3310	0.4652	0.1866	0.0172	0.0000
R4	0.5210	0.4253	0.0537	0.0000	0.0000
R5	0.2561	0.5164	0.2275	0.0000	0.0000
DR	0.2349	0.4610	0.2348	0.0693	0.0000

layers of protection or measures to optimise the robustness of the system. This approach may provide a viable approach where there is a lack of objective or statistical data in such an assessment for the port under investigation.

7 CONCLUSION

This paper proposes a methodology for evaluating the risk of disruption to seaport operations, in order to optimize the operational efficiency of the system.

In the risk-based modelling approach presented in this paper, input data are expressed by linguistic terms with their membership degrees. This approach presents a flexible framework for use when precise data is not available. The approach has the following advantages:

- It provides managerial insights to analysts in a rational, reliable and transparent manner for collaborative modelling of complex systems with a group of experts under situations of high uncertainties in data.
- It provides researchers with an effective tool to make full use of the information generated at the lowest level in design to evaluate the safety of the whole system for resilience improvement of its operations.
- It has been shown to be flexible in application, and can be useful in safety analysis and synthesis in many industrial environments.

It is envisaged that the proposed approach could provide risk managers and infrastructure analysts with a flexible tool for use in understanding the importance of developing organisational strategy in order to increase the resilience of the system to unforeseen operational uncertainties in a transparent manner.

ACKNOWLEDGEMENTS

This research was supported by the EU-funded project WEASTFLOWS (2011–2015).

REFERENCES

An, M., Huang, S. and Baker, C. (2007). Railway risk assessment-the fuzzy reasoning approach and fuzzy analytic hierarchy process approaches: A case study of shunting at Waterloo depot. In: Proceedings of the Institution of Mechanical Engineers, Part F: *Journal of Rail and Rapid Transit*, 221(3), pp. 365–383.

Bichou, K. (2008). Security and risk-based models in shipping and ports: review and critical analysis. OECD/ITF Joint Transport Research Centre Discussion Paper.

Dempster, A.P. (1968). A generalization of Bayesian inference. *Journal of the Royal Statistical Society.* Series B (Methodological), pp. 205–247.

Fritelli, J. (2005). Port and maritime security: background issues for congress. CRS report for congress. Congressional Research Service, Order code RL31733.

Handley-Schachler, M. and Navare, J. (2010). Port risk management and public private partnerships: factors relating to risk allocation and risk sustainability. *World Review of Intermodal Transportation Research*, 3(1), pp. 150–166.

Hultin, J.M., Pennotti, M., Ullman, H. and Stevens L.A (2004). Securing the port of New York and New Jersey: network-centric operations applied to the campaign against terrorism, *Transportation Research Board*, Access Number: 00980435.

John, A. (2013). Proactive risk management of maritime infrastructure systems: resilience engineering perspectives, PhD Thesis, Liverpool John Moores University, UK.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, 93(12), pp. 1781–1787.

Mantaras, R.L.D. (1990). Approximate reasoning models: Prentice Hall PTR, USA.

Mansouri, M., Nilchiani, R. and Mostashari, A. (2010). A policy making framework for resilient port infrastructure systems. *Marine Policy*, 34(6), pp. 1125–1134.

Miri Lavasani, S.M., Yang, Z., Finlay, J. and Wang, J. (2011). Fuzzy risk assessment of oil and gas wells. *Process Safety and Environmental Protection,* 89, pp. 277–294.

Moteff, J. and Parfomak, P. (2004). Critical infrastructure and key assets: definition and identification. CRS Report for Congress, Order Code RL32631.

Mokhtari, K., Ren, J., Roberts, C. and Wang J (2011). Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. *Journal of Hazardous Materials*, 192(2), pp. 465–475.

Mostashari A., Nilchiani, R., Omer, M., Andalibi, N. and Heydari, B. (2011). A cognitive process architecture framework for secure and resilient seaport operations. *Marine Technology Society Journal,* 45, 120–127.

Nair, R., Avetisyan, H. and Miller-Hooks, E. (2010). Resilience framework for ports and other intermodal components. *Journal of the Transportation Research Board.* 2166(1), pp. 54–65.

Ngai, E.W.T. and Wat, F.K.T. (2005). Fuzzy decision support system for risk analysis in e-commerce development, *Journal of Decision Support Systems*, Vol. 40, pp. 235–255.

Nilchiani, R. and Mostashari, A. (2008). An introduction to resilience in port infrastructure systems. White Paper Series, Hoboken: Stevens Institute of Technology.

Shafer, G. (1976). A mathematical theory of evidence. Vol. 1: New Jersey, Princeton University Press.

Slater, R. and Force, M.T. (1999). An assessment of the US marine transportation system: a report to congress. US Department of Transportation, Washington DC.

Taneja, P., Ligteringen, H. and Van Schuylenburg, M. (2010). Dealing with uncertainty in design of port infrastructure systems, *Journal of Design Research*, 8(2), pp. 101–118.

Wang, J. Yang, J. and Sen, P. (1995). Safety analysis and synthesis using fuzzy sets and evidential reasoning. *Reliability Engineering & System Safety.* 47(2):103–118.

Yang, J.B. (2001). Rule and utility based evidential reasoning approach for multi attribute decision analysis under uncertainties. *European Journal of Operational Research*, 131(1), pp. 31–61.

Yang, J.B. and Xu, D.L. (2002). On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty. Systems, Man and Cybernetics, Part A: Systems and Humans, *IEEE Transactions,* 32(3), pp. 289–304.

Yang, Z., Wang, J., Bonsall, S. and Fang, Q. (2009). Use of fuzzy evidential reasoning in maritime security assessment. *Risk Analysis,* 29, 95–120.

Yager, R.R. (2004). On the determination of strength of belief for decision support under uncertainty Part II: fusing strengths of belief, *Fuzzy Sets and Systems,* 142(1), pp. 129–142.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Methodology for evaluation of barriers for rig move operations

E. Okstad, S. Hauge & B.A. Mostue
SINTEF Technology and Society, Safety Research, Trondheim, Norway

H. Skår
Statoil ASA, Bergen, Norway

ABSTRACT: This paper presents a methodology for evaluation of safety barriers against major accidents in rig-move operations. A stepwise approach is suggested, which was identified and adopted in cooperation with marine experts from Statoil with partners. Barriers were identified on basis of a documentation review followed by workshops. The strength and shortages of technical, operational and organizational barriers have been focused. The novelty of the suggested approach lies in the way barrier information in rig-move operations are collected and assessed, and secondly, the way stakeholders and system experts are involved in the evaluation of the critical safety barriers. Of the most important learnings were the effective identification of measures for strengthening the existing barriers, and the process of identifying supplementary barriers.

1 INTRODUCTION

1.1 *Background*

Failures or weakening of barriers are frequent causes of undesirable incidents in the petroleum sector. The Petroleum Safety Authority in Norway therefore states in the Management Regulations that the relationship between risk assessments and barrier management must be clarified by the industry (PSA, 2010). This relationship is essential for the successful risk management of operations.

Marine operations and rig-move operations in particular, are lacking risk models that cover, or describe in an appropriate way, important barrier functions and systems. Therefore, Statoil suggested an evaluation of important barriers to be carried out according to the following three steps:

- Identify hazards and situations that may result in undesirable events
- Identify technical, operational and organizational barriers that exist, or are missing in order to prevent major accidents and serious incidents
- Assess the quality of technical, operational and organizational barriers as basis for suggesting safety improvements.

The current paper presents generic results from the above barrier evaluation and is based on project collaboration between SINTEF/MARINTEK and Statoil.

1.2 *Objectives*

The main objective of the paper is to present the methodical approach applied for evaluation of safety barriers in rig move operations. The methodology should focus on work laid down by oil companies in preventing major accidents and serious incidents associated with rig move operations. Hence, the approach should support work processes aimed at identifying and strengthening the most important safety barriers in this area of marine operations. The important questions are:

- What are the main barriers against incidents and major accidents in rig move operations?
- In what way can these safety barriers be identified and further strengthened?

2 RIG-MOVE OPERATIONS

2.1 *System descriptions*

The suggested methodology considers normal work processes in rig-move operations and the measures that are implemented to prevent associated accidents. Included are activities from the

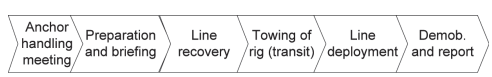


Figure 1. Phases of a rig move project.

early anchor handling meeting, through the operational phases until demobilisation, debriefing, and reporting.

2.2 *Requirements*

Different sources of information were applied to obtain an overview of the requirements related to rig-move operations. General information regarding work processes, activities and roles and responsibilities in rig move operations have been taken from the NWEA—Guidelines (NWEA, 2012). The guideline incorporate best practice and procedures from North Sea operating companies, logistics companies, ship owners, shippers and lessons from the appropriate national safety forums. The guideline does not supersede flag- and other legal requirements.

Internal procedures of the operating company might also describe the main structure of tasks, roles and responsibilities for a given assessment case. Finally, the operational requirements, limitations and constraints for a specific rig move operation are utilised as described in the respective Scope-of-Work document (SoW). The main reason is that much of the SoW descriptions typically are considered as formal requirements to each specific rig move operation.

2.3 *Interpreting the barrier concept*

As mentioned in the background section, barrier management has been highly focused in the Norwegian petroleum industry lately. Safety barriers are implemented to avoid hazards or accidents. When several barriers are in place to prevent an undesirable event or accident, this is often referred to as "defence in depth". The principles apply to safety in rig move operations as well. Several barriers must fail simultaneously in order for an accident to occur. This is often illustrated by the "Swiss cheese model" (Reason, 1997). The following barrier definitions are based on the memo "Principles for barrier management in the petroleum industry" (PSA, 2013):

2.3.1 *Barrier*

Barriers are technical, operational and organisational elements which are intended individually or collectively to reduce possibility for a specific error, hazard or accident to occur, or which limit its harm/disadvantages.

2.3.2 *Barrier Function (BF)*

A barrier function describes the task or role of the barrier. Examples include preventing leaks or ignition, reducing fire loads, ensuring acceptable evacuation and preventing hearing damage.

2.3.3 *Barrier Element (BE)*

Barrier elements are technical, operational or organisational measures or solutions which play a part in realising a barrier function.

2.3.4 *Performance Influencing Factor (PIF)*

Performance influencing factors are significant conditions for the ability of barrier functions and elements to perform as intended.

The following interpretation to rig move operations has been applied as to what could be identified as a barrier or a barrier element:

> *Barriers are measures that are implemented to oppose an undesirable chain of events occurring.*

In planning of risky operations or activities, it is often argued that the risk analysis in itself should be defined as a safety barrier. This implies that a Safe Job Analysis (SJA) before a specific anchor handling operation could be defined as a barrier. Our interpretation of the barrier concept does not open for this definition. Risk analysis including SJA is considered as a performance influencing factor in the way that it affects the quality (with respect to safety) of a work process, or planned operational activities. This is also in line with the PSA's interpretation of the barrier definition (PSA, 2013).

3 BARRIER EVALUATION APPROACH

3.1 *The six-step methodology*

A six-step methodology is suggested for the barrier evaluation. It describes the process for collection, systemization, visualization and evaluation of safety information related to rig move operations. The main activities were the document reviews and meetings with operational personnel of the company under study. Clarification of the system limits and a correct interpretation of rig move operations were important initial activities to ensure an appropriate basis for the barrier evaluation. Main input to the evaluation was requirements, procedures and reports covering relevant incidents and accidents as well as the operational knowledge of the involved experts.

3.1.1 *Step-1 Review of accidental events*

The rig-move study for Statoil was based on a total of 151 reports of experienced incidents. It spans from simple Synergi reports of minor incidents and near misses, to investigated in-depth studies of more serious events. Near-miss incidents (approximately 30 reports) were excluded from the review, mainly due to the minor risk potential (personnel injuries), but also project resource limitations.

Through the initial mapping, it was early identified that the main part of incidents with a major accident potential could be grouped into:

– Positioning failure incidents, and
– Anchor handling incidents.

By positioning failures we include incidents that relate to wrong navigation in rig move operations, either caused by missing navigation resources, technical failures on navigation equipment, or wrong configuration of such.

Anchor handling incidents include collisions with vessels involved in rig move operations and the anchor handling on deck. The main part of collision incidents are minor impacts occurring during operations at the field. Historically, the anchor handling incidents on deck were the most serious ones with respect to personnel injuries and harm to operating personnel.

Most of the events reported in Synergi are incidents more than accidents. For incidents, the Synergi database utilizes the following categorization:

– *Near misses*—Incidents that nearly have caused a more serious accident
– *Discrepancies*—The work as done deviates from written procedures or requirements
– *Conditions (technical or not)*—Vital characteristics or condition of important equipment or work practice is outside accepted limits

The above categorization is important in order to learn from reported incidents and understand the underlying causes.

Table 1 gives an overview of the received reports indicating the type of activity, type of documentation and category, year of occurrence, and number of events within each event category.

Of the positioning records there are four near misses, eight discrepancies and two conditions. The most frequent cause is wrong info in maps and positioning failures (six) and errors related to navigation equipment (four).

Of the anchor handling incidents, eight were investigated in-depth. Four of these caused personnel injuries, and three incidents had potential for such consequences. Concerning the other 99 anchor handling incidents, personnel injury was registered as a consequence in 15 of them. For the rest, damage to equipment and material was the typical result. Three of these incidents also resulted in delay in work progress and one resulted in spill to the environment.

Table 1. Number of reported incidents and events.

Activity	Category	Year	Number
Positioning (incidents)	Near misses	2004–2012	4
	Discrepancies	2005–2009	8
	Conditions	2008	2
Anchor handling	Investigated in-depth study	2008–2011	8
	Incidents	2011	50
		2012	43
		2013	6
	Near miss	2011	17
		2012	12
		2013	1
		SUM	151

3.1.2 *Step-2 Mapping of events*

The STEP-diagram method (Passmore, 1988) was used to map the work processes involved in the experienced incidents/events. Figure 2 illustrates an extract of such a mapping for the "Line recovery" phase at the field. Activities in the main work process are linked with solid lines in Figure 2, whereas actors indirectly involved are linked with dashed vertical lines to the core activities. The actors involved in rig move operations are specified to the left in the STEP diagram.

The following six different phases of a rig move project were covered in order to identify the most safety-relevant activities:

– Anchor handling meeting
– Preparation and briefing
– Line recovery at current location
– Towing of rig (or transportation) from the current location to new location
– Line deployment at new location
– Demobilisation and report

The experienced incidents and accidents were linked to the typical project phases and activities. Historical incidents being mapped are shown in

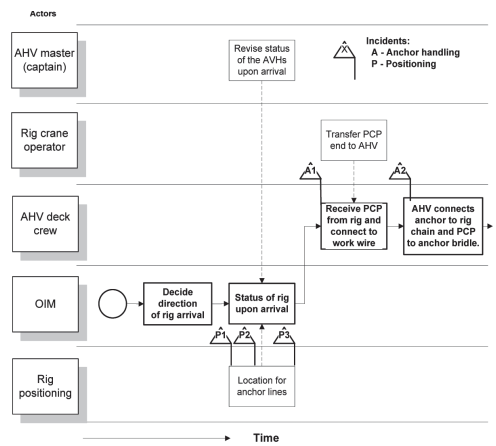


Figure 2. Extract of a STEP diagram: Line recovery.

"A" and "P" triangles for the anchor handling and positioning failures, respectively.

As indicated in Figure 2, clusters of reported incidents could be related to specific activity sequences in operation.

3.1.3 *Step-3 Scenario identification*

To facilitate the barrier analysis from an accident sequence perspective, the Bow-tie method (CGE, 2014) was used prior to and during a workshop (WS) with marine experts. The bow-tie diagram is a particularly suitable tool for visualizing barriers in safety critical operations, and is readily understood by non-specialists. Figure 3 shows an extract of a bow-tie diagram with some of the relevant barriers. The TOP event, representing loss of control, is indicated in the middle. To the left is what could cause the TOP event to occur, i.e. the initiating events or threats, and their associated preventing barriers. To the right are potential consequences and the mitigating barriers.

As background information for the scenario identification, PSA's RNNP project was used (PSA, 2012). Table 2 outlines the set of hazard and accident situations (Norwegian DFUs) that could lead to severe damage and loss of life in petroleum production.

Identification of possible accident scenarios and TOP events was based on the above DFU list. Events No. 5–9 were considered most relevant for rig move operations.

A list of six generic scenarios was defined and is shown below with the relevant DFU attached in brackets:

A. Collision between the anchor handling vessel and rig when the vessel arrives at the location from where the rig will be moved (DFU 5).
B. The tow line breaks during towing of rig from the current position to the new position when it passes close to another installation (DFU 6).

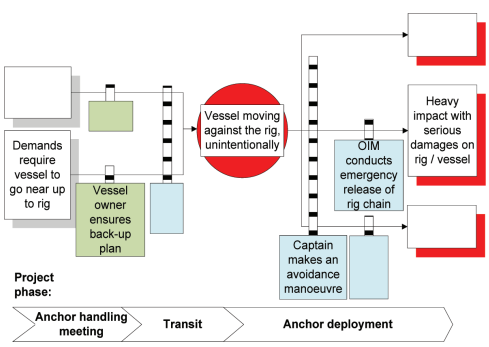


Figure 3. Extract of a Bow-tie diagram: Close to rig operation.

Table 2. DFUs according to RNNP (PSA, 2012).

No.	DFU
1.	Non-ignited hydrocarbon leaks
2.	Ignited hydrocarbon (HC) leakages
3.	Well incidents/loss of well control (well control events)
4.	Fire or explosion in other areas, not HC
5.	Ship on collision course (against the facility)
6.	Drifting object (against the facility)
7.	Collision with field-related vessel/installation/ shuttle tanker
8.	Damage to the device structure/stability/ anchoring/positioning errors
9.	Leakage from underwater production installation, pipeline/risers, buoy, and discharge hoses, etc.
10.	Damage to subsea production equipment/pipeline systems/diving equipment caused by fishing
11.	Evacuation (precautionary/emergency evacuation)
12.	Helicopter incident

C. An anchor handling vessel moves unintentionally against the rig in connection with the anchor handling operation for that rig (DFU 7).
D. Positioning errors with serious consequences resulting from errors in maps or lack of navigational equipment or resources, and the errors might not be detected during late planning and execution of the operation (DFU 8).
E. Severe loss of stability during execution of an anchor recovery operation (DFU 8).
F. The anchor is landed at wrong position because it did not engage correctly at the intended position and was dragged over existing production facilities/pipelines nearby (DFU 9).

The adapted scenario descriptions were made on basis of documented events and incidents, in addition to general experience/knowledge within the project group. Scenario A and C were again combined into a single collision scenario making the barrier analysis more effective. In addition, scenario D was selected to cover the positioning failures. As mentioned, the basis for selecting these scenarios was the mapping of incidents and events in the STEP diagram. The major-accident potential from the different types of events was also considered. According to the above grouping, the following three accident scenarios were chosen for further analysis:

– Scenario 1: Positioning failure prior to "grappling" (to retrieve anchor at current location)
– Scenario 2: Collision during close to rig operation
– Scenario 3: Collision due to operational/technical failure

The three scenarios above were visualized in preliminary bow-tie diagrams as preparation for further analysis. The respective TOP events were then:

– Grappling at wrong position (Scenario 1)
– Anchor handling vessel moving against the rig unintentionally (Scenario 2 and 3)

3.1.4 *Step-4 Identification of barriers*

Barrier identification and analyses were conducted in a Workshop (WS) with marine experts from Statoil and partners. Results from the WS were documented in the prepared STEP diagrams, preliminary Bow-tie diagrams and work sheets for further analysis. Only scenarios with end consequences implying a major accident potential were focused.

The WS was carried out in three steps:

1. Identification of possible initiating events and causes given the TOP event
2. Identification of accidental scenarios and possible consequences of the TOP event
3. Identification of frequency reducing barriers that may prevent the TOP event from occurring, and consequence reducing barriers that may prevent the TOP event from developing/escalating into a major accident

In the subsequent analysis the most important barriers were identified in revised bow-tie diagrams for the respective positioning failure- and collision scenarios. Color codes were applied to better differentiate between onshore and offshore barriers (activities) in the Bow-tie figures.

Each barrier function with the related barrier elements were discussed in assessment tables based on the revised bow-ties. Separate tables were made for the Initiating Events (IE) and End Consequences (EC), respectively. Table 3 and Table 4 below illustrate two extracts of such with a few examples of barrier functions and barrier elements. The single initiating event and end consequence been used are:

– IE1: Operational demands require vessel to go near up to the rig

Table 3. BF: Avoid a too short distance to rig.

No.	Barrier elements	PIF (examples)	Comments/ quality
IE1	Vessel owner who ensures back-up plan	SJA Team work MoC	A specific SJA is required
	QC marine operation who intervenes	Communication Competence Culture	–

Table 4. BF: Avoid serious damages from an impact.

No.	Barrier elements	PIF (examples)	Comments/ quality
EC1	Captain who makes an avoidance maneuver	Attention Competence HMI	The rig may cut mooring lines and drive off
	OIM who conducts emergency release of rig chain	Emergency response Design	–

– EC1: Heavy impact with serious structural damages on rig/vessel

Similarly Table 4 shows two barrier elements for the end consequence EC1.

Factors that could effect on the quality and effectiveness of barriers were identified thereafter. The notation Performance Influencing Factors (PIF) was applied to these factors. PIFs were identified for the barrier elements based on judgments in the WS, and further supplied by the project group afterwards. In the same process, comments to quality of the respective barrier elements were stated.

3.1.5 *Step-5 Evaluation of barriers*

Following the barrier assessments, the qualities of existing barriers are evaluated as basis for recommendations. Improvement measures for the existing barrier elements, or supplementary barrier elements were suggested. Barrier elements subject for recommendations were marked in the assessment tables. Measures could be related to the whole barrier function, or to single barrier elements only. The following three criteria were used to assess the quality of the barriers:

1. *Quality:* The extent to which the barrier functions as intended, e.g. contributes in preventing collisions?
2. *Actual use:* To what extent the barrier is actually in use to prevent, e.g. collisions?
3. *Vulnerability/resilience:* To what extent is the barrier function vulnerable to the influence of surroundings? If so, what are possibly the most important factors that influence the barrier function?

The above evaluation criteria are based on previous research (Hollnagel, 2008, Sklet, 2006). The same criteria were used in another relevant study on barriers against ship collisions (Kongsvik et al., 2012). Here the focus was also on barriers against collisions between vessels and offshore installations.

However, the criteria were adapted and simplified to fit offshore service vessels and related barriers against ship collisions.

3.1.6 *Step-6 Reporting and dissemination of results*

The study results were documented in a (restricted) technical report summarizing the most important barriers with recommendations for Statoil. One important result from the study was that of a total of 40 barrier elements that were identified, only five were technical barriers and the rest operational/organizational barriers. This seems to be typical for this kind of marine operations. Thus, when presenting the improvement measures we distinguished between the recommendations given to the technical and the operational/organizational barrier elements.

Following the report, a presentation of main results was prepared for internal dissemination in the company. Following the summary report, main results were presented in a HSE seminar held by Statoil, where leaders from the contracted ship owners participated. Finally, the study results with recommendations were discussed in a dissemination workshop with personnel from Statoil's rig move department.

3.2 *Evaluation of the approach*

The suggested approach involved relevant personnel from the company with its partners through participation in meetings and the WS. SINTEF/MARINTEK facilitated the WS with an interdisciplinary team of researchers. In addition to facilitating the WS, SINTEF/MARINTEK also contributed with knowledge within barrier management and marine systems.

The analysis of historical events and the preparation of STEP diagrams, bow-ties and work sheets were done in forehand. Although the approach as a whole has not been applied earlier, well defined methods were combined to form the whole methodology both during the preparation phase and accomplishment of the WS. A natural part of the process was thus to adjust the approach continuously based on findings and experiences, as well as feedback from the customer throughout the process.

The following describes some of the pros and cons with the applied approach, mostly seen from the facilitator's point of view. This may be a basis for improvements for similar projects in the future.

3.2.1 *Information*

The collected information prior to the barrier evaluation mainly included data documenting accidents and incidents related to rig move operations. An advantage is that most of the incidents in marine operations are reported in Synergi. However, when comparing the two mentioned groups of events (positioning and anchor handling failures), only the anchor handling incidents are typically investigated in depth. This could be due to the more extensive exposure of personnel on deck during anchor handling operations. Still, both categories appear to have major accident potential. Anyway, the different focus might lead to a distorted view of the risk. More information is typically found in investigation reports compared to "simple" Synergi reports. However, the discussions with the operating company and the WS are perceived to compensate for possible distortions and direct focus on the real safety issues.

3.2.2 *Study limitations/definition*

For the current case the definition of actual work processes and activities to cover was rather clear. Reference was made to process diagrams found in governing documents of the operating company. By using this in addition to scope of work descriptions for specific operations, a good overview was obtained. The conditions for defining an appropriate study basis were thus present.

3.2.3 *Methods applied*

As mentioned, bow-tie diagrams were used in the WS to visualize potential accident scenarios in order to identify the safety barriers. A challenge is that the bow-tie method does not visualise the actual sequences of potential accidental events. The existence of accidental sequences, their realism and knowledge to such must therefore to some degree be handled outside the bow-ties. Also the bow-tie approach does not illustrate the importance of the barriers, in terms of whether the barrier is sufficient to stop a developing event or must function together with other barriers. In that respect, the mapping of incidents and events in STEP diagrams was one of the tools for identifying scenarios. Through the STEP visualization, relevant project phases and activities could be viewed against the incidents. Then, it was easier to relate historical data of incidents to possible deficiencies or failure causes of "rig move operations" itself, and thereof, identification of scenarios.

The *top event*, interpreted as "loss of control" lead to the identification of *initial events* and possible *end consequences.* From this stage the bow-tie models functioned more as a tool for identifying failure causes and thus, the barrier elements against accidental sequences. Both preventive and mitigating barriers were highlighted.

Another constrain is that the bow-tie models may grow too large and become disordered. One

reason for this being that the bow-tie methodology in itself seems to lack a clear and consistent definition and limitation of what is a barrier. Therefore, one must constantly focus on what are barriers and what are performance influencing factors. For this purpose clear definitions must be available, and the group discussions need to be somewhat controlled. This is important simply to avoid ending up with "everything" being identified as barriers and a false impression of an extensive defense-in-depth system that is not real.

3.2.4 *Suggested measures—follow-up*

The recommendations resulting from the evaluation will obviously depend on company specific conditions and priorities. Several of the suggested measures are of operational and organisational character. The prevailing situation with significant turnover of experienced staff both within the rig fleet and ship owners *can* lead to lack of knowledge and experience. In particular this may result in inadequate knowledge concerning local conditions and systems at the offshore fields. It is therefore recommended to examine potential effects of such on the risk related to rig move operations (risk handling).

One of the recommended measures for improved safety in rig move operations is to implement greater degree of joint training of the crews on rigs and vessels. This kind of training might be one step to remedy the above mentioned trend.

4 DISCUSSION

4.1 *Implications of results*

The suggested approach encourages involvement from relevant stakeholders in a way that hopefully ensures participation and ownership to the results and recommendations. The quality of safety barriers for each of the scenarios and suggestions for improvements are discussed in relation to the most relevant project phases and activities. Comprehensive descriptions of barriers and their quality will be obtained. Secondly, by following the six-step methodology, a clarification of ownership and knowledge to the existing safety barriers are achieved, both within the oil company and its partners.

4.2 *Further research*

Since there are generally no physical obstacles to prevent a collision between a vessel and a rig, safety during rig move operations relies heavily upon operational and organizational measures. This implies that competence, motivation and training of the personnel involved become paramount. As part of the barrier management, PSA Norway states that performance requirements shall be developed also for operational and organizational barrier elements (PSA, 2013). Further work to increase safety in rig move operations should therefore include development of specific and verifiable competence, training and certification requirements to key personnel involved in the operations.

Joint training of crews on rigs and vessels was pointed out as an improvement measure. Research on state-of-the art within training and how to prepare for more joint training of the crews are therefore highly relevant. Important success criteria for such should be identified in near collaboration with the industry.

Another topic is whether to apply more safety-performance methods during the WS and discussions with the operating company, as supplement to the data-based scenario identification. As commented in the evaluation, the historical data of incidents and events may not reflect the whole risk picture. Positioning failures are less investigated even though they represent major accident potential. Risk based approaches (Øien, 2001) and safety performance based approaches (HSE, 2006, Sklet et al., 2010) could here be a supplement to the barrier and indicator identification.

5 CONCLUSION

A methodology for evaluation of safety barriers against major accidents in rig-move operations has been presented. Important input to the evaluation was requirements, procedures and reports covering relevant incidents and accidents as well as the operational knowledge of the experts involved in workshop discussions.

Clarification of system limits and interpretation of requirements to rig move operations also provided input for identifying and evaluating the barriers present during rig-move operations.

The review of historical incidents and events, along with mapping in STEP diagrams gave a good basis for the scenario identification. However, other approaches may also apply to this step as discussed in the previous section. Additionally, the bow-tie method for scenario analysis was valuable in sense of providing fruitful WS discussions. It also provided a good platform for the barrier evaluations and visualization of the main results.

The work is based on close cooperation between researchers and marine experts from the companies involved in rig-move operations. The work done and the suggested approach are contributions to the continuous work of limiting risk and reducing accidents during these operations. In this respect the suggested approach was a contribution

to their improvement processes. It is the authors believe that the generic approach could be useful for similar projects, or further research.

ACKNOWLEDGEMENTS

The authors also like to acknowledge the support from Statoil marine operations both in terms of contributions in writing the present paper, for the project collaboration, and for providing documentation and facilitating the necessary meetings and workshops.

REFERENCES

CGE. 2014. *The Bow-tie XP method, www.cgerisk.com* [Online]. CGE Risk Management Solutions. [Accessed].

Hollnagel, E. 2008. Risk plus barriers = safety? *Safety Science,* 46, 221–229.

HSE 2006. Developing process safety indicators. A step-by-step guide for chemical and major hazard industries. UK Health and Safety Executive.

Kongsvik, T., Bye, R., Fenstad, J., Gjosund, G., Haavik, T., Olsen, M.S. & Størkersen, K.V. 2012. Barrierer mot kollisjoner mellom fartøy og innretninger. Identifisering, vurderinger og mulige forbedringstiltak. (Unauthorised translation: Barriers against collisions between vessels and offshore facilities. Identification, assessment and possible improvement measures). Trondheim: NTNU Samfunnsforskning AS, Studio Apertura.

NWEA 2012. Guidelines for the Safe Management of Offshore Supply and Rig Move Operations. North West European Area.

Passmore, D.L. 1988. Investigating Accidents with Step—Hendrick, K, Benner, L. *Accident Analysis and Prevention,* 20, 153–154.

PSA 2010. Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (the Management Regulations). The Petroleum Safety Authority, Norway.

PSA 2012. Trends in risk level in the petroleum activity—Summary report 2012. The Petroleum Safety Authority, Norway.

PSA 2013. Principles for barrier management in the petroleum industry. The Petroleum Safety Authority, Norway.

Reason, J. 1997. *Managing the Risk of Organizational Accidents*, Aldershot: Ashgate.

Sklet, S. 2006. Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries,* 19, 494–506.

Sklet, S., Ringstad, A.J., Steen, S.A., Tronstad, L., Haugen, S. & Seljelid, J., et al. 2010. Monitoring of human and organizational factors influencing risk of major accidents. *SPE International conference on health, safety and environment in oil and gas exploration and production.* Rio de Janeiro, Brazil.

Øien, K. 2001. Risk indicators as a tool for risk control. *Reliability Engineering & System Safety,* 74, 129–145.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Performance of skimmers in the Arctic offshore oil spills

M. Naseri & J. Barabady
Department of Engineering and Safety, UiT The Arctic University of Norway, Tromsø, Norway

ABSTRACT: Oil spill removal techniques have been developed as passive barriers to reduce the severity of adverse impacts of oil spills on the environment. Among different oil spill removal methods, combination of skimmers and booms are more preferable environmentally, as they can recover the spilt oil from sea permanently. However, a number of factors such as harsh Arctic climatic conditions, presence of sea ice, remote distances, poor visibility, and less developed infrastructure threaten the overall performance of skimmers. Therefore, identifying such influencing parameters and evaluating their impacts on the overall performance of skimmers is of the utmost importance. In this study, the overall performance of skimmers in the Arctic offshore is discussed from the viewpoints of effectiveness and availability performance. Several operational conditions and their impacts on the availability performance of skimmers and their effectiveness in the Arctic offshore are further reviewed and discussed. Changes in physical and chemical properties of spilt oil and their contribution to the window-of-opportunity for a successful skimming operation are described, taking into account the severe Arctic climatic conditions.

1 INTRODUCTION

The increasing trend of oil and gas activities in the Arctic offshore has raised major concerns about oil spills and their impacts on the Arctic's ecologically sensitive environment. To decrease the severity of such impacts, oil spill clean-up technologies are developed as passive barriers to oil spills. Various techniques are available for removal of offshore oil spills, such as in-situ burning, use of dispersants, and mechanical methods. Oil skimmers are one of the essential categories of mechanical recovery methods that generally are used in combination with containment booms (Fingas 2011, Potter et al. 2012).

There are different types of skimmers that vary in different aspects such as size, working principle, and performance criteria. To plan an oil spill removal operation using mechanical methods, it is essential to estimate the amount of oil that can be recovered by a specific type of skimmer during a given period of time. To determine if a specific skimmer performs as per design, its effectiveness can be evaluated based on three measures stated by the manufacturer (Jensen & Mullin 2003, Schulze 1998):

- *Recovery Efficiency:* the ratio of oil to the recovered mixture, expressed as a per cent;
- *Throughput Efficiency:* the ratio of oil recovered to the encountered oil, expressed as a per cent;
- *Oil Recovery Rate:* the rate at which pure oil is being recovered in barrels per hour (or in cubic meters per hour).

These measures vary based on the type of skimmer type, its characteristics, and are defined for a known range of operational conditions. However, in practice, a skimmer may not recover oil as it is stated by the manufacturer. In other words, the amount of oil that a skimmer can recover with a given period of time depends not only on its working principle, type, size, and performance criteria, but also on a number of operational conditions such as physical and chemical properties of spilt oil, weather conditions, personnel skill, and sea state (Broje & Keller 2006, Broje & Keller 2007, Fingas 2011, Jensen & Mullin 2003, Nordvik 1995). Concept of system effectiveness then may be utilized to evaluate the extent, to which a system meets the planned objectives or the objectives stated by the by the manufacturers (ISO 2005). In this regard, the operational conditions and their impacts on the throughput efficiency, recovery efficiency and oil recovery rate of skimmers are discussed in the context of the *effectiveness of skimmers*.

Availability performance of skimmers is another factor that must be assessed carefully in order to plan the type and the number of required skimmers for a specific oil spill removal operation. Availability can be simply defined as "the item's capability of being used over a period of time" (Stapelberg 2009). In other words, one needs to ensure that skimmers are able to fulfil their function (i.e. skimming of oil from water surface) within a given period of time, and if they fail, they can be restored to their functioning state within a minimum time interval. Moreover, to have a sustain-

able skimming operation, performance of pumps, connections, separation facilities, and storage and transportation systems must be also evaluated and improved accordingly. However, the focus of this study is mainly on the skimmers' performance.

Considering the operational conditions in the Arctic offshore, there are various parameters, which may give rise to the probability of failure of different systems utilized. For example, low Arctic temperatures may increase the failure rate of the systems due to their adverse effects on the material properties such as metals and plastics (Singh 2013). Therefore understanding the key operational conditions and their effects on the various aspects of the performance of skimmers play crucial roles in every skimming operation.

The aim of this paper is to review and discuss the various aspects of the performance of skimmers in the Arctic offshore. The key operational conditions and their effects on the performance of oil skimmers are also reviewed and discussed.

Section 2 describes the main types of skimmers and their working principles. Section 3 is devoted to a general discussion on the skimming operations in the Arctic offshore. Sections 4 and 5, discuss various key operational conditions that can affect the availability performance of skimmers and their effectiveness, respectively. In section 6, the effect of the weathering processes on the skimming operations are discussed from the viewpoint of window-of-opportunity. Conclusions are given in section 7.

2 SKIMMERS

Skimmers are mechanical devices designed to skim the spilt oil from water surface. There are various types of skimmers categories based on different parameters, such as size, working principle, recovery efficiency, oil viscosity range, oil recovery rate, throughput efficiency. Skimmers can operate in either a stationary or a mobile (advancing) mode. Some of them are equipped with storage tanks and water/oil separation facilities, while some other types pump the recovered mixture into external storage and separation facilities (Broje & Keller 2006, Fingas 2011, ITOPF 2012, Jensen & Mullin 2003, NOAA 2010). One of the most efficient ways of using skimmers in open waters is to combine them with containment booms. Booms can contain the oil and increase the thickness of oil slick, so that and the skimmer can skim the oil with a higher recovery rate. A typical configuration of a skimmer combined with containment booms is depicted in Figure 1.

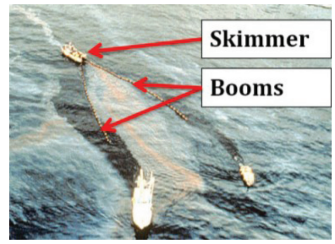


Figure 1. V-configuration of booms combined with a skimmer that is located at the apex of the two booms (Fingas 2011).

Based on their working principles, skimmers can be classified into two main categories: *oleophilic or sorbent surface and non-oleophilic surface skimmers*.

Oleophilic surface skimmers use a surface, to which oil can adhere, and thus be removed from water surface. A wiper blade or a pressure roller then removes the oil from skimmer surface and deposits it into an onboard container. The output mixture of the skimmer may also be directly pumped into storage and separation facilities on a barge. Various types of oleophilic surface skimmers are available based on the process of oil adsorption, including: disk; drum; brush; belt; and rope skimmers.

Non-oleophilic surface skimmers mainly include weir, suction and elevating skimmers. *Weir skimmers* are submerged holding tanks, equipped with a suction pump, recovering oil from water surface based on the gravity difference of oil and water. *Suction or vacuum skimmers* use a vacuum or slight differential pressure to skim the oil from the water surface. In *elevating skimmers*, a paddle belt, wheel or a conveyor belt with ridges is adjusted to the top of the water layer. Oil is then moved up the recovery device into the storage tank (Fingas 2011, Potter et al. 2012, Schulze 1998, Ventikos et al. 2004).

Various skimmers have different performance criteria. Accordingly, selection of the appropriate type of skimmer needs an adequate evaluation of several parameters, such as operational conditions (i.e. wave height, wind and current speed, properties of spilt oil, etc.); effect of such conditions on the effectiveness of skimmers; availability performance of the skimmers under severe climatic conditions; regulations; and requirements defined by the stakeholders.

3 SKIMMING OPERATION IN THE ARCTIC OFFSHORE

To evaluate the overall performance of a skimming operation in the Arctic offshore, at first one must determine how much oil is available to be

skimmed by the skimmer (i.e. oil encounter rate). Spill rate, the degree that oil has spread, containment efficiency of booms, the sweeping area of the skimmer, winds, and characteristics of waves and currents are the main parameters that determine the oil encounter rate (Fingas 2011, ITOPF 2012, Jensen & Mullin 2003). The use of booms improves the oil encounter rate by containing the spilt oil and increasing the thickness of oil slick. Boom efficiency itself is a function of spill rate, weather conditions, currents and waves characteristics (Fingas 2011, Jensen & Mullin 2003, Lee & Kang 1997, Nordvik 1995).

Especially in open waters, due to the fluctuations in the water/oil interface and the working principle of the skimmer itself, some water will be always skimmed together with oil. Accordingly, the output of skimmer will be a mixture of oil/water that must be later separated. Such mixture is then pumped into storage tanks and separation facilities. Separation and storage generally takes place on the barge, especially in the offshore oil spill removal operations. In some cases, the recovered mixture is transported off-site for further separation. Recovered oil and produced wastes are then transported for final disposal, recycle or reuse (Fingas 2011, ITOPF 2012, Jensen & Mullin 2003, Nordvik et al. 1996). These steps are illustrated in Figure 2.

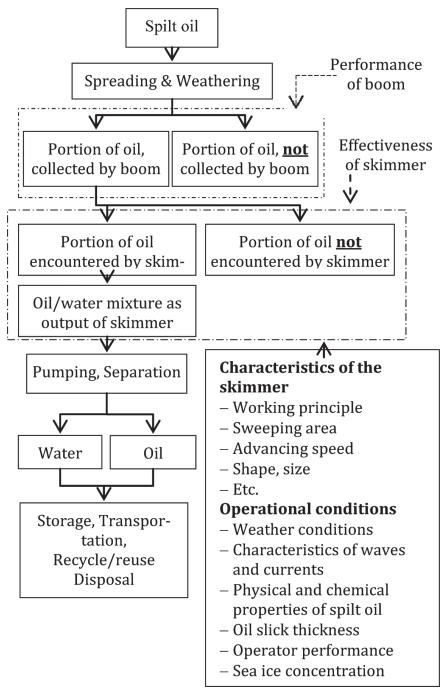


Figure 2. Illustration of offshore oil spill removal process using skimmers combined with booms.

Therefore, to have a sustainable skimming operation, in addition to the performance of skimmers, the overall performance of all the processes of containment by booms, storage, separation, and transportation, must be assessed, as well. The overall performance of the systems can be discussed from two prospective as in the following:

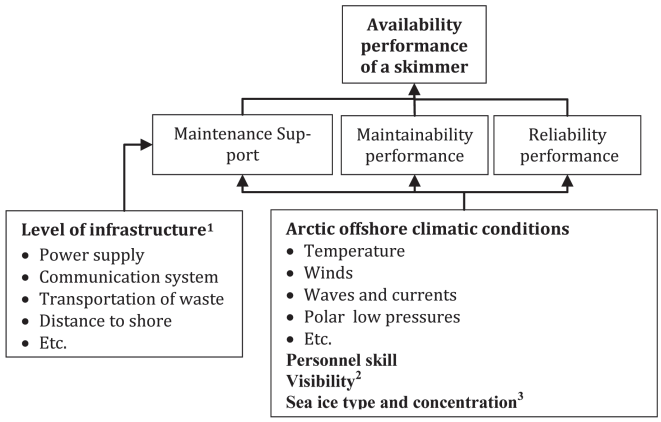
First, the system must be in working state. In other words, it must be able to function as per designed, and if it fails one must ensure that the system can be resorted to the working state within a minimum period of time. These concepts are discussed in the context of availability performance (Barabady et al. 2010, Stapelberg 2009).

Second, while the system is in working state, it must be able to deliver, produce, or recover as per design. For instance, pumps must have the ability to pump the recovered mixture into the separation facilities with a rate determined by the manufacturer. As another example, skimmers must be able to skim the oil from water surface as per designed rate. These concepts are discussed from the viewpoint of system effectiveness.

Although there are a large number of different systems being used in every skimming operation, this study mainly discusses the overall performance of skimmers. Both availability performance of skimmers and their effectiveness are affected by a series of operational conditions such as severe climatic conditions of the Arctic offshore, waves, currents, etc. These sets of conditions must be identified and their effects on the overall performance of skimmers must be assessed accordingly.

4 PARAMETERS THAT AFFECT THE AVAILABILITY PERFORMANCE OF SKIMMERS

To evaluate the availability performance of a skimmer, at first one needs to focus on its elements: *reliability performance, maintainability performance, and maintenance support performance* (Barabady et al. 2010). Reliability of a system is defined as "the probability that a system will perform a specified function within prescribed limits, under given environmental conditions, for a specified time" (Stapelberg 2009). In other words, the failure rate of a skimmer depends on a number of parameters including environmental (operational) conditions. Low ambient temperature, wave height, current speed, sea ice concentration, and wind speed are some examples of operational conditions in the Arctic offshore. Figure 3 depicts some of the operational conditions that may affect the availability performance of the skimmers intended to be used in the Arctic offshore.



Comments: 1- Available waste disposal/recycle/reuse options plays a crucial role in the whole oil spill removal operations
2- Visibility may be limited because of fog, snow storm, rain, and seasonal darkness
3- Sea ice type and concentration may affect the maintenance support performance

Figure 3. Key operational conditions that influence the availability performance of a skimmer in the Arctic offshore.

For instance, plastics and metals develop brittleness and lose their flexibility at low Arctic temperatures (Dutta 1988, Singh 2013). As another example, low Arctic temperature together with waves, currents, and winds increase the viscosity of crude oils drastically through some weathering processes such as emulsification and evaporation (Brandvik & Faksness 2009, Fingas 2011, Fitt-Rasmussen et al. 2012, Nordvik 1995). Pumping of highly viscous oils may lead to mechanical failures in pumps and connections (Fig. 4) (NOAA 2010).

Clogging of skimmers with some pieces of sea ice is another example, which can result in a failure in a skimmer being operated in the Arctic offshore (Schulze 1998, Shum & Borst 1985). Moreover, in low Arctic temperatures, splash of water on skimmers and connections can cause spray icing. The skimmed water may also freeze inside the hoses, connections, separation and storage facilities (Potter et al. 2012).

Maintainability performance is another element of availability performance of a system. When a skimmer fails, the crew must be able to repair the failed component or to provide a new one. The required time to bring the failed component/system back to the operating state is known as *repair time* and is a measure of system maintainability; the lower the repair time, the higher the maintainability performance (Stapelberg 2009). Weather conditions, such as rain, snow, storms, low ambient temperature, etc. are important factors that may increase the repair time and consequently the operation downtime. Performance of the maintenance crew is also a crucial parameter that may affect the repair time and thus maintainability and availability of the skimmer.



Figure 4. Burst hose as a result of excessive pressure from pumping highly viscous oil (NOAA 2010).

To avoid excess downtime, it must be ensured that required resources such as maintenance crew and required spare parts and tools must be available upon request under given conditions and a maintenance policy (Barabady et al. 2010). This is known as maintenance support performance, which is the third element of the availability performance of a system. Harsh climatic conditions of the Arctic offshore, less developed infrastructure in the Arctic regions, and remoteness may cause unpredicted delays in the provision of spare parts, which consequently results in an additional increase in operation downtimes.

Therefore, it is of the utmost importance to determine the conditions under which a skimmer is intended to be used. The effects of such conditions

on various elements of the availability performance of the skimmers must also be evaluated accordingly. Various failure modes of skimmers in severe climatic conditions of the Arctic offshore must be identified and evaluated accordingly. Accordingly, some modifications to the skimmers may need to be done in the design phase. For instance, selection of appropriate materials that are tolerable for extremely low temperatures can significantly increase the reliability performance of the skimmers. In the planning phase, one also needs to evaluate the compatibility of the skimmer with sea ice type and concentration. Adequate heating systems must be implemented to avoid spray ice on the facilities and also to prevent the skimmed water from freezing inside skimmers, pumps, or other facilities utilized in skimming operation.

Required spare parts, tools, and skilled maintenance crew must be available upon request. Maintenance support must be planned taking into account the uncertainties in the prediction of severe weather conditions. Adequate working conditions must be provided for the operators and maintenance crew. For example, they must be equipped with appropriate clothing to withstand the low Arctic temperatures and be able to perform their job.

5 PARAMETERS THAT AFFECT THE EFFECTIVENESS OF SKIMMERS

To evaluate the effectiveness of skimmers, at the first step, one must identify the rate at which oil becomes available to the skimmers (also known as oil encounter rate) (ITOPF 2012). Further, it is crucial to identify how much water will be skimmed together with oil. This determines the basis for further separation, storage, and transportation of the recovered mixture. There are various factors that may affect the oil encounter rate, including: characteristics of waves and currents; sea ice type and concentration, performance of containment booms; characteristics of skimmers (i.e. shape, size, tow speed, operation mode, sweeping area, etc.) (Fig. 2) (Fingas 2011, ITOPF 2012, Schulze 1998).

Some of these parameters make it difficult to achieve the designed efficiency and oil and recovery rate of skimmers in real oil spills (Schulze 1998). For instance, it is quite challenging to simulate the exact characteristics of open-water waves, currents, and winds in tank tests where performance of skimmers is tested by manufacturers. Therefore, it is of the utmost importance to identify the operational conditions, and assess their impacts on the effectiveness of skimmers. This provides a basis to estimate the number and type of required skimmers, booms, and the time that the additional skimmers need to be available on-site. In the following, the key parameters that influence the effectiveness of skimmers are described in more details.

5.1 *Oil slick thickness*

Slick thickness is the most important factor to determine the effectiveness of the skimming operations; the thinner the oil slick, the lower the oil encounter rate (Schulze 1998). The degree that oil spreads on the water surface is highly influenced by winds, waves, and currents. Additionally, oil slick thickness may vary with physical and chemical properties of spilt oil, such as viscosity, density and interfacial tension (Castro et al. 2010, NOAA 2010). Such properties change over time due to the effects of the weathering processes (Fingas 2011, Fritt-Rasmussen et al. 2012, NOAA 2010, Payne & McNabb 1991). Use of containment booms can prevent further spreading of the spilt oil and thus significantly increase its thickness.

5.2 *Oil viscosity*

Various types of hydrocarbon oils have different viscosities. Other factors such as weathering processes can contribute to the changes in viscosity of oil. For instance, viscosity of spilt oil can rise from a few centipoise to more than 160,000 centipoise (cP) due to the effects of weathering processes (Andrade et al. 2013). Based on the various factors such as working principle of skimmers, their size, and shape, an increase in oil viscosity may either increase or decrease the final oil recovery rate (Broje & Keller 2006, Broje & Keller 2007, Fingas 2011, ITOPF 2012). Figure 5 shows oil recovery rate of smooth and grooved drum skimmers with respect to the viscosity of oil. As shown in this figure, different types of smooth and grooved disk skimmers have various trends of oil recovery rate with an increase in oil viscosity.

5.3 *Operator performance*

Human error is an inevitable part of any operation. The influence of human performance becomes crucial in cases where operators directly guide the skimmers through the oil slick. Human performance itself is adversely affected by the severe climatic conditions in the Arctic region. Low ambient temperature, combined with winds can decrease the felt temperature by operators (i.e. wind chill effect) (Bluestein & Quayle 2003, Osczevski & Bluestein 2005). Extremely cold weather may cause some health issues for the operators and thus deteriorate their performance.

Poor visibility due to foggy weather, and seasonal darkness periods in the Arctic offshore are

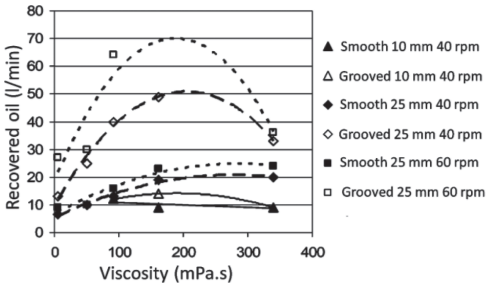


Figure 5. Effect of oil viscosity on the net recovery efficiency of smooth and grooved drum skimmer with different geometrical properties (1 mPa·s = 1 cP) (the viscosities given here, are just some examples to show the various trends of oil recovery rate versus viscosity; the viscosity of weathered oils may be quite larger than these values) (Broje & Keller 2006).

other factors that may reduce the efficiency of human performance. This consequently reduces the efficiency of the skimming operation, as operators need to monitor the spilt oil layer and its probable loss from booms and skimmers.

Therefore, to improve the human performance in skimming operations, adequate clothing is required to provide better working conditions for the operators. Especial cameras and artificial lighting are also required to help the operators to distinguish the spilt oil.

5.4 *Climatic conditions*

Weather conditions may influence the effectiveness of skimmers in various ways. They may alter physical properties of spilt oil through weathering processes. The degree at which the oil spreads on water surface is also a function of climatic conditions, and characteristics of waves and currents.

Winds and waves, in general decrease the effectiveness of skimmers (Fingas 2011, Schulze 1998, Ventikos et al. 2004). This is mainly due to the splash of oil over skimmers, and also because rough waters move the skimmer collection mechanism away from the oil layer on the water surface. However, there are some types of skimmer, such as rope skimmers, whose performance is less affected by waves (Fingas 2011, ITOPF 2012, Potter et al. 2012, Schulze 1998).

Currents also contribute to the effectiveness of skimmers by reducing the oil encounter rate. Fast currents can cause the oil to escape under the collection booms (Al-Majed et al. 2012, Castro et al. 2010, Schulze 1998). Currents may also swamp intakes or cause surface oil to move across the collection element so fast that it cannot be effectively recovered. To have a more efficient skimmer in fast currents, skimmers must be equipped with a collection element, which is able to move with a zero relative velocity to the currents (Schulze 1998).

5.5 *Sea ice concentration*

Performance of skimmers in ice-infested waters depends not only on the weather conditions, waves and currents, but also on the sea ice type and concentration. Sea ice can affect the effectiveness of skimmer in different ways. Ice pieces can clog skimmers their hoses, storage tanks and pumps, especially if there are considerable amount of brush ice (Broje & Keller 2006, Schulze 1998, Shum & Borst 1985).

High concentration of sea ice, on the other hand, may benefit the overall skimming operations by reducing the spreading of spilt oil (Brandvik & Faksness 2009, NOAA 2010, Potter et al. 2012) as spilt oil can be entrapped in pools surrounded by ice. Moreover, presence of ice floes can damp the wave energy and thus benefit the skimmer performance by providing calm water situations (Fritt-Rasmussen et al. 2012, NOAA 2010).

Sea ice also affects both the rate and extent of the changes in the physical and chemical properties of the spilt oil through its effects on the weathering processes (Brandvik & Faksness 2009, Fritt-Rasmussen et al. 2012, Ornitz & Champ 2002). Weathering processes have different rates and extents, depending on sea ice concentration. Among different weathering processes, water uptake by spilt oil (i.e. emulsification) and oil evaporation are the most important ones (Díez et al. 2007). The rate of these processes decreases at high concentrations of sea ice (e.g. 70–90% ice concentration) because oil film is thicker and has a smaller surface area (Brandvik & Faksness 2009, Fritt-Rasmussen et al. 2012, Potter et al. 2012). Both the rate and extent of weathering processes affect the viscosity of spilt oil and thus the response efficiency of the skimmers. Table 1 presents the oil water content of a specific crude oil after 2.5 days in different sea ice conditions. The original crude oil viscosity at 13 °C was about 7 cP. As stated in this table, sea ice only affects the oil water content and viscosity of weathered oil when its concentration is high.

Table 1. Effect of sea ice concentration on the viscosity of a specific crude oil and its water uptake (Brandvik & Faksness 2009).

Sea ice coverage	Oil water content	Dynamic viscosity, cP
Open water	38–41%	4000
30%	38–41%	3500
90%	20%	1500

Therefore, to select skimmers, pumps, connections, etc., one must consider mixed effects of sea ice concentrations and weathering processes on the viscosity of spilt oil, as efficiencies and performance of skimmers and pumps vary based on oil viscosity.

6 WEATHERING PROCESSES AND WINDOW-OF-OPPORTUNITY

Immediately after that an oil spill occurs, a series of transformation processes take place, whereby the physical and chemical properties of spilt oil change. Such processes are known as weathering processes that include for instance evaporation and emulsification. Both the rate and extent of weathering processes mainly depend on the weather conditions, time, and the chemical composition of the spilt oil (Boehm et al. 2008, Díez et al. 2007, Fingas 2011, Nordvik 1995).

Evaporation of lighter components of the spilt oil causes the remaining oil to have a significantly higher viscosity compared to the original spilt oil (Al-Majed et al. 2012, NOAA 2010, Prince et al. 2002). For instance, the results of a field study showed that the viscosity of a 3-day weathered oil increased from 22 cP at 5 °C to about 2000 cP for a light crude oil from the Barents Sea (Fritt-Rasmussen et al. 2012). Additionally, evaporation of the lighter components increases wax content as well as the portion of heavier molecules in the residual oil, resulting in a huge increase in oil pour point (i.e. the temperature where the oil does not flow freely anymore) (Brandvik & Faksness 2009, Potter et al. 2012). An increase in oil pour point may adversely affect the whole skimming operation by reducing the pumping efficiency.

Emulsification (i.e. dispersion of one liquid into another one in the form of small droplets) (Fingas 2011, Nordvik 1995) may occur due to the mixing effect of waves and currents. Viscosity of an emulsified oil increases due to the presence of water droplets in the continuous oil phase (Brandvik & Faksness 2009, Fingas 2011, Ornitz & Champ 2002). Increased oil viscosity due to emulsification can be as high as 500 to 800 times than the original oil (Fingas 2011).

Therefore, considering the spreading of oil and the changes in its physical and chemical properties, one should define a time-frame during which a specific response action (e.g. skimming operation) is viable. Such time-frame is known as window-of-opportunity (Nordvik 1999, Ornitz & Champ 2002). Establishing the appropriate window-of-opportunity depends on the working principles of skimmers and probable changes in the properties of the spilt oil. This should take into account the effect of climatic conditions, waves, currents, etc. on the weathering processes and spreading of oil. Spill rate and duration is another parameter that affects the number of skimmers, booms separation and storage facilities, etc. (Nordvik 1995, Nordvik 1999, Ornitz & Champ 2002, Potter et al. 2012).

One also needs to consider the uncertainties in prediction the climatic conditions in the Arctic offshore. Unpredicted downtimes contribute to extensive changes in the properties of spilt oil through weathering processes. Improving availability performance of skimmers, pumps, connections, and other required facilities greatly reduces the operational downtimes. Additionally, it must be noted that the operational conditions in the Arctic offshore are far different from those in test tanks. Various types of sea ice, storms, high waves, strong currents, snow, rain, etc. are common parameters in open waters while they may not be considered in test tanks. This increases the level of uncertainties in planning the skimming operations.

7 CONCLUSION

To increase the efficiency of an oil spill removal operation, one needs to improve the performance of oil skimmers by ensuring that they are in working state upon request. Furthermore, to increase the clean-up rate, skimmers must have high efficiency and recovery rate. In other words, both the rate and portion of the recovered oil in the oil/water mixture must be as high as practically possible.

High levels of recovery rate and efficiency cannot be achieved without accounting for the effects of operational conditions on both of the availability performance of the skimmers and their effectiveness.

The key operational conditions in the Arctic offshore include severe climatic conditions; seasonal darkness; poor visibility; remoteness; lack of well-developed infrastructure; sea ice; etc.

On the other hand, with regards to the changes in physical and chemical properties of spilt oil over time, the skimming operation must be done within an appropriate time-frame, known as window-of-opportunity. In this regard, failures of the skimmers and other machinery, as well as the uncertainties in the prediction of weather condition must be taken into account accordingly.

To have a sustainable skimming operation, it is vital to assess the performance of all the involved systems and facilities such as pumps, connections, hoses, separation facilities, and storage and transportation systems. Such assessments must be performed taking into account the impacts of operational conditions in the Arctic offshore.

REFERENCES

Al-Majed, A.A. Adebayo, A.R. & Hossain, M.E. 2012. A sustainable approach to controlling oil spills. *Journal of Environmental Management* 113(0): 213–227.

Andrade, F. Lutz, G. Lyra, A.P. Ranieri, A. & Lemos, B. 2013. Oil Spill Response Equipment and Techniques for Waxy Oils in Brazil, *SPE Latin-American and Caribbean Heath, Safety, Environment and Social Responsibility Con*ference, 26–27 June, Lima, Peru.

Barabady, J. Markeset, T. & Kumar, U. 2010. Review and discussion of production assurance program. International *Journal of Quality & Reliability Management* 27(6): 702–720.

Bluestein, M. & Quayle, R. 2003. Wind Chill. In: J.R. Holton, J.A. Curry and J.A. Pyle (Editors), *Encyclopedia of Atmospheric Sciences*. Academic Press, Oxford: 2597–2602.

Boehm, P.D. Page, D.S. Brown, J.S. Neff, J.M. Bragg, J.R. & Atlas, R.M. 2008. Distribution and weathering of crude oil residues on shorelines 18 years after the Exxon Valdez spill. *Environmental science & technology* 42(24): 9210–9216.

Brandvik, P.J. & Faksness, L.G. 2009. Weathering processes in Arctic oil spills: Meso-scale experiments with different ice conditions. *Cold Regions Science and Technology* 55(1): 160–166.

Broje, V. & Keller, A.A. 2006. Improved mechanical oil spill recovery using an optimized geometry for the skimmer surface. *Environmental science & technology* 40: 7914–7918.

Broje, V. & Keller, A.A. 2007. Effect of operational parameters on the recovery rate of an oleophilic drum skimmer. *Journal of Hazardous Materials* 148(1–2): 136–143.

Castro, A. Iglesias, G. Carballo, R. & Fraguela, J.A. 2010. Floating boom performance under waves and currents. *Journal of Hazardous Materials* 174(1–3): 226–235.

Díez, S. Jover, E. Bayona, J.M. & Albaigés, J. 2007. Prestige oil spill. III. Fate of a heavy oil in the marine environment. *Environmental science & technology* 41(9): 3075–3082.

Dutta, P.K. 1988. *Behaviour of materials at cold regions temperatures—Part 1: Program rationale and test plan*. New Hampshire: US Army Engineer Research and Development Centre.

Fingas, M. 2011. *Oil spill science and technology*. Boston: Gulf Professional Publishing.

Fritt-Rasmussen, J. Brandvik, P.J. Villumsen, A. & Stenby, E.H. 2012. Comparing ignitability for in situ burning of oil spills for an asphaltenic, a waxy and a light crude oil as a function of weathering conditions under arctic conditions. *Cold Regions Science and Technology* 72(0): 1–6.

ISO, 2005. *ISO 2009:2005 Quality management systems—Fundamentals and vocabulary*. Geneva: ISO.

ITOPF, 2012. *Use of Skimmers in Oil Pollution Response—Technical Information Paper 5*. Canterbury: The International Tanker Owners Pollution Federation Limited (ITOPF).

Jensen, H.V. & Mullin, J.V. 2003. MORICE—new technology for mechanical oil recovery in ice infested waters. *Marine Pollution Bulletin* 47(9–12): 453–469.

Lee, C.M. & Kang, K.H. 1997. Prediction of oil boom performance in currents and waves. *Spill Science & Technology Bulletin* 4(4): 257–266.

NOAA, 2010. *Characteristics of Response Strategies: A Guide for Spill Response Planning in Marine Environment*. Seattle: National Oceanic and Atmospheric Administration (NOAA).

Nordvik, A.B. 1995. The technology windows-of-opportunity for marine oil spill response as related to oil weathering and operations. *Spill Science & Technology Bulletin* 2(1): 17–46.

Nordvik, A.B. 1999. Time window-of-opportunity strategies for oil spill planning and response. *Pure and applied chemistry* 71(1): 5–16.

Nordvik, A.B. Simmons, J.L. Bitting, K.R. Lewis, A. & Strøm-Kristiansen, T. 1996. Oil and water separation in marine oil spill clean-up operations. *Spill Science & Technology Bulletin* 3(3): 107–122.

Ornitz, B.E. & Champ, M.A. 2002. Chapter 7—The Technology Windows-of-Opportunity Oil Spill Response Strategy. In: B.E. Ornitz & M.A. Champ (eds), *Oil Spills First Principles*. Elsevier: Oxford.

Osczevski, R. & Bluestein, M. 2005. The new wind chill equivalent temperature chart. *Bulletin of the American Meteorological Society* 86(10): 1453–1458.

Payne, J.R. & McNabb, G.D. 1991. Oil-weathering behavior in Arctic environments. *Polar research* 10(2): 631–662.

Potter, S. Buist, I. Trudel, K. Dickins, D. & Owens, E. 2012. *Spill Response in the Arctic Offshore*, American Petroleum Institute: Washington DC.

Prince, R.C. Owens, E.H. & Sergy, G.A. 2002. Weathering of an Arctic oil spill over 20 years: the BIOS experiment revisited. *Marine Pollution Bulletin* 44(11): 1236–1242.

Schulze, R. 1998. *Oil spill response performance review of skimmers, 34*. ASTM International: West Conshohocken.

Shum, J. & Borst, M. 1985. Ohmsett tests of a pore-mob skimmer in ice-infested waters 1. *Proceedings of International Oil Spill Conference* 1985(1): 31–34

Singh, R. 2013. Chapter 7—Material Properties in Low Temperature Environment. In: R. Singh (eds), *Arctic Pipeline Planning*. Gulf Professional Publishing: Boston.

Stapelberg, R.F. 2009. *Handbook of reliability, availability, maintainability and safety in engineering design*. Springer.

Ventikos, N.P. Vergetis, E. Psaraftis, H.N. & Triantafyllou, G. 2004. A high-level synthesis of oil spill response equipment and countermeasures. *Journal of Hazardous Materials* 107(1): 51–58.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Rethinking nuclear safety management: Injunction as a meta-concept

S. Agulhon
MINES ParisTech, PSL Research University, CRC—Centre de Recherche sur les Risques et les Crises, Sophia Antipolis, France

D. Pécaud
Institut de l'Homme et de la Technologie, Polytech'Nantes, Nantes University, Nantes, France

F. Guarnieri
MINES ParisTech, PSL Research University, CRC—Centre de Recherche sur les Risques et les Crises, Sophia Antipolis, France

ABSTRACT: The management of safety is marked by strong procedural features and permanent adjustments of social actors to situations. Focusing on these two noticeable aspects of its operational reality, we propose to go hunting for new food for thought: rethinking safety management in the light of the meta-concept of injunction.

In order to understand the nature of safety injunction, we will analyze it through two approaches: a scientific one and a philosophical one. As a mass communication device triggering heteronomy to its receivers, safety injunction appears as a basis for safety management concepts. So one can note that safety injunction is a meta-concept to talk about safety.

But philosophy and sciences do not insist on the same aspects of this meta-concept. Philosophy analysis leads us to think that safety injunction is linked to a model and introduce new elements in it through experience while a scientific point of view is more focused on safety injunction output with some cause-effect pathways dealing with struggles for power at organizational and social scales.

However, as scientific safety injunction analysis also implies normativity and subjects' perceptions issues in its scale tension showing the difficulty to master safety injunction. That is why; one can conclude that safety injunction cannot be separated either from practice or experience. This interesting result not only helps to define safety injunction but is also an important parameter to be considered in the design of an appropriate methodology.

In order to deploy and animate risk prevention measures, the nuclear industry mainly uses injunctions for safety which are practically based on the rise of expectations projected on to a unit from outside (Boussard, Demazière & Milburn 2010). The aim of this article is to define injunction as a meta-concept for safety management, that is to say a concept aiming to provide the firm grounds to a language attempting to talk about scientific concepts while discovering their meaning (Lacour 2005).

First, we will define injunction around safety through a scientific and philosophical approach. Then we will analyze its impacts at a social and organizational level and the consequences lead on safety management in high risk organizations. On the one hand this will lead to notice the interest to consider injunction as a meta-concept for safety management, but, on the other hand, this will underline the necessity not to reify injunction that is to say disregarding the role of its experience in the field provided.

1 WHAT IS SAFETY INJUNCTION?

1.1 *Injunction as a meta-concept for safety*

To master safety, high risk industries follow a general trend of "normalization of social interactions and practices, leading to the bureaucratization of everyday life, a phenomenon long envisioned by Max Weber and regularly reassessed and commented by sociologists" (Bieder & Bourrier 2013). The existence of rules and the integration of these observations into a symbolic universe (in a large sense) allow us to state that we are before the presence of a human fact (Granger 1992).

This human fact can be scientifically cut-up and analyzed to draw its meaning, revealing a structure referring to a "cybernetic" model in which "energetic"[1]

[1]A one-plan model in which organizations receive an input and transform it into an output like a machine (Granger 1992).

organization is regulated at an informational level, in a flow of information through a network. But this scientific approach of the human fact disregards how humans experience toward a safety injunction since it only focuses on its structures.

If safety is an output of an injunction produced by social actors, then injunction would be a meta-concept for safety, thus a concept on which the language of safety relies on to make meaning through experienced actions.

Reducing the safety injunction to a mechanism of cause and effect suppresses the possibility to inquire about what really is at stake: the heteronomous[2] tension that it applies on individuals. For this reason, we will also propose to set up a philosophical scaffold around the organization of this experience with the purpose to understand safety injunction.

1.2 *Safety injunction in philosophy*

Neo-classic philosophy, the historical mainstream of contemporary thinking, reduces individual behaviour and collective functioning to the *homo œconomicus* model, whose vices would lead to the general interest. A classic example is given to us by Adam Smith, who wrote that "it is not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner, but from the attention they pay to their own interest. We address ourselves, not to their humanity but to their egoism; and we don't talk to them about our needs but always about their advantages" (Smith 1776)[3].

Even if this model is rather closed, loops would exist opening the way to the positivist modernization front started by the Enlightenment (Latour 2012). In this world portrait, injunction would inject in the autonomous and rational individual the necessary elements to perpetuate his or her capacity to make the "right" choices, just as it would inject into society the necessary elements to go on with the course of civilization. Briefly said, injunction would be the meta-concept "opening" and adjusting our understanding of the world along with the knowledge production progress. Injunction as a meta-concept would be hence defined as a heteronomous device at the service of a neo-classic instrumental rationality. Furthermore, the hypothesis of transparency of information inherent to the instrumental rationality ideal is an assumption far away from concrete action, just as the pure and perfect competition principle in economics. As for recruitment, the decision to join a firm is more complex than suggested by classic Supply and Demand Theories. The desirability of a movement is related to a lot of subjective variables. "Whether dissatisfaction with the organization leads to withdrawal depends on whether the participant perceives the "employment contract" as given or as subject to change. Where the contract is viewed as unchangeable, the only options are to "accept" or to "reject". Where the contract can be changed, participation by no means precludes internal conflicts and bargaining" (March & Simon 1993).

1.3 *Safety injunction in sciences*

Injunction, as a meta-concept for safety, looks like mass communication triggering heteronomy on its individual receivers. At a large scale, individuals would introject the content of a message. As a result the content of the message would become their own subjective meaning, making of this message the source of their motives to take any action, instead of looking for those motives in themselves.

At the Oak Ridge National Laboratory in 1947, safety injunction took shape concretely through preventive posters warning the staff of the Manhattan Project of radiation risks.



Figure 1. Radiation risk prevention poster in Oak Ridge (USA).

[2]Heteronomy: when one does not follow its own rules by looking after his reasons to act in external things. Heteronomy is opposed to autonomy.

[3]Tough Adam Smith is not a neo-classic but a classic economist, neo-classic theory is based on his "invisible hand" metaphor.

As the poster suggests, individuals are the particular dispositions of the safety injunction hence their subjectivities are more or less called upon, depending on the practices linked to the injunction. In the case of an order, the compliance of individuals is weaker than it would be through a message diffusing an ISO norm relying on a participatory basis.

In the case of the preventive poster mentioned above and presented below, the staff members are called upon twice. They must learn to be aware of an invisible hazard and develop the proper discipline to work in a radioactive environment at the same time.

2 HOW DOES THE SCIENTIFIC CONCEPT OF INJUNCTION ON SAFETY WORK?

Scientific analysis of injunction on safety as a meta-concept on the field shows a double mechanism: injunction as a flux and instrumentalized injunction, at social and organizational levels respectively.

2.1 *Injunction as a flux*

Injunction on safety comes from the desire to respect our society values such as life, leisure or work. As a consequence, individuals want to stick to moral (to put it in a nutshell: value aggregation) as those values are important to them. When it comes to action, social actors expect a form of ethics (an applicable moral) from each other that suits social values. Not only the social actors find normal or acceptable a practice that matches their ethics but they also expect others to behave according to the same ethics.

Injunction as a flux is a support that transports permeable expectancies that appear for action. Injunction on safety as a support diffuses expectancies though a network crossing society. There is no determined reaction due to injunction diffusion.

Expectancies that feed the flux come from all kind of human and non-human network-actors. They have no determined origin. As Egyptian mosquitoes, hardly definable targets that "forge links and arouse chain reactions" (Callon 2006), injunction as a flux does not structure society but crosses it, transmitting what it brings.

The example of the Oak Ridge Laboratory poster on which an operator pays his respects to a radioactive source in a zone with a "Radiation, Danger, Keep away" sign illustrated with two sentences "Radiation need to be feared … but it must command your respect", directly shows injunction as a flux. Indeed, "Radiation need to be feared" is a general message. One must be afraid of radiations as they have an impact on health. One should not brave the danger as it could be interpreted as an insult to life keeping.

2.2 *Instrumentalized injunction*

In organizations, applying injunction as a flux implies a contextualization of it in order to reach a goal. For instance, to be authorized to produce for the nuclear industry. The decision-maker selects in the flux the closest expectancies toward the actual action processes.

When organizations seek for some particular elements, injunction is applied as a medium to get it. In other words, injunction is instrumentalized to fulfil objectives. In an analysis based on the actor-network theory, organizations involve their stakeholders by using points and arguments referring to economics or social depending on those actors position toward organizational goals. As one can see "it is clear […] that stakeholders mobilization thus their concrete implication in the action plan goes through a problematization phase to build a sense to action that can be accepted by all" (El Abboubi & Cornet 2010). This is precisely in this step that organizations can associate stakeholders which can be quite hostile at first glance. In this move, organizations absorb their position in the action plan which was their initial goal. Then, they can submit workers mass to legitimate policies. Instrumentalized injunction has been derived from the flux to serve action for the firm sake.

In the risk prevention campaign of Oak Ridge, the intended effect is the modification of operators' behaviours facing a risk through a visual support. Operators are encouraged to discipline and to command respect as one can note with the character attitude. Indeed, he placed his cap on his chest, as soldiers does to show respect toward important people.

3 INJUNCTION ON SAFETY AND NORMATIVITY

Uniformisation of perceptions and practices due to injunction on safety and safety apprehension as a social value lead to constraint individuals. How can we understand this normativity?

3.1 *Safety in society*

Scientific analysis of injunction on safety as a meta-concept implies at the same time a reduction of normativity to an object and an objective representation of normativity. For centuries the sovereign power had the privilege to "make one die or let one live" (Foucault 1976), but in the Classic Age, the sampling mechanisms needed to defend and

maintain the sovereign tend not to be the major form of power exercise anymore. Sampling mechanisms become "a piece among others that has incentive functions, that reinforce, control, supervise, arise and organize the forces they submit: a power made to produce forces, to increase and order them instead of preventing, breaking or destroying them" (Foucault 1976).

This "biopouvoir" as modern power over life supposes universalist human well-being conceptions and the end of some practices judged as unethical by stakeholders such as dose management (high exposure to radiations during short periods of time coupled with high team turn-over to maintain or increase nuclear industry production). At the same time, sensibilisation to rules work is encouraged by decision-makers considering that it is important to protect workers by making them aware of their workplace risks.

Injunction on safety tend to neutralize spoilers that justify its existence rather than to ensure the appropriate behaviour according to its standards. The use of injunction in safety management tends to stamp out and alleviate life roughness.

But this way to proceed fails to recognise the interpretation and normativity reorganizations in other normativity signification systems. Indeed, no one can really anticipate operators' receptions and feelings towards the poster campaign and its collective effect. But, this recognition defines our relationship with phenomenological experience that is to say how facts appear to me in my own subjectivity. We will now analyze injunction on safety psychological effects.

3.2 *Injunction on safety psychological effects*

Injunction on safety is not made to equilibrate the communication relationship between transmitter and receiver. It demonstrates power relationships and a social order in which we are all involved. This struggle for power and influence on the receiver is part of injunction authoritarian character. Not following the path is a potential threat toward the social group cohesion.

So, "statistically, threat becomes a moderator variable instead of a direct predictor: an interaction model" (Feldman 2013). "In brief, this model posits that the underlying basis of authoritarianism is the conflict between the values of autonomy/independence and social conformity. People who are predisposed toward authoritarianism value social conformity over autonomy because they believe that strongly held and rigorously enforced norms and values are needed to maintain social cohesion and order" (Ibid).

Radiation threats brought by the "Radiation need to be feared … but it must command your respect" poster remind the reader of the rule. This imperative is due to the serious aspect of the subject. Beyond danger and risk, operators have to be professionals in their attitude by wearing equipment and being focused. As a consequence, the operator designed on the poster does not smile but appears as responsible.

This example illustrates that what is invested in our safety apprehension "is less reality than a particular knowledge of what is real […]. The knowledge contained in the mythical concept[4] is a confuse knowledge, formed by smooth and unlimited associations. This open character of the concept must be stressed; this is absolutely not an abstract and purified essence; it is a non-formed, instable, unclear condensation which unit and coherence particularly depend of its function. In this sense, one can say that the fundamental character of the mythical concept is to be appropriated" (Barthes 1957). The real image of safety is deleted for injunction on safety meta-concept which is a system in a system dealing with sense and interpretation.

Making the operators aware of danger by using fear mechanisms is an incentive to make them actors of their own safety by protecting themselves. But such a safety management also triggers numerous tensions in organizations as the whole is not the sum of its parts.

4 INJUNCTION ON SAFETY META-CONCEPT IMPACT ON SAFETY MANAGEMENT IN ORGANIZATIONS

4.1 *A scale tension between autonomy and heteronomy*

A philosophical approach of injunction on safety shows a tension between subjects' autonomy and injunction heteronomy process. Organizational objectives and values were "initially […] imposed on the individual by the exercise of authority over him; but to a large extent the values gradually become 'internalized' and are incorporated into the psychology and attitudes of the individual participant." (Simon 2000). So, an operator in a zone exposed to radiations that has incorporated Oak Ridge poster to his representations can possibly prevent a colleague from staying too long in front of a radioactive source were sieverts are released in important quantity.

However, when the receiver catches injunction on safety message, he internalizes to his representations and practices. The heteronomous mechanism addressed to individuals does not

[4]Or meta-concept in the present article.

impede individuals from overcoming what is being imposed. Although "events are directed from outside to inside" (Horkheimer 1936), one can also note that the internalized message of injunction changes due to its appropriation by social actors.

As injunction on safety message tends to be diffused at large scale, the number of people with their own and changing representations is multiplied. This individual process becomes a collective fact influencing collective representations guiding the decision-maker. In other words, injunction as a flux and instrumentalized injunction can be combined. As a matter of fact, one can see that safety expertise power is balanced with the necessity for workers mass to integrate safety in their job. While expertise is stuck to support functions, its general knowledge is aspired, modified and adapted to the core functions of the firm, in operators' job descriptions. Furthermore, to be funded, expertise is also led to develop its knowledge depending on operational needs.

4.2 *The injunction mastering impossibility*

The slip of injunction on safety message creates some unexpected and unpredictable effects for the decision-maker. Indeed, validating a risk prevention campaign does not mean that the decision-maker masters all operators' reactions (indifference, careful reading or contempt).

When action representation is linear and derived from a decision coming from a reflexion, it is implied that there is intentionality in the process. But, one cannot control all his acts (Reason 1990) or all his communication effects (Adorno 1954).

In the perspective of a Reflexion-Decision-Action model, a decision-maker that cannot obtain the result he wanted would have taken the wrong decision. Combining injunction on safety as a meta-concept and a philosophical approach allows us to imagine that a decision-maker would gather information on factors that could influence his action result, such as federation or separation of social groups or an informal leader's sensitivity.

Decision-maker's goal would be to limit the gap between his result and what was expected. Decision would not be good or bad. What would be at stake would be its normal appearance to the largest number of people who might be concerned by it (Alter 2009).

The risk prevention poster lets the operator act in the most suitable way for him by delegating to him his risk evaluation. While fixing a normative horizon, injunction let the operator determine what to do and what adjustments are necessary in his practice. In the end, the decision-maker has to believe in his influence skills but also in operators' work.

5 INJUNCTION AS A META-CONCEPT TO UNDERSTAND SAFETY?

Understanding injunction on safety meta-concept inscription in safety management has led us to consider it with a scientific analysis but also to balance it with a philosophical approach.

Injunction on safety meta-concept, as a concept to provide basis to a language aiming to talk about scientific concepts by finding their signification (Lacour 2005), is quite interesting as we can formulate and give a sense to human facts. The notion of meta-concept gives order to a conceptual system so it is reflexive.

However, capturing injunction on safety with a meta-concept reifies it and conducts to a paradox: the loss of its reference. Injunction on safety is also an experience-based element, it is a phenomenological manifestation.

Injunction on safety is the meta-concept through which one can understand safety in action and its management. But it is also by its prism that we crystallize expectancies toward our existence.

Concerning methological issues, one should first analyze empirically injunction on safety by observing actors possibly submitted to injunction in their experience before reshaping the meta-concept.

6 CONCLUSION

Injunction on safety allows us a glimpse on operational safety by its apprehension as a meta-concept. But it also makes underlying and structuring safety logics appear under the condition to be kept in experience field too.

REFERENCES

Adorno, T.W. 1954. How to Look at Television, *The Quarterly of Film Radio and Television*, Vol. 8 No. 3: 474–488.

Alter, N. 2010. *Donner et prendre: la coopération en entreprise*, Paris: La Découverte/Poche.

Austin, J.-L. 1991. *Quand dire, c'est faire*, Paris: Editions du Seuil.

Barthes, R. 1970. *Mythologies*, Paris: Editions du Seuil.

Bieder, C., Bourrier, M. 2013. *Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization?*, Farnham: Ashgate Publishing Limited.

Boussard, V., Demazière, D. & Milburn P. 2010. *L'injonction au professionalisme*, Rennes: Presses Universitaires de Rennes.

Brossat, A. 2009. Pouvoir pastoral et « vie bête », *Revue Appareil,* n° 4: 1–8.

Callon, M. 2006. L'Egypte et les experts, *Gérer et comprendre*, n°86: 12–26.

Callon, M., & Latour, B. 2006. Le grand Léviathan s'apprivoise-t-il ? In M. Akrich, M. Callon & B. Latour (eds), *Sociologie de la traduction—Textes fondateurs:* 11–31, Paris: Presses des Mines de Paris.

El Abboubi, M. & Cornet, A. 2010. L'implication des parties prenantes comme un processus de construction sociale. Analyse à partir de la théorie de l'acteur-réseau, *Management & Avenir*, 3 n°33: 275–297.

Feldmand, S. 2013. Comments on: Authoritarianism in social context: The role of threat, *International Journal of Psychology*, 48:1:55–59.

Foucault, M. 1976. *La volonté de savoir*, Paris: Tel Gallimard.

Granger, G.G. 1992. A quoi sert l'épistémologie ? *Droit et Société*, 20/21:35–42.

Granger, G.G. 1999. Principes scientifiques, Principes philosophiques, *Principia*, 3(1):87–99.

Horkheimer, M. 1996. *Égoïsme et émancipation. Contribution à une anthropologie de l'âge bourgeois*, Paris: Gallimard.

Lacour, P. 2005. Faire sens: Essai sur la philosophie selon Gilles-Gaston Granger *in « L'objet de la philosophie d'aujourd'hui » ATALA*, n°8:129–139.

Latour, B. 2012. *Enquête sur les modes d'existence: Une anthropologie des Modernes*, Paris: La Découverte.

March, J.A. & Simon, H.A. 1993. *Organizations*, Massachusetts: Blackwell.

Reason, J. 1990. *Human Error*, Cambridge: The Press Syndicate of the University of Cambridge.

Simon, H.A. 1997. *Administravite Behavior: A study of decision-making processes in administrative organizations*, New-York: The Free Press.

Smith, A. 1776. *Recherche sur la nature et les causes de la richesse des nations*, Chicoutimi: Université du Québec.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Using IRIDM & VTA to support the risk management of the research reactor Maria

M. Borysiewicz, K. Kowal & S. Potempski
National Centre for Nuclear Research (NCBJ), Otwock-Świerk, Poland

ABSTRACT: The aim of this article is to present how to integrate safety, security and economic issues in the risk management process of the nuclear reactors based on operating experience of the research reactor Maria, operated by National Centre for Nuclear Research (NCBJ). According to the recommendation of International Atomic Energy Agency (IAEA) the risk management of nuclear facilities should be performed by usage of the Integrated Risk Informed Decision Making (IRIDM) methodology. In this work the IRIDM approach has been improved by application of the Value Tree Analysis methods in order to support decision making process on the reactor fuel conversion.

1 INTRODUCTION

The relationship between the main stakeholders of the nuclear industry is similar all over the world. Especially, there is always a regulatory body established to enforce the nuclear law and to control if that law is obeyed by the facility operators in order to ensure appropriate level of safety for the people. If non-compliance with the regulations is demonstrated the regulatory body applies appropriate sanctions against the operator, including cancelation of the license for nuclear activity. Therefore the decision making on nuclear installations should be performed in balanced and comprehensive manner that brings transparency and auditability of that process. Then the regulatory body is able to verify how the implementation of particular decision would affect the risk associated with the facility operation (IAEA 2001).

Until now, the commonly applied approach to the decision-making on nuclear facilities was based on Deterministic Safety Assessment (DSA), where a set of rules and requirements has been defined in order to ensure a high level of safety. This was done by applying the defense in depth principles and adequate criteria for safety margins (IAEA 2009).

Nowadays, the standard approach is based on combining the insights from both the DSA and Probabilistic Safety Assessment (PSA). The PSA provides estimation of the probability and consequences of all accident scenarios possibly leading to the core melt and radiological releases (IAEA 2010).

However, the decision making on nuclear facilities require much more inputs than only the DSA and PSA insights. Beyond the safety goals there are also financial indicators, organizational aspects, security systems, social doubts etc. The consideration of such a wide range of issues is a complex multi-attribute process. In order to meet this challenge it is recommended to implement the model of Integrated Risk Informed Decision Making (IRIDM) developed by International Atomic Energy Agency (IAEA) and United States Nuclear Regulatory Commission (U.S. NRC) (IAEA 2010, US NRC 2009).

IRIDM is a process where a number of qualitatively different inputs, corresponding to different types of risk, are jointly taken into account in the decision making. Relative importance of the IRIDM inputs depend upon the decision to be made and should be weighted quantitatively. The weights assigning, however, is quite subjective and bases mainly on the engineering judgment. This is the main disadvantage of that process which can be improved by application of the Value Tree Analysis (VTA) methods as it was described in this article.

The aim of this work is to present the possibility of practical implementation of IRDM and VTA in the decision making process on fuel conversion of the research reactor Maria. The conversion means giving up of High Enriched Uranium fuel (HEU) containing 36% of U-235 and replacing it with Low Enriched Uranium fuel (LEU) with only 19.7% U-235. The decision on the fuel conversion was dictated by the security reasons with accordance to the Global Threat Reduction Initiative (GTRI) recommendations. However, since the decision has been made, it became necessary to determine how to perform this process in an optimal manner. Basic criterion was to maintain the previous operating parameters of the reactor while meeting all safety requirements after the conversion (Borysiewicz et al. 2013).

2 THE IRIDM APPROACH

According to the basic framework of the Integrated Risk Informed Decision Making process, consideration must be given to the requirements of both regulatory body and operator in order to draft a preliminary set of options that potentially could solve the analyzed issue (Fig. 1).

However, to make the final decision and choose one from the preliminary set of options, specified inputs must be established, namely the standards and good practices, operating experience, deterministic and probabilistic considerations, organizational and security systems and other factors such as research or economic insights. Relative importance of each element depends upon the decision to be made and should be weighted qualitatively. This process leads to evaluation and reduction the preliminary set of options. Finally one of them should be chosen, implemented and monitored. Moreover, if the performance of just implemented decision is not satisfactory corrective actions should be undertaken and the list of option needs to be redefined (IAEA 2011).

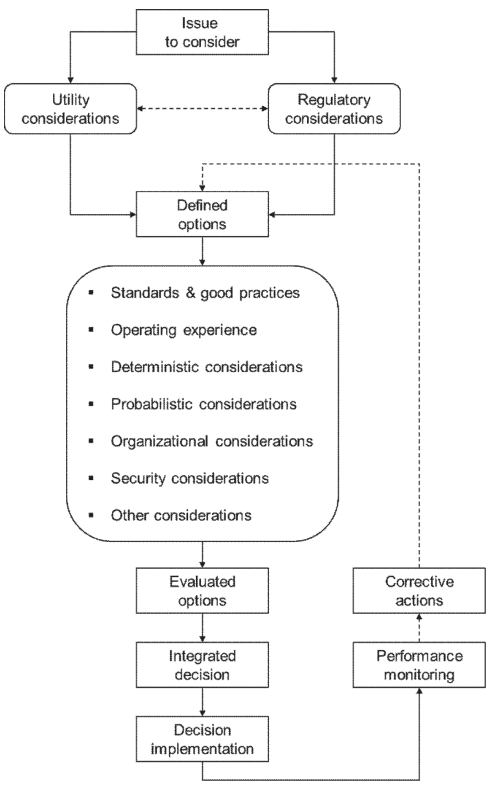


Figure 1. Organizational framework and key elements of the IRIDM process (IAEA 2011).

3 THE VTA METHODS

While the IRIDM framework itself seems to be very well organized its practical implementation may be difficult due to the problem with the inputs prioritization. It is because the weights assignment process is quite subjective, based on engineering judgment and dependent on particular issue being addressed. This is the main disadvantage of that process which can be improved by application of the Value Tree Analysis (VTA) methods (Borysiewicz, in press).

The VTA approach can be applied in the IRIDM inputs prioritization and the decision options evaluation by usage of several techniques. The most important ones are the following:

- SMART (Simple Multi-Attribute Rating Technique)—a two-way process: first the worst attribute is selected, then the others are scored by the ratio related to it (Edwards 1977).
- SWING (SMART with Swing Weighting)—the process starts from choosing the most important attribute then the other weights are defined by making relations to it (Edwards et al. 1994).
- SMARTER (SMART Exploiting Ranks)—first, ranking of attributes is made, then the weight W_i is determined for i-th input according to the formula (Edwards et al. 1994):

$$W_i = \frac{1}{N}\sum_{n=i}^{N}\frac{1}{n}, \tag{1}$$

where N number of attributes.

- Value function *val* that has the following properties: if $x \sim y$ then $val(x) = val(y)$, i.e. if two attributes give the same impact then their weights are equal, and if $x < y$ then $val(x) < val(y)$, i.e. if attribute x is less important than y then the value of y is higher than the one of x. The key point here is the shape of the function: linearity reflects simple mapping of the parameter values, while, for example, a concave exponential curve means that any changes in the lower region of the parameter space are more important than the changes of the same size in the upper region; for a convex function the situation is opposite.
- AHP (Analytical Hierarchy Process)—a pairwise comparison matrix A is first created, where a_{ij} is the estimated ratio of weights W_i and W_j, i.e. $a_{ij} = W_i/W_j$ (consequently $a_{ji} = 1/a_{ij}$). If the matrix is consistent (i.e. $a_{ij} = a_{ik} \cdot a_{kj}$) then the method can be reduced to simple weighting. However, this is not always true because the judgements of decision makers does not have to be consistent. For consistent matrix it can be seen that all eigenvalues are ones, except the highest one equals to N, i.e. $AW = NW$. For inconsistent case one wants

to be in accordance with the consistent one—therefore, the vector of weights is found as an eigenvector of maximal eigenvalue: $AW = \lambda_{max} W$ (Saaty 1980, Saaty 1980, Salo et al. 1992).

4 CONVERSION OF MARIA REACTOR CORE

The research reactor Maria is a multi-purpose, high flux, pool type reactor, moderated with water and beryllium with graphite reflector and pressurized channels consisting of 22 concentric six-tube assemblies of fuel elements. The active length of the fuel assemblies is 1 m. The reactor was designed with a high degree of application flexibility and it has been using the high enriched uranium fuel (UO_2-Al alloy) with aluminium cladding since it began the operation. The fuel channels are situated in a matrix containing beryllium blocks and enclosed in a lateral reflector made of graphite blocks in aluminium cans. Maria is equipped with vertical channels for irradiation of target materials, a rabbit system for short irradiations and 7 horizontal neutron beam channels. The nominal reactor's power is 30 MW_t while thermal neutron flux density is $4.0 \cdot 10^{14}$ n/cm^2 s. This reactor is suitable for testing of fuel and materials for the nuclear power engineering, neutron studies (radiography, activation analysis and transmutation doping) and for the scientific research in the field of condensed matter physics. However, its main application is the radioisotopes production. Maria is one of the few reactors able to produce Mo-99 which is essential for the diagnosis of cancer in medical centers all over the world.

Ensuring the continuity of molybdenum supplies excludes the long term shutdown of the reactor and requires to maintain approximately the same thermal power after the core conversion. Therefore, since the conversion leads to decrease of U-235 enrichment the volume of fuel itself has to be increased. For that reason the present fuel channel configuration—that bases on 6 concentric tubes (Fig. 2)—will be replaced with a new one, which consists of 5 tubes but with different diameters and thicknesses.

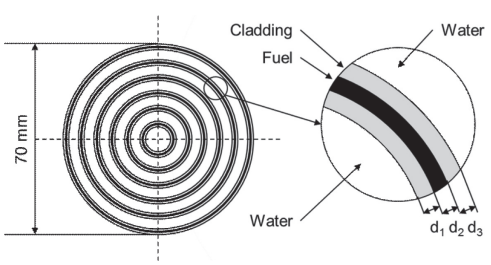


Figure 2. Horizontal cross section of the high enriched uranium fuel element of the research reactor Maria (Borysiewicz 2013).

The thermal hydraulic analysis showed that the cladding temperature for both types of fuel elements are almost the same, e.g. maximum cladding temperature on the internal surface of the tube is 425 K and 426 K for LEU and HEU respectively. However, the maximum heat flux on the external wall of the fuel tube is 2,61 MW/m^2 and 2,04 MW/m^2 for the LEU and HEU fuel respectively. Moreover, the data acquired from the performed measurements point out that the coefficient of hydraulic resistance for LEU fuel elements exceeds by around 30% the resistance coefficient for the HEU fuel (Dorosz et al. 2009).

The required coolant flow rate through the new LEU fuel channel is at least 30 m^3/h while in the HEU fuel it is equal to 25 m^3/h. This difference implies the necessity of increasing the mass flow in the new channels up to 120% of previous nominal flow. However, since the existing infrastructure is not sufficient to increase the mass flow, this process requires replacement of the primary cooling channel pumps. It complicates the whole procedure and makes the fuel conversion much more expensive than it was expected. Therefore, the implementation of IRIDM has been proposed in order to determine the best solution of the problem.

5 IRIDM & VTA METHODS APPLICATION

The IRIDM process has been organized in a form of facilitated workshop with representatives of the regulatory body (National Atomic Energy Agency) and utility (National Centre for Nuclear Research). The stakeholders considered a possibility of initiating the partial conversion process before modernization of the pump system. In such a case the whole procedure would be performed in a gradual way and the most burned-up HEU fuel would be unloaded first. Thus, the following options has been defined:

- Option 1: Partial core conversion before change of the pumps (with higher flow rate) without any additional criteria.
- Option 2: Partial core conversion before change of the pumps (with higher flow rate) but with additional criteria.
- Option 3: Rejection of partial core conversion before change of the pumps

When the consensus has been obtained that the results from DSA, PSA and economic analysis will have the highest impact on the final decision, the ranking of these inputs was performed. The highest priority was given to the deterministic

aspects (max. clad temp., max. heat flux and the hydraulic resistance). This choice comes from the fact that during the operation of reactor, it is necessary to maintain safety limits and requirements of defense in depth methodology. Probabilistic aspects in general should stay in conjunction with the deterministic results. Moreover, the proposed changes in the reactor fuel and the cooling system requirements could have an impact on the safety systems reliability, core damage probability, and radioactivity releases frequency. Thus, the Probabilistic Aspects (PSA) has been assigned at the medium weight. Obviously, the economic issues have a lower importance when compared to the safety aspects. However, the decisions on nuclear facilities are often somehow motivated by economics. In this case it was considered what are the costs of core conversion, what part of these costs may be covered from own resources, and what is the payback period of the investments.

When a compromise was reached in the process of prioritisation of the IRIDM inputs, a relative importance of *i*-th of them was expressed by W_i. Within each input the appropriate attributes were identified and the prioritisation of these attributes was made by assigning weight A_{ij} for each *j*-th attribute of the *i*-th input. For assessment of both W_i and A_{ij} the SMART method could be used. However, this approach involves a degree of subjectivity due to the necessity of the relative weights determination. In order to remedy these difficult the SMARTER method, reduced only to the rank order criteria, was applied.

Then, the s_{ikj} factor describing how the implementation of option *k*-th would affect the attribute *j* of input *i*, was calculated by usage of the concave function $val(\alpha)$, with α given by the following formula:

$$\alpha_x = \frac{x^a - x^f}{x^a - x^i}, \tag{2}$$

where x^a is the acceptable value of the parameter x which cannot be exceeded because of the official regulations, safety goals or internal policy of the operator. Variables x^i and x^f describe the initial (actual) value of the parameter and its final value (after implementation of *k*-th decision option), respectively.

Once when the values of all attributes for each input were determined, there was a possibility to calculate a final score *S* for each option via the formula:

$$S_k = \sum_i W_i \sum_i A_{ij} \cdot s_{ijk}. \tag{3}$$

In such a way a value tree diagram was constructed which is shown in Figure 3.

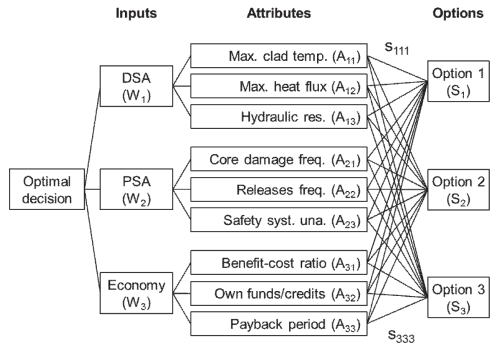


Figure 3. The value tree diagram developed to support decision-making on Maria reactor fuel conversion.

6 RESULTS AND CONCLUSIONS

Option 1 (conversion before change of the pumps without additional criteria) has been recognised as the best solution from the economic point of view. The radioisotopes can be produced continuously and no additional changes in the organizational system are needed. However, this option has an overall negative impact on both DSA and PSA. This is because the primary cooling channel pumps are not efficient enough to provide appropriate mass flow after conversion. Consequently the safety margins cannot be maintained. Therefore, this option was rejected due to the highest negative impact on the safety aspects.

Option 3 (replacement of the pumps before fuel conversion) was the best solution in terms of safety. However, this option assumes a long-term shutdown of the reactor. This generates significant economic losses associated with interruption of the isotopes production. Additionally, it needs some changes in the organizational system at the time of the replacement process. These are the main reasons why option 3 was rejected as well.

Option 2 (partial core conversion before change of the pumps starting from the most burned-up HEU fuel) has been chosen even though that there is slightly negative impact on both safety and economic aspects. Moreover, the additional requirements meaning criteria on power limits have been proposed. Due to the power limits slightly lower production of isotopes is expected. However, the economic losses are not as high as in option 3. Thus the option 2 is much safer than the first one and still very attractive economically. This is also the most balanced solution in the terms of risk distribution between different IRIDM inputs.

REFERENCES

Borysiewicz, M. et al., 2013. An application of IRIDM in the decision making process on fuel conversion of the Maria reactor. *Informatics Control Measurement in Economy and Environment Protection,* (3): 3–6.

Borysiewicz, M. et al., 2013. An application of the Value Tree Analysis methodology within an Integrated Risk Informed Decision Making on the nuclear facilities. *Reliability Engineering and System Safety*, in press.

Dorosz, M. et al., 2009. Hydraulically measurement to compare fuel elements types MC5 and MR6. *IAE Internal Report*, Otwock-Świerk.

Edwards, W., 1977. How to Use Multi Attribute Utility Measurement for Social Decision-making. *IEEE Transactions on Systems, Man and Cybernetics,* 7(5): 326–340.

Edwards, W. et al., 1994. SMARTS and SMARTER: Improved Simple Methods for Multiattribute Utility Measurement. *Organizational Behavior and Human Decision Processes,* 60(3): 306–325.

International Atomic Energy Agency, 2001. *Training the staff of the regulatory body for nuclear facilities: A competency framework*. Vienna: IAEA.

International Atomic Energy Agency, 2009. *Deterministic Safety Analysis for Nuclear Power Plants*. Vienna: IAEA.

International Atomic Energy Agency, 2010. *Development and Application of Level-1 PSA*. Vienna: IAEA.

International Atomic Energy Agency, 2011. *A Framework for an Integrated Risk Informed Decision Making Process*.Vienna: IAEA.

Saaty, T.L., 1980. *The Analytic Hierarchy Process*, New York: McGraw-Hill Inc.

Saaty, T.L., 1994. Highlights and critical points in the theory and application of the Analytic Hierarchy Process. *European Journal of Operational Research*, 74(3): 426–447.

Salo A.A. et al., 1992. Preference Assessment by Imprecise Ratio Statements. *Operations Research,* 40(6): 1053–1061.

United States Nuclear Regulatory Commission, 2009. *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making*. Washington: US NRC.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Evaluation of risk impact of equipment ageing and asset management for LWR GEN II and III NPPs in the horizon 2020

S. Martorell, I. Martón & S. Carlos
Department of Chemical and Nuclear Engineering, Universitat Politècnica de València, Valencia, Spain

A.I. Sánchez
Department of Statistics and Operational Research, Universitat Politècnica de València, Valencia, Spain

ABSTRACT: This paper focuses on the incorporation of not only equipment ageing but also maintenance and surveillance management programs explicitly into PSA (Probabilistic Safety Assessment) models and data. Thus, a new kind of Ageing PSA (APSA) modelling is proposed to be considered in the framework of the Risk Informed Decision Making according to R.G. 1.174 (USNRC, 2011) published by the US Nuclear Regulatory Commission (US NRC), which is intended to be used to support risk-informed decisions on the improvement of asset management programs and technical specification requirements of critical equipment of Nuclear Power Plants (NPP). An example of application is also presented in this paper that centers on critical equipment of a Nuclear Power Plant in order to evaluate the risk impact of considering the combined effect of equipment ageing and maintenance and surveillance management programs along design life operation of NPP (equipment design life management) and beyond along the extended period after receiving approval eventually for the NPP long term operation (equipment extended life management). The impact of several alternatives proposed is also discussed.

1 INTRODUCTION

One of the main challenges for 2020 horizon is to maintain fission technologies competitiveness by research and technological development necessary in order to allow a safe Long Term Operation (LTO) of the nuclear reactors in operation nowadays (GEN II and III).

For example, in 2020 most of the Nuclear Power Plants (NPP) in Spain, which are Light Water Reactor (LWR) type, would be operating for around 40 years, which is the plant design life, and they will face the Periodic Safety Review (PSR) to obtain, eventually, life extension approval for the LTO from the regulatory body (usually 10 years).

During the design life, licensee of NPP must perform the necessary activities for ageing management of Structures, Systems and Components (SSCs), which include considering measures for monitoring, control and mitigation of the mechanisms of physical ageing of SSC adopting the necessary maintenance and surveillance activities in scope of asset management programs.

An important part of PSR involves the evaluation of risk impact of how current equipment ageing and maintenance and testing programs management would jeopardize NPPs safety for the extended period and, eventually, adoption of an ageing management plan and reformulation of current operational requirements such as surveillance requirements.

Probabilistic Safety Analysis (PSA) is an essential tool for assessing, maintaining, assuring and improving the nuclear power plant safety. It is an essential and efficient tool for evaluation of risk impact in the framework of the Risk Informed Decision Making according to R.G. 1.174 (USNRC, 2011), which is adopted by many regulatory bodies. Often, neither the effect of equipment ageing nor maintenance and testing programs are explicitly considered in PSA models and data, e.g. adoption of constant failure rate instead of age dependent failure rates.

This approach of consideration of the ageing contribution will most likely result in underestimation of component unavailability and cost, particularly for an aged one. So, unavailability and cost models integrating component ageing and the effects of test and maintenance activities must be considered. However, the current standard PSA do not adequately address important ageing issues, which could have a significant impact on the conclusions drawn from PSA studies and applications where plants are operated at an advanced age or long term. In addition, all NPP have a large variety of testing, maintenance and inspection programs,

which can mitigate more or less the effects of ageing, it is obvious that the extent to which the components are susceptible to ageing degradation differ considerably. The ageing effects can be seen at the component level, at system level or at the plant level.

Nowadays, different approaches to develop Ageing PSA (APSA) are being proposed to account for equipment ageing (Nitoi et al., 2010; Volkanovsky, 2012). In these approaches, different methods for prioritization of the NPP components considering the implication of their ageing on the core damage frequency of the NPP for different test and replacement intervals are shown.

In this respect, lessons learned on ageing assessment, modeling and management of SSC of NPP in the framework of international programs and initiatives (GALL, IGALL, ….) should be fully integrated within advanced PSA models and data (USNRC, 1991; USNRC, 1991; IAEA, 2013).

In this paper, a new kind of Ageing PSA (APSA) modelling is proposed, which incorporates the impact of not only equipment ageing but also maintenance and testing management explicitly into PSA models and data, which is intended to be considered in the framework of the Risk Informed Decision Making according to R.G. 1.174 (USNRC, 2011) published by the US Nuclear Regulatory Commission (US NRC). This APSA could be used to support risk-informed decisions on the improvement of asset management programs and technical specification requirements of critical equipment of Nuclear Power Plants (NPP).

An example of application is presented that focusses on critical equipment of a Nuclear Power Plant in order to evaluate the risk impact of considering the combined effect of equipment ageing and several alternatives of maintenance and surveillance management programs along design life operation of NPP (equipment design life management) and beyond along the extended period after receiving approval eventually for the NPP long term operation (equipment extended life management).

2 MODELING RISK IMPACT OF EQUIPMENT AGEING CONSIDERING MAINTENANCE AND TESTING

2.1 *Failure rate model. Ageing and imperfect maintenance incorporation*

Traditionally, in the Probabilistic Safety Analysis (PSA) in Nuclear Power Plants (NPPs) it is assumed a constant standby failure rate, $\lambda(t) = \lambda_0$.

In this paper, reliability models at component level are reformulated using age-dependent models to estimate the effect of ageing on the unavailability PSA models.

Different models of age-dependent reliability have been proposed in the literature (Kim et al., 1992; Kim et al., 1994). The selection of the most adequate model depends on aspects such as component type, its operation mode, the ageing mechanisms considered or maintenance and surveillance testing programs performed.

Effective Preventive Maintenance (PM) programs are essential for ensuring acceptable operational reliability throughout the service life of nuclear power plants. The role of PM are to detect and mitigate component degradation managing of ageing effects.

To ensure effectiveness of PM programs, they should be periodically reviewed and modified on the basis of operating experience. Consequently, the age of the component is a function of maintenance activities performed during its design life and its effectiveness. So, it is necessary to include the effect of maintenance on the age of the component and on its reliability.

An imperfect maintenance model has been adopted with the aim of include the effect of maintenance on the age of the component. Maintenance imperfect models consider that each activity improves the state of the component by some degree, depending on its effectiveness.

Among the different models of imperfect maintenance that exists, in this paper the "Age Proportional Reduction" (PAR) model, proposed by (Martorell et al., 1999) is adopted. In the PAR approach, each maintenance activity is assumed to reduce proportionally the age gained from the previous maintenance. In this model, the effect of the maintenance is introduced by using an effectiveness parameter, ε, ranged in the interval [0, 1]. If ε = 0, the previous models simply reduces to an "as bad as old" situation, while if ε = 1 they are reduced to an "as good as new" situation.

Assuming that the time during which a component is out of service as a result of maintenance activity is negligible compared to the time between two consecutive maintenance, age of the component in the period m+1 between m and m +1-maintenance activity is given by:

$$w_{m+1}(t) = w_m^+ + (t - t_m) \tag{1}$$

where w_m^+ is the age of the component immediately after the maintenance number m, t is the chronological time and t_m is the time which the m-activity maintenance is performed. Using the expression of w_m^+, formulated in the reference (Martorell et al., 1999) age of the component in the period m+1 between m and m+1-maintenance activity is given by:

$$w_{m+1}(t) = t - \varepsilon \cdot t_m \tag{2}$$

In the literature, different ageing models are considered being the most common used the linear model, Exponential, Weibull… (Vesely et al., 1990).

In this paper, the linear ageing failure has been considered being this the simplest dependent model. This model assumes that the failure rate has a linear increase with the time, which can be expressed as (USNRC, 1992):

$$\lambda(w(t)) = \lambda_0 + \alpha \cdot w(t) \tag{3}$$

where α represents the linear ageing factor and $w(t)$ is the component's age which depends on the preventive maintenance applied to the component and $w(t)$ is the age of the component at a chronological time. So, the linear failure rate model shown above assumes that the total failure rate is the sum of random failures, λ_0, and ageing, $\alpha \cdot w(t)$.

Using Equation 1, Equation 2 and Equation 3, induced failure rate after m-maintenance is obtained as follow:

$$\lambda_{m+1}(t) = \lambda_0 + \alpha \cdot (t - \varepsilon \cdot t_m) \tag{4}$$

Then, it is formulated the average failure rate, λ^*_{m+1}, over the period between two consecutive maintenance activities, m and m+1 using the following expression:

$$\lambda^*_{m+1} = \frac{1}{t_{m+1} - t_m} \int_{t_m}^{t_{m+1}} \lambda_{m+1}(t) dt \tag{5}$$

Equation 5 represents an average failure rate between two consecutive maintenance activities which includes the effect of the ageing using a linear model, and the effect of the preventive maintenance performed on the component modelled as a PAR model.

2.2 *Risk impact*

PSA is a method of estimating mathematically the likelihood and consequences of potential accidents at Nuclear Power Plants (NPPs). The major advantage of PSA is the possibility of in-depth qualitative and quantitative analysis of NPP actual configuration with definition of factors characterizing of contribution to the general risk of reactor core damage.

The evaluation of ageing performed using PSA applications can allow to evaluate the component ageing impact to the unavailability of the safety systems, to show an increasing of core damage frequency due to the ageing of safety important components and structures, and to propose optimal test and preventive maintenance intervals. It should be noted that the core damage frequency could increase significantly due to the ageing degradation of components (Vesely et al., 1990).

In order to characterize the risk impact of component ageing and service wear effects, it is necessary to characterize the age dependent nature of the change in plant risk to incorporate into PSA models the degradation of the components due to ageing and the maintenance and surveillance program.

RG 1.174 (USNRC, 2011) establishes two risk metrics for evaluating the risk impact of whatever change to the licensing basis (Martorell et al., 2014), which are herein adapted to address the risk impact of equipment ageing.

Using a level 1 PSA, the required risk metrics for the evaluation of ageing are the annual average baseline CDF before ageing (named herein CDF_b) and the change in the annual average baseline CDF due to equipment ageing, which can be formulated as follows:

$$\Delta CDF = CDF_a - CDF_b \tag{6}$$

where CDF_b and CDF_a are the CDF before (b) and after (a) considering the ageing effect, respectively.

3 EVALUATION OF RISK IMPACT OF AGEING

In this paper, the three steps based approach for the evaluation of risk impact of ageing addressing identification, treatment and analysis of uncertainties in an integrated manner is adopted as proposed in Ref. (Martorell et al., 2014). The approach proposed is based on the use of the Ageing PSA and consist of: 1) modeling of risk impact including identification of ageing and other uncertainty sources, 2) assessment of risk impact including uncertainty treatment and 3) analysis of risk impact including importance and uncertainty analysis. The approach is coherent with the general principles of risk-informed decision-making framework.

What concerns risk modeling, it uses the APSA modeling introduced in section 2 and emphasizing the identification of not only the usually addressed sources of uncertainty linked to PSA models and data but also the sources of model and parameter uncertainties associated with the assumptions in maintenance and testing modeling. Random and parametric uncertainties are built into the structure of the PSA model itself. It is this aspect of uncertainty that gives PSA the probabilistic part of its name. They are typically characterized by establishing probability distributions on the parameter values. However, there may be different options or alternatives on how the models should be formulated. Examples include approach to modeling

human performance, common-cause failures, ageing, maintenance effectiveness, etc.

Risk assessment is proposed by formulating the usual risk metrics for analyzing Surveillance Requirement changes in the literature, as introduced in section 2.3. It is proposed treatment of model and parameter uncertainties based on traditional sensitivity studies and uncertainty assessment respectively, the latter based of the probabilistic approach for uncertainty formulation and propagation by standard Monte Carlo Sampling (MCS) technique.

Risk analysis is based on the well-established comparison of the assessment of risk impact of the change including treatment of uncertainties with acceptance guidelines. Thus, the numerical acceptance guidelines are given in RG 1.174 in terms of regions defined in the space of values $\{CDF_b, \Delta CDF\}$ where the results of the impact on risk are placed (see RG 1.174 (USNRC, 2011) for a more detailed description of such regions). The decision on the acceptability of the change must be based on a full understanding of the contributors to the PSA based results and the impacts of the uncertainties, both those that are explicitly accounted for in the results and those that are not. Therefore, the different regions of the acceptance guidelines introduced in RG 1.174 require different depths of analysis. Thus, when the results {CDF, ΔCDF} obtained are well away from the criteria boundaries, any concerns about the impact of a potential bias caused by the uncertainty tends to be a lesser concern. However, when the result of anyone is close to the boundary, then the appropriate representation of the uncertainty could make the difference between being above or below the boundary. In addition, it is proposed also the use of both traditional importance measures and uncertainty importance measures (sensitivity analysis) in order to analyze respectively how basic events and parameter uncertainties influence the risk impact of the change proposed and its uncertainty. The former helps to identify the main risk contributors and eventually the chance for adopting compensatory measures in order to the make NPP ageing acceptable. Uncertainty importance measures help to identify which of uncertain parameters are most significant contributors to risk impact uncertainty and eventually the need of limiting the impact of the effect of particular uncertainties.

4 APPLICATION CASE

4.1 *Problem description*

This section presents a simple example of application that focusses on analyzing the influence of considering the effect of ageing of a single critical component of a NPP depending on several maintenance and surveillance programs alternatives along the operational NPP design life (equipment design life management) and beyond along the extended period for the NPP long term operation (equipment extended life management).

In this work, a Motor-Operated Valve (MOV) of the Auxiliary Feed Water System (AFWS) has been selected based on several arguments. First, the basic event representing MOV "fails to remain open" is one of the most important contributors to the CDF based on the standard PSA available. Second, equipment aging, preventive maintenance and surveillance requirements are meaningful for this MOV. This basic event is modelled as a standby-related failure. This valve is normally open and its function is to control the flow from AFWS until Steam Generators on the secondary of a typical Pressurized Water Reactor (PWR) NPP.

4.2 *Risk modelling and data*

A level 1 standard PSA at power considering internal events only is available, i.e. allowing obtaining the CDF as risk metric. The level 1 PSA used has been developed at component level, so that, the level of detail is appropriate to support the analysis of equipment ageing addressing maintenance and testing. Consequently, there is a need of refining the level 1 PSA modeling only to address equipment ageing, i.e. to obtain the APSA, by replacing the standard failure rates and equipment unreliability models by the new ones proposed in section 2.

For sake of simplicity in the problem formulation and discussion of results, only the MOV of the AFWS is considered in order to formulate the APSA for this simple example of application. Table 1 shows data used for modelling the MOV basic event into the level 1 APSA, including description of parameters and corresponding constant value or probability distribution function (pdf). In the same way as in the standard PSA, all variables except motor-operated failure rate have been considered constant, i.e. mean values have been used. MOV failure rate has been modeled as a random variable assuming a Gamma probability distribution.

In Table 1, the value of the linear ageing factor (α) has been obtained from a generic data base, which is known as TIRGALEX (Levi et al., 1998). TIRGALEX considers that the value of α in the case of motor-operated valves is equal to $4.11 \cdot 10^{-11}$ h^{-2}. Furthermore, the value of Test interval (T) is taken from current Surveillance Requirements in Technical Specifications, which impose an operational test of this MOV at least

Table 1. Reliability, maintenance and surveillance data of basic event.

Parameter	Description	Parameter type	Parameter/value
λ_0 (h^{-1})	Motor operated valves initial failure rate	Random variable	Gamma ($4.45 \cdot 10^{-08}$, 0.5, $11 \cdot 10^{06}$)
T (h)	Test interval	Constant	13140
α (h^{-2})	Ageing factor	Constant	$4.11 \cdot 10^{-10}$
M (h)	Maintenance interval	Constant	4320
ε	Maintenance effectiveness	Constant	0.8
L_D (yr)	Remain design life period	Constant	10
L_E (yr)	Life extension period	Constant	10

every plant shutdown for refuelling. In addition, time-directed preventive maintenance, with periodicity M and corresponding effectiveness ε, given in Table 1 is based on current practice at NPP.

As it has been mentioned in the introduction, in 2020 most of the Nuclear Power Plants (NPPs) in Spain would be operating for around 40 years, which is the plant design life, and they will face the Periodic Safety Review (PSR) to obtain, eventually, life extension approval for the LTO from the regulatory body. So, in this paper, two points of time are considered: a) remaining design life period (L_D), i.e. 10 years, and b) life extension period (L_E), i.e. 10 more years after the remaining design life.

4.3 *Assessment of risk impact*

In this section, the CDF has been assessed using the APSA modelling developed from the standard PSA modeling and data available and with the additional data in Table 1, as described in the previous section. The conditional values have been derived as usual, e.g. as proposed in (Martorell et al., 2014), using now the APSA. In addition, the values of CDF_b and ΔCDF have been obtained using Equation 6 as proposed in section 2.3.

Tables 2 and 3 show the results for the current surveillance and maintenance policies as compared to several sensitivity analyses. In particular, Table 3 summarizes the results of a number of simulations performed in order to evaluate the risk impact of equipment ageing and testing and maintenance for the design life operation under current maintenance and testing policies (Case 1) and for the design life operation and the LTO of the NPP under alternative maintenance and/or testing policies (Case 2 to 5). Table 2 provides de CDF_b which is common for all cases.

4.4 *Analysis of risk impact*

In this section, risk assessment results are compared against acceptance guidelines in RG 1.174.

Table 2. Results of CFD_b for all cases (CDF with no ageing, current CDF).

Study (L_D;L_E;M;ε;T)	CDF_1 ($year^{-1}$)		
	Mean	5% perc.	95% perc.
Base case (10;0; 4320; 0.5; 4616)	1.03E-05	3.06E-06	2.43E-05

Couples of values {CDF_b. ΔCDF} are used to evaluate the risk impact of equipment ageing under current (Case 1) and alternative (Case 2 to 5) maintenance and testing policies. According to RG 1.174, the appropriate numerical measures to use in the comparison of the PSA results to the acceptance guidelines are mean values. Those mean values refer to the means of the probability distributions that result from the propagation of the uncertainties on the input parameters and those model uncertainties explicitly represented in the model (middle point for each couple in Figs. 1 and 2).

In this paper, two different contexts are studied. The first one corresponds to design life management (Case 1 vs 2), see results in Figure 1, and the second one focuses on a possible NPP life extension for LTO (Case 3 against 4 and 5), i.e. extended life management, see Figure 2. These contexts are explained in detail in the next sext subsections and the numerical results are shown in the Tables 2 and 3.

4.4.1 *Design life management period*

A key aspect of NPP life management in a RIDM context is to evaluate the risk impact of existing maintenance and testing programs in managing aging of systems, structures and components. The effectiveness of existing maintenance and testing practices are herein evaluated, using the proposed methodology, in terms of the risk impact of equipment ageing because of the implementation of such practices.

Table 3. Results of CFD_a and ΔCDF for each case (ageing scenario and different maintenance and testing periods).

Study (L_D;L_E;M;ε;T)	CDF_1 (year^{-1})			ΔCDF (year^{-1})		
	Mean	5% perc.	95% perc.	Mean	5% perc.	95% perc.
Case 1 (10;0;4320;0.8;4616)	1.03E-05	3.46E-06	2.43E-05	1.04E-06	4.75E-07	2.66E-06
Case 2 (10;0;2160;0.8;4616)	1.01E-05	3.70E-06	2.32E-05	8.56E-07	7.14E-07	1.61E-06
Case 3 (10;10;2160;0.8;4616)	1.05E-05	3.57E-06	2.47E-05	1.26E-06	5.89E-07	3.12E-06
Case 4 (10;10;720;0.8;4616)	1.02E-05	3.67E-06	2.33E-05	9.56E-07	6.87E-07	1.71E-06
Case 5 (10;10;2160;0.8;2160)	1.00E-05	3.38E-06	2.38E-05	7.57E-07	3.98E-07	2.25E-06

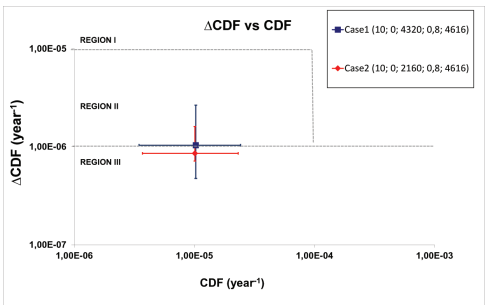


Figure 1. Couples {CDF_b. ΔCDF} of the Case1 and 2 in the context of life management considering (L_D;L_E;M;ε;T).

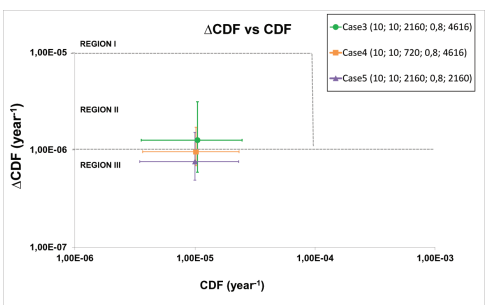


Figure 2. Couples {CDFb. ΔCDF} of the Case 3 to 5 in the context of life extension management considering (L_D;L_E;M;ε;T).

In this context, two cases have been considered, which are summarized in Figure 1. First, in Case 1, CDF_a has been calculated at the end of the design life (10 years from now) considering current maintenance and testing programs, where preventive maintenance interval equals to 4320 hours. Thus, the objective of this case is to determine the ΔCDF at the end of the design life for the current life management of this particular MOV. In Figure 1, one can realize couple {CDF_b, ΔCDF} is placed in the Region II according to RG 1.174. In this region, as established in this Regulatory Guide, improvements should be proposed in order to move the couple from this region to Region III. Therefore, it seems appropriate to implement some kind of compensatory measure for ageing management. Thus, Case 2 is considered that focuses on analysing the effect of the maintenance interval on the risk level. Consequently, the maintenance interval, M, is reduced to be 2160 hours. By repeating the calculation of the same couple for the new maintenance interval, keeping the other parameters at the same values, one can observe in Figure 1 that the new point representing Case 2 confirm that the change in the maintenance interval during its remaining design life period moves it to Region III.

4.4.2 *Extend life management period*

An important part of a PSR close to the end of the design life of the NPP should involve the evaluation of risk impact of how current equipment ageing and maintenance and testing program would jeopardize NPPs safety for the extended period. Eventually, if compensatory measures are necessary to managing ageing in an appropriate way, it should include also assessment of the effectiveness of managing equipment ageing by adopting alternative maintenance management programs and/or reformulation of current operational requirements such as surveillance requirements for the extended life period.

Case 3 to 5 have been formulated to show simple examples of the evaluations of the risk impact of MOV ageing along the extended life period under different maintenance and testing strategies. The results are represented in Figure 2. Thus, Case 3 considers the improved design life management of the MOV (Case 2) remains the same for the extended life period. For Case 3, the point {CDF_b, ΔCDF} moves to Region II again, which means that some kind of compensatory measure for ageing management would be welcome for the extended life. Two

alternatives have been considered in order to manage the ageing of the component. First alternative (Case 4) consists of a change in the preventive maintenance interval for the extended life period, which is reduced to be 720 hours from the previous 2160 hours for the design life period. Second alternative (Case 5) consist of a change in the surveillance test interval for the extended life period, which is reduced to be 2160 hours from the original 4616 hours for the design life period. Both compensatory measures move the result couple from Region II to Region III.

5 CONCLUDING REMARKS

Most NPP in Spain, which are Light Water Reactor (LWR) type, would be operating for around 40 years in approximately ten years from now, which is the plant design life, and they will face the Periodic Safety Review to obtain, eventually, life extension approval for the LTO from the regulatory body (usually for 10 more years). This PSR will require specific requirements related to evaluation of ageing, maintenance and surveillance programs for not only the design life but also for the extended life.

This paper presents new kind of Ageing PSA (APSA) modelling to be considered in the framework of the Risk Informed Decision Making according to R.G. 1.174, which is intended to be used to support risk-informed decisions on the effectiveness of asset management programs and technical specification requirements of critical equipment of Nuclear Power Plants (NPP). This APSA can help in performing the Periodic Safety Review to support risk-informed decisions required to obtain approval from the regulatory body for continuing NPP operation. This APSA incorporates not only equipment ageing but also maintenance and surveillance testing requirements explicitly into APSA models and data as compared to previous APSA.

The results obtained from the different example of application cases developed show how the risk impact of ageing depends on not only ageing of critical equipment but also on maintenance and testing practices. This way, the APSA allows addressing explicitly the role of compensatory measures in terms of improved maintenance and surveillance requirements programs in satisfying safety criteria as imposed by current NPP regulation.

The CDF evaluation has been developed using age-dependent reliability, availability and risk models and data, which allows obtaining results that are more realistic. The results are analysed in the framework of risk-informed decision-making established in RG 1.174.

Finally, this paper presents a preliminary study in which only one critical component has been considered into the APSA. Future work should consider at least all critical components and use plant-specific ageing data in order to obtain plant-specific robust results.

ACKNOWLEDGMENTS

Authors are grateful to the Spanish Ministry of Science and Innovation for the financial support of this work (Research Project ENE2010-17449 and ENE2013-45540-R) and the doctoral fellow (BES-2011-043906).

REFERENCES

International Atomic Energy Agency (IAEA), 2013. International Generic Ageing Lessons Learned (IGALL) for Nuclear Power Plants, IAEA Safety Report, DD1085, Vienna, 2013.

Kim IS., Martorell S., Vesely WE., Samanta PK. Quantitative evaluation of surveillance test intervals including test-caused risks. NUREG/ CR-5775. Washington: US NRC. 1992.

Kim IS., Martorell S., Vesely WE., Samanta PK. Risk analysis of surveillance requirements including their adverse effects. *Reliability Engineering and System Safety* 1994; 45: 225–234.

Levy I., Wreathall J., DeMoss G., Wolford. A., Collins. E.P., Jarrell. D.B. (1988). Prioritization of TIRGALEX recommended components for further ageing research. NUREG/CR-5248. Washington. DC: US NRC.

Martorell S., Sanchez A., Serradell V. Age-dependent reliability model considering effects of maintenance and working conditions. *Reliability Engineering and System Safety* 1999; 64: 19–31.

Martorell S., Villamizar M., Marton I., Sanchez A., Carlos S., Villanueva J.F. Evaluation of risk impact of changes to surveillance requirements addressing model and parameter uncertainties. *Reliability Engineering and System Safety* 2014; 126:153–165.

Nitoi, M., Rodionov A. Guideline for Selection of Systems, Structures and Components to Be Considered in Ageing PSA, JRC IE Report, EUR 24503 EN, doi:10.2790/21975, Petten, Netherlands, 2010.

Sanchez A., Carlos S., Martorell S., Villanueva J.F. Addressing imperfect maintenance modelling uncertainty in unavailability and cost based optimization. *Reliability Engineering and System Safety* 2009; 94 (1): 22–32.

U.S. Nuclear Regulatory Commission. An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities. RG 1.174. Revision 2. Washington DC, 2011.

U.S. Nuclear Regulatory Commission. Nuclear Plant Aging Research (NPAR) Program Plan, NUREG-1144, US NRC, Washington, D.C, 1991.

U.S. Nuclear Regulatory Commission. Approaches for Age-Dependent Probabilistic Safety Assessments with Emphasis on Prioritization and Sensitivity Studies. NUREG/CR-5587. SAIC-92/1137. Washington DC, 1992.

U.S. Nuclear Regulatory Commission. Generic Aging Lessons Learned (GALL) Report, NUREG-1801 U.SNRC, 2001.

Vesely W.E., Kurth R.E., Scalzo S.M. Evaluations of core melt frequency effects due to component ageing and maintenance. NUREG/CR-5510. Washington. DC: USNRC, 1990.

Volkanovsky A. Method for assessment of ageing based on PSA results, *Nuclear Engineering and Design* 2012; 246: 141–146.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safety of the new control command European System

M. Siergiejczyk
Faculty of Transport, Warsaw Technical University, Warsaw, Poland

M. Pawlik & S. Gago
Warsaw Railway Institute, Warsaw, Poland

ABSTRACT: Radio-communication as a transmission media for the railway control command systems has to ensure appropriate safety and reliability. Lowering transmission safety and reliability cause whole system safety lowering. European Train Control System (ETCS) which is a modern control command systems is currently being installed on many railway lines in Europe and in many countries outside Europe. ETCS can be installed in two basic configurations—ETCS level 1. and ETCS level 2. ETCS level 2 use railway mobile radio-communication (GSM-R) as a basic transmission media for transmission of the Movement Authorities which define limits for safety movements of the trains (ETCS). Therefore RAMS of ETCS and of the GSM-R are crucial for safety of the railway transportation. However RAMS requirements for ETCS are defined (UIS 1998) while RAMS requirements for GSM-R are practically not defined. Transposing ETCS RAMS requirements to GSM-R is possible only partly.

As a result we are facing necessity to define GSM-R RAMS requirements which will be taken into account during ETCS installation and commissioning. This article analyse associated challenges taking into account implementation possibilities as well as their influence on construction and exploitation of the GSM-R layers. Article includes also proposed solutions to be taken into account during installation and exploitation which are seen as appropriate by authors.

1 INTRODUCTION

GSM-R digital networks are used by many European and non-European railway infrastructure managers and corresponding railway undertaking. The underlying concept of the International Railway Association UIC (French abbreviation *Union Internationale des Chemins de fer*) was to ensure uniform European communication system based on the results of the collective dedicated project named EIRENE (*European Integrated Railway radio Enhanced Network*) (International 2006, UIC 1998). Implementation of the GSM-R communication system ensures calculable financial results for railway transport as a whole transport system (Pawlik 2007). Railway lines capacity is growing, border disruptions between railway systems of the neighbouring countries is lowering—additional traction units and additional tracks for shunting disappear, necessity of the different drives and different equipment in traction units is strongly minimised and as a result time needed to pass borders is limited significantly (Sameni 2012). Border disruptions starts to be comparable with other transport media. Additionally railway undertaking gain unified transmission media which can be used e.g. for transport monitoring or failures quick detection.

GSM-R is a mobile digital cellular phone system which is based on public GSM however offers wider range of functionalities. Its infrastructure namely transmission antennas are situated along the railway lines. In some cases GSM-R is crucial for the railway traffic control command solutions. Precisely the *European Rail Traffic Management System* (ERTMS) comprising:

- *European Train Control System* (ETCS) which is a modern control command systems ensuring transmission and collection of the crucial data relating to the train running like running speed, position, running mode, etc.,
- *Global System for Mobile Communication—Rail* (GSM-R) which is as a basic transmission media for ETCS in one of its basic configurations named ETCS level 2 passing Movement Authorities which define limits for safe movements of the trains.

superior significantly vitality of the GSM-R as a safe transmission provider (Pawlik 2010).

Trains due to extremely big masses (up to over 3 000 tones) and relatively high speeds (up to over 200 km/h) gain high kinetic energy having at the same time adhesive coefficient about eight times lower than road vehicles. As a result braking distance for trains are long and each accident appearing inconsiderable may cause catastrophic consequences (Pawlik 2010). This is why railway movements are regulated by signalling systems ensuring meeting following safety related functionalities:

- keeping safe distances between trains running on the tracks between stations—train spacing management,
- preventing setting conflicting train routs for the trains running in to and out from the stations—train routing management,
- locking of the mobile elements of the switches for entire train in correct positions—preventing derailments caused by switch movements under trains,
- protection of the level crossings constituting by the roads and railway lines one level—ensuring automatic level crossing protection as well as putting appropriate signs on the rail and road side,
- enabling safe incorporation of additional trains from the branches, sidings, industrial tracks etc. without creating disturbances—train movement start-up procedures.

Pointed functionalities require trackside as well as on-board (mobile) equipment which should be analysed separately. This article is focusing on the GSM-R trackside safety challenges taking into account applicable specific conditions.

2 STATE OF THE ART ARCHITECTURE AND FUNCTIONALITIES

Presently all ERTMS considerations related to both ETCS level 1 and ETCS level 2 assume independency of ETCS and GSM-R. It can be seen not only in technical document but even in legal resolutions of the European Community up to independent verifications of conformity with European requirements.

The safety of the ETCS system is defined in (UIS 1998) by respective level (SIL4 as defined in EN 50 129). Safety of the GSM-R system is not defined by documents. The same situation take place for all RAMS requirements. As a result it is not possible to verify directly whether transmission is adequate from the safety point of view or require undertaking special additional means by enhancing reliability and availability (Pawlik 2013). Whereas safety is a must, high reliability and availability are very important as means supporting safety and not directly by themselves. Therefore reliability and availability have to be analysed also from the operational and economical point of view (Anderson 2013). Such analyse requires understanding of the architecture, functionalities and data transmission principles.

2.1 *GSM-R architecture*

Depending on the railway line GSM-R ensures voice and/or data transmission using cellular digital mobile system. BTS base stations along the railway lines as well as architecture of the connectivity are function dependent—transmission safety, reliability, availability—voice, data transmission. As a result locations of the BTS base stations as well as connectivity principle have to be determined line by line taking into account class and purpose of the line, required capacity and required safety measures (Pawlik 2007).

GSM-R is based on phase 2 of the public GSM, including both GSM basic functions and GSM 2+ additional services (broadcasting, group calls, GPRS, priority calls).

2.2 *GSM-R basic functionalities—voice*

GSM-R offers for the railway infrastructure managers and railway undertakings following services and functionalities:

- VBS (*Voice Broadcast Service*)—voice information is transposed to many predefined users which cannot answer. Predefined groups can be modified automatically depending on time or manually in emergency,
- VGCS (*Voice Group Call Service*)—voice information is transposed bi-directionally with many predefined users which can answer. Every user can activate and dis-activate its own participation in information exchange. Teleconference ends on initiator request or system dispatcher or by barren time limit which is predefined on SIM card,
- eMLPP (*enhanced Multi-Level Precedence and Preemption*)—priority is given to limited number of users ensuring quick voice information exchange in emergency situations. Call setting time for priority calls has to be below 2 seconds including disconnecting of the on-going calls (International 2006),
- FA (*Functional Addressing*)—numbers are given to railway employees based on their operational functions instead of using terminal numbers Operational functional numbers are given by

local leading station or by dispatcher dedicated authorised to define, change and delete numbers linked to certain terminals,
- LDA (*Location Dependent Addressing*)—voice communication with railway employees fulfilling certain operational functions which is changing in relation to train localisation or dedicated calling area. Location is mainly defined by cellular identity however to ensure better location dependent addressing additional information can be used as on-board localisation systems, trackside information e.g. from ETCS balises or other fixed installation,
- GPRS (*General Packet Radio Service*)—is intended for ETCS track-train transmission of vital data in at large stations and density areas,
- eREC (*enhanced Railway Emergency Call*)—emergency calls for train drivers, dispatchers and other dedicated crucial personnel in critical situations which require suspend of the operation in certain area or undertaking other action. Railway Emergency Call for trains must be delivered to all train drivers and all respective dispatchers.

2.3 *GSM-R additional functionalities—data*

GSM-R also ensures data exchange for:

- track-train data communication which to ensures correct functioning of the control command and signalling systems. For instance for ETCS to ensure safe communication between Radio block Centre and on-board main vital computing equipment,
- transmission of informative text messages as well as text messages which require driver confirmation. Lack of confirmation automatically causes train braking,
- transmission of data in other applications for railway operation e.g. supervision of train movements to support logistic chains and networks, collection of trackside and on-board diagnostic data to lower maintenance costs and for passengers e.g. ensuring accessibility of time schedules and connections of the trains, weather predictions, possibly internet based on package GPRS or EDGE transmission,
- fax data transmission.
- Both track-train data for control command and text messages can be send point-point as well as using broadcasting functionality.

As all other telecommunication systems GSM-R has to ensure data transmission in predefined time and predefined error rate. Both must be adequate to required high safety and high reliability in the railway environment. This is crucial for infrastructure managers and railway undertaking as it influences directly safety and fluid traffic flow.

3 GSM-R SAFETY

3.1 *GSM-R safety related transmission*

Increasing safety is ensured by using for GSM-R frequency band other than for public GSM. Railway dedicated GSM-R works in the band 876–880 MHz (uplink) and 921–925 MHz (downlink), while public GSM works in the band 890–915 MHz and 935–960 MHz ensuring safe band independency. Additional increase of data transmission reliability is ensured by appropriate radio coverage along railway lines which depend on train speeds. For line speeds below 220 km/h (train speeds below line speed) radio coverage has to be equal or higher than –95 dBm. For line speeds over 280 km/h (train speeds below line speed) radio coverage has to be equal or higher than −92 dBm. Radio coverage for lines with only voice transmission is lowered by 3 dB. Lines should be covered with those radio coverage with probability equal or higher than 95% on each 100 meters of the railway line, while handover between neighbouring cellular areas should be achieved in normal conditions not less than 99,5%.

Additional important parameter which shows GSM-R operating correctness is the Quality of Service (QoS) which is composed by probability of the incorrect connections, data transmission delays, limited jiter and predefined failure rates (European 2005).

3.2 *GSM-R safety related architecture*

Telecommunication safety is a set of procedures and processes which ensure high availability and reliability due to appropriate system structure namely by redundancies and fail-safe transmission backbone. GSM-R architecture must be designed in a way ensuring minimising operational disruptions in case of failures of one or many elements. Serious damage (disaster) of the GSM-R means interruption of service on entire network which last longer than predefined maximal recovery time. That requires procedures and processes ensuring *Disaster Recovery.* Those processes and procedures together with resetting of the applications, data, equipment and transmission compose overall plan ensuring continues operation. Such plan is based on scenarios which assume failures of the components. Base on scenarios bottlenecks in safe system operation are being find and can be mitigated (Siergiejczyk 2012). Most common and popular way to enhance safety, reliability and availability is adding redundancies both in relation to data and in relation to equipment which can be multiplied base on different principles e.g. n+1, 1+1, 1:n (Siergiejczyk 2013). Operation

of such elements can assume hot or cold reserve. Redundancy may affect:

– whole system,
– some subsystems e.g. BSS, NSS, OMC,
– some elements e.g. MSC, HLR, VLR,
– some components e.g. processing boards known as internal redundancy.

Recovery time depend on configuration and complexity of the network. For GSM-R it always below four hours, however building new NSS may need even some months.

UIC documents (International 2006, International 2006, UIC 1998) suggest doubling radio coverage for lines equipped with ETCS level 2 by doubling BTS base stations (collocated or alternated) and appropriate construction of the BSS (redundant BSC base stations controllers which are also connected to different MSCs). More redundancies mean higher system cost and to some extend lower disturbances of operation however switching times have to be taken into account.

Redundancy is also important in fixed transmission systems. Using self-recovering structures SDH, ensuring double optical cables constitute important elements influencing GSM-R safety and reliability. It is described in details by 'L. Pushparatnam—T. Taylor GSM-R Implementation and Procurement Guide 15.03.2009 Paris' (Pushpartnam 2009) which as an example in point 6.6.3.5 states *'For information and only as an example, here below we are presenting as a return of experience in the case of an operational network—the availability* figures *for 2008, kindly offered by ProRail:*

Overall network availability: 99, 97%
Dispatcher systems availability: 99, 91%
GSM-R for ETCS network availability: 99,999%

According this document safety of the GSM-R cannot be defined by SIL4 as definition of 'critical failure' depends on line (long, short, high speed, suburban dens traffic).

Document UIC ERTMS Users Group dated 30/09/98 „ERTMS/ETCS RAMS Requirements Specification Chapter 2—RAM" (UIC 1998) ETCS hardware availability under certain conditions was calculated on the level of A = 0,99985. Italian railways (RFI) assumed for ERTMS availability calculations for high speed network the same availability for ETCS and GSM-R (together with trackside transmission):

$$A_{ERTMS} = A_{ETCS} \cap \cdot A_{GSMR} \quad (1)$$

As a result un-accessibility of the GSM-R in a year is about 79 minutes. In theoretical calculations (Ding 2010), assuming certain availability of the GSM-R subsystems (NSS, BSS, transmission system (optical cables and SDH equipment) and different configurations received un-accessibility times are:

– for single equipment (NSS, BSS) availability 99,962386% un-accessibility time 198 min/year,
– doubled equipment (NSS, BSS) availability 99,999945% un-accessibility time 0,29 min/year.

Base on this calculations it has to be assumed that un-accessibility 79 min/year cannot be reached with single GSM-R equipment (NSS and BSS).

It has to be pointed in recapitulation that direct data regarding availability and un-accessibility of the GSM-R are not available. 'Annex A to the Commission Decision dated 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system (2012/88/UE)' specification defining reliability and availability requirements has status 'reserved' which shows that European Commission see the need for such requirements but it is still not available.

4 PRESENT GSM-R SAFETY ASSURANCE

In the 'GSM-R Implementation and Procurement Guide' (Pushparatnam 2009) chapter 6.5.3.2 points that However, several of the railways of the Member States, as well as the UIC Safety Committee have stated that the GSM-R system itself does not possess any safety requirements. The basis of this assertion is as follows:

– telecommunications services are used to support safety-related railway applications. However, safety is assured by means of applications external to the telecommunications bearer, or by means of operational procedures. Telecommunications are simply used as a non-safety-related bearer service;
– in order to ensure adequate safety of those applications which use telecommunications services, the telecommunications systems themselves have certain dependability requirements (in terms of reliability, availability and maintainability) but no specific safety requirements as such;
– the GSM-R system is no exception to this rule. It has no specific safety requirements and need not therefore be associated with a specific Safety Integrity Level (SIL);
– certification will however be required for certain GSM-R system elements. For example:
– compliance with ETSI norms, assurance of transmission and frequency aspects, health and safety of individual persons, etc;
– certification of railway-specific elements such as EMC, interoperable functions, ability to be used in a railway environment and supplementary national functions. Certification requirements

are likely to be identified either by European Norms (CENELEC, CEN) or by UIC rules (UIC leaflet 751-4 etc).

5 NEW PROPOSED GSM-R SAFETY ASSURANCE

We do not agree with some of the above arguments. Ascertain putting practically equal sign between requirements for public GSM and railway dedicated GSM-R is not acceptable due to vital role of GSM-R in the ERTMS system. GSM-R system has to ensure:

- transmission of safety related data for ETCS namely movement authorities defining speed and distance limitations which can be used by trains for safe movements,
- vital generating and vital receiving railway emergency calls REC,
- redundant architecture as suggested in UIC documents (International 2006, UIC 1998, Pawlik 2007) (double radio coverage, double NSS). This principle is used for GSM-R In contradiction public GSM networks do not have such suggestions and public operator using 100% redundant network is hard to find.

In the 'GSM-R Implementation and Procurement Guide' (Pushparatnam 2009) chapter 6.5.3.3 states 'In order to interpret the assertion that no safety requirements are to be placed upon GSM-R, it is important for each railway to identify exactly which applications are being referred to. In particular:

- there are many applications external to GSM-R (e.g. ETCS) which will make use of GSM-R as a bearer service;
- there are also several applications internal to GSM-R (e.g. railway emergency calls, driver-controller calls, DSD messages) which are provided by the GSM-R telecommunications service and which use a GSM network as a radio bearer.'

Therefore it is understandable why there are no safety requirements for GSM-R and at the same time puts obligation to keep above mentioned radio coverage level in relation to line speed ensuring probability equal or higher than 95% on each 100 meters of the railway line. It can be expressed by following notation:

$$L_z = \sum_{i=1}^{n} lz \leq 5\ m \tag{2}$$

where:

Lz—sum of the length of the sections with reduced radio coverage,

l_z—length of the i-ted section with reduced radio coverage.

Length of the "radio hole" in GSM-R which can cause transmission errors for ETCS is 5 m.[1]

Time (T)during which radio-modem is in the "radio hole" depends on the length of the hole (lz) *and from speed of the traction unit* (v).

$$T = \frac{lz}{v} \tag{3}$$

As an example time when radio-modem is in a hole when train is moving with the speed of 250 km/h and the hole length is 5 m is 72 ms (in a hole of 01 m—1,44 ms)[2].

Document (European 2005) states that in normal operational conditions overall time used for single data transmission between interlocking and ETCS on-board via Radio Block Centre (RBC) on high speed lines is about 4 s.

Taking that into account together with other above statements it is questionable why many documents suggest multiplying GSM-R infrastructure to ensure high redundancy. A simple answer is that redundancies increase safety, reliability and availability of the GSM-R. Unfortunately basic data are not available and have to be determined by infrastructure managers.

In accordance with 'Commission Decision dated 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system (2012/88/UE) chapter 2.3' "a train equipped with Class A on-board train protection for level 1 need not be equipped with a GSM-R data radio but must already implement all level 2 functions so as to ensure that the mere connection of a GSM-R data radio at a later stage will ensure it is equipped for level 2". Therefore it can be assumed that:

- ETCS level 1 can be seen as a solution for transition period,
- GSM-R trackside should be constructed in configurations enabling future operation of the ETCS level 2,
- ETCS level 1 can operate with analogue voice communication systems VHF,
- ETCS level 2 cannot operate without GSM-R therefore ETCS level 2/3 constitute with GSM-R integrated system named ERTMS,
- it has to be analysed whether GSM-R and ETCS are independent or dependent from reliability and availability point of view. For this

[1]That requires measurement samples collected every 10 cm (some countries are using 7,5 cm or even 4 cm).

[2]In accordance with above equation when l_z *is constant* and $v \to 0$ in result $T \to \infty$; longer time means higher probability of the failure causing emergency braking (e.g. data transmission long lack) causing possibly derivative train stopping in a radio hole.

article it is assumed that GSM-R and ETCS are independent as ETCS failure do not influence GSM-R operation and GSM-R failure influences ETCS operation however it can be neglected.

As a result relation between ETCS and GSM-R in ERTMS can be noted as following:

$$\text{ERTMS} = \text{ETCS} \cap \text{GSM-R} \tag{4}$$

Future analyse will be done with most restrictive requirements for GSM-R system namely for data transmission services, which are used for the safe rail transport management based on ETCS level 2/3. For other GSM-R services e.g. *Voice* reliability and availability requirements are less restrictive. GSM-R system has a network character both hardware and software dimension (Network-Centric Systems) and therefore traditional equation is:

$$A = \frac{MBTF}{MBTF + MTTR} \tag{5}$$

which for availability of GSM-R means masking of system reliability. Systems with high availability can be very reliable—especially regarding software errors e.g. system standstills or bags which are removed by diagnostic and watchdog programs. Additionally as a result of internal redundancy time needed for failure removal can be very short—counted in miliseconds or a few seconds. Some publications expression "reliability" for hardware-software systems should be possibly replaced by expression "dependability", which is better defines states of such systems.

GSM-R system infrastructure is composed from a few subsystems e.g. BSS, NSS OMC etc. Failures within some subsystem do not influence safety of the rail traffic.

Incidents which can happen in GSM-R system can be subdivided in following groups:

– critical e.g. losing data transmission,
– important e.g. losing redundancy, keeping data transmission,
– less important e.g. opening BTS base station door without authorisation, keeping data transmission.

Moreover incidents may happen presently and in the future in different places influencing big areas or limited areas, for instance:

– losing data transmission in NSS subsystem cause failure in the whole area covered by such NSS (practically on all railway lines which are served by such NSS),
– losing data transmission in BSC base stations controller do not cause negative consequences on lines which are served by other controllers,
– losing data transmission in BTS base station cause negative consequences only on the area served by this basic transmission station (practically on about 7 km of the railway line) and only if at the same time there is a train at this section (terminal EDOR).

GSM-R system dependability depends mainly from critical failures e.g. long lack of data transmission which can possibly cause emergency braking. In case of BTS base stations the length of the time window with failure is also important. Probability of critical failure on the section served by basic station is a function of the time the train is on such section, time window with failure and frequency and length of the telegrams which are exchanged.

$$P_{ki} = f(t_p, t_o) = f(v_t, l_c, t_o, \omega, w) \tag{6}$$

where:
t_p—time window when train is in single cellular area
t_o—failure time
v_t—train sped
l_c—length of the single cellular area
ω—frequency of telegrams exchange between $\text{ETCS}_{\text{trackside}}$ and $\text{ETCS}_{\text{on-board}}$
w—length of the telegrams in bits

According ETCS SRS recommendations frequency of telegrams exchange by ETCS is between 1 and 255 seconds while the length of the telegrams are up to 960 bits. Therefore time when the train is in the area served by one BTS base station can be expressed as:

$$t_p = l_c / v_t \tag{7}$$

Time when all the trains are in the time unit in the area served by one BTS base station can be expressed as:

$$T_o = \sum_1^n \frac{1}{v} \tag{8}$$

where:
T_o—time window when trains are in single BTS base station area
n—number of trains in time window
l—length of the railway line served by chosen BTS base station area
v—train speed in chosen BTS base station area

Assuming that basic station is serving 7 km long section of the railway line and the speed of the trains is 250 km/h, we can calculate time window when the train is in single cellular area

as a bit over 100 s. As a result on a line with 30 pars of trains daily within one basic station all the trains together will remain cumulatively 6000s which is around 7% of the day, which means that 93% of time even critical failures in a BTS base stations may have no influence on railway traffic safety. This means also that MTBF is composed by two elements which are: system working time and system readiness time and therefore availability of the BTS base station can be expressed as:

$$A = \frac{Operating\ Time + Operable\ Time}{Operating\ Time + Operable\ Time + Downtime} \quad (9)$$

When failure occurs within sending or receiving of the telegram from Radio Block Centre to the train or vice versa and last long enough to cause losing data transmission between RBC and train it leads up to train emergency brake. As shown on the Figure 1. below such transmission is additionally protected by Euroradio coding/decoding layer separately operating trackside and on-board. If as a result of a failure time window without data transmission is short enough that it does not cause emergency brake of the train then ETCS does not see lack of data transmission. Re-establishing connection means first synchronization of the equipment and then data transmission related to safe train traffic management reaching speed appropriate for the section (energy losing and train delay as braking is more intense e.g. 0,5 m/s^2 than acceleration e.g. only 0,3 m/s^2).

Similar analyse should be done for BSC base stations controller. In practice BSC base stations have big hardware and software redundancy and their reliability is at least on the level of 99,999% (BSC base stations controller unavailability is at average 3 min per year).

Similar analyse should also be done for other subsystems of the GSM-R system taking into account:

– dimension of the influence area,
– time for removing critical errors,
– failure mischievousness and
– influence from occurrence of fires, lightning, floods, etc.,

for the working dependability of a whole GSM-R system.

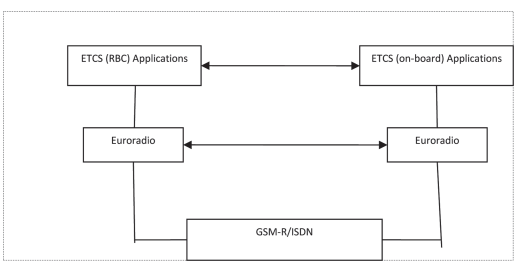


Figure 1. Communication between ETCS trackside and on-boars equipment (Europen 2005).

6 CONCLUSIONS

Findings show that practically:

– GSM-R voice transmission is not critical for ERTMS safety, reliability and availability while data transmission is critical,
– redundancies within BSS subsystem as well as multiplying whole BSS are inefficient and therefore economically questionable however technically possible,
– redundancies within NSS subsystem as well as multiplying whole NSS significantly influences GSM-R and ERTMS safety, reliability and availability. NSS installations are serving large areas and therefore both fate and regular failures may affect railway transport even of a whole country. Therefore NSS subsystem strongly requires redundancies. Proposed solution is a whole subsystem redundancy 1+1 composed by whole set of equipment located in two different cities powered by different large area public power stations.
– Necessity for following works:
– It is necessary to elaborate mathematical model verifying independency assumption ERTMS = ETCS ∩ GSM-R,
– GSM-R Safety, reliability and availability should be defined by countable values,
– It is necessary to define 'critical failure' including time correlation between failure and train location,
– Dedicated analyse has to be done to find how long time trains can be in radio hole without effective influence on train running safety.

REFERENCES

Anderson D.J. Brown T.J. Carter C.M.: System of Systems Operational Availability Modelling, Sandia National Laboratories, October, 2013.

Ding Xun, Chen Xin, Jiang Wenyi: The Analysis of Gsm-R Redundant Network and Reliability Models on High-speed Railway. 2010 International Conference on Electronics and Information Engineering (ICEIE 2010). Kyoto, Japan 2010.

ETCS System Requirements Specification version 2.3.0.d.

European Economic Interest Group-European Rail Traffic Management System 04E117 ETCS/GSM-R Quality of Service—Operational Analysis, date:14/10/05.

International Union of Railways, Project EIRENE—Functional Requirements Specification, 2006.
International Union of Railways, Project EIRENE—System Requirements Specification, 2006.
Pawlik M. Bezpieczeństwo ruchu kolejowego w legislacji unijnej, Technika Sterowania Ruchem, 4/2007, Warszawa 2007.
Pawlik M. Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS. Technika Transportu Szynowego 1/2007.
Pawlik M. Zarządzanie ryzykiem w transporcie kolejowym, Technika Transportu Szynowego 9/2013, Warszawa 2013.
Pawlik M. Żurkowski A.: Ruch i przewozy kolejowe. Sterowanie ruchem; KOW, Warszawa 2010.
Pushparatnam L. Taylor T.: GSM-R Implementation and Procurement Guide V 1.0 15.03.2009, UIC ISBN 978-2-7461-1631-3.
Sameni M.K. Railway Track Capacity: Measuring and Managing University of Southampton Faculty of Engineering and the Environment Transportation Research Group; Thesis for the degree of Doctor of Philosophy October 2012.
Siergiejczyk M. Gago S.: Zagadnienia bezpieczeństwa systemu GSM-R w aspekcie wspomagania transportu kolejowego. Logistyka Nr. 6/2012. Wyd. ILiM, Poznań 2012.
Siergiejczyk M. Gago S.: Problemy zapewnienia bezpieczeństwa informacyjnego w sieci GSM-R, Konferencja Transport XXIw. Ryn wrzesień 2013r.
UIC ERTMS Users Group, 30/09/98 „ERTMS/ETCS RAMS Requirements Specification"

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

All swept up: An initial classification of NSA surveillance technology

M. Cayford, C. van Gulijk & P.H.A.J.M. van Gelder
Delft University of Technology, Delft, The Netherlands

ABSTRACT: The study was initiated as part of the FP7 SURVEILLE project commissioned by the European Commission. The goal is to examine the mass surveillance technology used by the NSA in the programs revealed by the Snowden leaks. This paper forms the basis from which to study the effectiveness of these surveillance technologies. Novelty: While there have been a lot of headlines regarding what the NSA is purportedly doing, discussion of the technology used to do this is scarce to nonexistent. There is also the problem of different programs being revealed via different media sources, thus making it difficult to know and follow the information being revealed regarding NSA programs. This paper attempts to bring the NSA programs and methods into one place, categorize those that are similar, and analyze the probable surveillance systems used. Relevance: This work is the beginning of developing a method of evaluating the effectiveness of surveillance technologies, the lack of which is notable in government oversight mechanisms. Methods and findings: The methods for this research begin with a review and analysis of the leaked NSA information and documents. Further, a study of articles delving deeper into the NSA programs is conducted. Lastly, the research focuses on a technical understanding of the technology involved through readings and interviews with experts. It is found that these numerous programs can be classified in a few categories of surveillance technology. This initial study forms for the basis for evaluation of the effectiveness of these technologies.

1 INTRODUCTION

Many types of surveillance (phone tapping, collecting metadata, intercepting mail) used by the NSA are not new to the world of espionage. What is new in surveillance, thanks to huge advances in technology, is mass surveillance. In the digital age in which everyone's communication and information is stored and transmitted online it is now possible to gather massive amounts of information rather easily. What formerly would have required a laborious process of monitoring physical mail, tracking targets' movements, and entering homes or offices to gain information about a target's activities, contacts, financial information, etc., can now be done largely by monitoring their online activity. And in a post-9/11 era where terrorism is a primary concern of governments, all this information can be swept up not just about one person, but about thousands, potentially even everyone, in the event that this information may prove useful later, and in the interest of identifying and apprehending terrorists before they are able to act.

The objective of this paper is to gather information about technical systems that the NSA uses to perform mass surveillance to be able to later analyze their effectiveness to determine to what extent and at what cost these systems achieve their objectives as stated by the NSA. The analysis was performed from the perspective of risk control. That is to say, the assessment focuses on an integral analysis of the system rather than on computer science aspects.

This paper will provide an initial classification of NSA surveillance technologies as they have been revealed in the recent Snowden leaks. The classification aims to group the technology behind the confusing array of NSA operations and programs, and to rate it on a scale of mass to targeted surveillance. The following surveillance technology categories are examined: wiretaps (2.1), PRISM (2.2), decryption (2.3), exploitation (2.4), analysis tools and databases (2.5). We then classify these technologies as they relate to mass or targeted surveillance (3).

Two factors have influenced our research. One is that what kind of surveillance technology the NSA uses and how it works is all classified information. Therefore much of our examination and explanation is educated guessing based on recent leaks, previous revelations, and an understanding of what methods and devices are available. Secondly, the stories on the Snowden leaks have been published in a multitude of media sources in various countries. This renders it more difficult to gather pertinent information into a meaningful ensemble. Further, these leaks continue and information on these systems may consequently change. There-

fore these are initial steps to understand NSA surveillance technology and will be updated and improved as necessary.

2 NSA SURVEILLANCE TECHNOLOGIES

2.1 *Wiretaps*

Wiretaps on fiber-optic cables are likely the means by which the NSA accesses and captures vast amounts of internet data. This would provide the basis for it to analyze and map the information, identify specific targets, and deploy malware attacks. The conclusion that the NSA is tapping fiber-optic cables is based on three things: 1) According to an NSA slide, "Upstream" is "the collection of communications on fiber cables and infrastructure as data flows past." 2) The GCHQ operation TEMPORA is known to be tapping into fiber-optic cables and to be working with the following telecom companies: BT, Verizon Business, Vodafone Cable, Global Crossing, Level 3, Viatel, and Interoute. (Ball et al. 2013) 3) A 2006 court case against AT&T, which disclosed that the NSA was wire-tapping fiber-optic cables at AT&T's internet exchange point in San Francisco.

2.1.1 *Fiber-optic cables*

Fiber-optic cables carry the world's communications across the globe. More than 550,000 miles of these undersea cables connect our world, (Fulghum 2010) carrying 99 percent of the world's intercontinental data (Timberg & Nakashima 2013).

Standard fiber-optic cables over land consist of 144 individual glass fibers; those undersea consist of only 8 individual glass fibers. Each fiber carries 40–160 light wave signals and each of these signals handles 10–40 gigabits of traffic. (Fulghum 2010) The data is turned into "ultra-short flashes of light. These flashes represent the zeros and ones that all digital information is comprised of. A photodiode at the end of the cable turns the light flashes back into electrical signals." (Schmidt 2013) The signals, however, have to be re-amplified with a regenerator about every 80 kilometers otherwise they will drop. Each fiber optic has to be to re-amplified separately, so the fiber optics must be laid out separately rather than bundled together. If a cable was to be secretly tapped this is the weak point at which it could be more easily done (Schmidt 2013).

2.1.2 *Fiber-optic splitters*

An even easier way to tap fiber-optic cables is to have the consent of the telecommunications company to split the wires. This was the case with AT&T—the company allowed the NSA to tap its cables.

To intercept AT&T's signal at 611 Folsom St. in San Francisco, the NSA installed splitters. A splitter is a piece of equipment that physically splits the cable and sends the signal in two different directions. The simplest form of splitter is a "T" which has one signal coming in and two signals going out. The NSA splitters used in this case were 50/50 splitters—of the signal that came in, 50% of it went out one fiber and 50% went out the other. This does not refer to 50% of the data, but to 50% of the signal. That is, the signal is split in half, making it weaker, but 100% of the data is sent through each of the two signals. Essentially this means that a copy of the data is being made. The data is then sent on its way to its original destination through one signal, and a copy of this data is sent into another cable owned and operated by the NSA. (See Fig. 1.)

Effectively, these splitters were installed at an Internet Exchange Point. At the San Francisco facility AT&T exchanged internet traffic with 16 companies with which it had peering arrangements. The splitters diverted traffic related to AT&T's Common Backbone, the network that provides internet access (as opposed to telephone traffic). It is believed that all, or substantially all of AT&T's peering traffic was diverted through the splitters, but that its own traffic was not. The splitters were placed on the fiber-optic cables belonging to these 16 ISPs before they reached the AT&T Common Backbone. Thus, their traffic was copied, but AT&T's own traffic was not (Marcus 2006).

2.1.3 *Deep packet inspection*

After passing through the splitters, the copied data was sent into a secure room at the San Francisco facility where it was processed by Narus equipment.

Narus is Deep Packet Inspection (DPI) technology. DPI is the inspection and analysis of internet traffic in real time. It extracts basic protocol information, such as source and destination IP

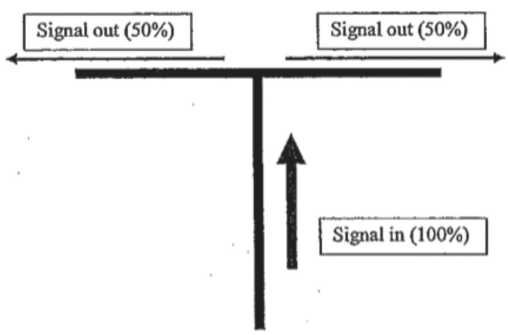


Figure 1. 50/50 splitter (Source: *Declaration of J. Scott Marcus*, p. 13).

addresses, as well as the deeper layers of the traffic, which consist of the actual content of the traffic.

DPI was designed by engineers for Internet Service Providers (ISPs) to optimize their networks. "The primary technical capability underlying DPI is the ability to recognize. DPI has been developed to detect, for example, applications, protocols, media content, viruses or data in a specific format, such as credit card numbers." (Asghari et al. 2012) Once data is recognized the ISP can manipulate it, for example, by blocking or prioritizing certain traffic. It can also carry out notification actions, such as "generating reports, alarms or billing incidents." (Asghari et al. 2012) Using DPI, ISPs can prioritize applications like VoIP to improve service or identify illegal downloads. In other words, ISPs use DPI to look at the internet activity of their customers and act upon it.

The Narus system at the AT&T San Francisco facility consisted of two parts—the Narus Semantic Traffic Analyzer (STA) 6400 and the Narus Logic Server. Part one of the system—the STA 6400—monitors data packets for metadata that matches "key pairs," such as "a specific IP address or a range of IP addresses, a keyword within a Web browser request, or a pattern identifying a certain type of traffic such as a VPN or Tor connection." (Gallagher 2013) The matching packets are put into the second part of the system, the Narus Logic Server. This second part consists of analytic processing systems that re-assemble the network sessions of the matching packets, mine them for "metadata, file attachments, and other application data" then index and deposit the data into a database. (Gallagher 2013) Narus is capable of processing huge volumes of data and of storing the traffic that it captures.

The amount of internet traffic that Narus can handle monitoring is directly related to how many rules have been loaded into the machine watching the metadata flow past (part 1 of the system). The more rules, or pre-configured filters, turned on, "the more compute power burned and memory consumed per packet, and the fewer packets that can be handled simultaneously." (Gallagher 2013) In the Narus system, if all the pre-configured filters are turned on then the system can monitor 12 gigabits out of 20 (on a two-way 10 gigabit Ethernet connection). To make the system more efficient and able to monitor more of the 20 gigabits flowing past, some of these filters have to be turned off. "In other words, to handle really big volumes of data and not miss anything with a traffic analyzer, you have to widen the scope of what you collect" (Gallagher 2013).

Also present at the AT&T facility was what was referred to as the "SG3 backbone." This was a private backbone network, separate from AT&T's backbone. It was believed that this indicated that after the Narus equipment collected and processed data of interest, the data was sent via the SG3 backbone to central locations for further analysis. (Marcus 2006).

2.1.4 *Possible additional locations of NSA splitters*

AT&T staff revealed that besides San Francisco, NSA surveillance sites also existed in Atlanta, Los Angeles, San Diego, San Jose, and Seattle. Using criteria based on the assumption that the NSA would want to intercept the most data with the fewest number of splitter sites, researchers at the University of Toronto have identified another 12 cities that likely host NSA splitters. Of 1,319 U.S.-only internet data traffic routes in the researchers' database, only seven did not pass through one of these 18 cities suspected to have NSA surveillance sites. That means that with splitters at these locations the NSA could intercept 99% of U.S.-only traceroutes (Clement 2013).

2.1.5 *Concluding remarks on fiber-optic cable tapping*

The splitters at the AT&T San Francisco location were never known to be removed. The aforementioned NSA "Upstream" slide mentions several code names in relation to the Upstream program—FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR. These code names reportedly refer to specific telecommunications companies such as A&T. (Cohn 2013) It seems likely that the NSA surveillance technology being employed in Upstream are splitters placed on the fiber-optic cables along with DPI technology. The program, MUSCULAR, in which the NSA exploits the data links connecting Yahoo and Google data centers, could also be using splitters and DPI to tap the fiber-optic cables connecting the data centers.

Deploying splitters on fiber-optic cables is clearly mass surveillance since a copy of all data is made. And in this instance DPI would also qualify as mass surveillance since the parameters are set wide to capture as much data as possible.

2.2 *PRISM*

The Guardian article revealing the PRISM program reported that this program gave the NSA direct access to the servers of major internet providers such as Google, Apple, Skype, and Yahoo. The slide speaks of PRISM "collection directly from the servers" of nine U.S. internet services providers. The interpretation by *The Guardian* and *The Washington Post* was that this meant these companies were collaborating with the NSA to give it a direct connection to their servers, to

"unilaterally seize" all manner of communications from them. (Greenwald & MacAskill 2013) This proved, however, to be erroneous.

The "direct access" described here is access to a particular foreign account through a court order for that particular account, not a wholesale sucking up of all the information on the company's users. The court order gives the NSA access to the targeted account as well as to the accounts it is in contact with. This follows in the same principle of a court order on a phone number yielding the phone numbers the targeted phone has communicated with (with the obvious difference of a Facebook page containing content, while phone metadata does not). The NSA and the attorney general serve a court order on one of these companies for one or more foreign accounts, say for example, several Facebook accounts in Pakistan. Those accounts are then monitored and their activity is sent back to the NSA. This is where "direct access" fits in—the NSA has access to the account in real time. (Soar 2013) Marc Ambinder, writing in *The Week*, speaks of a 'mirror' of the accounts that the company somehow creates and only the NSA has access to. When the selected account is updated the Facebook server and the mirrored server are both updated in real-time. PRISM is the tool that allows the analyst to monitor and analyze this data and all the data on foreign targets provided to the NSA by internet companies in the U.S. (Ambinder 2013).

PRISM, then, is a targeted technology used to access court ordered foreign internet accounts.

2.3 *Decryption, or circumventing encryption*

One of the NSA's core missions is to decipher and break codes. Interestingly, however, the leaks have shown that the majority of the NSA's decryption efforts do not involve actually breaking codes, but exploiting human elements and implementation software to circumvent encryption. Further, while mass surveillance programs aid in identifying machines to exploit, the actual decryption—or circumventing of encryption—is done on a targeted, rather than mass surveillance scale.

BULLRUN is the NSA's program dealing with defeating encryption. The Classification Guide for Project BULLRUN states that the NSA has "some capabilities" against encryption in HTTPS, VoIP, Secure Sockets Layer (SSL; used for online banking), VPNs, SSH, and Webmail. The Guide also make explicit that "capabilities against a technology' does not necessarily equate to decryption."

The NSA has various methods for defeating encryption—obtaining encryption keys, backdoors, influencing encryption standards, and brute force. To obtain encryption keys the agency issues court orders requiring companies to turn over keys; hacks into companies to obtain the keys; or secures companies' willing collaboration. The agency reportedly maintains of database of the keys it collects. (Simonite Sept. 6, 2013) The NSA has also persuaded or coerced companies into installing backdoors into their security systems. It can then get around the encryption by using these backdoors.

The agency purportedly influences encryption key standards. This would probably be done through the National Institute for Standards and Technology (NIST) "which sets U.S. cryptography standards and is influential worldwide." (Simonite Sept. 9, 2013) The MIT Technology Review's IT editor for hardware and software argues that it is unlikely that the NSA compromised many of these most widely used standards because there were developed by open groups outside the U.S. The one standard it did play a significant role in developing is part of a cryptography toolkit—Suite B—used by the U.S. government and its contractors. "Introducing backdoors into that would seem counterproductive to the NSA" (Simonite Sept. 9, 2013).

The NSA also uses brute computer force to break weak encryption. Therefore, although there is not yet evidence that the NSA has cracked SSL, experts have long warned that the keys typically used with SSL are not long enough. A government agency or a large company with significant resources could break the 1,024 bits long keys that most sites use for SSL. Longer keys are necessary to protect against this kind of attack, but few companies use them. (Google and Facebook are just this year switching to longer keys. Google's key will be 2,048 bit.) (Simonite Sept. 9, 2013).

The NSA capabilities under BULLRUN are interesting because they show the limits of its abilities. The agency cannot break encryption. Its attacks against encryption use must be done on a case-by-case basis. However, it also illustrates its ability (and potential) to bring more data under its surveillance by bypassing encryption. Obtaining each individual key or backdoor access is targeted; what this yields could be targeted or mass surveillance (e.g. it could read all the traffic of a company once it has the encryption key). Where on the mass-targeted scale decryption falls is therefore somewhat variable. We have chosen to place it towards the mass end of the scale but not fully in the mass surveillance category since encryption keys and backdoors can give it access to non-target data, but the agency does not have the capability to unilaterally bypass all encryption.

2.4 *Exploitation*

To exploit—hack into—computers and other devices the NSA utilizes its secret servers and software and hardware implants.

2.4.1 *Secret servers*

The NSA's attacks using FOXACID are a good example of both its exploitation techniques and how it circumvents encryption. FOXACID is a Computer Network Exploitation system that matches potential targets with prepared attacks. It is a modular system that allows exploits to be changed if discovered and only launches certain attacks against certain targets. FOXACID is used to perform all kinds of attacks. One example is attacks against Tor users (Schneier Oct. 4, 2013).

Tor—The Onion Router—is an online anonymity network. It is a problem for law enforcement because criminals use it for communication and it makes identification of the user, hence, the criminal, excessively more difficult. Tor works by routing data packets through multiple nodes, or relays, rather than taking the most direct path. Each relay only knows the relay the data came from and the next relay it is going to. To the websites visited, the location of the Tor user appears random.

To execute an attack, the first step is to identify Tor users on the internet. This is easy for the NSA to do because the characteristics that make Tor anonymous also make all Tor users look the same on the internet. However, the user's identity and location remain unknown. "The NSA creates 'fingerprints' that detect http requests from the Tor network to particular servers." (Schneier Oct. 4, 2013) The fingerprints are then put into a database and data analysis tools are used to sort through all the internet traffic the NSA monitors to identify Tor connections.

Once a Tor user is identified the NSA uses its secret servers on the internet backbone, codenamed QUANTUM, to redirect those users to other secret servers, codenamed FOXACID. Because QUANTUM servers are at key locations on the internet backbone, they can react faster than other websites and thus impersonate the website the user is wanting to access. They can respond to the request before the actual website can and they look the same as the actual website. The target's browser is thereby fooled into contacting the FOXACID server. These kinds of attacks are a sort of race and are hard for anyone besides the NSA to execute because they depend on "a privileged position on the internet backbone" (Schneier Oct. 4, 2013). This is known as a man-on-the-side attack.

"By the time the NSA tricks a target into visiting one of those servers, it already knows exactly who that target is, who wants him eavesdropped on, and the expected value of the data it hopes to receive." (Schneier, Oct. 15, 2013) Based on this, FOXACID automatically determines which exploits are best to serve against the particular target. It performs a risk-benefit analysis, considering factors such as the technical sophistication of the target, the value gained from a successful attack, the risk of discovery, the value and rarity of the exploit, etc. (Schneier, Oct. 15, 2013) In the case of Tor, FOXACID attacks through the Tor browser bundle (a group of programs designed to make the installation and use of Tor software easier), exploiting vulnerabilities in the Firefox web browser. Once an attack has been successfully executed, the infected computer calls back to the FOXACID server, which then further infects the computer, compromising it long-term and providing the NSA with ongoing information (Schneier Oct. 4, 2013).

Note that although the NSA can execute these attacks against Tor it cannot do so on a large scale. Nor can it do so on demand. These are targeted attacks against individual users, not blanket attacks against all Tor users. According to 2012 NSA PowerPoint slides, the agency "will never be able to deanonymize all Tor users all the time." It has had success de-anonymizing "a **very small fraction** of Tor users" with manual analysis, but has had no success in de-anonymizing a Tor user on demand. (Bold in original document.)

This is apparently the same kind of attack that the GCHQ used against Belgacom. When targeted employees visited their LinkedIn profiles a secret served responded with a fake page that infected their computer with malware. (*Spiegel Online* staff 2013)

2.4.2 *Software and hardware implants*

In December 2013 *Der Spiegel* published a leaked document of a sort of catalog of NSA spy technology. It included both software and hardware implants for exploiting mobile phones and their networks, computers, routers, and servers, among others. To give a couple of examples: SOMBERKNAVE, a software implant for Windows XP, uses the computer's unused wireless device to contact the NSA remote operations center and makes the targeted device controllable remotely. When the target is using the wireless card, SOMBERKNAVE is inactive. RAGEMASTER is a hardware implant hidden in the monitor cable that allows the NSA to see whatever appears on the monitor of the targeted computer.

Like the attacks performed by the secret servers, these implants are targeted surveillance, being targeted at specific devices. In some cases, however, they could move along the scale towards mass depending on how they are used. For example, the implants for professional routers could potentially gather information on non-targets, depending on whether the organization itself or someone within the organization using the router is the NSA's target. It has also been reported by some sources that at least one of these systems—NIGHTSTAND—has been used from drones to target certain geographical

areas. (Appelbaum 2013) For this reason we classify exploitation on the targeted end of the scale, but not completely in the targeted category.

2.5 *Analysis tools and databases*

NSA has a myriad of data analysis tools and databases to process the data it collects. XKEYSCORE is both an analytical tool and database. We have chosen to focus on this system as an example of NSA databases, as it is often mentioned in reporting on NSA leaks, and is at the same time, perhaps, the most complex and difficult to understand.

After the attacks of 9/11 the NSA needed a quick way to increase its internet surveillance. It accomplished this by purchasing "off-the-shelf" systems such as Narus. The result was that a lot of data was collected. The problem for the NSA was where to store it and how to get it there. "Even when you store just the cream skimmed off the top of the 129.6 terabytes per day that can be collected from a 10-gigabit network tap, you're still faced with at least tens of terabytes of data per tap that need to be written to a database." (Gallagher 2013) It was physically impossible for the NSA to get all that information back to its central database. So it created XKEYSCORE. XKEYSCORE solves the problem by storing the data packets in local caches rather than sending it back to a central database. Since the advent of XKEYSCORE the agency can now store 3 days worth of raw packet data and 30 days worth of metadata in the local caches.

XKEYSCORE *is not* the system that actually captures the data via the fiber-optic cable tap. The system that captures data packets from NSA wire taps is code-named TURMOIL. XKEYSCORE processes the data that TURMOIL brings in.

It processes it by running plug-ins, analysis engines that look for specific content in the captured data packets. XKEYSCORE has plug-ins for email addresses, phone numbers, webmail and chat activity, and extracted files, among others. "For selected traffic, XKEYSCORE can also generate a full replay of a network session between two Internet addresses." (Gallagher 2013) The plug-ins extract the metadata from each internet session and index it into tables. XKEYSCORE can track, cross-index, and search any kind of metadata that can be extracted from an internet session—log ins, email addresses, the use of encryption, language use, IP address geolocation, etc.

There are approximately 150 XKEYSCORE sites around the world. These sites include wiretaps at telecommunications companies' peering sites (such as the AT&T case), systems connected to friendly foreign intelligence agencies' collection sites, and mid-ocean fiber-optic cable taps (executed by F6, the joint CIA-NSA Special Collections Service). Only information that is related to specific cases is sent back to the NSA's central database. The data in the local caches is available to analysts through federated search while it is being stored (Gallagher 2013).

To perform a search request an NSA analyst creates a query. This query is sent to all the XKEYSCORE sites. Analysts can search by hard selectors (e.g. email addresses) or soft selectors (e.g. language). So if an analyst does not have a hard selector, such as an email address or phone number for a known target, he/she can do a search for a category of information, such as all encrypted Word documents or all VPN (virtual private network) startups in a given country. (NSA XKEYSCORE slides 2008) Any kind of query can be created as long as the plugin exists. XKEYSCORE combines and returns all the responses to the query.

Using XKEYSCORE is apparently how the NSA can identify Tor users—this is a category that can be queried. Another category that can be searched is exploitable machines—"Show me all exploitable machines in country X." (NSA XKEYSCORE slides 2008) When the NSA's Tailored Access Operations (TAO) identifies a computer as a target it loads its fingerprints, or unique identifiers, into XKEYSCORE's fingerprint ID engine. In the case of Microsoft system crashes XKEYSCORE identifies these error reports and sends an automatic notification, enabling TAO to exploit the machine. (Spiegel staff 2013)

Like Narus, XKEYSCORE performs best when it 'goes shallow,' that is, fewer filters are applied to determine which data packets are captured. This means that a lot of information is collected, including, undoubtedly, information unrelated to NSA targets. XKEYSCORE, therefore, classifies as mass surveillance technology.

3 FINDINGS

Based on information currently available on the above NSA surveillance technologies, we have given them an initial and basic rating on a mass to targeted surveillance scale (See Fig. 2.)

The NSA's use of splitters on the fiber-optic cables of companies like AT&T is clearly mass surveillance. This surveillance technology indiscriminately copies all data, sweeping up vast amounts of data belonging to non-targets.

PRISM, by contrast, is a targeted surveillance method and is therefore placed at the other end of the scale.

The NSA's decryption program is a little less clear cut. The NSA does not have the capability to unilaterally bypass all encryption. However, once it does have an encryption key or a backdoor, for

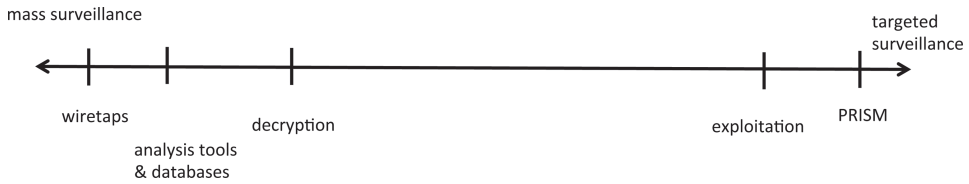


Figure 2. Classification of NSA surveillance technology.

example, it can have access to far more data than just that belonging to specific targets. For this reason we have classified it as one step down from the mass surveillance of wiretaps.

The surveillance technology used for exploitation is targeted. However, as previously stated, in some cases it may be aimed at groups of people, which include non-target subjects. Therefore we have classified exploitation as targeted surveillance but not completely in the category of targeted.

Whether or not analysis tools and databases are mass or targeted surveillance is dependent upon the data that is put into them. Examining all databases is beyond the scope of this paper. We have taken XKEYSCORE as an example, and found that because it sorts and stores volumes of data obtained via mass surveillance methods, it is also mass surveillance technology.

4 CONCLUSION

This paper aimed to create some structure for the many NSA surveillance programs recently revealed in the Snowden leaks. It was an initial step to classify the surveillance technologies and rate them according to mass and targeted surveillance. We found that in most cases (PRISM being the exception) several programs could be classified under one technology category. Further, while some of these programs have been portrayed as mass surveillance, they are, in fact, targeted. Lastly, further research is needed to determine if these technologies are effective.

Future work will examine subsequently leaked NSA programs, adding to and/ or adjusting the categories of surveillance technology as needed. This will form the basis from which to analyze the effectiveness of the NSA surveillance technology; to what extent and at what cost does it achieve its goals.

REFERENCES

Ambinder, Marc. "Solving the Mystery of PRISM." *The Week*, June 7, 2013. http://theweek.com/article/index/245360/solving-the-mystery-of-prism.

Appelbaum, Jacob. *30c3: To Protect And Infect, Part 2*, presentation at Chaos Communication Congress, Germany, December 2013. http://www.youtube.com/watch?v=b0w36GAyZIA&feature=youtube_gdata_player.

Appelbaum, Jacob, Judith Horchert, & Christian Stöcker. "Shopping for Spy Gear: Catalog Advertises NSA Toolbox." *Spiegel Online*, December 29, 2013. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Asghari, Hadi, PhD Candidate, Economics of Cybersecurity, TBM, TU Delft. Author's Interviews November 18, 2013 and March 7, 2014. Email correspondence, November 21, 2013.

Asghari, Hadi, Michel van Eeten, & Milton Mueller. "Unravelling the Economic and Political Drivers of Deep Packet Inspection." 21. Baku, Azerbaijan, 2012.

Ball, James, Luke Harding, & Juliette Garside. "BT and Vodafone among Telecoms Companies Passing Details to GCHQ." *The Guardian*, August 2, 2013. http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

Brown, Dr. Ian, Associate Director of Oxford University's Cyber Security Centre and Senior Research Fellow at Oxford Internet Institute. Author's email correspondence, March 25, 2014.

Clement, Andrew. "IXmaps—Tracking Your Personal Data through the NSA's Warrantless Wiretapping Sites." Toronto, ON, Canada: ISTAS, 2013.

Cohn, Cindy. "Witness Statement of Cindy Cohn." Big Brother Watch v. United Kingdom, European Court of Human Rights, September 27 2013.

Fulghum, David A. "Pressure Mounts to Find New Science to Meet Cyber-Intel Needs." *Aviation Week & Space Technology*. March 29, 2010: 58.

Gallagher, Sean. "Building a Panopticon: The Evolution of the NSA's XKeyscore." *Ars Technica*, August 9, 2013. http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/.

Greenwald, Glenn, & Ewen MacAskill. "NSA Prism Program Taps in to User Data of Apple, Google and Others." *The Guardian*, June 7, 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Marcus, J. Scott. "Declaration of J. Scott Marcus in Support of Plaintiff's Motion for Preliminary Injunction, Tash Hepting, Gregory Hicks, Carolyn Jewel and Erik Knutzen et al. v. AT&T Corp et al.," U.S. District Court for Northern District of California, 2006.

NSA. “Tor Stinks.” Slides, June 2012.
NSA. “XKEYSCORE.” Slides, February 25, 2008.
Schmidt, Fabian. “Tapping the World’s Fiber Optic Cables,” *DW.DE*, June 30, 2013. http://www.dw.de/tapping-the-worlds-fiber-optic-cables/a-16916476.
Schneier, Bruce. “Attacking Tor: How the NSA Targets Users’ Online Anonymity.” *The Guardian*, October 4, 2013. http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.
Schneier, Bruce. “Crypto-Gram Newsletter, October 15, 2013,” October 15, 2013. https://www.schneier.com/crypto-gram-1310.html.
Simonite, Tom. “Circumventing Encryption Frees NSA’s Hands Online.” *MIT Technology Review*, September 6, 2013. http://www.technologyreview.com/news/519131/circumventing-encryption-frees-nsas-hands-online/.
Simonite, Tom. “NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds.” *MIT Technology Review*, September 9, 2013.
Soar, Daniel. “How to Get Ahead at the NSA.” *London Review of Books*, October 24, 2013.
Staff. “Inside TAO: Documents Reveal Top NSA Hacking Unit.” *Spiegel Online*, December 29, 2013. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.
Staff. “GHCQ Targets Engineers with Fake LinkedIn Pages.” *Spiegel Online*, November 11, 2013. http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Study of the security of processes running in computer operating systems

I.J. Jóźwiak
Faculty Informatics and Management, Wrocław University of Technology, Wrocław, Poland

A. Szleszyński
General Tadeusz Kościuszko Military Academy of Land Forces, Wrocław, Poland

ABSTRACT: A process is the main part of a computer operating system. Its role is to fulfil its task(s). But if it contains errors it may disrupt the proper work of the host computer operating system. Any disruption affects host computer operating system security. In this paper, the authors evaluated behaviour of a test process and its influence on the increasing use of operating memory, which is the element of the host computer operating system efficiency. Then an interaction between processes was evaluated.

1 INTRODUCTION

Nowadays, operating systems are used in multitasking environment. This means that it is possible to support multiple processes that share their operating memory, Central Processor Unit (CPU) time, and input and output devices. This activity is related to the switching processes coordinated by a special program called scheduler. An initiation of a new process in an operating system means that a user has necessary privileges to do that. For an operating system security it means that at least one of the safeguards is omitted.

From this moment the process receives an access to operating system functions and to computer hardware controlled by an operating system. So, if the program was written in such a way, it may initiate numerous malicious actions such as: observing a user to find out personal passwords, attempting to transfer illegal data transfers, encrypting available data or disturbing the work of host computer operating system. The last activity may be possible due to improper requests operating system's kernel functions (Tannenbaum & all, 2006).

The goal of this paper is to study the way the processes may interact with each other, what kind of disturbance may be expected in case of malicious activity in one or more processes? The authors have not found answers to those questions in the available literature on the subject.

The answer is derived from the experiment conducted on some operating systems used by business and education organisations. During the research authors used their own software written in Object Pascal programming language. The Object Pascal belongs to a group of high level and object oriented programming languages. It does not offer the possibility to manipulate a value of specified operating memory cell. All of those operations are executed by using operating system Application Programming Interface (API). The Pascal programming language was not created with the purpose to build the new operating system[1] so it does not offer the functionality and flexibility such as Assembly or C programming languages. Because its functionality is limited, the attempt to create any malicious software requires special techniques to achieve effects similar to those using Assembly or C programming languages. It is similar situation to that of using the script programming languages[2] running on commercial and non-commercial operating systems.

2 PROBLEM IDENTIFICATION

The aim of this work is to find out the answers for three questions "How a single process, run on operating system, can violate an operating system security?", "How the single process influence on operating system performance?", "How to measure the extent of damages resulting from such action?".

The choice of the availability attribute depends on the information technology system providing

[1]Different as C programming language which was used to create the Unix operating system.
[2]i.e. Visual Basic Script from Windows operating system or Perl Script Programming Language for Linux.

the data necessary to make decisions. The lack of necessary information on time for a decision maker means that there is no information at all (Michalski, 2007). In addition, the information make 70 per cent of the value of manufactured goods and services (Michalski, 2007).

The main goal of the information technology system is to deliver reliable and well addressed information to right people at the right time according to the 'need to know' rather than 'nice to know' rule. The same requirement is true for information technology systems in which a human-to-machine interaction or just machine-to-machine interaction exist.

The issue of process security is vital because running of the process in operating system means that the operating system security subsystem is omitted. It is so because only the authorized user may run a process. Moreover, working on operating system process gives an access to all computer resources allocated to the user in accordance with the security settings.

3 EXAMINING OF OPERATING SYSTEM EFFICIENCY

To answer the three questions stated above it would be necessary to conduct the research by using the analysis of influence of the processes on three security attributes such as confidentiality, integrity and availability. The aim of this work is to find what consequences result from the malicious activity of the single process. Then, the next question is to be answered—how destructive this situation could be for other processes running on an operating system?

The mechanism of malicious activity is not well known. The literature available to the authors do not describe the exact mechanisms of malicious code. One of the possible reasons is that the analysis of malicious code operation requires a lot of technical knowledge. The specialized software is necessary to test malicious behaviour. It is difficult to examine the structure and behaviour of malicious codes. Some of them have a built-in self-protection mechanism against the software structure and behaviour analysis.

There is not many information about the influence of the malicious software on stability of an operating system performance. This results from the operating systems manufacturers not interested in detailed description of the methods used to exploit vulnerabilities of their products.

The authors are going to study the behaviour of processes running on an operating system. At the beginning, the authors decided to check the possibility of the availability attribute violation. To measure the system performance there was a simple application created. The application makes an addition of two integers. That activity is repeated forty times in a program loop. The result of the operation is written to memo component, subsequently those data is used to derive all necessary calculation and statistics. The results of the experiment would be used to calculate a mean time of the process. The mean time of a sequence of actions shows the efficiency of the system. Next parameter is the utilization rate of CPU of the computer by each of the running processes.

Very similar method would be used concerning the data integrity verification.

As the first parameter to examine, an operating memory usage was chosen. During the experiment, the increase of the amount of operating memory for test process was checked. Data in Table 1 shows the increase of used memory allocated to the test processes.

Position 0 shows the amount of memory allocated to the test process after loading it into operating memory before it was run. After the first run of process the amount of operating memory allocated to the processes increased 16 times (from 8.93 MB to 145.39 MB), it is the biggest value. The next growths were much lower than the first one. It means that the first run of a process needs more memory (16 times more). Next runs of the test process need just two times bigger the memory than a previous one. However, the amount of operating memory between positions 0 and 4 runs of the process required 62 times more RAM (Random Access Memory, also called operating memory) than right after loading. At the end, the single run of the test process allocated more than 0.5 GB RAM what was more than 25%[3] (Solomon, 1998) of operating memory allocated to run all the

Table 1. Operating memory usage by test process (source: authors own work).

No. of test process run	RAM memory allocated for test process [MB]	Increase of allocated RAM memory for the test process [MB]
0	8.93	–
1	145.39	136.46
2	281.36	135.9
3	497.49	216.13
4	553.30	55.81

[3]Some operating systems divides RAM installed into computer into operating system functions and processes run on it. The half of RAM is reserved for running kernel functions and the second half for processes run.

processes in the operating system. The comparison of proportional increase of allocated RAM, between each run of the test process, is shown in Table 2.

The analysis of the availability of information can be realised by measuring the time of execution of each part of the task. The test process makes the addition of two numbers from 1 to 100 then elements and the result are converted to string value. String value is added to memo control that is inside the main form. The statistical parameters of the results of the test process operation are presented in Table 3.

The mean value for the fourth run of the process is six times longer than it was during the first run of process. An explanation for data shown in Table 3 is that the of increase the amount of RAM influences the execution time. It is because the operating system has to provide the memory management for the rest of operating processes. The jumping increase of the amount of RAM needed to provide for the process results in more frequent use of the virtual memory disc. This kind of disc uses the hard drive to store data needed for switching processes. But the access time to hard disc is 1000 times longer than access time to RAM. That is the reason of the increase of the process operation time. The distribution of execution time for four runs of the test process is shown in Figure 1.

Table 2. Proportional increase allocated RAM memory for the test process (source: authors own work).

No of test process run	Proportional increase of allocated RAM memory for test process between it subsequent run
0	–
1	16
2	2
3	2
4	1

Table 3. Descriptive statistics of the time of execution the test process (source: authors own work).

	Number of act the test process			
Statistical parameter	I	II	III	IV
Mean [s]	0.518	1.450	2.384	3.368
Standard deviation [s]	0.261	0.280	0.284	0.286
Median [s]	0.507	1.467	2.379	3.355
Maximum value [s]	0.967	1.919	3.089	3.978
Minimum value [s]	0.094	0.998	1.935	2.901
Interval of values [s]	0.873	0.921	1.154	1.077
Most frequent value [s]	0.421	1.326	2.028	3.042

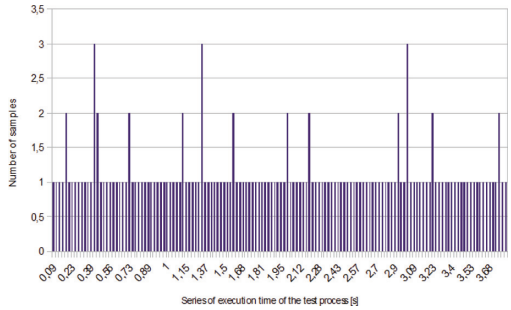


Figure 1. Series of execution time for four run of the test process (source: authors own work).

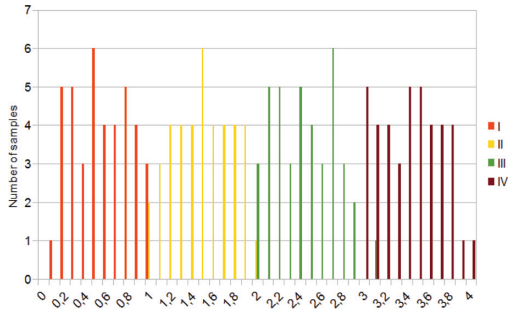


Figure 2. Distribution of execution time for four operations of the test process (source: authors own work).

The data gathered during the experiment were used to present the distribution functions for all four operations of the test process. Data gathered during the experiment were used to present the distribution functions for all four operations of the test process.

It was made in order to compare them to each other. The graph of the distribution functions of the execution time is shown in Figure 2.

The biggest difference in value is observed during the third run of the test process (Fig. 2). This is the result of the highest increase of the amount of RAM allocated for it. During the third process operation 216 MB growth of the amount of RAM is observed. The difference between the lowest and the highest value of the execution time of the test process is 1.154 s. Dynamic change of RAM allocated for the test process force the memory management subsystems to handle other processes and allocate them to the virtual memory if necessary. Computer operating system memory manager has to store information about memory pages, counters of instructions and value of CPU registers at the virtual memory drive. The virtual memory drive is controlled by the computer hard disk drive. Because the virtual memory uses com-

puter hard disk drive, the time needed to access the data is 1000 times longer than in case of RAM.

The lowest scatter of values of the execution time is observed during the first operation of the test process. Although during that action the amount of RAM proportionally rises 16 times (see Table 2), the dynamic increase of the amount of memory has no influence on the scatter of the time of process execution.

Almost all, except the second one, distribution functions of the execution time of the test process shown in Figure 2, show that they are multi-mode. Only the second run of the test process is similar to one-mode distribution. The total interval of the operation time of the test process is between 0.094 s and 3.97 s.

The increase of the amount of RAM for proper operation of one process requires more frequent use of virtual disk. That may imply the longer time of process execution and may result in the lower efficiency of the system. In the worst case scenario, there may be not enough space on the hard disk drive. If computer hard disk drive does not have sufficient space to store all the data related to all working processes, the host computer operating system may break down. Such a situation requires the restoration of the operating system. Unexpected failure may stop computer work for a long time (hours or even days). During that time, information stored on computer hard disk is not available. It is possible that some files stored on hard disk may lose their integrity as a result of a computer failure.

3.1 *Evaluation of the correlation between two independent working processes*

During the next experiment, the influence of one working test processes on the second test process was evaluated. At the beginning, the second process was started-up without the test processes. Then, time of completing the main task was recorded. After that, both processes were run concurrently and the time of completing the main task was recorded. The second process makes only the addition of two integer variables and the result is assigned to third integer variable, but the result of this operation is not sent to an output device such as computer monitor. Values for both test processes measured out during the experiment are shown in Table 4.

The data shows that the influence of any working process on the other working process is negligible. It was not possible to observe any big differences in the time of execution of the second test process. We may conclude, that if a process does not use output devices, the differences in execution time in both experimental cases are negligible.

Table 4. The comparison of the execution time the second test process (source: authors own work).

No of operation the second test process	Without acting test process [s]	With acting test process [s]
1	0.187	0.203
2	0.234	0.265
3	0.234	0.265
4	0.234	0.265
5	0.234	0.234
6	0.218	0.280
7	0.219	0.265
8	0.250	0.249
9	0.250	0.265
10	0.250	0.266
11	0.281	0.265
Average:	0.236	0.257

Time needed to transfer data from computer operating memory to device memory is far longer than in case when all the results are stored into computer operating memory. Because all the results of the second process were stored in computer operating memory, the differences between the execution time are small (Table 4). The difference between the average value of the execution time in each case is 0.021 s.

4 CONCLUSIONS

The evaluation of the efficiency of the host computer operating system shows that it is possible to cope with the rapid increase of the operating memory use. Rapid growth of RAM allocated to a process affects the time of its execution. The test process execution time rose more than 3 times.

During the experiment it was observed that if the process does not use memory-consuming external devices, the increase of the execution time was less than 9% in both test cases. In conclusion, the influence of interaction between two processes is negligible.

REFERENCES

Love R. 2010. *Linux Kernel Development*, Pearson Education.

Michalski A. 2007. *Information Availability in Enterprise*, Silesian University of Technology, Zabrze.

Silberschatz A., Galvin P.B., Gagne G. 2009. *Operating Systems Concepts. Eight edition*, John Wiley & Sons.

Solomon D.A 1998. *Inside Windows NT. Second Edition*, Microsoft Press.

Tanenbaum, A.S., Herder, J.N., and Bos, H. 2006. *Can We Make Operating Systems Reliable and Secure?*, IEEE Computer, vol. 39, pp. 44–51, May 2006.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Control-in-the-loop Model Based Safety Analysis

P.-Y. Piriou, J.-M. Faure & J.-J. Lesage
Automated Production Research Laboratory, Ecole Normale Superieure, Cachan, France

ABSTRACT: In most cases, Model Based Safety Analysis (MBSA) of critical systems focuses only on the process and not on the control system of this process. For instance, to assess the dependability attributes of power plants, only a model (Fault Tree, Markov chain …) of the physical components of the plant (pumps, steam generator, turbine, alternator …) is used. In this paper, we claim that for repairable and/or phased-mission systems, not only the process but the whole closed-loop system Process/Control must be considered to perform a relevant MBSA. Indeed, a part of the control functions aims to handle the dynamical mechanisms that change the mission phase as well as manage repairs and redundancies in the process. Therefore, the achievement of these mechanisms depends on the functional/dysfunctional status of the control components, on which these functions are implemented. A qualitative or quantitative analysis method which considers both the process and the control provides consequently more realistic results by integrating the failures of the control components that may lead to the non-achievement of these mechanisms. This claim is exemplified on an industrial study case issued from a power plant. The system is modeled by a BDMP (Boolean logic Driven Markov Process), assuming first that the control components are faultless, i.e. only the faults in the process are considered, and afterwards that they may fail. The minimal cut sequences of the system are computed in both cases. The comparison of these two sets of minimal cut sequences shows the benefit of the second approach.

1 INTRODUCTION

Model-Based Safety Analysis (MBSA) can be defined as "an approach in which the system and safety engineers share a common system model created using a model-based development process" (Joshi et al. (2006)). MBSA performed for critical controlled systems are most often applied on a model of the process alone. This is the case for example in Chaux et al. (2012) and Sondermann-Woelke et al. (2012). In particular, the last publication highlights the role of control for the application of redundancies, but does not consider control failures. These approaches take into account mechanisms of reparations and redundancies in the plant but they omit that the functions which manage these mechanisms can fail, as well as the components which support them. Two kinds of control failures can then be distinguished: software and hardware based. This paper does not consider the software failures because they can be avoided (or at least limited) by using one of the numerous existing formal verification techniques, like for instance model checking (more details on this issue may be found in Berard et al. (2001)). But with the increase of the digital components in complex controlled systems, dependability studies performed for these systems cannot underestimate probable failures of the control components. Indeed, even if these components have a good reliability, their failures remain possible, especially when the concerned systems have a long lifespan. Moreover, new studies integrate more and more injuries whose causes are external (fire, flood, terrorist attacks …). These injuries concern the plant components as well as those of the controller without distinction between them. Hence control should be considered in the loop for MBSA practices, and this paper aims to show that this issue carries significant consequences on both the modeling and the results.

Indeed, the more complex the system is the more switching mechanisms appears in the controlled process (due to fault tolerance, mission phase changes, maintenance based on autotest …). These switching mechanisms are handled by functions implemented into components of the control. Therefore, the achievement of these mechanisms depends on the ability of the control components to perform them. Hence, the failure of the control components may lead to the non-achievement of these mechanisms, what may have a significant influence on the results of a qualitative MBSA. Moreover, the formalism for performing MBSA are generally not made for taking into account the loss of these switching mechanisms.

In order to illustrate this issue, the paper considers an industrial controlled system on which a comparison study is performed. First the system failure is represented by a model that complies with the BDMP formalism. Second, the minimal cut sequences are extracted from this model. Section 2 describes the case study and gives the definition of the BDMP formalism. Section 3 applies the MBSA stated above while considering only the process failures. Then a control architecture is described, and added to the model in section 4. For integrating these new failures in the model, three models are proposed and discussed. In the same section, the set of minimal cut sequences is updated, and compared with the previous one. This comparison shows that the control failures have a significant influence on the qualitative analysis of the system. Finally, the last section draws up concluding remarks and outlooks.

2 BACKGROUND

This section introduces the case study used in this paper and recalls the basics of the BDMP formalism.

2.1 *The coolant feeding system*

In order to exemplify our claim, we consider the case study presented in Chaux et al. (2012). It is a coolant feeding system issued from a power plant. Its purpose is to supply cooling fluid to the steam generator. It is composed of two redundant groups of pumps, and a strongly redundant power supply (Fig. 1). The two groups of pumps are series-connected and the first one is powered by the power supply. The power supply of the second group of pump is not considered here.

Six kinds of components can be identified:

- The Grid (Grid) is the source of electricity supply.
- The electric Transformers (Tr1 and Tr2) decrease the voltage (from 400 kV to 6.6 kV).
- The Distribution Boards (DBA1, DBA2, DBB1 and DBB2) transfer the electricity from their inputs to their output.
- The Diesel generators (Diesel1 and Diesel2) are other possible sources of electricity supply.
- The Extraction pumps (Ex1, Ex2 and Ex3) provide a sufficient flow of cooling water.
- The Feeding Turbo Pumps (FTP1 and FTP2) pressurize the cooling water.

All the components may fail and be repaired. The diesel generators and the pumps may fail not only when they are active but also when they are dormant. The system fails when its supply function cannot be achieved. To avoid this general failure, several redundancies are defined:

- An active material redundancy is defined for the group of components (DBB1, DBB2).
- A passive functional redundancy is defined for the groups of components (DBB1, Diesel1) and (DBB2, Diesel2).
- A simple passive material redundancy is defined for the group of components (Tr1, Tr2), (DBA1, DBA2), (FTP1, FTP2).
- A 2 out of 3 passive material redundancy is defined for the group of components (Ex1, Ex2, Ex3). If one of the two primaries pumps fails, the third is activated.

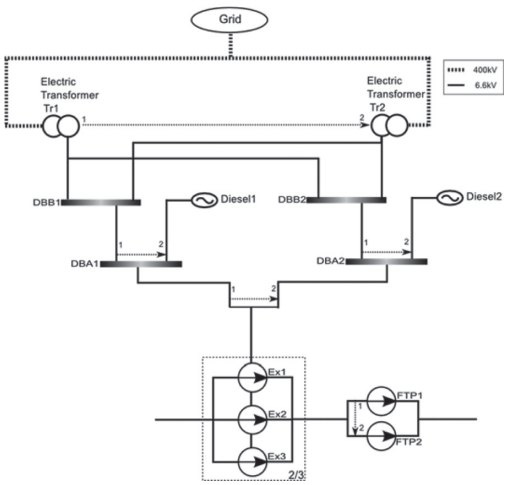


Figure 1. Schema of the coolant feeding system process.

2.2 *Recall on the BDMP formalism*

The BDMP is a formalism defined by Bouissou & Bon (2003) to address the dynamic modeling issues while preserving the structure-expressiveness of tree based formalisms (fault tree approaches). Indeed, a static fault tree model aims to describe the system failure as a combinatorial expression on the failures of its leaves (a leaf model a component). The BDMP formalism keeps the same idea, but the Boolean basic leaves of the tree are replaced by dynamic ones specified by Markov Chains (MC). In particular, repairable components can be considered. Moreover, these MC can consider non dysfunctional events to model switching between different operations modes (active, dormant …). The occurrence of these non-dysfunctional events is managed by triggers. In particular, a passive redundancy mechanism can be modeled by such a trigger. Hence, a BDMP model can be implicitly defined as a multi-top

coherent tree structure whose leafs are triggered MC. Since it is the unique formalism dedicated to the modeling of dynamic repairable systems, it is relevant to model the case study considered in this paper.

Most often, only two kinds of leaves are used and are called *F* and *SF*. The *F* leaves describe components fallible only in active mode, whereas *SF* leaves describe components fallible in both active and dormant modes ($L = L_F \cup L_{SF}$) The behavior of these leaves is specified by the models depicted on Figure 2. Since this paper addresses a qualitative analysis only, the labels of the arcs correspond to events. For performing a quantitative analysis, they should be considered as probability rates. In this figure: the events a-X, d-X, f-X-a, f-X-d and r-X, denote respectively the activation, the deactivation, the failure in active mode, the failure in dormant mode and the reparation of a component X. The two mainly used kinds of logic gates in a BDMP are *AND* and *OR*. But some works use an additional kind: the *PAND* gate. Such a gate expresses a dynamic logic: the failure status of a *PAND* gate is *True*, if and only if the failure status of all its children is *True* and have commuted from *False* to *True* in a predetermined order (generally from left to right in the tree).

Let us call the children of a given node (leaf or gate) the leaves of the sub-tree whose node is the root (if the node is a leaf then it has a single child: itself). Let T_i be a trigger, and ($Orig(T_i)$, $Dest(T_i)$) denoted respectively its origin and destination nodes. While $Orig(T_i)$ is not failed, the children of $Dest(T_i)$ stays in the dormant mode (the children of kind *SF* can still fail). When $Orig(T_i)$ fails, the MC of the children of $Dest(T_i)$ are triggered to the active mode, as soon as $Orig(T_i)$ is repaired. Then, they are put back in the dormant mode. For a better description of the BDMP semantics, see Chaux et al. (2011).

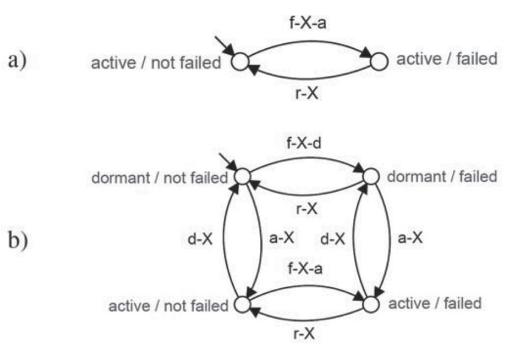


Figure 2. Behavior of the most used BDMP leaves: a) the *F* leaf; b) the *SF* leaf.

3 SAFETY ANALYSIS CONSIDERING ONLY THE PROCESS FAILURES

In this section, a BDMP model of the system is built considering only the failures of the process components. Then a qualitative analysis based on this model is performed.

3.1 *Building the BDMP model of the process*

Figure 3 shows the BDMP model of the coolant feeding system process.

The scenarios implicitly described by this BDMP model can be explicitly represented by the sequences of dysfunctional events that can occur. The next subsection aims to determine among them the shortest sequences which lead to the system failure.

3.2 *Extracting the minimal cut sequences*

In the dependability scope, a qualitative study consists in determining the main weaknesses of a system. This knowledge can be used for easing the qualitative study, what become essential when complexity increases.

For static systems, these analyses consist in determining the *Cut,* which is defined by Birnbaum et al. (1961) as a set of failed components that leads to the system failure. A *Minimal Cut* of a static system has then been defined by Rauzy (2001) as a prime implicant of the related Boolean function which can be modeled using fault trees.

For dynamic systems, the system failure depends not only on the set of failed components but also on the order of occurrences of these components failure events. Then *Cut Sequences* and *Minimal Cut Sequences* have been defined by Tang and Dugan (2004), as respectively *Cuts* and *Minimal Cuts* whose component failures have been ordered.

But when the considered system contains repairable components, the failure events are not sufficient to describe all the possible way to fail. Then a *Cut Sequence* is redefined as a sequence leading to the first system failure. Chaux et al. (2013) proposes a framework to give a formal definition of *Minimal Cut Sequences*. Informally, the set of *Minimal Cut Sequences* (MCS) is the minimal set of sequences of minimal length that are necessary and sufficient to describe the whole set of cut sequences.

In order to extract these MCS, we use the algorithms defined in Chaux et al. (2011) and Chaux et al. (2012). The first one transforms a BDMP model into a finite state automaton and the second one extract the MCS of a finite state automaton. Several MCS limited to the length 5 (selected arbitrary among the 84 existing) extracted

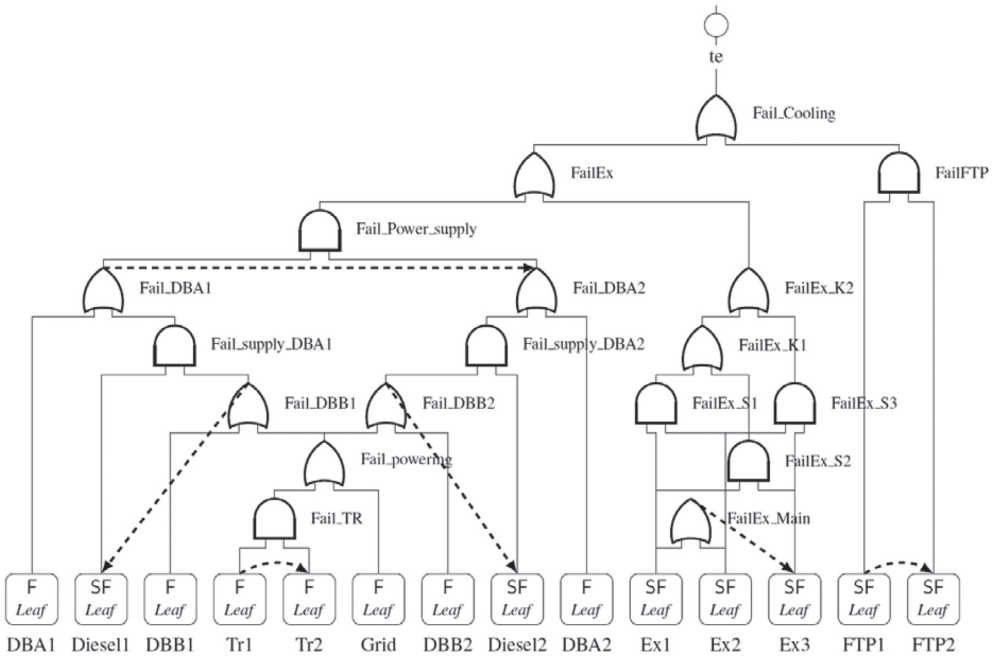


Figure 3. BDMP model of the coolant feeding system process.

Table 1. Examples of MCS of length from 2 to 5 considering only the failures of process components.

Length	Sequences
2	f-DBA1-a,f-DBA2-a
	f-Ex1-a,f-Ex3-a
	f-FTP2-d,f-FTP1-a
	… (6 others)
3	f-Die1-d,f-Die2-d,f-Grid-a
	f-DBA1-a,f-Die2-d,f-DBB2-a
	f-Grid-a,f-Die1-a,f-DBA2-a
	… (16 others)
4	f-DBB1-a,f-Die1-a,f-Die2-d,f-DBB2-a
	f-Tr1-a,f-Die1-d,f-Die2-d,f-Tr2-a
	… (36 others)
5	f-Tr1-a,f-DBB1-a,f-Die2-d,
	f-Die1-a,f-Tr2-a
	f-DBA1-a,f-DBB2-a,r-DBA1,
	f-Die2-d,f-DBA1-a
	… (15 others)

from the BDMP model described by the last subsection (Fig. 3) are sum up on Table 1.

Let us remark that from length 5, the MCS may contain repair events. For instance, the sequence f-DBA1-a → f-DBB2-a → r-DBA1 → f-Diesel2-d → f-DBA1-a, is minimal because the failure in dormant mode of the component Diesel2 may not occur without the previous reparation of the component DBA1. Then there exists no shorter cut sequence to fail by this way.

4 SAFETY ANALYSIS CONSIDERING THE CONTROL IN THE LOOP

In this section, the control system which manages the process components, and in particular the mechanisms of redundancies, is introduced. The modification of a BDMP model containing triggers is discussed. Then the control system failures and reparations are integrated to the BDMP model given in the last section. Finally, the MCS of the complete system are extracted and compared with the previous ones.

4.1 *Description of the control architecture*

A control architecture can be defined as the allocation of the control functions on the control components. In this paper, we focus on the control functions which manage the redundancies defined for the process. Moreover, only the passive redundancies require a switching management. Then among the redundancies defined in the subsection 2.1, only six are concerned. Let R_A, R_B, R_C, R_D and R_E be the functions which manage the switching between respectively (DBB1, Diesel1), (Tr1, Tr2), (DBA1, DBA2), (FTP1, FTP2), (Ex1, Ex2, Ex3). Since the switching between (DBB2, Diesel2) is of the same kind that the one between (DB1, Diesel1), it is also managed by R_A.

Each function R_X (for $X \in \{A, B, C, D, E\}$) is implemented on a couple of redundant PLC (Pro-

grammable Logic Controller): (PLCX1, PLCX2). The PLCs are connected to the process via two redundant buses (BUS1, BUS2). These redundancies are active, that is mean all the components are working, and the information must be treated and carried by at least respectively one PLC and one BUS. The control architecture of the coolant feeding system is depicted on Figure 4.

The loss of a switching function R_X (for $X \in \{A, B, C, D, E\}$) allocated to the components PLCX1 and PLCX2 can be represented by the BDMP model reported in Figure 5.

4.2 *Modeling a switching function in a BDMP model*

In this work, a switching mechanism consists in the transfer of the service achievement from a component (or sub-system) to another. The expected behavior of a passive redundancy can then be defined with two conditional switching mechanisms ("component" can be replaced by "sub-system" below):

- *Replacement switching*: if the main component fails then a switching must occur from the main component to the spare one.
- *Withdrawal switching*: if the main component is repaired then a switching must occur from the spare component to the main one.

Thereby, if the function which manages the redundancy is lost, these switching cannot occur when they should do. In particular, if this function is lost after the failure of the main component but before its reparation, the withdrawal switching cannot occur.

Since the semantics of a BDMP trigger complies with this definition (sub-section 2.2), a passive redundancy can be correctly modeled by such a trigger. Then the loss of the function which manages a redundancy corresponds to the loss of the corresponding trigger in the BDMP model. Figures 6, 7 and 8 show three possible models of the loss of the switching function R_D for the subtree corresponding to the feeding turbo pumps (gate FailFTP and leaves FTP1 and FTP2).

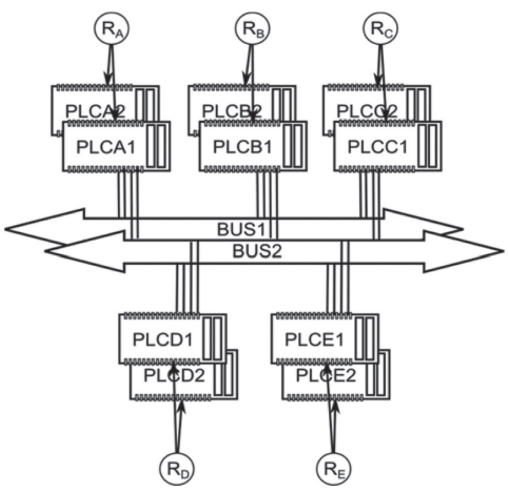


Figure 4. Schema of the control architecture.

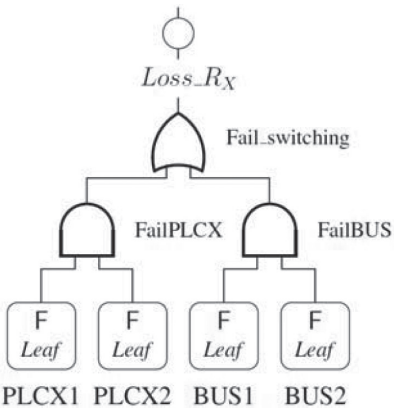


Figure 5. BDMP model representing the loss of a switching.

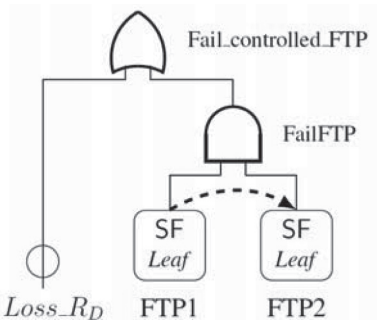


Figure 6. First solution to model the loss of a trigger in a BDMP model.

The first proposition (Fig. 6) expresses that while the switching function is loss, the group of pumps cannot perform its service even if none of them has failed. This model is very pessimistic because the main pump does not need the switching function for working alone. However in the case of a material redundancy, the function that manages a redundancy and the function that control the process components involved in this redundancy, are allocated on the same control components. Indeed, there is no need to be able to switch between two components if it is not possible to control them. In this case, the loss of the switching function occurs as the same manner as the loss of the control function. And this model expresses that when the switching function is loss, the control function is

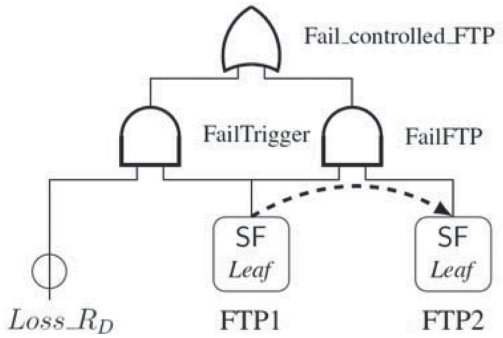


Figure 7. Second solution to model the loss of a trigger in a BDMP model.

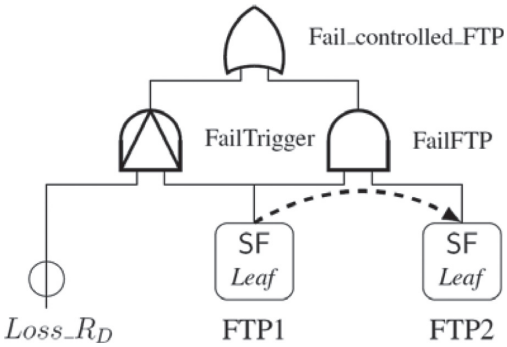


Figure 8. Third solution to model the loss of a trigger in a BDMP model.

also loss; then the group of pumps can actually not perform its service.

The second proposition (Fig. 7) expresses that while the switching function is loss and the main pump failed, the group of pumps cannot perform its service.

The third proposition (Fig. 8) expresses that if the main pump fails after the loss of the switching function, then the group of pumps cannot perform its service (the gate FailTrigger is a PAND).

In order to choose between these three propositions, let us consider the critical sequence: f-FTP1-a → f-Loss RD-a → r-FTP1 → f-FTP2-a. The expected behavior described by this sequence is informally reported below:

1. Initially, the service is provided by FTP1.
2. After the failure of FTP1, the replacement switching occurs (from FTP1 to FTP2) by means of the function R_D.
3. After the loss of R_D, the service is still provided by FTP2.
4. After the reparation of FTP1, the withdrawal switching (from FTP2 to FTP1) cannot occur because of the loss of R_D; then the service is still provided by FTP2.
5. After the failure of FTP2, the service is not provided anymore (even if FTP1 had been repaired).

Let us remark that since this sequence leads to the first failure of this sub-system, it is a cut sequence for this sub-system. Table 2 compares the accuracy of the three models proposed for this sequence. The accuracy criterion is here the conformance between the expected and the modeled behavior. The cells show the pump which provides the service, if any and the symbol Ø otherwise. Let us remark, than the last event is called f-FTP2, because it corresponds to f-FTP-d in the BDMP models, but should be f-FTP2-a in the reality.

Table 2 shows first that none of the models is perfectly accurate. Indeed, a perfectly accurate model would specify exactly the same behavior as the expected one for any sequence. Moreover, the third model is the closest of the reality, but it is not conservative. Indeed, it misses at least the cut sequence considered above. It is also the case for the second model. We are then constrained to choose the first model, because despite its bad accuracy, it is the only one which is conservative. This discussion shows that the BDMP formalism (the unique one which is dedicated to model the repairable dynamic system) has not the semantics required for correctly model the loss of a trigger. More generally, the gates of a BDMP are focused on the failure events and not the repair events. Then the consequences of the reparation of the trigger's origin are fixed by the semantics of a trigger, and cannot be changed by modifying the structure.

4.3 *Integrating the control failures in the BDMP model*

Figure 9 shows the BDMP model of the entire controlled coolant feeding system. This model had been constructed by applying the model chosen in the last subsection for each passive redundancy. The new gates are darkened. The intermediate events of kind $Loss_R_X$ (for $X \in \{A, B, C, D, E\}$) should be replaced by the corresponding sub-tree (see Fig. 5).

4.4 *Comparing the new MCS with the previous one*

Considering the control failures brings many new sequences as can be seen on the Table 3 that sums up several MCS selected arbitrary. Since the process has not been changed, it can still fail as presented in the last section. Then the new MCS includes the previous one. But 94 new sequences are added to the 84 previous ones (for the sequences of length

Table 2. Confrontation of the behavior described by the three models to the expected one on a critical sequence.

Sequence	$1 \xrightarrow{f-FTP1-\alpha} 2$	$\xrightarrow{f-LOSSR_D-\alpha} 3$	$\xrightarrow{r-FTP1} 4$	$\xrightarrow{f-FTP1} 5$	
Expected	FTP1	FTP2	FTP2	FTP2	Ø
1st model	FTP1	FTP2	Ø	Ø	Ø
2nd model	FTP1	FTP2	Ø	FTP1	FTP1
3rd model	FTP1	FTP2	FTP2	FTP1	FTP1

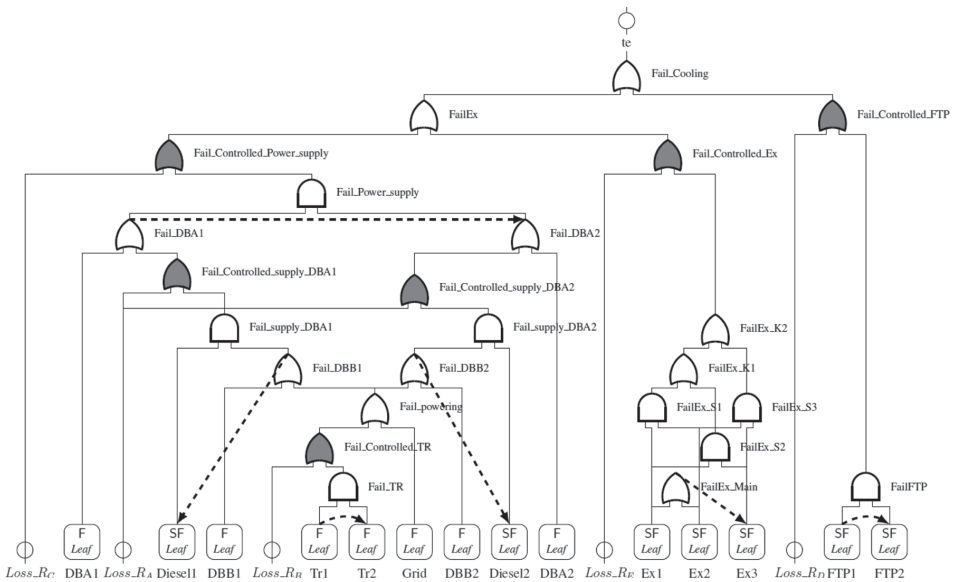


Figure 9. BDMP model of the controlled coolant feeding system.

lower than 5). Among them, 10 new sequences of length 2 show that the buses and the PLC which host the function R_A, R_C, R_D and R_E are very critical. Indeed, the achievement of the system function depends directly on the success of these groups of redundant component. Moreover, 54 new sequences of length 4 and 30 new sequences of length 5 that mix failures of both process and control components appear.

For instance, the sequence f-PLCB2-a → f-Die2-d → f-PLCB1-a → f-DBA1-a describes the behavior informally reported below:

1. Initially, the power supply is performed by the first line (Grid, Tr1, DBB1, DBA1) and the pumping services by Ex1, Ex2 and FTP1.
2. After the failure of PLCB2, nothing happens because it is in active redundancy with PLCB1.
3. After the dormant failure of Diesel2, nothing happens because the power supply is still performed by the first line.
4. After the failure of PLCB1, the controlled transformers are considered unavailable; then DBB1 and DBB2 either. The switching function R_A is not lost then the replacement switching from DBB1 to Diesel1 occurs. The power supply is performed by Diesel1 and DBA1.
5. After the failure of DBA1, the first line cannot supply the power anymore. The switching function R_C is not lost then the replacement switching from the first line to the second one occurs. But DBB2 does not transfer the power supply (because of the failure of the controlled transformers). The switching function R_A is still not lost then the replacement switching from DBB2 to Diesel2 occurs. But Diesel 2 has already failed in dormant mode. Then there is no other way for performing the power supply. Hence the coolant feeding system fails.

This set of MCS is a pessimistic representation of the weaknesses of the system considering both the process and the control. The number of MCS extracted is more than twice bigger when the control is considered. This observation confirms that the control should be taken into account in

Table 3. Examples of MCS of length from 2 to 5 considering the failures of both process and control components.

Length	Sequences
2	**f-PLCA1-a,f-PLCA2-a**
	f-BUS1-a,f-BUS2-a
	f-Ex1-a,f-Ex3-a
	… (16 others)
3	f-Die1-d,f-Die2-d,f-Grid-a
	f-DBA1-a,f-Die2-d,f-DBB2-a
	f-Grid-a,f-Die1-a,f-DBA2-a
	… (16 others)
4	**f-PLCB2-a,f-Die1-d,**
	f-Die2-d,f-PLCB1-a
	f-PLCB2-a,f-Die2-d,
	f-PLCB1-a,f-DBA1-a
	f-Tr1-a,f-Die1-d,f-Die2-d,f-Tr2-a
	… (90 others)
5	**f-Die2-d,f-PLCB1-a,f-DBB1-a,**
	f-Die1-a,f-PLCB2-a
	f-DBA1-a,f-DBB2-a,r-DBA1,
	f-Die2-d,f-DBA1-a
	… (45 others)

the MBSA studies for systems that bring many switching mechanisms. Let us remark that the results depend on the architecture choice for the control as well as the process. Then another choice of allocation of the control functions on the control components would lead to different results.

5 CONCLUSIONS

This paper claims that the failures of control components should not be omitted in the MBSA. A comparative study is performed on an industrial example. The system is modeled by a BDMP considering first only the process failures, and then considering also the control failures. The failures of control components may lead to a loss of the switching functions which handle the redundancy mechanisms between the process components. Hence we propose a modification of the model for considering the loss of these switching functions in a BDMP model. The study shows first that the set of MCS extracted is twice bigger from the model of the controlled process than from the model of the process (without taking into account the control). Furthermore, it shows that BDMP formalism is not fully adapted to deal with this issue.

Since this formalism does not allow us to describe correctly the loss of a switching function, ongoing works are aiming to define an extension of this formalism which offers that possibility. Furthermore, the consideration of failures in a closed loop system raises a failure propagation in-the-loop issue that cannot be addressed by a method based on tree formalism like BDMP. Hence, developing a qualitative analysis that deals with this issue is also under investigation.

ACKNOWLEDGEMENT

This work is funded by the French Investment of Future: "Generic Components of Embedded Software" as part of the CONNEXION project.

REFERENCES

Berard, B., M. Bidoit, F.A., Laroussinie F., Petit A., Petrucci L., & Schnoebelen P. (2001). *Systems and Software Verification. Model-Checking Techniques and Tools*. Springer. LSV.

Birnbaum, Z., Esary, J. & Saunders S. (1961). Multi-component systems and structures and their reliability. *Technometrics* 3(1), pp. 55–77.

Bouissou, M. & Bon J.-L. (2003). A new formalism that combines advantages of fault trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering and Systems Safety* 82(2), pp. 149–163.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. September (2011). Qualitative analysis of a BDMP by finite automaton. In *20th European Safety & Reliability Conference,* Troyes (France), pp. 2055–2057.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. June (2012). Systematic extraction of minimal cut sequences from a BDMP model. In *21th European Safety & Reliability Conference*, Helsinki (Finland). Session 16B, 8 pages.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou M. September (2013). Towards a unified definition of minimal cut sequences. In *4th IFAC DCDS*, Volume 4, York (UK). 6 pages.

Joshi, A., Heimdahl, M.P., Miller, S.P., & Whalen, M.W. February (2006). *Model-Based Safety Analysis*. Technical Report NASA/CR-2006-213953.

Rauzy, A. (2001). Mathematical foundations of minimal cutsets. In *IEEE Transactions on Reliability* 50(4), pp. 389–396.

Sondermann-Woelke, C., Meyer, T., Dorociak, R., Gausemeyer, J., & Sextro W. June (2012). Conceptual design of advanced condition monitoring for a self-optimizing system based on its principle solution. In *21th European Safety & Reliability Conference*, Helsinki (Finland). session 28, 10 pages.

Tang, Z. & Dugan, J. (2004). Minimal cut set/Sequence generation for dynamic fault trees. In *Reliability and Maintainability, 2004 Annual Symposium-RAMS*, Los Angeles (USA), pp. 207–213.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Developing a shared information surface for offshore work permits

S. Sarshar & G. Rindahl
Institute for Energy Technology, Center for Integrated Operations in the Petroleum Industry, Norway

C.S. Olsen, J.M. Røsok, M. Eskerud, O.G. Nedrebø, P.J. Berg & G. Misund
Østfold University College, Norway

ABSTRACT: The work permit process offshore is established to maintain control of which activities that are to be carried out on the installation and to manage their risk. This paper reports on the development of a shared information surface which can support the assessment of work permits. Findings from an initial usability study are provided.

1 INTRODUCTION

A field study was conducted on an offshore installation with the aim of studying communication of risk in the planning process and how technology can better support mediation of this through the planning process. The aspects of risk communication and management in the offshore work permit system are reported in (Sarshar et al., 2013) while this paper reports on one application of the technology aspects. The question is what information and knowledge do we recommend to depict on a shared surface to provide situation awareness at a glance. This paper reports on the development of a concept for providing overview of ongoing and planned maintenance activities at an installation, based on learnings from observations and interviews (Skjerve et al., 2011, Sarshar et al., 2013) with personnel involved in assessment of offshore work permits.

Integrated Operation (IO) in the petroleum industry has for many years included distributed collaboration as a key support capability. The technologies used to enable distributed collaboration, e.g. between onshore and offshore, have evolved from phone calls and teleconference to video conferencing rooms, to desktop solutions and lately towards more mobile solutions (Sarshar & Rindahl, 2014). As described by Kaarstad and Rindahl (2011) IO can improve access to information and provide a shared awareness in decision-making. One important feature is the increased availability of real-time data that makes it possible for personnel at different locations to cooperate based on a shared and up-to-date description of the operational situation. Another important enabler of improved decision-making in IO is a shared collaboration surface. A shared collaboration surface can provide a common and coherent representation of goals and activities and what the participants understand to be the agreed decision. Further, using such a collaboration surface, the participants can give their confirmation of the understanding of the decision, and it can be saved for future reference. This increases understanding and commitment within the team, and significantly reduces the risk of later, possibly wrong or vague, interpretations.

Chapter 2 describes in brief the work permit system followed by previous work in chapter 3. The method and approach for the development is described in chapter 4. Chapter 5 describes the interactive surface developed and chapter 6 describes the initial usability study of the tool. Chapter 7 discusses the results from the usability study before conclusions are made in chapter 8.

2 THE WORK PERMIT SYSTEM

Planning of offshore activities can be divided in different time horizons: a main plan has the horizon of several years, a yearly plan spans for one year, operational plan for three months, work order plan for one or two weeks and work permit plan which has the horizon for the next 24 hours.

The work permit system is established to maintain control of which activities are to be carried out on the installation and to manage their risk. Activities that typically require a work permit is maintenance work be it on the process equipment, pipes or structure of the platform. There are two main categories; corrective or preventive maintenance. Work permits are divided in two levels to differentiate between their impacts on risk. High-risk jobs which e.g. require welding are of level 1 while lower risk jobs are of level 2. Jobs that have been identified as no risk activities do not require a work permit

and typically include jobs inside the living quarter, in office spaces or in workshops. We limit our scope to tasks that require a work permit.

There are several technical disciplines offshore including process technicians, instrument technicians, electrical technicians and mechanical technicians. Each discipline goes through the work orders which they are responsible for and divide the task through the week with respect to their priority and available resources.

A work order describes a job package and can normally be divided into subtasks that can be carried out in sequence. Before any of these can be performed, the personnel that shall execute a task must apply for a work permit. The work permit system is established to ensure scrutiny of factors related to HSE (Health, Safety and Environment) before job execution. The work permit for each task is discussed between representatives from the various disciplines in plenum and the job description and related safety measures are evaluated. Examples of such are safety equipment needed to perform the job safely. A general work permit flow is described in (NOG, 2006). After job execution, the job responsible logs feedback from the execution and closes the job in the maintenance management system.

The management systems for work orders and work permits are typically specialized enterprise resource planning ICT tools, like SAP ERP. These are good at managing data related to these activities, but are not normally regarded as best in human-interaction in terms of supporting decision making and providing a good overview.

3 THE IO-MAP PROTOTYPE

The IO-MAP prototype tool (Skjerve et al., 2011) was developed to explore how future technology could enhance collaboration between distributed teams, e.g. onshore and offshore. It was developed to visualize work permits and potential associated risk related to HSE using a graphical map representation. The work permits were given a geographical location and displayed in a map view. The usability study from this prototype shows that there is a huge potential in visualizing and presenting information this way. The project reported on in this paper makes use of learnings from the IO-MAP development and design (Braseth & Sarshar, 2012). Figure 1 illustrates the 2nd version of the IO-MAP tool.

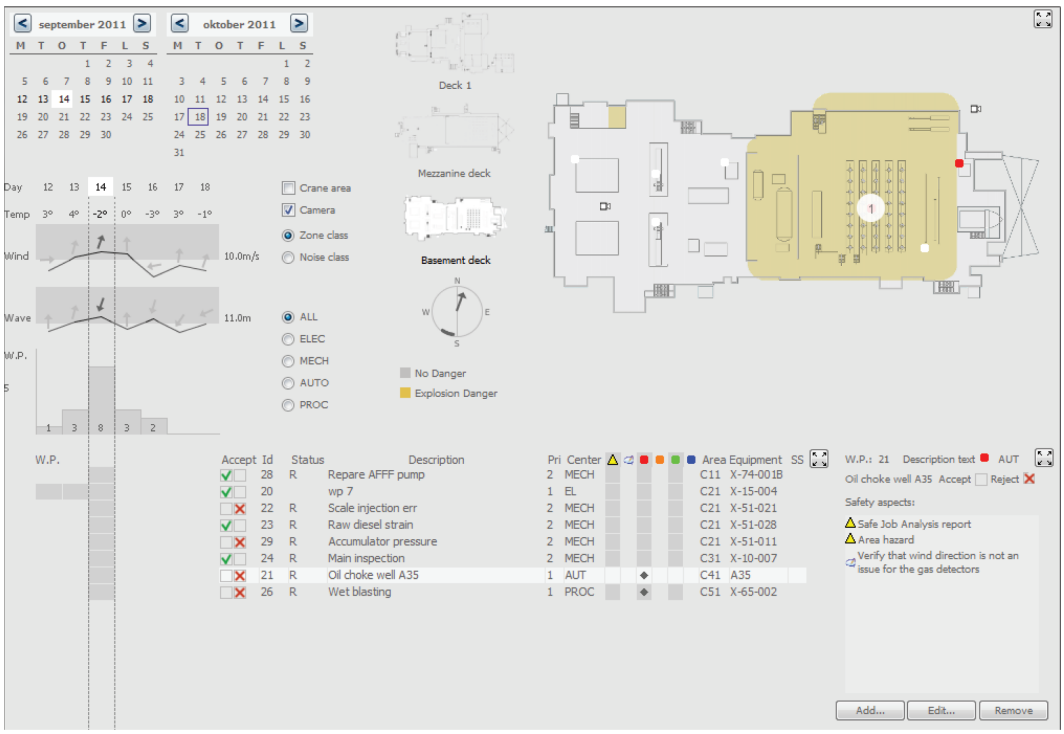


Figure 1. The 2nd version of the IO-MAP tool (Braseth & Sarshar, 2012).

4 METHOD

4.1 *Design rationale*

The focus of the design process was to create a large collaborative touch surface, which facilitated easier collaboration and discussion between technicians offshore. Design choices were therefore made on the background of creating a clear visualization of the current activity level on the installation to improve the decision making process. The design also aimed to create a means for accumulating different observations from different planners, further encouraging a discussion regarding the planned work permits.

4.2 *Iterative process*

The prototype's design was created through an iterative process consisting of several workshops. On two occasions expert evaluations with different interaction designers were conducted. The design phase spanned a total of eight iterations, where each workshop or expert evaluation resulted in a new iteration. After the final iteration, the resulting design was implemented in a high fidelity prototype.

4.3 *Implementation*

The design was implemented using various web technologies, namely JavaScript, SVG, and PHP. The architecture is based on traditional client-server architecture, with a database and client-side scripts on the server side, and scripting on the client-side to handle touch events, changes to the user interface, and calls to the server. The prototype was organized into six modules: Map, legend, activities, news, weather and info. The map module contains an SVG map of a selected deck, and shows activities based on location. Each activity on the map listens to touch events that trigger an "information box" to show and display information about the selected activity. The activity module is implemented as a bar chart using the JavaScript library d3.js, and based on a sorting algorithm that decides the placing of the different activities.

5 THE INTERACTIVE SURFACE

The interface design was based on a literature research on visualization and interaction design. Additionally, the design choices relied on IFE's (Institute for Energy Technology, Halden) expertise and experience with designing user interfaces for industrial control rooms. The design of the IO-MAP tool is the closest project to ours. While the focus when developing the IO-MAP tool was on the planners onshore, the tool developed here focuses on work permits planned to be carried out or under execution on current day.

The developed interactive surface is illustrated in Figure 2. The color scheme of the prototype is

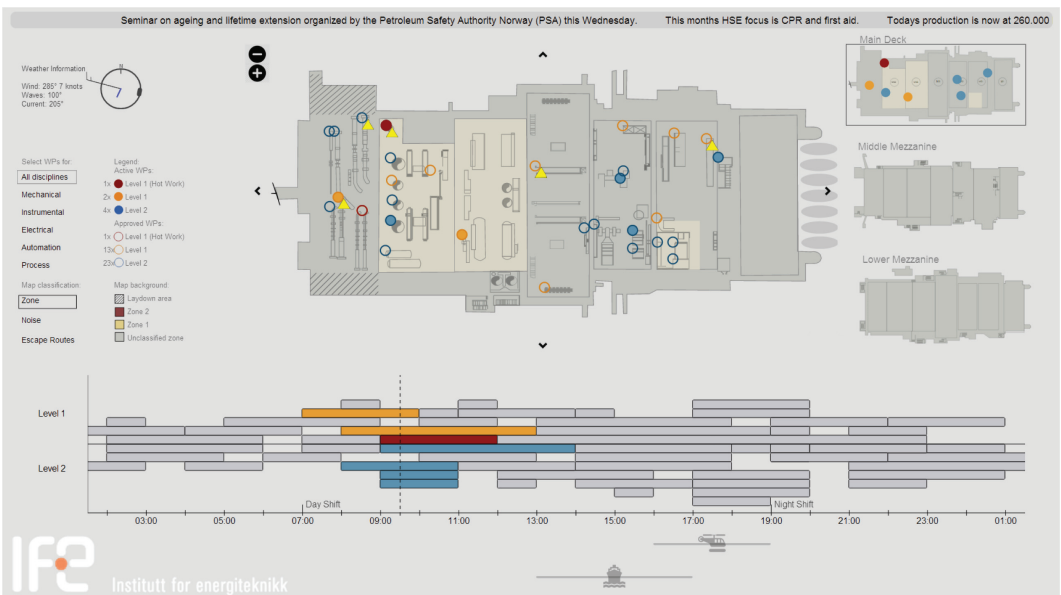


Figure 2. The interactive surface (HIØ, 2013).

muted, and strongly influenced by the IO-MAP prototype. The muted background without hard lines or borders is based on the design principles of Edward Tufte (Tufte, 1990), a design choice also used in several other interfaces created at IFE.

A grey color scheme was used for text and borders in order to avoid hard lines. Additionally, strong colors were avoided, and used deliberately only for warnings and potential hazards.

To maintain a user-friendly interface, the Schneiderman's principles (Schneiderman & Plaisant, 2010) were applied. The principle of consistency was maintained by using the same selection type for the corresponding elements in the prototype. Example of this is selection of decks where selected thumbnails in the map module were marked by a grey frame. Furthermore, active work permits on the map and selected work permits in the graph or map were marked by the same white border.

The prototype consists of six modules: legend, activity, info, weather, news and map. The map module presents the deck of an offshore installation. Thumbnails representing other decks in the installation can be used to change the deck displayed in the map module. An additional feature provided by the map module is the possibility to zoom in on the selected map. When zoomed in one or more levels, the map offers a more detailed view of the deck, displaying smaller equipment not presented in the previous zoom level. When zoomed in, the map can also be "panned" using a drag gesture. In order to maintain overview of the platform, changing deck while zoomed in will retain the zoom and pan placement of the map. This way, looking for dangers in the levels above or below an activity is easier and encouraged.

Work permits are classified using three different colors. Level 1 work permits are colored yellow, and work permits involving hot work are colored red. Level 2 work permits are colored blue. Work permits involving hazards will display warnings in form of a yellow triangle next to the circled work permit on the map. Activities, which are scheduled but not started, are visualized as unfilled circles. When a job is started, the circle is filled using the corresponding color. By selecting an activity on the map using the tap gesture, the information box module is invoked.

The information box module contains information regarding the highlighted activity, in the form of a transparent pop-up box. The information displayed is: Work Permit ID, Equipment ID, Work Permit Level, start and end times, a textual description of the work permit, a hot work tag, discipline tag and a hazard description. This box provides contextual information regarding the selected work permit and is displayed both when interacting with the map module, as well as the activity module.

The activity module consists of work permits of all types visualized as bars. Each work permit bar has a start and stop time which is extracted from a database. The work permits are placed in the graph using a simple algorithm, sorting the jobs by length and work permit type. The work permits, which are not currently active, are displayed as grey. A currently active work permit is displayed using its corresponding color. These colors are explained in the legend module.

Furthermore, the legend module explains the color codes of the different map zones such as "laydown area" as well as a count of currently active and scheduled work permits. The legend allows for filtering both active and scheduled work permits by discipline such as "Mechanical" and "Electrical". These filters could help different planners focus on their discipline and its interaction with others, as they have different backgrounds, experiences and concerns when conducting their planning. This filtering also affects the count of current jobs, in order to allow the users to quickly assess the current activity level on the platform for the chosen discipline. As a final functionality, the map can also be edited to different map classifications, highlighting noise levels, escape routes or the default view presenting the different classification zones of the deck.

The weather module provides the information surface with valuable condition information such as wind force and direction as well as wave and current direction. This weather info may be relevant to leaders and technicians before the work permit is initiated. This module along with the news module works in isolation from the other modules, but serves the surface in providing a better overview of the platform. The news module displays announcements and news, which may be relevant to the execution of planned work permits.

6 USABILITY STUDY

The functional prototype was evaluated in a usability test, by two participant groups. The first group was students with previous IO backgrounds, and the second group was employees at IFE with relevant experience the field of IO or the petroleum industry. The participants were not actual end users.

The main purpose of the usability test was to assess to what extent the prototype facilitates a group of users to perceive an overview of the activity level on a petroleum installation. Another focus of the evaluation was to appraise if the prototype visualizes risk and concurrency conflicts. A final aspiration was to evaluate if the prototype can be useful as a tool for a group of people to

collaborate and discuss the plan and ongoing activities. The usability test was conducted at IFE's Future Laboratory, see Figure 3. Previously, the prototype was prepared and tested to be working on a large touch surface in the Future Laboratory. Although, not all planned features were ready for testing core functionality was implemented. At the time of testing, area selection, equipment selection and the weather module was not implemented, and therefore not tested in the scenarios.

Zooming on the map for greater detail was implemented, however, as there were issues with this functionality; this was also omitted from the scenarios.

The usability test consisted of five phases: Introduction, training session, scenarios, questionnaire and interview. In the introduction the participants were provided a small introduction of the evaluation and the prototype, and were then asked to sign a form of consent. In order to prepare the users for the prototype, there was a small training session in which the users were trained in the functionality of the prototype. A technical assistant was the tutor for this session, and helped the participants navigate and understand the functionality of the prototype. Following the training session, each participant was assigned a fictive role for the scenarios. These roles were based on actual job descriptions for onshore and offshore personnel. Each role had different goals and responsibilities to keep in mind during the testing. The roles included:

- Platform Manager
- Health, Safety and Environment Manager
- Maintenance and Operation Manager
- Leader of Mechanical technicians
- Leader of Electrical technicians

The scenarios were created to be as realistic as possible, and were designed to enable the users to test all the functionality in the prototype. There were a total of six scenarios. The scenarios were created to explore different possibilities of using the prototype to evaluate the work permits of the day plan. The intent of the scenarios was also to find potential conflicting activities, consequences of delayed activities or possible hazards. As each participant had his or her own goals concerning their role, the user test format facilitated discussion surrounding the scenarios. In order to facilitate discussion, the scenarios were made to be approved



Figure 3. Illustration of the interactive surface in use on a large touch screen at IFE's Future Laboratory.

by one point of view, but not another. In addition to the scenarios, there were hidden conflicting work permits and problems in the schedule. These "Easter eggs" were hazards, which would cause problems in carrying out the planned activities.

After the participants had completed the different scenarios, they were asked to fill out a questionnaire. The questionnaire was based on a questionnaire previously used in the usability study to evaluate the IO-MAP (Skjerve et al., 2011). The questionnaire was divided in three parts: participant's background, information—and risk visualization, and usability. The usability test was concluded with a semi-structured group interview, designed to gain further understanding of the participant's experience of the prototype, and to facilitate a group discussion concerning the scenarios and the prototype. Most of the questions in the interview were intended to give an answer to whether or not the prototype fulfilled the research questions. Additional questions were based on observations from the solving of the scenarios.

7 RESULTS

The results from the questionnaire are displayed in Table 1 and Table 2, which are divided in two parts. The first part concerns the scenarios; how easily they could identify risk, and how well the prototype visualized information. The other part consists of statements based on the System Usability Scale (SUS), where every other statement is positive, and the other negative. All statements are ranged from the scale of 1 (strongly disagree) to 7 (strongly agree).

Table 1. Student group results.

Question no	Avg	Min	Max	SD
Scenario evaluation				
1	3.33	4	5	0.58
2	2.66	2	6	1.15
3	4	3	6	1.73
4.1	2.66	2	4	1.15
4.2	2	1	3	1
4.3	4	4	4	0
Prototype evaluation				
1	3.33	1	7	3.21
2	5.66	5	7	1.15
3	3	2	4	1
4	5.66	4	7	1.58
5	2.33	2	3	0.58
6	5.66	4	7	1.53
7	1.66	1	3	1.15
8	4.33	3	6	1.53
9	2	1	3	1
10	6.33	6	7	0.58
11	1.66	1	2	0.58

Table 2. IFE employee's results.

Question no	Avg	Min	Max	SD
Scenario evaluation				
1	3.33	4	5	0.58
2	2.66	2	6	1.15
3	4	3	6	1.73
4.1	2.66	2	4	1.15
4.2	2	1	3	1
4.3	4	4	4	0
Prototype evaluation				
1	3.33	1	7	3.21
2	5.66	5	7	1.15
3	3	2	4	1
4	5.66	4	7	1.58
5	2.33	2	3	0.58
6	5.66	4	7	1.53
7	1.66	1	3	1.15
8	4.33	3	6	1.53
9	2	1	3	1
10	6.33	6	7	0.58
11	1.66	1	2	0.58

7.1 *Interviews*

What was your overall impression of the prototype? The participants agreed that the overall impression was good. It was stated by one of the participants that the prototype was intuitive and pleasant to use. Another participant stated that "The prototype is a great discussion tool for gathering different domain knowledge in a group", and argued that this was probably the greatest strength of the prototype.

What do you feel worked well? What did not work well? Why? The option to filter on disciplines was regarded as a very useful function, and the fact that all information was displayed in one page was considered to be good, as it was easy to get an overview of the situation without navigating to different pages. The prototype received negative feedback in regards to responsiveness, and the participants felt the hardware did not respond well to the touch gestures. Regarding visualization, it was suggested to add arrows to escape routes. Some participants also felt that it was difficult to locate a specific activity, and suggested adding an ID in addition to the circle representing an activity.

What were your thoughts on solving the different scenarios? The participants thought the task of solving the scenarios went very good, some also said it was fun. The only scenario they agreed were troublesome was the one where they had to find an

activity with the only information given was the ID and the discipline.

Were some of the scenarios more difficult to solve than others? One of the groups had trouble with the scenario where they had to find an activity with crane work that could not be executed while the helicopter was on deck. They explained that they did not know about the expression "laydown-area", which was the clue to discovering this hazard.

How was it working collaboratively on the prototype? Several of the participants felt that this was one of the strengths of the prototype, while one of participant mentioned that while it was good for discussion, simultaneous interaction was not possible.

Do you have any suggestions for improving the prototype? Many of the suggestions for improvement were mentioned earlier in the interview, such as adding IDs to the activities, and adding arrows to the escape routes. Other improvements that had been mentioned earlier were adding crane activities as a discipline, and being able to drag the timeline to a different time, or rearranging the activities. Other suggestions were to visualize the number of workers for each activity, and to display an indication of the duration of an activity on the map.

8 CONCLUSIONS AND FURTHER WORK

The primary objective of the project was to create a prototype of a collaborative interactive surface intended to facilitate discussions concerning the day plan, and to give a clear visualization of the amount of activities on a petroleum installation. Based on the results from the initial usability tests we can conclude that the prototype has achieved the objectives of displaying a clear overview of the activity level, and facilitated a group to collaborate and discuss the day plan. The reason why the prototype could accommodate for such behavior is that an interactive surface which gives a clear visualization of the activities—their location and the surrounding circumstances—allows for more accurate discussion than without the use of visualization. Consequently it is easier for the individuals within the group to imagine the impact of each activity, and share this observation with the rest of the group. By gathering these individuals in front of the interactive surface it is likely that they will identify more potential hazards, errors and inconsistencies of the day plan than they would alone, or without the use of the tool. The systems they have available today are mostly one user desktop software solutions which do not support groups collaborating.

Further work include to test the tool with offshore personnel and other end users to get input for improvements and to better understand the overall objective of how technology can better mediate risk communication in IO.

ACKNOWLEDGEMENTS

The authors wish to thank the Center for Integrated Operations in the Petroleum Industry and the partners involved in this research.

REFERENCES

Braseth. A.O. & Sarshar, S. 2012. Improving Oil & Gas Installation Safety Through Visualization of Risk Factors, in Proc. of the *SPE Intelligent Energy International*, March 27–29, Utrecht, The Netherlands, 2012.

Kaarstad, M. & Rindahl, G. 2011. Shared Collaboration Surfaces to Support Adequate Team Decision Processes in an Integrated Operations Setting. In Proc. of the *ESREL 2011 Conference*, Troyes, France, 18th-22nd Sept. 2001. Advances in safety, reliability and risk management/Bérenguer, Grall & Guedes Soares (eds.). CRC Press, 2011, ISBN 978-0-415-68379-1.

Norwegian Oil and Gas Association (NOG) 2006. *Recommended Guidelines for Common Model for Work Permits (WP)*, rev. 2, 2006.

Østfold University College (HIØ), 2013. Online: http://www.it-stud.hiof.no/h13d28.

Sarshar, S., Skjerve, A.B. & Haugen, S. 2013. Towards an understanding of information needed when planning offshore activities. In Proc. of *Risk, Reliability and Societal Safety, ESREL 2013*, September 29th–October 2nd, Amsterdam, Netherlands, 2013.

Sarshar, S. & Rindahl, G.: Integrated Operation Collaboration Technologies—Remaining Challenges and Opportunities. In Proc. of the *SPE Intelligent Energy Conference and Exhibition* held in Utrecht, The Netherlands, 1–3 April 2014.

Schneiderman, B., & Plaisant, C. 2010. *Designing the User Interface*. (M. Hirsch & S. Sellinger, Eds.) (5th ed.). Pearson.

Skjerve, A.B., Sarshar, S., Rindahl, G., Braseth, A.O., Randem, H.O., Falmyr, O., Sand, T., & Tveiten, C.K. 2011. *The Integrated Operations Maintenance and Modification Planner (IO-MAP): The first usability evaluation—study and first findings,* Center for Integrated Operations in the Petroleum Industry, Project 4.1: Future Collaboration Environments, Halden, Norway, 2011.

Tufte, E.R. 1990. *Envisioning Information*. Graphics Pr. p. 82–83.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Graphical technique for practical dependability management

L. Barberá & A. Crespo
Department of Industrial Management, School of Engineering, University of Seville, Spain

K. Kobbacy
School of the Built Environment, Maxwell Building, University of Salford, UK

P. Viveros
Department of Industrial Engineering, Universidad Técnica Federico Santa María, Valparaíso, Chile

ABSTRACT: GAMM (Graphical Analysis for Maintenance Management) is a method that supports decision-making in the overall maintenance management through the visualization and graphical analysis of data, which has been developed and published by the authors. In addition, it allows for the identification of anomalous behavior in the equipment analyzed, whether derived from its own operations, maintenance activities, improper use of equipment or even as a result of design errors in the equipment itself. As a basis for analysis, the GAMM method uses a nonparametric estimator of the reliability function using all historical data or, alternatively, part of the history, allowing it to perform an analysis even with limited available data.

However, for successful results are strictly necessary the experience and advanced knowledge about maintenance management process. With regard to the interpretability of GAMM method, a set of basic rules have been developed in this paper. This set of rules aim to help and support to maintenance managers to get a right and objective interpretation, improving the decision making. Typically, engineers have validated intelligent software system performance by running test cases through a system and comparing results against known results or expert opinion. We adopt this method of validation by comparing the results of selected cases by GAMM with the recommendations of HIMOS (Hybrid Intelligent Maintenance Optimization System, University of Salford), which was compared and validated by an expert panel.

1 INTRODUCTION

The importance of the maintenance function management has grown in the past decade as a result of the continuous advancement of industrial organizations towards more efficient operations and improved productivity (Kah 2001). The basic concept leading to the maintenance engineering is the continuous improvement of the maintenance management process by incorporating knowledge, intelligence and analysis. They support the decision-making in the field of maintenance and are designed to enhance the global output of economic and operational result (Barbera 2012).

The development and application of graphical tools supporting decision making in the area of operational reliability (Birolini 2007) is a fundamental task to achieve an accurate and efficient management of assets and resources in an organization, even when there is a large number of devices with functional configuration that is highly complex. To obtain real applications of analytical models, practical, functional, innovative and simple tools must be generated (Barbera 2013). This will help to make tactical and operational decisions easier. Additionally, the development of simple technical tools to facilitate the exercise of analysis and results outcome (Nelson 1969) provides a framework for the control and monitoring of action plans implemented in terms of maintenance activities.

The GAMM (Graphical Analysis for Maintenance Management) (Barbera 2013) method is a graphical tool based on collected data related to the sequence of technical equipment revisions. This method of graphic analysis adds variables with useful information that allows the management to visualize support patterns and make decisions in the overall maintenance management, such as: number of technical revisions performed, type (corrective or preventative), duration, operational failure during the routine service, reliability of the equipment before the service, or the variability of equipment failure over a period of time. Moreover,

GAMM provides a visual representation from a complete or partial historical record of the maintenance work performed, showing different patterns of analysis that provide useful information for decision making and problem solving (Barbera 2013).

To help maintenance managers to make decision making based on GAMM analysis and interpretation, this article proposes a set of rule-based GAMM for preventive maintenance program evaluation. The maintenance manager will be able to make the best decision making according to some basic rules about the GAMM graphics (Graphic 1, Graphic 2). The set of rules provides easy access to certain variables patterns showing useful information for maintenance management and decision making in the short, medium and long term. This paper is a complementary research of GAMM method, published by Barberá et al. in 2013.

2 PROBLEM STATEMENT AND PURPOSE OF STUDY

GAMM method (Barbera 2013) is a support tool for operational maintenance management and preventive maintenance program evaluation. The tool provides useful information regarding the reliability and maintainability of systems or equipment for analysis when considering variables such as type of intervention, duration of intervention or the existence of a stop during the intervention of the equipment/system. This broadens the spectrum display for maintenance management, acquiring new evaluation parameters and graphically determining possible areas of improvement.

The graphics of GAMM (Graphic 1, Graphic 2) illustrate aspects such as: trend of the interventions, deviation in the frequency of preventive interventions, reliability function, efficiency of maintenance operations, impact by unavailability, quality in the intervention performance, quality in use and operation of equipment by staff responsible of it, among others. Thus, the tool proposed provides information that is useful, clear and easy to interpret.

However, for successful results are strictly necessary the experience and advanced knowledge about maintenance management process. With regard to the interpretability of GAMM method, a set of basic rules have been developed in this paper. This set of rules aim to help and support to maintenance managers to get a right and objective interpretation, improving the decision making. Afterwards, in this paper we adopt the method of validation using data of (Kah 2001), by comparing the results of selected cases by HIMOS with the recommendations of an expert panel and GAMM method.

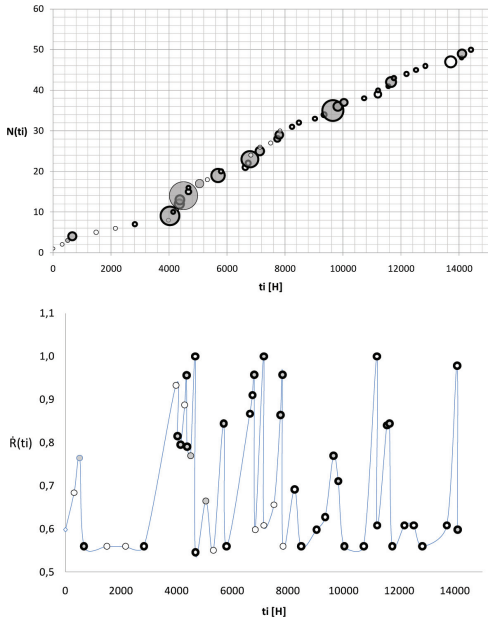
HIMOS (Hybrid Intelligent Maintenance Optimization System) is a system for decision support in maintenance management. More specifically, HIMOS helps to determine the optimal maintenance policy, essentially the frequency of Preventive Maintenance (PM) which minimizes the sum of down time due to PM and CO (Corrective Maintenance). HIMOS uses an 'intelligent' decision support system to carry out an automated analysis of the maintenance history data. Maintenance data are presented to the system and the most suitable mathematical model from a model-base is identified utilizing a hybrid knowledge/case based system (KBS = CBR) (Kah 2001). Thus initially a rule base is applied to select a model. If no model is matched, the system reverts to its historical case-base to match the current case with a similar case that has been previously modelled. This double reasoning adds to the system's true learning capabilities (intelligence) and increases the rate of success of model selection. The study results include optimal PM intervals for a sample of industrial data sets.

3 REVIEW GAMM METHOD

According to (Barbera 2013), the Graphical Analysis for Maintenance Management (GAMM) is a quantitative and qualitative analysis method that intends to support decision making in maintenance management using the logic of a dispersion diagram and also integrating the following variables: type of intervention, duration of intervention, and state of equipment/system during the intervention. The combination of these new variables with a graphic display (Graphic 1 and 2) of the sequence of interventions generates synergies with regard to the information given by the diagram, thus establishing new sources of analysis.

In addition, GAMM is able to estimate the reliability function, which is calculated using the algorithms on the basis of the nonparametric method of Nelson–Aalen, and evaluated in the time ti, that is, in the moment before the intervention. The estimation method can consider both the historic full data and the censored historical data.

GAMM provides useful information regarding the reliability and maintainability of systems or equipment for analysis. This broadens the spectrum display for maintenance management, acquiring new evaluation parameters and graphically determining possible areas of improvement. The graph-



Figures 1 and 2. Examples of the graphs generated by GAMM (Graphic 1, Graphic 2).

ics of GAMM illustrate aspects such as trend of the interventions, deviation in the frequency of preventive interventions, reliability function, efficiency of maintenance operations, impact by unavailability, quality in the intervention performance, quality in use, and operation of equipment by staff responsible of it, among others.

GAMM allows viewing different patterns of analysis that provide useful information to assist decision making at the operational level, for example:

- Trends in the behavior of the interventions.
- Preventive Maintenance (PM) deviation: adding variable analysis as the type of intervention can display the frequency of completion of PM (programmed) and therefore can track and monitor the attainment of the established PM frequencies in the program.
- Quality of operations and/or PM: a graphic display of interventions by type (preventive or corrective) provides the sequence recognition of certain patterns that can define the quality of operation and/or the performing PM activities. This way, by observing corrective interventions within preventive ones, sequences of corrective short term stop pages and accumulation of corrective interventions immediately follow a PM intervention; the existence of problems in the execution of the duties or how the equipment operates is evident.
- Reliability function: GAMM shows the reliability of the equipment/system at preintervention, complementing the analysis of the quality of operation and/or PM. This demonstrates, for example, the existence of corrective interventions in periods of high levels of reliability (this indicate abnormal premature failure).
- Efficiency and quality in the implementation of interventions: the duration of each intervention is represented by the size of the bubble in GAMM (Graphic 1). This variable identifies those interventions that are beyond the average times of intervention, questioning if the schedule of the workload is right or if the deviation in execution times is due to external factors such as lack of tools, waiting for parts, lack of staff training, and so forth.
- Impact on production: the stop variable (Det) determines the status of equipment/system at the time to intervene. The bubbles with hard shaded border represent interventions in which the equipment stops, affecting their individual availability and possibly affecting the overall system availability.

Finally, GAMM is a quantitative and qualitative analysis that intends to support the decision making in the overall maintenance management (Barbera 2013), which helps to reduce the high costs of unavailability of the system or the maintained equipment as well as the costs associated with unforeseen maintenance interventions. The combination of analysis patterns presented provides valuable information to implement action plans to improve the global maintenance management. This specifically included the performance of equipment and, ultimately, to achieve a management that is efficient, effective, and opportunistic, identifying gaps to help determine the root causes thereof.

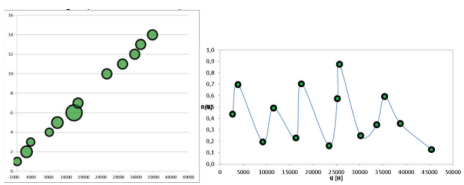
4 RULE BASE OF GAMM METHOD

In the industrial environment, it requires expertise to choose the most appropriate decision to a situation represented by real world data. To help maintenance managers to make decision making based on GAMM analysis and interpretation, a set of rule-based GAMM for preventive maintenance program evaluation is required. The maintenance manager will be able to make the best decision making according to these set of rules about the GAMM graphics (Graphic 1, Graphic 2). The rules provides easy access to certain variables patterns showing useful information for maintenance management and decision making in the short, medium and long term.

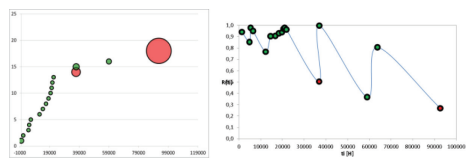
Table 1. Rule base of GAMM method.

Rule 1	If the Graphic 1 shows a line of $N(t_i)$ (number of interventions) vs t (time) which has approximately constant slope and $R(t_i)$ ranging between $R(t_i)$ max = 1.00 and $R(t_i)$ min = 0.70, then you have an acceptable[R1.1] maintenance program. If the line of $N(t_i)$ vs t has not a constant slope or $R(t_i)$ has sudden or large fluctuations, then the maintenance program is not optimal. R1.1: regular number of maintenance events over an increasing operating time which means that a certain average reliability over time is guaranteed thanks to your maintenance activities.
Rule 2	If number of PM[1] interventions > 80% of the total interventions ($N(t_i)$), then it could be considered as an acceptable[R2.1] level of PM. If number of PM interventions > 95%, then increase PM interval could be considered[R2.2]. If number of PM interventions < 80%, then it could be necessary to evaluate the quality and frequency of the PM interventions. Decrease PM interval could be considered[R2.3]. R2.1: according to many industry best practices. However we should check the effects of existing failures and how they are distributed just in case they may become critical (size of the circle). R2.2: Number of PM interventions > 95% could also be a consequence of excessive maintenance to some non-critical failure modes. R2.3: Number of preventive interventions below 80% are scenarios showing room for potential improvement of PM policies.
Rule 3	If there are CO[2] interventions carried out in periods of high reliability ($R(t_i) > 0.85$) or shortly after a PM intervention (less time than the average duration between PM interventions), then the PM task before that CO intervention could be poor (problems in the execution of PM intervention) or the failure could be the result of improper equipment operation, among others, and it is necessary to evaluate it.
Rule 4	If there is a logic/constant pattern of PM durations[R4.1] (downtimes, according to the tasks carried out on each intervention), then the PM program duration shows consistent maintainability. If there is a high variability of PM durations, then deviations in execution time due to external factors (lack of tools, waiting for parts, lack of staff training, accessibility problems, etc.) should be checked. R4.1: However, in some cases there are two or more different patterns of PM duration due to, e.g., overhauls.
Rule 5	If the temporal pattern of time between PM interventions is not constant, then the maintenance program is probably not well scheduled or its fulfillment should be reviewed.

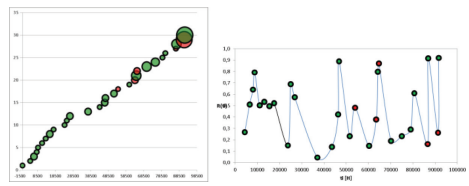
[1]Preventive maintenance.
[2]Corrective maintenance.



Figures 3 and 4. Graphic 1 and Graphic 2 of GAMM for using data set 1.



Figures 5 and 6. Graphic 1 and Graphic 2 of GAMM for using data set 2.

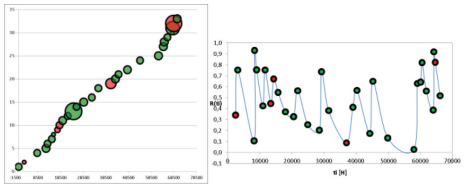


Figures 7 and 8. Graphic 1 and Graphic 2 of GAMM for using data set 3.

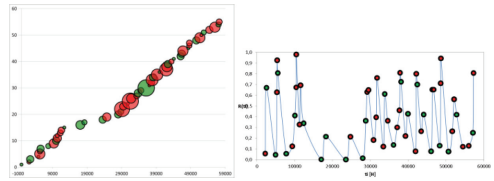
5 VALIDATION OF RULES

Validation aims at substantiating that GAMM performs with an acceptable level of accuracy. In the literature several validation methods are found. In (O'Keefe 1987), there is a review of qualitative and quantitative validation methods for expert systems. In O'Leary 1987), a different framework for system validation is suggested, which includes content validity, criterion validity, objectivity and reliability. Typically, engineers have validated intelligent software system performance by running test cases through a system and comparing results against known results or expert opinion. We adopt this method of validation by comparing the results of selected cases by GAMM with the recommendations of HIMOS, which was compared and validated by an expert panel.

To validate the use of the proposed interpretation rules, GAMM method was applied to analyze a total of 5 sets of historical data, from the petrochemical industry (Kah 2001).



Figures 9 and 10. Graphic 1 and Graphic 2 of GAMM for using data set 4.



Figures 11 and 12. Graphic 1 and Graphic 2 of GAMM for using data set 5.

Table 2. Comparison between HIMOS and GAMM recommendations for 5 data sets.

Data set 1	
HIMOS	Increase PM interval from 135 to 176 days (CBR-Geometric I model)
GAMM	R(ti) has sudden or large fluctuations: **maintenance program is not optimal**. Number of PM interventions > 95%: **increase PM interval could be considered**. There is a logic/constant pattern of PM durations (downtimes, according to the tasks carried out on each intervention): **PM program duration shows consistent maintainability**. The temporal pattern of time between PM interventions is not constant: **maintenance program should be reviewed**.
Data set 2	
HIMOS	Increase PM interval from 177 to 403 days (CBR-RPOW model)
GAMM	The line of N(ti) vs t has not a constant slope and R(ti) has sudden or large fluctuations: **maintenance program is not optimal**. Number of PM interventions > 95%: **increase PM interval could be considered**. There is a logic/constant pattern of PM durations (downtimes, according to the tasks carried out on each intervention): **PM program duration shows consistent maintainability**. The temporal pattern of time between PM interventions is not constant: **maintenance program should be reviewed**.
Data set 3	
HIMOS	Increase PM interval from 159 to 223 days for the first sequence but gradually decrease to 86 days (tenth sequence) (NHPPScoSpm model)
GAMM	R(ti) has sudden or large fluctuations: **maintenance program is not optimal**. Number of PM interventions > 95%: **increase PM interval could be considered**. There are CO interventions carried out in periods of high reliability (R(ti) > 0.85) and also shortly after a PM intervention (less time than the average duration between PM interventions): **PM interventions before that CO interventions could be poor** (problems in the execution of PM intervention) or the failure could be result of improper equipment operation **and it is necessary to evaluate them**. There is a logic/constant pattern of PM durations* (downtimes, according to the tasks carried out on each intervention): **PM program duration shows consistent maintainability**. The temporal pattern of time between PM interventions is not constant: **maintenance program should be reviewed**.
Data set 4	
HIMOS	Increase PM interval from 108 to 140 (first sequence)–117 (tenth sequence) days (RPDWSco)
GAMM	R(ti) has sudden or large fluctuations: **maintenance program is not optimal**. Number of PM interventions > 95%: **increase PM interval could be considered**. There are CO interventions carried out shortly after a PM intervention (less time than the average duration between PM interventions): **PM task before that CO intervention could be poor** (problems in the execution of PM intervention) or the failure could be the result of, improper operation of equipment **and it is necessary to evaluate them**. There is a logic/constant pattern of PM durations* (downtimes): **PM program duration shows consistent maintainability.** The temporal pattern of time between PM interventions is not constant: **maintenance program should be reviewed**.
Data set 5	
HIMOS	Decrease PM interval from 103 to 21 days (Delay-time Model, Weibull distribution, manual selection mode)
GAMM	Graphic 1 shows a line of N(ti) (number of interventions) vs t (time) which has partially constant slope and R(ti) has sudden or large fluctuations: **maintenance program is not optimal**. Number of PM interventions < 80%: **it could be necessary to evaluate the quality and frequency of the PM interventions. Decrease PM interval could be considered**. There are CO interventions carried out in periods of high reliability (R(ti) > 0.85) and shortly after a PM intervention (less time than the average duration between PM interventions): **PM task before that CO intervention could be poor** (problems in the execution of PM intervention) or the failure could be the result of improper operation of equipment **and it is necessary to evaluate them**. There is a high variability of PM durations: **deviations in execution time due to external factors (lack of tools, waiting for parts, lack of staff training, accessibility problems, etc.) should be checked.** The temporal pattern of time between PM interventions is not constant: **maintenance program should be reviewed**.

In (Kah 2001), these data sets were analyzed by an expert panel (five experts in maintenance modeling) and HIMOS with the aim of comparing their recommendations of appropriate maintenance policies for each data set. Table 2 summarises the recommendations of HIMOS and GAMM.

It is interesting that, being the general HIMOS advice is in accord with GAMM, GAMM is able to show additional information considering different variables and using the same data sets.

As can be seen in Table 2, for each data set there was general agreement between the results produced by HIMOS and the recommendations of GAMM. Thus, it was agreed that the proposed rule base is suitable for the right and objective interpretation of GAMM method, improving the decision making based on this method.

This expertise is usually provided in a Knowledge-Based System (KBS) or 'intelligent' DSS (IDSS) by the knowledge subsystem. In GAMM, this expertise concerns the right interpretation of the graphs (performed from a data set) based on the rule base proposed. The rules were developed by looking for patterns in different data sets for different equipments and considering all aspect of GAMM method, such as: relative numbers of CO and PM events, range of PM intervals, intervention durations and reliability before of each intervention, among others. The knowledge base implemented in GAMM consists of the set of 5 rules shown in Table 1.

6 CONCLUSIONS

The aim of this paper was to present and validate a proposed rule base to help and support to maintenance managers to get a right and objective interpretation of the graphs of GAMM method, which has been developed and published by the authors. Additionally, for validation of the proposed interpretation rules, GAMM method was applied to analyze a total of 5 sets of historical data (shown in the appendix) from the petrochemical industry, previously analyzed by HIMOS. Comparing their recommendations, for each data set there was general agreement between the results produced by HIMOS and the recommendations of GAMM.

As a future research line, it is interesting that the joint application of HIMOS and GAMM could be considered as a quantitative and qualitative analysis that intends to support the decision-making in the overall maintenance management and helps to reduce the high costs of unavailability of the system or equipment, as well as the costs associated with unforeseen maintenance interventions. The combination of the different analysis patterns provides valuable information to implement action plans to improve the global maintenance management. This specifically included the performance of equipment/systems by optimization of the PM cycle interval for a repairable system (frequency) and, ultimately, to achieve a management that is efficient, effective and opportunistic, identifying gaps to help determine the root causes thereof. So, the joint application of HIMOS and GAMM could be a support tool for operational maintenance management of short and medium term. They provide useful information, clear and easy to interpret which can be checked with one another in order to determine the optimal maintenance policy (frequency of preventive maintenance). This broadens the spectrum display for maintenance management, acquiring new evaluation parameters and determining possible areas of improvement. This way it could be possible to show quantitative and qualitative maintenance implemented activities and its operational implications on the reliability and maintainability of the equipment or system, within the maintenance management process.

REFERENCES

Barberá L., Crespo A., Viveros P., Stegmaier R. 2012. "Advanced model for maintenance management in a continuous improvement cycle: integration into the business strategy". International Journal of System Assurance Engineering and Management, (Jan–Mar 2012) 3(1):47–63. DOI 10.1007/s13198-012-0092-y.

Barberá, L., Crespo, A., Viveros, P. & Arata, A. 2013. "The Graphical Analysis for Maintenance Management Method: A Quantitative Graphical Analysis to Support Maintenance Management Decision Making". Journal of Quality and Reliability Engineering International, Vol. 29, 77–87. Copyright © 2013 John Wiley & Sons, Ltd. DOI: 10.1002/qre.1296.

Birolini A. 2007. "Reliability Engineering". 5th ed. Springer Berlin Heidelberg New York. ISBN 978-3-540-49388-4.

Kobbacy K.A.H. and J. Jeon. 2001. "The development of a Hybrid Intelligent Maintenance Optimisation System (HIMOS)". Journal of the Operational Research Society (2001) 52, 762–778. © 2001 Operational Research Society Ltd. All rights reserved. 0160-5682/01.

Nelson, W. 1969. "Hazard Plotting For Incomplete Failure Data", Journal of Quality Technology 1, pp. 27–52.

O'Keefe R.M., Balci O. and Smith E.P. 1987. "Validating expert system performance". IEEE Expert Winter: 81–87.

O'Leary D.E. 1987. "Validation of expert systems—with application to auditing and accounting expert systems". Decis Sci 18: 468–486.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A discussion of the risk-management and the rule-compliance regulation regimes in a security context

S.H. Jore & A. Moen
University of Stavanger, Norway

ABSTRACT: In recent years, the use of risk-management approaches for protecting vital societal functions and critical objects has increased in many countries. In Norway, new object security legislation based on a risk-management approach has been passed, and new standards for security risk analysis have been developed.

Hopkins (2011) has described two different regimes for regulating risk; "the risk-management regime" and "the rule-compliance regime". This paper aims to describe the consequences of these two regimes in a security context, and to discuss some of the challenges of applying a risk management regime within the area of security. We conclude that risk-management and rule-compliance are intertwined and complementary strategies. The issue, therefore, is not to decide between the two; it is to get the balance right.

There are some aspects with security risks that make the application of a risk-management regime challenging; Terrorism is a highly uncertain risk and the political aspect of the threat and how to handle it implies that the risk of terrorism is highly ambiguous. Acts of terrorism are obscure, low-frequency events where strategically calculating human beings are the ones who possess the threat. Terrorists can strike suddenly, without warnings and cause enormous damage. Additionally, often the area of security is just one of several risks an organization has to take into account, and most organizations will have the main focus on safety risks because these will be assessed to have a higher probability of occurring. Furthermore, most organizations in Norway lack security competence, benchmarking is difficult because the area is often classified, and little is known about the effect of counterterrorism measures.

1 INTRODUCTION

While security from intentional acts, such as terrorism, used to be an area of secrecy where the security services played a central part, mitigation and protection from the threat of terrorism has nowadays become an area where citizens, companies and different official bodies have a shared responsibility. This is reflected in the many official strategies against terrorism which have been published in most Western countries in recent years (Aly, 2013; Jore, 2012). In order to manage the risk of terrorism, governments in most Western countries have highlighted risk-management thinking as a tool for protecting critical objects and critical infrastructures against the threat of terrorism, especially after the terrorist attack in the US on September 11th 2001 (9/11) (Office U. S. G. A., 2005).

Traditionally, Norway was seen as a quiet outpost of Europe. However, in the aftermath of the 9/11 terrorist attack the focus on terrorism as a risk against Norwegian society has gradually increased (Jore & Njå, 2008). The bombing of the Norwegian government complex and the shooting massacre on the island of Utøya on 22. July 2011 where totally 77 people were killed (Gjørv, 2012), and the terrorist attack on the Algerian oil facility in In Amanas in January 2013 where 5 Norwegians employees in the Norwegian oil company Statoil were killed (Statoil, 2013), have further increased the focus on protection from the threat of terrorism in Norway. After these two incidents, both evaluation reports concluded that there had not been sufficient focus on security from intentional acts, and that the attack could either have been avoided or the impacts could have been reduced if the companies or official bodies responsible had taken the necessary precautions (Gjørv, 2012; Statoil, 2013). In the aftermath of these events new object security legislation based on a risk-management approach was passed in January 2011 (Forsvarsdepartementet, 2011), and in order to lay a foundation for better risk analysis of intentional acts three standards for protection against intentional acts have either been published or are in progress (Standards Norway 2012; 2014a,b).

Several scholars have over the years discussed and described two different regimes for regulating risk. Different terminologies have been used to describe these two regime (Ayres & Braithwaite, 1992; Gunningham & Rees, 1997; Baldwin & Cave, 1999; Hale et al., 2002; Hood et al., 2001; Lindøe,

2002; Hutter & O'Mahony, 2004; Hutter & Power, 2005; Hutter & Jones, 2007; Braut & Lindøe, 2008; Baldwin et al., 2010; Coglianese & Mendelson, 2010; Baram et al., 2013. Hopkins (2011) refers to these regimes as the "risk-management regime" and the "rule-compliance regime". The distinction and the balance between these two regimes have been extensively discussed, and most regulatory regimes today build on a mixture of these two regimes. However, most of these discussions have been related to the area of safety from non-intentional accidents. The consequences and the balance between the two regulatory regimes have not been discussed in relation to security from intentional crimes. This paper aims to describe the consequences of these two regimes in a security context, and to discuss some of the challenges of applying a risk-management regime within the area of security. In line with Piètre-Cambacédès & Chaudet (2010) we call protection from terrorism or other intentional crimes for security—in contrast to safety risks witch implies protection from non-intentional acts.

We conclude that risk-management and rule-compliance are intertwined and complementary strategies. The issue, therefore, is not to decide between the two; it is to get the balance right. Furthermore, because of the nature of the security risk the risk-management regime is challenging in a security context.

2 THE RULE-COMPLIANCE REGIME

Historically, rule-compliance was the dominating approach for how to regulate hazardous activities. Governmental regulation of HSE was during the first part of the 20th. Century dominated by a top-down command and control-based regulatory model characterized by prescriptive regulations, involving detailed, specific and often technical requirements. During this time period, the authorities met new risks related to technological development by applying more prescriptive regulations. In most industries, such as nuclear and oil and gas, risk management was traditionally based on this prescriptive regulating regime, in which detailed requirements for the design and operations were specified (Lindøe, Kringen, & Braut, 2012). Although this regime is often referred to as the historical regime which today is challenged by the risk-management regime, this regime is still present in many sectors. In the area of security, this is the regime which is applied for example in the post-911 aviation security regime.

2.1 *Advantages with the rule-compliance regime*

In the rule-compliance regime, the authorities set out detailed regulations in order to steer the direction of companies, or others, in their security work. This will lead to a uniform implementation of security measures, meaning that each organization or critical infrastructure covered by a specific regulation will have the same level of security independently of an organization's perception of available resources, threat picture and former experience with the threat of intentional crimes. In a security context, this means that organizations or owners of critical infrastructures will implement the same level of security measures independently of whether a company or an owner of a critical object belong to a sector which has historical experience with acts of intentional crimes or terrorism. The post 9/11 aviation security regime illustrates this point. After the 9/11 terrorist attack, harmonization of airport security was the main goal of the EU regulations. As a consequence, all commercial airports in Europe had to follow the same security regime regardless of national or local threat assessments or previous experiences with acts of terrorism (Engen & Olsvik, 2010; Jore & Njå, 2012). The outcome of this regime was that small airports in rural parts of Norway were bound by the same regulations as giant airports in Europe such as Frankfurt or Heathrow.

The rule-compliance regime might lead to an easier management process within an organization, because the government agencies or supranational official bodies, such as the EU, have set the rules for when and how to implement security measures. The organization itself does not have to invest time and resources in evaluations of whether it should implement security measures or not, and this can make the decision-making process easier for the organization or the owner of a critical infrastructure or object. In aviation, the airports simply follow the regulations dictated by the EU. There is no decision-making process on each airport for deciding whether the airport should implement the measures or not.

It can also be claimed that the rule-compliance regime simplifies the job of the official bodies responsible for inspections since it is easier for official bodies to clarify whether a company has the expected level of security or not (Lindøe et al., 2012; Stålesen, 2011). The task of those who are doing inspections is simply to decide if the rules are followed or not, and not to decide whether the security measures are effective and in line with the threat landscape.

2.2 *Challenges with the rule-compliance regime*

Despite these advantages with the rule–compliance regime, there are also some challenging aspects with this way of managing security risks.

2.2.1 *The rules are in focus*

One challenging aspect with the rule-compliance regime is that it is the rules that are in focus, and not necessarily how to achieve the optimal level of security. Companies and inspectors operating in this security regime will be concerned with whether the rules are followed rather than how to achieve the optimal level of security from intentional crimes. In aviation, the prescriptive and detailed regulation regime offers no opportunity to locally assess and mitigate the risk of terrorism, unless there is an assessment leading to a strengthening of security beyond minimum requirements. Studies of the post-9/11 security regime in aviation have showed that the industry informants have been skeptical about the actual risk-reducing effects of the new security regime. They described several areas where the detailed and stringent regulations were problematic or burdensome or did not make any logical sense (Engen & Olsvik, 2010; Jore & Njå, 2012).

Moreover, if risk management is built on general rules rather than specific threat and vulnerability assessments for each and every organization; many organizations will implement security measures on a higher level than necessary and by this leading to an unnecessary level of costs and inconveniences for the company and its employees.

2.2.2 *A reactive regime*

Another challenging aspect with this approach is that since the process of changing regulation takes time, this security regime does not facilitate for quick changes in the regulations if the threat landscape changes. The rule-compliance approach has a tendency to involve a reactive response from the regulated organizations, meaning that rules are often made because a terrorist attack or a revealed terrorist plot have revealed vulnerabilities of the current security system. In aviation, numerous regulations have been added to the existing regulations because perpetrators have tried or carried through attacks against the system or because of revealed plots; The 2001 "shoe bomber" incident led to the shoe removal and screening policy, the liquid and gel ban policy was instituted after the 2006 plot to blow up planes bound for the United States with liquid explosives, and the 2009 Christmas Day bomber incident, where the perpetrators were carrying explosives in their undergarments, led to the deployment of advanced imaging technologies and pat-downs for all passengers. In all these cases, the changes in the regulations were a direct response to the attempt to commit an intentional crime (Jacobson, 2012). In fact, the whole new security regime in aviation was a direct response to the 9/11 terrorist attacks (Birkland, 2004; Engen & Olsvik, 2010; Salter, 2008).

3 THE RISK-MANAGEMENT REGIME

As mentioned earlier, the authorities traditionally met new challenges of technological development, related to risks and accidents by applying more prescriptive regulations. However, as time went by more detailed regulations were passed. The amount of regulations gradually increased to the point where it was completely unwieldy (Hale, Hopkins, & Kirwan, 2002; Lindøe, 2012). At the end of 1990's a review of the law and management structure in HSE area in Norway, displayed that there was over 60 laws and 1000 regulations governing this area (Lindøe, 2012).

In the 1970's, a new regulatory regime emerged, and the focus changed from detailed governmental control towards an internal control regime (Lindøe, 2012). In most industries the rule-compliance regime gradually was replaced by more goal-oriented regimes, focusing on what to achieve rather than on the means of doing so. Goal orientation and risk characterizations were two major components of this new regime that has been endorsed by international organizations and various industries (Aven & Renn, 2009).

The risk-management regime builds on the assumption that organizations or owners of critical infrastructures have the necessary competence for knowing what type of risks the organization can face in the future, and know the appropriate means for how these threats should be met. Consequently, the assumption is that organizations, because of their knowledge, have the ability to describe what may happen in the future, to assess associated risks and uncertainties and to choose among alternatives. (Aven, 2003). The assumption is that risk assessments should be a part of the decision support in a decision-making process in order to make ideal decisions about how to find the optimal level of security.

3.1 *Security is an organization's responsibility*

In the area of security, the state has traditionally been the one responsible for protecting citizens from acts of terrorism (Jore, 2012). However, the introduction of the new Norwegian object security regulation passed in 2011 (Forsvarsdepartementet, 2011), was based on what Hopkins (2011) refers to as a risk-management regime. This regulation gave the departments the responsibility of pointing out critical objects within its jurisdiction. The object security regulation contains a risk-based approach to how to protect a critical object, and it is the owner of the critical object which is responsible for conducting a risk analysis of valuation of assets, threats and vulnerabilities which will lay the foundation for what measures the organization should

implement. Owners of critical objects are also responsible for the implementation of risk reducing measures and to bear the associated costs.

The implementation of the new object security regulation marked a shift in who bear the responsibility for protecting citizens from acts of terrorism and other intentional crimes. A regulation founded on a risk–management approach entails that the responsibility for security no longer is dictated from the state but is delegated to the organizations that own critical objects or critical infrastructures. This implies a change in the role of the state regarding security related issues. In a rule-compliance regime, the state is a protector of law and the primary task is, by the use of legitimate authority, to force organizations to fulfill their obligation of following laws and regulations within legal binding norms. Anyone violating laws can be sanctioned and punished. In the risk-management regime the role of the state is not to enforce companies to follow certain rules, but to arrange for and assist organizations in finding the optimal level of security. This means that the official bodies responsible for inspection working in this regulation regime, have a different role than the inspectors working in the rule-compliance regime. The role of the official bodies doing inspections in the risk-management regime is to check if the organizations have carried through risk assessments and implemented measures in accordance with the risk assessments. The role of the inspector is, thus, changed from a punisher to an adviser.

3.2 *Flexible and in line with the current threat landscape*

In the risk-management regime the knowledge that an organization has regarding its assets, values, and vulnerabilities and associated threats is in focus. This means that the organizations have more flexibility in how to arrange its security regime, and can direct the security system against the threats that are considered to be most critical to the organization. Consequently, the organization can protect the assets which are assessed to be most valuable, and organizations can change and adapt security measures if the threat landscape changes. Despite these advantages, there are also some challenging aspects with the risk-management regime.

3.2.1 *The risk-management regime is no practical guide*

According to Renn (2008) there are various types of risks. For simple risks, the cause for the risk is well known, the potential negative consequences are obvious, the uncertainty is low and there is hardly any ambiguity with regard to the interpretation of the risk. Simple risks are recurrent and unaffected by ongoing or expected major changes. Consequently, statistics are available and the application of statistics to assess the risks in statistical terms is meaningful.

Renn draws attention to the fact that not all risks are simple: they cannot all be calculated as a function of probability and effect. Such risks are called systemic risks. The term systemic describes the extent to which a risk is embedded in the larger contexts of societal processes. The management of systemic risks, such as terrorism, requires a more holistic approach to hazard identification, risk assessment, and risk management because investigating systemic risks goes beyond the usual agent-consequence analysis. Systemic risks are not confined to national borders or a single sector and do not fit the linear, mono-causal model of risk. They are complex (multi-causal) and surrounded by uncertainty and/or ambiguity (van Asselt & Renn, 2011).

The goal of a terrorist attack is not only to cause damage but also to produce a signal effect of meanings. Thus, terrorism is also a crime against the mind (Burgess, 2007; Crelinsten, 2009; Jackson, Jarvis, Gunning, & Smyth, 2011). Subsequently, activists can gain extensive attention with threats only, and it is hard for society to assess what plans and capability actually are behind the threats. In other words, terrorism is a highly uncertain risk and the political aspect of the threat and how to handle it imply that the risk of terrorism is highly ambiguous. Acts of terrorism are obscure, low-frequency events where strategically calculating human beings are the ones who possess the threat. Terrorists can strike suddenly, without warnings and cause enormous damage to society. In order for a terrorist attack to be effective, the terrorists must keep a low profile; thus, a terrorist threat will be secret by nature and, therefore, to a large degree, not knowable by those who are responsible for the security (Aradau & van Munster, 2007).

What risk means in a security context and how the risk can be expressed and managed, is a contested topic in the scholar literature (Bier & Von Winterfeldt, 2007; Deisler Jr, 2002; Jore & Njå, 2010; Willis, 2007). Traditional quantitative risk analysis calculates risk based on the probability of an incident multiplied with the consequences. Newer perspectives often include uncertainties not captured in the probability or the background knowledge that the traditional risk estimates are based on (Aven, 2011). According to Aven (2013), in the area of security, application of probabilities is commonly avoided; it is said that they are impossible to determine and that they are of little interest as a tool to support the decision making. Often qualitative assessments are performed on the basis of judgments of actors' intentions and capacities, without references to a probability scale.

These views are reflected in the three standards for protection against intentional acts which have either been published or are in progress in Norway (Standards Norway 2012; 2014a,b). In these standards, risk is defined as a combination of valuation of assets, threats and vulnerability (Standards Norway 2012). The definition, thus, differs from the general ISO definition of risk being the "combination of the probability of an event and its consequence (ISO 2002). However, some targets are more attractive than others and as a consequence more likely to become a terrorist target. Even if the probability aspect is removed from the risk analysis the organization, in an actual decision-making context, still has to address this issue because to make decisions concerning risks means to direct the resources at the most likely targets.

Another challenge for organizations responsible for the risk assessment of intentional acts is how to include the relevant range of possible scenarios of intentional acts. The selection of scenarios is often heavily influenced by the last incident or the current understanding of the security landscape (Karlsen & Jore, 2013). After the terrorist attack in Norway 22/7 2001 and the In Amenas attack the commission reports concluded that the people responsible for security had not envisioned the scenarios that materialized.

These are all aspects of the terrorism risk contributes to that a risk management regime cannot provide any clear answers.

3.2.2 *No benchmarking for when to implement security measures*

A risk-management approach is no practical guide; it does not give any clear guidance for what is an appropriate level of security or any benchmarking for when a company has achieved the "right" level of security.

For a company standing in a concrete decision context, the risk level falls somewhere on a continuum from extreme to insignificant; if the threat is extreme, the company needs to eradicate the threat with every possible means. If the threat is insignificant, the organization can invest the money and resources on other things. However, for most organizations that conduct a security risk analysis the risk assessment will fall somewhere in between the risk continuum, and the organization will have to decide whether the risk is so severe that there is a need for implementing security measures or not.

Regulation based on a risk-management regime does not give any clear guidance in the decision-making context. In each case the risk has to be judged as falling on one or the other side of a line: on one side, a certain action is required; on the other, it is not. In other words, the risk continuum must be converted into a dichotomy for the purposes of decision-making. Thus, the risk-management approach does not in general provide much guidance to those faced with these decisions, that is, it does not offer a way of deciding whether the risk is acceptable or not (Hopkins, 2011). In the area of security this gets even more complicated; since most assessments and decisions regarding security measures are classified, an organization will in a concrete decision-making context often lack information about how other organizations have arranged their security system. This could also be a challenge for the directorates responsible for inspection. According to the object security regulation it is the directorate in each sector that is responsible for the inspections within its jurisdiction. Most of these directorates do not have security as their main activity, and will probably lack the experience and the competence on how to deal with security threats.

3.2.3 *Organizations can be tempted to lower the risk assessments to save money*

The purpose of risk management is to ensure that adequate measures are taken to protect people, the environment, and assets from harmful consequences of human activities. The extent to which risk reducing measures are justified depends on the balance between costs and benefits in terms of safety gains (Aven & Renn, 2009).

To handle security risks will for most organizations not be their main activity, and most organizations will probably have other risk related areas that are assessed to have a higher probability of occurring, such as non-intentional accidents.

According to the Norwegian object security regulation it is the organizations themselves that have to pay for the security measures. The consequence of this could be that many companies can be tempted to lower the risk level to save the investments in security system. Thus, trust is a fundamental character of the risk-based regime. Such a regime is based upon a belief about the regulated wanting and pursuing the best solutions available.

3.2.4 *In the risk management regime security becomes an ongoing process*

A risk management regime is challenging for the organizations because it requires that the organizations put lots of efforts into the risk management process. This approach moves the focus from governmental inspections checking compliance with existing rules, towards inspiring the industry to develop their own systems of internal control and management. In this regime, the organizations are forced to evaluate and report upon their own self-regulatory strategies in order to enable the regulatory authority to judge if the objectives of the regulations are met. Thus, the risk management process becomes central. In other words, security in this perspective is not just a check

list that can be completed, but an ongoing process where the organizations continuous have to monitor that the security system is in accordance with the threat assessments.

However, many companies may not fully understand the threat situation or what measures can be implemented in order to reduce the threat. Today, many Norwegian companies operate on an international or global basis. This means that organizations need to be updated on the local security situation and the threats assessments needs to be updated. Still, even for organizations operating solely on the national level in Norway, most organization will not have the necessary competence and mean to conduct meaningful threats assessments. As a consequence the organizations will have to rely on risk assessments done by the authorities or companies that sell risk assessments.

3.2.5 *Organization lacks knowledge of the effect of counterterrorism measures*

The objective of risk-based security management is to identify risks before they materialize in the form of an intentional crime. Once risks have been identified, preventive measures can be taken to eliminate the risks or to reduce the probability of the occurrence of such events. Although this is an attractive idea, little is known about how well security measures actually works. In research, minor attention has been paid to the effectiveness of counterterrorism measures. Lum, Kennedy and Sherley (2006) discovered an almost complete absence of research that evaluated counterterrorism measures. From the evaluations they found, it appeared that some interventions either did not achieve the outcomes sought or sometimes increased the likelihood of a terrorist attack.

LePorte and Frederickson (2002) have demonstrated that it is almost impossible to measure the efficiency of counterterrorism measures because it is impossible to know if the absence of terrorist attacks means that the security measures are effective or whether there never existed a terrorist threat in the first place. This means that organizations will lack knowledge regarding the risk reducing effect of countermeasures and also the means for evaluation whether the measures are effective or not.

4 THE RELATIONSHIP BETWEEN THE TWO RISK REGIMES

In this paper we have presented the risk-management regulation regime as a contrast to the rule-compliance regime. However, Hopkins (2011) claims that these are not mutually exclusive approaches; they are complimentary. This is also the case for the area of security in Norway. Also organizations who work under the rule-compliance regime work under a regime that acknowledges that security risks can be assessed and managed. In order to determine the appropriate rules, most likely a risk assessment is behind that decision. This risk-assessment is just removed one step from the end point decision-maker. In the case of airport security, the risk assessments are done by the European Aviation authorities, and not by national or local assessors.

Furthermore, behind the introduction of a risk-management security regime lays another rule, this time a legislative requirement that risk-assessments should be conducted. Behind the risk-management regime introduced in Norway, lays the Security Act which demands that owners of critical objects need to carry through the risk-management regime. Moreover, the security risk analysis standards that have been developed and are in progress can be seen as a guide for helping companies to interpret and deal with risk-management regulation—because organizations still needs rules to guide them in their security work. From this point of view, risk-management and rule-compliance are intertwined and complementary strategies. The issue, therefore, is not to decide between the two; it is to get the balance right.

One appropriate question to ask is whether the risk management security regime represents a new regime or if it is just a broadening of an already existing regime? Within the area of port security, the introduction of new port security regulations[1] can be interpreted within the trend of moving from prescriptive, detail-oriented regulations towards more flexible, risk-management based regulations. The new Norwegian regulations tend to take a more flexible form while referring to the more detail-oriented demands in international regulations (IMO's International Ship and Port facility Security code, ISPS, and EU-regulation 725/2004 on enhancing ship and port facility security). To what extend the regime has actually changed to a more risk-management based regime is not evident. However, this underline the fact that regulatory regimes hardly ever are purely risk-management based, but often tend to be a hybrid version of the risk-management based and rule-compliance approaches.

A risk management approach offers no clear guidance for what is an appropriate level of security or any benchmarking for when a company has achieved the "right" level of security. In order to support the companies in their decision making of whether action are required or not, detailed guidance standards are often offered for how to

[1]Regulation on Protection of Harbours and Regulations on Protectin of Port Facilities (29 May, 2013) was implemented May 1, 2012, replacing the former Regulations on Protection of Ports and Port Facilities against terrorist attacks, etc. 3 July 2007.

assess risk and whether or not action is required. Such non-legal standards are more easily updated, ensuring the regulations to keep up with the development. Thus, by implementing a set of more detailed standards to support the risk-management based regulations contributes to a better balance between the risk management approach and the rule-compliance approach. This however, requires a robust system for updating of the standards.

5 CONCLUSION

This paper has described the consequences of the rule-compliance and the risk-management regime in a security context, and discussed some challenges of applying a risk management regime within the area of security. We claim that risk-management and rule-compliance are intertwined and complementary strategies. The issue, therefore, is not to decide between the two; it is to get the balance right.

In the rule-compliance regime, the authorities set out detailed regulations in order to steer the direction of companies, or others, in their security work. This will lead to a uniform implementation of security measures, meaning that each organization covered by a specific regulation will have the same level of security independently of an organization's perception of available resources, threat picture and former experience with the threat of intentional crimes. In a security context, this means that organizations or owners of critical infrastructures will implement the same level of security measures independently of whether a company or an owner of a critical object belong to a sector which has historical experience with acts of intentional crimes.

In the risk-management regime the knowledge an organization has regarding its assets, values, and vulnerabilities and associated threats is in focus. This means that an organization has more flexibility in how to arrange its security regime, and can direct the security system against the threats that are considered most critical to the organization. Consequently, the organization can protect the assets which are assessed to be most valuable, and the organization can change and adapt security measures if the threat landscape changes.

Although these aspects with the two security regimes also are present within the area of safety, there are some aspects with security risks that make the application of a risk-management regime more challenging; Terrorism is a highly uncertain risk and the political aspect of the threat and how to handle it imply that the risk of terrorism is highly ambiguous. Acts of terrorism are obscure, low-frequency events where strategically calculating human beings are the ones who possess the threat. Terrorists can strike suddenly, without warnings and cause enormous damage. In order for a terrorist attack to be effective, the terrorists must keep a low profile; thus, a terrorist threat will be secret by nature and, therefore, to a large degree, not knowable by those who are responsible for security. Additionally, often the area of security is just one of several risk issues an organization has to take into account, and safety risks are areas where the organization will have its main focus because many of these risks will be assessed to have a higher probability of occurring. Furthermore, most organizations in Norway lack security competence, benchmarking is difficult because the area is often classified, and little is known about the effect of counterterrorism measures.

Since the risk-management approach is no practical guide and does not give any clear guidance for what is an appropriate level of security, it is reasonable to assume that many organizations in Norway are "struggling" with adapting to this new regime. This is a topic further research should look into.

REFERENCES

Aly, A., 2013. The policy response to home-grown terrorism: reconceptualising Prevent and Resilience as collective resistance. *Journal of Policing, Intelligence and Counter Terrorism, 8*(1), 2–18. doi: 10.1080/18335330.2013.789594.

Aradau, C., & van Munster, R., 2007. Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations, 13*(1), 89–115.

Aven, T., 2003. Foundations of risk analysis: a knowledge and decision-oriented perspective. Chichester: Wiley.

Aven, T., 2011. *Quantitative risk assessment: the scientific platform*. Cambridge: Cambridge University Press.

Aven, T., 2013. Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. *Reliability Engineering & System Safety, 119*(0), 229–234. doi: http://dx.doi.org/10.1016/j.ress.2013.06.044.

Aven, T., & Renn, O., 2009. The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Journal of Risk Analysis, 29*(4), 587–600.

Ayres, I. and Braithwaite, J., 1992. *Responsive regulation*: transcending the deregulation debate. New York, Oxford University Press.

Baldwin, R. and Cave M., 1999. *Understanding Regulation*: Theory, Strategy and Practice. New York: Oxford University Press Inc.

Baldwin, R., et al., 2010. *The Oxford Handbook of Regulation*. Oxford: Oxford University Press.

Baram, M., et al., 2013. Risk Governance of Offshore Oil and *Gas Operations*. Camebridge: Camebridge University Press.

Bier, V.M., & Von Winterfeldt, D., 2007. Meeting the Challenges of Terrorism Risk Analysis. *Risk Analysis: An International Journal, 27*(3), 503–504.

Bigo, D. (Ed.)., 2010. *Europe's 21st century challenge: delivering liberty.* Farnham: Ashgate.

Birkland, T.A. (Writer), 2004. Learning and Policy Improvement After Disaster: The Case of Aviation Security [Article], *American Behavioral Scientist*.

Braut, G.S. and Lindøe P., 2008. *Robustness in self-regulatory risk regimes*: The Norwegian experience in perspectives of legal law systems. Working on Safety. Crete.

Burgess, P.J., 2007. Social values and material threat: the European Programme for Critical Infrastructure Protection. *International Journal of Critical Infrastructures 3,* (No 3/4), 471–487.

Coglianese, C. and Mendelson E., 2010. *Meta-regulation and Self-regulation*. The Oxford handbook of regulation. R. Baldwin, M. Cave and M. Lodge. Oxford: Oxford University Press.

Crelinsten, R.D., 2009. *Counterterrorism*. Cambridge: Polity.

Deisler Jr, P.F., 2002. A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism. *Risk Analysis: An International Journal, 22*, 405–414.

Engen, O.A., & Olsvik, E.A., 2010. Security in civil aviation post 9/11 (pp. S. 2323–2329). Boca Raton, Fla.: CRC Press.

Forsvarsdepartemente, 2011. Forskrift om objektsikkerhet (2011). LOV-1998-03-20-10-§17.

Frederickson, H.G., & LaPorte, T.R., 2002. Airport Security, High Reliability, and the Problem of Rationality. *Public Administration Review, 62*, 33–43.

Gjørv, A.B. m. f., 2012. Rapport fra 22. juli-kommisjonen: oppnevnt ved kongelig resolusjon 12. august 2011 for å gjennomgå og trekke lærdom fra angrepene på regjeringskvartalet og Utøya 22. juli 2011. Avgitt til statsministeren 13. august 2012 (Vol. NOU 2012:14). Oslo: Statens forvaltningstjeneste. Informasjonsforvaltning.

Gunningham, N. and Rees J., 1997. *Industry Self-Regulation: an Institutional Perspective*. Law and Policy 19(4): 363–414.

Hale, A.R. and Baram, M.S., 1998. *Safety management*: the challenge of change. Oxford: Pergamon.Hale.

Hopkins, A., & Kirwan, B., 2002. *Changing regulation: controlling risks in society*. Amsterdam: Pergamon.

Hood, C., et al., 2001. *The Government of Risk*: Understanding Risk Regulation Regimes. New York, Oxford University Press Inc.

Hopkins, A., 2011. Risk-management and rule-compliance: Decision-making in hazardous industries. *Safety Science, 49*(2), 110–120. doi: http://dx.doi.org/10.1016/j.ssci.2010.07.014.

Hutter, B.M. and Jones C.J., 2007. *From government to governance*: External influences on business risk management. Regulation & Governance 1: 27–45.

Hutter, B.M. and O'Mahony J., 2004. *The Role of Civil Society Organisations in Regulating Business*. London, ESRC Centre for Analysis of Risk and Regulation. Discussion Paper available at: http://www.lse.ac.uk/collections/CARR/pdf/Disspaper26.pdf.

Hutter, B.M. and Power M., 2005. *Organizational Encounter with Risk*. Cambridge: Cambridge University Press.

Jackson, R., Jarvis, L., Gunning, J., & Smyth, M.B., 2011. *Terrorism A Critical Introduction*. New York: Polgrave Macmilian.

Jacobson, S., 2012. Watching through the "I"s of aviation security. *Journal of Transportation Security, 5*(1), 35–38. doi: 10.1007/s12198-011-0078-z.

Jore, S.H., 2012. *Counterterrorism as risk management strategies* (Vol. nr. 178). Stavanger: UiS.

Jore, S.H., & Njå, O., 2008. Protection from half-criminal windows breakers to mass murderers with nuclear weapons: changes in the Norwegian authorities' discourses on the terrorism threat (Vol. Vol. 4, pp. S. 3077–3084).

Jore, S.H., & Njå, O., 2010. Jore, S.H., & Njå, O. (2010). Risk of terrorism—a scientifically valid phenomenon or a wild guess? The impact of different approaches to risk assessment. Critical Approaches to Discourse Analysis across Disciplines. *Critical Approaches to Discourse Analysis across Disciplines, 4*(2), 197–216.

Jore, S.H., & Njå, O., 2012. *A discussion on small countries' adaptation to globalised security in aviation.* Paper presented at the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 PSAM & ESREL.

Karlsen, J.E., & Jore, S.H., 2013. *When hindsight is utterly wrong—how to overlook a non-plausible future.* Paper presented at the The 22nd SRA-E Conference, Trondheim.

Lindøe, P., 2012. Risikoforståelse og myndighetskontroll *Risiko og Tilsyn* Oslo: Universitetsforlaget AS.

Lindøe, P., Kringen, J., & Braut, G.S., 2012. *Risiko og tilsyn: risikostyring og rettslig regulering*. Oslo: Universitetsforl.

Lindøe, P., 2002. Arbeidsmiljøregulering i de nordiske *landene*. Tidsskrift for ARBEIJDSLIV.

Lum, C., Kennedy, L., & Sherley, A., 2006. Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2*(4), 489–516. doi: 10.1007/s11292-006-9020-y.

Office, U.S.G.A., 2005. GAO Report to Congressional Requesters, RISK MANAGEMENT Further Refinement Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.

Piètre-Cambacédès, L., & Chaudet, C., 2010. The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety". *International Journal of Critical Infrastructure Protection, 3*(2), 55–66. doi: http://dx.doi.org/10.1016/j.ijcip.2010.06.003.

Renn, O., 2008. *Risk governance: coping with uncertainty in a complex world.* London: Earthscan.

Salter, M.B., 2008. *Politics at the airport*. Minneapolis: University of Minnesota Press.

Statoil, 2013. The In Amenas Attack-Report of the Investigation into the terrorist attack om In Amenas. Prepared for Statoil ASA's Board of directors. In S. s. i. Board (Ed.).

Stålesen, J.S., 2011. *Security styring i petroleumssektoren*. Stavanger: J.S. Stålesen.

Van Asselt, M.B.A., & Renn, O., 2011. Risk governance. *Journal of Risk Research, 14*(4), 431–449. doi: 10.1080/13669877.2011.553730.

Viscusi, W.K., & Zeckhauser, R.J., 2003. Sacrificing Civil Liberties to Reduce Terrorism Risks. *Journal of Risk & Uncertainty, 26*(2/3), 99–120.

Willis, H.H., 2007. Guiding Resource Allocations Based on Terrorism Risk. *Risk Analysis: An International Journal, 27*(3), 597–606. doi: 10.1111/j.1539-6924.2007.00909.x.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk management in anchor-handling operations: The balance between control and autonomy

J. Røyrvik
NTNU Social Research, Trondheim, Norway

K. Skarholt & G.M. Lamvik
SINTEF Technology and Society, Trondheim, Norway

J.R. Jonassen
Stord/Haugesund University College, Haugesund, Norway

ABSTRACT: The purpose of this paper is to explore different safety cultures in anchor-handling operations in the Norwegian offshore petroleum industry; how the crew and management cope with both critical and dangerous operations, compared to the periods in-between operations that are characterized by routine work. Between operations, officers function as middle managers fulfilling organizations needs for control, predictability and audit requirements. During operations, dangers and complexity demands full focus and presence towards that specific situation. Thus, the different demands are balanced by actualizing two different safety regimes and work practices. The discussion in the paper is based on two research projects conducted in 2009 and 2013, focusing on safety conditions at anchor-handling vessels.

1 INTRODUCTION

1.1 *Anchor-handling operations*

Anchor-Handling Tug Vessels (AHTVs) perform what is known as *advanced marine operations*, *extreme marine operations*, or simply *anchor-handling operations*. Anchor-handling vessels are an important part of the offshore operations in the production of oil and gas on the Norwegian Continental Shelf (NCS). According to statistics from the Norwegian Shipowners' Association, the offshore industry in Norway consists of approximately 340 vessels, where AHTV and supply vessels are the biggest category. The fleet is the second biggest offshore fleet in the world next to the US. Furthermore, this industry employs more than 12500 people and delivered 24 percent of the total value creation within the Norwegian maritime industry in 2012 (Maritimt Forum 2012). Moreover, in 2011, this industry is said to create values of more than NOK 30 billion, in an industry that creates about 150 billion in total.

The operations on board an AHTV vessel involve many dangerous work situations, which demand a strong focus on safety before and during operations. Seafaring has mortality rates considerably higher than populations ashore (Hansen et al., 2002; Roberts, 2002).

The standard rig move operations are integrated; anchors are recovered to the AHTVs, the rig moved to a new location, and anchors are placed at the new location and connected to the rig—all in one operation. This operation may take 6–10 days and requires a rather stable weather window. Also, it requires tight coordination between the parties; the rig and 2–3 anchor-handling vessels, where one of them has the lead.

1.2 *Rule-based offshore petroleum culture*

The offshore petroleum industry in Norway is controlled by regulations, guidelines, and standardization of operations. In this way, the industry is characterized by a rule-based organizational culture and structure, with normative concepts of behaviour. The aim of a rule-based safety regime is to reduce accidents on board and to develop a safe workplace. The regulating authority for all vessels and movable rigs on the Norwegian Continental Shelf is the Norwegian Maritime Directorate.

The planning of offshore operations has to follow certain guidelines. A "Risk assessment document" is prepared by the operator, the oil company, or a company contracted as Marine Representative. The planning is based on experiences of what could occur or previously have occurred. The guidelines are the NWEA, version 2 regulations.

This is a generic document, which is intended for continuous updating during the preparation period and during operations, in accordance with the incidents occurring. A preparatory meeting is arranged with all parties present. The Guidelines and Risk assessment are presented and discussed. The risk assessment is revised as a result of feedback from that meeting.

When the vessels are hired from the spot marked, there are no vessel representatives at the above meeting. Long-term contracts, however, allow such representation.

At the base during mobilisation, the marine representative arranges a familiarisation meeting for all vessel crew. This is a presentation of scope and a safety brief.

1.3 *Safety culture*

The relation between safety and culture has been one of the main topics of safety research for the last decade (Guldenmund, 2007; Haukelid, 2008; Stiansen, 2009). Research has shown that the cultural aspects of work practice influence safety as much as technology and formal organization structures.

According to Gherardi et al. (1998), safety is strongly linked to the work practice of a community. It is a collective competence that has developed through experience and training of seamanship. This also influences what is considered safe or dangerous behavior during operations on board. The seamen's identity is shaped by what is appropriate within the norms and values of the culture on board, and influence the way they perceive safety rules (Knudsen, 2005). According to Knudsen (2009), good seamanship is a blend of professional knowledge, professional pride, and experience-based common sense.

Safety is also strongly linked to management of safety, where the aim is to control and measure an organization's operational performance. According to Petersen (1978), safety conditions can be identified, predicted and controlled—through the means of defined work processes and procedures. Planning and setting goals are also a part of safety management.

In this paper, we address both these views of safety: 1) the importance of the culture of the seaman crew due to safety and 2) the impact of the offshore control routines concerning safety.

2 METHODS

The collection of data is based on qualitative methodology, involving semi-structured interviews, unstructured conversations and observations onboard AHTVs during operations. One researcher covered integrated operations over a period of one year (2009–2010) and one researcher covered a week's operation during a pre-lay operation in 2013. The main data source from the one-year fieldwork is thus participation on board AHTVs and interaction with crews on these vessels (Røyrvik 2012). In addition to participation and observation, structured and semi-structured interviews from all positions on board were conducted, on board narratives were collected, and operation documents were studied. In addition, the researchers participated in relevant contexts, such as operations planning, pre-operational meetings, AHTV operational and safety procedure simulator training programs and R&D related contexts.

The positions interviewed in the 2013 data collection were: captain, first officer, chief engineer, deck foreman, ROV supervisor, surveyor, mooring supervisors/controllers and marine representative for the operator (oil company). Interviews were transcribed from audio files, as all interviews were recorded. The quotes used in this article are all translated from Norwegian. Observations with conversations in between interviews were conducted over a period of around 14 hours daily. Observational notes were taken at the time the observation was made or shortly thereafter and included in a field log as documentation. As the observations, participation and interviews that form the empirical basis of this article were made and conducted in 2009 and 2013, respectively, comparisons allow for discussion on developments in both operational practices and safety management.

3 RESULTS

Based on the analysis from the fieldwork, we will describe the characteristics of the working and living conditions on board the anchor-handling vessels. Overall, we found that the management and crew of seamen on board both strongly prioritize safety to avoid occupational accidents and major organizational disasters. How this is performed is very much affected by the fact that these vessels are part of a long-standing sailor tradition and a strong industry managerial regime. Thus, the officers are expected to function both as ship officers, focusing on seamanship, yet at the same time as middle managers of the greater corporations. The role as middle manager involves detailed planning and control in an effort to follow safety procedures and routines.

Depending on the organization of the particular operator, the oil company, as many as seven different parties may be involved in an anchor handling and rig move operation. The oil company may

choose to include several of the functions from internal resources or use outsourced resources. The functions or processes involved are: A drilling management responsible for planning and drilling, an offshore marine representative advising the drilling management and operator being the representative on board the senior AHT, a planner function/company, drilling company/rig owner, site survey to confirm the correct site, navigation company to find and document the correct location, weather forecasting company and anchor and mooring handlers.

3.1 *Anchor operations*

The core function of AHTVs is to reposition oil-rigs, floating installations that are anchored to the seabed while they search for oil. In principle, an anchor operation consists of three parts: recover anchors at rig location, tow the rig to new location, and release anchors and reposition them on the seabed according to position data. Traditionally, an anchor operation consists of three main parts: 1) the pulling of an anchor, loosening the rig from the sea bed, 2) tugging the rig to a new position, and 3) anchoring the rig in place at that new position. Such operations involve coordinating four AHTVs and one rig. Furthermore, an operation typically involves recovering and repositioning eight anchors, with each vessel working with and taking on board two anchors and their anchor systems.

The new pre-lay type operation consists of one recovery and pre-lay operation and one concerted (4–5 days) rig move (1–2 days). This requires two sets of anchor mooring spreads, one owned by the mooring equipment supplier and the other often owned by the rig company. The spread is left on the seabed from a previous rig move about 2 weeks prior. Anchors (usually 8) are all recovered and brought to the new location and spread according to a spread plan and buoyed with light buoys. On the rig moving day, the anchors at the "old" location are all buoyed, the rig is moved with the help of two AHTVs, wires are recovered and the rig connected.

Prior to any operation, a decision has to be made whether to carry it out as a pre-lay or integrated operation. There are advantages and disadvantages to both types of operations, and they both involve comprehensive planning: mooring analysis and equipment, vessel requirements, additional personnel, logistics, notification of others parties of location, and various risk assessments, such as Safe Job Analysis (SJA).

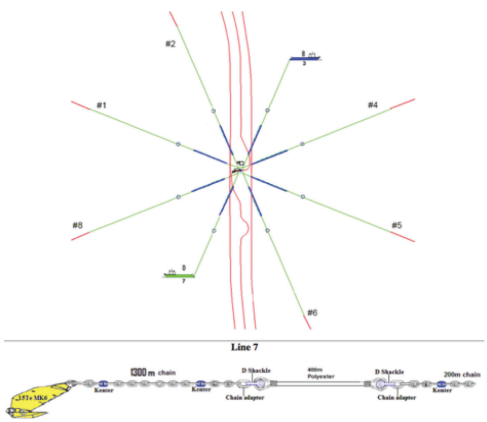


Figure 1. Map of an anchor system—and specifications of anchor # 7.

3.2 *AHTV vessels*

The AHTVs vary in terms of hull design, and there are different kinds of propulsion systems, as well as anchor handling systems. Some of the more modern AHTVs are equipped with an ROV (Remotely Controlled Vehicle) to inspect the seabed and recover the anchor lines. This significantly reduces the need for grappling functions (see section below). Nevertheless, there are some characteristic similarities between all AHTV vessels, like the positioning of the living quarters and bridge afore, the long working deck at sea level and the large winches mounted to the living quarters facing the work deck. The dual work chairs of the coxswain and the winch operator are another special feature of AHTVs. During operations, their work positions are at the bridge, overlooking the work deck. Independent of the type of AHTV, the positions on board are highly specialized, from the bridge and deck to the engine department.



Figure 2. An AHTV docked at Kristiansund.

The vessel is built specifically for towing and oilrig anchoring. Towing implies towing a rig from one location to another, and oilrig anchoring means anchoring the rig so it sits steadily in the water. To achieve this, four or five vessels must collaborate to stretch and tighten the enormous wires or chains, and anchor them to the ocean floor. The anchor is sometimes a kilometer away from the rig, so the thick wires are bound to be very heavy.

To cope with the great forces of the wire or chain, as well as nature, the vessels are very powerful and thus very demanding on resources. As the operations also take place some distance from shore, the vessels usually spend weeks offshore to get as much work done as possible on each trip. Each vessel can be considered to be a complete and integrated organization, because of the limited physical frames the crew live and work within over some time. The crew all have different tasks, qualifications and responsibilities, and everyone and every task is necessary in order to be able to stay offshore for such extended periods of time every trip. Some are responsible for food, some for cleaning, and some for maintenance of the vessel.

3.3 *Positions on board*

The crew consists of a minimum of 13: four on the bridge, four on deck, four in the engine room and one cook. Usually though, cadets and apprentices join the crew in training to become officers or able seamen, and it is common that the size of the crew varies between 15 to 20.

The four people working regularly on the bridge hold positions of captain, chief officer and first and second mate (sometimes two first mates). These four work closely together. During operations, the captain and one mate work on one shift together, and the chief officer and the other mate work the second shift. The shifts rotate—six hours of work and six hours of sleep, which implies that for twelve hours a day, two of the officers sit next to each other on the bridge collaborating on controlling the tension of the anchor systems, coordinating the work on deck to minimize risk, and making sure that the vessel is working properly. Between operations, they are also working and living closely together, and although other aspects, such as age and different personalities, influence the way the crew interact with each other, it is clear that "the bridge" defines both work and social roles and relations.

This is true also for the other positions on board. The able seamen, also working in pairs during operations, have their own work areas—the work deck—and resting area—the dirty mess, which allows for the seamen to rest and wait for orders still in their work outfits.

The work carried out in the engine room is considered a bit more separate than the other tasks on board. As with the other positions, they work in pairs (and depending on the engine, there may be a daytime electrician as well), monitoring the systems on board the ship, tinkering with the engine and spending their working hours mostly without having to coordinate their work much with anyone other than the captain.

As a crew works closely together, a collective practice of both work and social interaction develops. This is true both for those working in similar positions as well as for those working at similar times. During operations, the same ABs and officers will collaborate around the clock, as well as eat and sleep at the same times. As a result, although conducting the same work, crew on different vessels, as well as different shifts and the different positions on board may both work and socialize differently.



Figure 3. In between anchor operations: cargo-run.

3.4 *In between operations*

Anchor operations must be performed during specific *weather windows*. A weather window in this context means predicted weather conditions that are defined as safe enough for the time it takes to carry out the operation. The technical definition of a weather window, in this context, is when the *significant wave height* is predicted to be less than 3.5 meters 1.5 times the predicted operational time (DNV rules for marine operations). A typical operation may last for many days. Therefore, in the North Sea, and especially during the winter months, anchor-handling involves a lot of waiting around and working in-between operations.

If the weather forecasts predict an extended waiting period, the crews will stop working shifts and work on maintenance during the day, perhaps washing down or painting the vessel, fixing tools,

checking the electrical systems and so on. As hiring an AHTV is expensive for operators, they may decide to use the vessel in other types of operations, if the waiting period is predicted to last long. These operations, such as cargo runs, are considered to be considerably less difficult and dangerous, and, as a consequence, the atmosphere on board during such operations is more relaxed, and the crew is more sociable and talkative.

The workday is also very much characterized by paperwork and safety management. Most tasks performed on board include some type of risk, either from being performed in an exposed environment (such as outside in high waves, or high up somewhere), from involving heat (such as welding work), or from working with hazardours substances (like paint or gasses) or closed environments.

In these cases, and many others, permissions are required in order to perform the tasks. SJAs are performed, and an officer, together with the one who performs the task, must sign that they have performed the analysis and that they have taken every safety precaution required.

3.5 *Advanced operations*

The first step of an operation is to lower the grapple in to the sea. The able seamen have prepared and positioned the grapple at the back of the ramp on the work deck. Grappling means fishing with the grappling hook, for a wire located on the seabed, which is connected to the anchor at one end. This process may take some time, and can't be carried out by the bridge alone, so, depending on the time of day, it is common for the rest of the crew to come and observe the grapple being lowered and the grappling to begin. It is a bit of a competition between the vessels to see who is the first to recover the wire/chain and bring it on board, and so the atmosphere on the bridge is slightly excited and easy. As soon as the wire/chain is on board though, it is secured by the so-called "shark jaw" (a device that locks the wire and later chain in position), and it is time for the sailors to go out on the work deck and connect the wire to the vessel's winch, and for the bridge to apply tension to the system.

From the moment that the wire is connected to the vessel and tension is applied to the system, the situation, and thus also the atmosphere, change dramatically. Now, if something goes wrong, simply sailing away is no longer an option (as the vessel is connected to an external system), and the energy that could be released if anything were to happen is potentially catastrophic due to the tension of the system. As a consequence, everyone, and the vessel itself as a collective entity, goes in to a focused state of mind. Silent concentration falls over all aspects of the boat and crew; all interaction is reduced to carrying out the operation, like a purposive bubble of extreme presence.

The majority of the hours during an operation, are spent "driving the chain". In the North Sea, depending on the depth, an anchor may lay a kilometer or so from the rig. And when the chain between the rig and the anchor is either recovered or put down into the sea, the winches that either pull or release propel the vessel—while the propellers or thrusters are used to maintain position or a specific heading. This work goes on for hours and hours, in a monotonous and, at first glance, seemingly routine way.

Although this seems like a routine part of the operation, it has proven to be very dangerous work. Every chain link weighs about 20 kg, and handling and controlling a one-kilometer chain is thus highly demanding on both equipment and crew. The incident involving Bourbon Dolphin showed the consequences of losing control of such forces; the currents affected the chain, which in turn dragged the vessel out of position. The crew and the vessel fought the forces that pulled them off course for hours, but a fatal turn of events, after

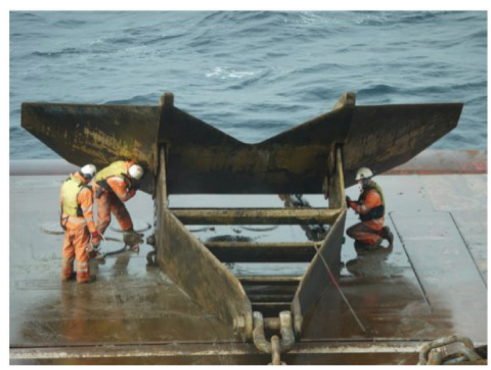


Figure 4. On-deck personnel working on an anchor.



Figure 5. The bridge—winch is handled from the left chair, the vessel from the right.

hours of fighting, caused the ship to suddenly capsize. This final and tragic event happened very fast, as the weight of the chain made the pull direction drag from the port side after a maneuver intended to ease tension and increase the maneuverability.

It is literally a matter of life and death for the bridge crew to maintain their focus and control the situation in order to follow the precise line of motion that ensures the tension and pull, keeping the vessel in the right position. When anchors are set, they are tested for tension. The anchors are pulled with a set force, called bollard pull, in order to test if the anchor is able to hold its position in the seabed during a calculated 100 years worth of impact from weather conditions. During the test, the bridge is mostly silent. Everyone is waiting for the moment of truth; will the anchor hold or break? Thumbs up if the test is successful and the anchor is holding within the seabed. If not, the process has to be repeated all over again, and the operation is redone.

The great tension of the anchor systems poses a considerable danger, not just for capsizing the vessel. More often, accidents or so-called near-miss-incidents endanger the sailors working on deck. The wires recovered from the seabed might be twisted, releasing energy stored by the twist when they are pulled up. If a wire snaps, the backlash would seriously hurt anyone being hit. The entire system of activities is potentially dangerous, and at the same time, the work conducted out on deck is both physically demanding and conducted in harsh environments. Therefore, it is of great importance that there are no misunderstandings, that the deck is clear when tension is released on the system, that a bolt is not left inside or not fastened when it should not, and so on. The bridge and the deck crew therefore depend on knowing that the others involved knows every situation as well as they do themselves.

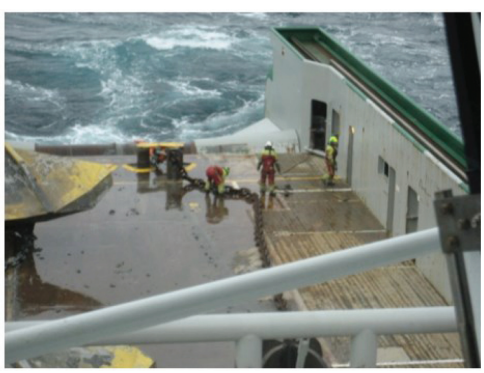


Figure 6. On-deck work during an operation—seen from the bridge.

4 DISCUSSION

This paper explores the safety culture at two levels: 1) the culture and work practice among the seamen on board performing the operations (occupational culture), and 2) the organizational culture of the offshore petroleum industry in Norway, i.e. safety management systems/regimes that involve detailed planning and control of operations. These two organizational cultures have different ways of perceiving and performing safety.

4.1 *Two modes of work*

The two safety cultures described above are reminiscent of how Pool (1997) and Weick & Sutcliffe (2007) describe so-called High Reliability Organizations (HROs), exemplified by a nuclear aircraft carrier from the US Navy and Diablo Canyon nuclear power plant in California. A central issue in Pool's discussion focuses on how certain organizations can be strictly hierarchal, with factors such as rank and routine, and being more dynamic in character on the other. The latter mode is of crucial importance when the organization is facing stress, for example during the launching and recovering of planes on board an aircraft carrier. The gear engaged "when things heat up", is distinguished by a focus on communication and expertise, rather than rank, stability, predictability and thick manuals. The success of high reliability organizations lies in their ability to include, request and balance these two "modes of operation" within their organization. This requires, for example, involvement from everyone in the organization. One should, on board the aircraft carrier, be able to achieve a situation where "the welfare of the ship and crew is [seen as] everyone's responsibility" (1997:261). Pool continues by stating that: "Besides communication, high reliability organizations also emphasize active learning, not simply the memorization of procedures. Employees should not only know why the procedures are written as they are, but should be able to challenge them and look for ways to improve them" (1997:266). Being part of this process of active learning, the rotation of crews is portrayed as an advantage for the organization rather than an obstacle. As Pool argues: "The collision of fresh, sometimes naïve approaches with a conservative institutional memory produces a creative tension that keeps safety and reliability from degenerating into a mechanical following the rules" (1997:261). This argument shows both the existence of two modes of work, and how safe work practices stems from the co-existence of these.

On board an AHTV, the transition between the two modes is very noticeable. First, there are structural changes in how the crews organize

and conduct their work. They begin working six hour shifts at their respective work positions, not allowing for any non-work related social interaction except during meals. Second, there are very noticeable changes in the atmosphere on board. The crewmembers' presence changes very much—they are quietly focused on the tasks they conduct. Words exchanged are work-related, information-redundant messages such as "clear deck" or "release tension". The atmosphere mirrors the tension of the anchor system, when the weak link is broken, the crew ease out.

4.2 *Occupational culture*

The social organization of a ship is often characterized as a "total institution" (Goffman, 1961). To enter into a total institution is to leave a multitude behind and instead be surrounded by and eventually be part of a universe, which is "something more than a formal organization, but […] something less than a community" (Goffman 1961:103).

Total institution refers to the fact that a ship is not divided into isolated arenas for interaction, but instead represents a collapse in that respect, in the sense that the seafarers on board spend 24 hours a day in the same place, and the activities they engage in—both related to work and leisure—are carried out simultaneously and with the same people. The seafarers on board are there to make sure the operation goes smoothly and on schedule. In other words, a ship is first and foremost a place for work.

We found that during anchor handling operations, it is much more important to "have control" than to control and audit the job. In order to manage having control among the seamen, one important assumption is competence, training, work experience and autonomous tasks on board. The findings from the interviews illustrate this, as one of the seamen on deck experienced the importance of autonomous tasks: *"If the foremen is giving orders all time on deck, you may feel unsecure about the work tasks. Then things may go wrong. Luckily, our manager doesn't tell us what to do in detail."* Being a good seaman seems to have much to do with working autonomously, without having someone telling you what to do, and to deal with unforeseen events as they arise.

We found management style to be essential in the effort to empower crewmembers. Based on our findings, the management on board holds the belief that crewmembers learn what to do by performing work tasks. As one of the deck foremen stated: *"When new seamen arrive on board, I think it's very important to let them know what's happening on the vessel. It's important to be hands-on and allow the new seamen to be actively involved in the operations. This is how they learn."* This is another example of how the management on board is involving the crew*: "I'm not a kind of manager that tells the seamen what to do. Here, we plan and do the operations together, and it works well."* We find that the managers on board empower the crew to develop practical skills and being able to perform as a team.

This is in accordance to one of the five principles of HRO; deference to expertise, established by Weick & Sutcliffe (2007), focusing on the respect of the HRO for the expertise held by the operator. Decisions regarding how to perform are made at the front end of the operation, rather at the top. This recognizes and takes care of the knowledge held by front end operators. In anchor handling operations the expertise on how to best perform safely stays with the deck team as a team. The Captain is in charge of what to do according to the scope of work, but he mostly leave to the team how to perform. The effectiveness of knowledge and experience sharing in a team will, however, depend upon the openness and trust established (Jonassen, 2014).

4.3 *Balancing regimes*

Within the oil and gas industry in Norway, major companies have largely standardized the work processes on board in an effort to control and measure operations. Safety management systems (regulations, procedures, work processes) may influence safety on board in a positive way, such as carrying out necessary operations planning.

In the case from 2013, we found that a new position had been included on board the AHTV. The mooring equipment, such as anchors, links and buoys, is often hired from a mooring company for pre-lay operations. The company will then supply and control the complete logistical chain, including control work on board. Controllers are positioned on board to control, in detail, all the mooring equipment and register all the numbers on individual pieces. They socialize with the crew, as they spend time together in the dirty mess while waiting in between operations. In addition to other possible gains, this position may be seen as serving the needs of both the organization (by auditing the work, registering and reporting) and the situation (as the controller is not disturbing the performance or presence of the sea farers). Although the formal reason for this position is to serve the control function, their presence is socially accepted by the added on board value they provide and their position among and with the ABs in the dirty mess. Ideally then, this type of resource both adds to the structure and standardization (needs of the organization) and contributes to on board flexibility.

From the example above, the addition of the controller function seems to contribute to a stronger focus on controlling safety on board. Making sure work processes comply with strict safety requirements and routines, leads to more administrative work on board, compared to earlier. According to Knudsen (2009) and Antonsen (2009), the seamen seem to have an aversion against the introduction of new rules and requirements by written procedures. They don't consider this very useful for operations. The seamen perceive it as traditional ideals of seamanship being under attack by attempts to regulate work by formal regulations and more paperwork.

There appears to be a great deal of inconsistency between the informal ideals for work performance and the formal ideals conveyed by safety procedures (Antonsen, 2009). Formal work requirements seek to standardize work processes. Standards can be seen as formalized rules that serve to prescribe and document efficiency and control within and across organizations. According to Mintzberg (1988), there are four different forms of standardization: standardization of work processes (specification of how worked is to be performed), outputs (what is to be done), skills (education and certification of competence) and norms (share a common set of beliefs).

Another effect of standardization is simplification, which is a two-edged sword. On the one side it helps people to better understand and remember. On the other it covers the fact that a complex structure or organization actually is complex. Imposing an image of simplicity may lead to dangerous situations. The reluctance to simplify is another of Weick & Sutcliffe's principles of HROs. Standardization reflects the experiences of past and may represent a hindrance to solve or prevent future problems. As Hollnagel argues: "Safety cannot genuinely be improved only by looking to the past and taking precautions against accidents that have happened. Safety must also look to the future. It must be proactive" (Hollnagel, 2008).

Standardization may be contrasted with improvisation. Improvisation refers to what is not planned for and involves a low degree of predefined structures. The weakness of standardization may be less room for improvisation (Antonsen, Skarholt and Ringstad, 2012). According to Antonsen et al. (2012), improvisation skills are necessary when unforeseen situations occur on board. In such situations, the management and crew have to quickly find solutions that have not been planned for and for which no procedures exist. The ability to improvise is very much dependent on the empowerment and autonomy among the crewmembers, in addition to knowledge of each other's experience and competence. This kind of expertise develops in a strong community where seafarers share norms and identities. Leadership practices influence the crew's ability to act in such situations.

5 CONCLUSIONS

The aim of this article was to discuss how a rule-based safety management culture and an occupational culture influence safety on board. On board anchor handling vessels, cultural traits of both industrial management and experience-based seamanship is present. Between operations, officers function as middle managers, filling the organization's needs for control, predictability and audit requirements. During operations, danger and complexity demand complete focus on and presence in that specific situation. The different demands are thus balanced by actualizing two different safety regimes and work practices.

We found that the seafarer's skills, experience and close collaboration are strengths in terms of safety on board. Safety is, to a great extent, a matter of maintaining control over work carried out within an organization. In this paper, we have discussed how control is gained through good seamanship characterized by a culture of empowerment, responsibility, experience, and, not least, a strong focus on safe conduct during the operations.

We conclude that rule-based safety and the work practice among the crew on board are mutually dependent. Safety management systems (regulations, procedures, work processes) influence safety on board in a positive way, for example by requiring necessary operations planning. However, the need for control in the offshore oil and gas industry seems to increase, as seen for example through the new control position and function on board. In the future, the challenge thus becomes maintaining what is considered to be good seamanship; professional knowledge, professional pride, and experience-based common sense.

ACKNOWLEDGEMENTS

The Norwegian Research Council and companies in the petromaritime industries in the Haugesund and Ålesund regions, Norway, have funded the project RISKOP, Managing Risk in Offshore Operations at Stord/Haugesund University College, in collaboration with SINTEF.

REFERENCES

Antonsen, S. 2009. The relationship between culture and safety on offshore supply vessels. *Safety Science* 47: 1118–1128.

Antonsen, S., Skarholt, K. & Ringstad, A.J. 2012. The role of standardization in safety management—A case study of a major oil & gas company. *Safety Science* 50: 2001–2009.

Gherardi, S., Nicolini, D. & Odella, F. 1998. What do you mean by safety? Conflicting perspectives on accident causation and safety management in a constriction firm. *Journal of Contingencies and Crisis Management* 6: 202–213.

Goffman, E. 1961. Asylums: *Essays on the social situation of menthal patients and other inmates.* Garden City, New York: Anchor Books.

Guldenmund, F.W. 2000. The nature of safety culture: A review of theory and research. *Safety Science* 34: 215–257.

Hansen, H.L., Nielsen, D. & Frydenberg, M. 2002. Occupational accidents aboard merchant ships. *Occupational and Environmental Medicine* 59 (2), 85–91.

Haukelid, K. 2008. Theories of (safety) culture revisited—An anthropological approach. *Safety Science* 46: 413–426.

Hollnagel, E. 2008. Risk + barriers = safety? *Safety Science* 46: 221–229.

Jonassen, J.R. 2014. Effects of Multiteam Leadership on Collaboration and Integration in Subsea operations. *International Journal of Leadership Studies*, Regent UniversitSchool of Business and Leadership, VA, forthcoming.

Knudsen, F. 2005. Sømandskab, arbeijdsidentitet og sikkerhedsregler hos danske sømænd (Seamanship, work identity and safety rules of Danish seamen). Tidsskriftet *Antrolopogi.*

Knudsen, F. 2009. Paperwork at the service of safety? Workers' reluctance against written procedures exemplified by the concept of "seamanship". *Safety Science* 47: 295–303.

Maritimt Forum, 2012. Maritim Verdiskapingsbok, Maritimt Forum, Oslo.

Mintzberg, H. 1988. The structuring of organizations. In Segal-Horn, S. (ed.), *The strategy reader*. Blackwell, Malden, 238–265.

Petersen, D. 1978. *Techniques of Safety Management.* McGraw-Hill, New York.

Pool, R. 1997. *Beyond engineereing. How society shapes technology.* Oxford University Press.

Roberts, S.E. 2002. *Hazardous occupation in Great Britain*. Lancet (9332), 543–554.

Røyrvik, J. 2012. *Værvinduet—en teknologisk artikulert entitet i oljeindustriens erobring av natur.* Thesis submitted for PhD in social anthropology, Trondheim: NTNU.

Weick, K.E. & Sutcliffe, K.M. 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* 2nd ed. John Wiley & Sons, Inc.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safety and environmental control of industrial activities in France: A negotiated relationship

V. Sanseverino-Godfrin
Center for Research on Risks and Crises (CRC), Mines-ParisTech, PSL Research University, Sophia-Antipolis, France

ABSTRACT: Environmental regulation aims to ensure that industrial activities cause the least possible damage. In France, this includes checks of regulatory compliance by environmental inspectors. In cases of non—or partial compliance, the Environmental Code gives inspectors the power to impose sanctions: fines and/or imprisonment. In theory, the relationship between the "inspector" and the "inspected" refers to a person with powers similar to those of the police who can punish all kinds of non-compliance, and another person considered to be an "offender". In reality, the objective of environmental inspectors is not to apply sanctions, but to promote economic development, by finding solutions that enable compliance with environment protection and safety regulations.

1 INTRODUCTION

The inspection of industrial activities is a necessity. Mainly it is a question of sustainability—to protect the environment and natural resources from damage caused by these activities—but it also concerns the safety of people, evidenced by the many victims of major industrial accidents (Bhopal in India, Enscheda in the Netherlands, BP Texas City in the United States, and AZF in France, etc.). Environmental regulation aims to ensure that industrial activities cause the least possible damage. For instance, the operators of industrial plants in the European Union must comply with Seveso Directive regulations preventing pollution and risks. But it is not enough to provide regulations, it is also necessary to check that the regulations are correctly applied. In France, the risk of pollution caused by certain industrial plants (*Installations Classées pour la Protection de l'Environnement*) means that environmental inspectors (*Inspection des installations classées)* regulatory check their compliance with a special juridical framework. In cases of non—or partial compliance, the French Environmental Code gives inspectors the power to impose sanctions: fines and/or imprisonment. In theory, the relationship between the "inspector" and the "inspected" (a private or public person, or a business) refers to a person with powers similar to those of the police who can punish all kinds of non-compliance, and another person considered to be an "offender". However, in reality the objective of environmental inspectors is not to apply sanctions, but to promote economic development, by finding solutions that enable compliance with environment protection and safety regulations.

This article shows that environmental inspectors negotiate their relationship with the entity they inspect, notably since the reform of the Environmental Code, which came into effect on 1 July 2013 and changed their role.

The article compares recent sociological studies of environmental inspectors, and the current state of regulations related to industrial activities in France. It gives also some examples from other countries, which are similar to the French situation. It addresses the question of whether safety imperatives can be negotiated.

The methodology consists of a bibliographic review of inspection and regulatory compliance, especially the sociological and juridical literature. It also examines the new control procedures contained in the Environmental Code (Articles L 170-1 and following). This review is complemented by a study of reports prepared by French inspection agencies (available on the internet), especially those of the agency in the *Provence-Alpes-Côte d'Azur* region. Finally, we study legal verdicts published on the official French website *Légifrance*, to identify information concerning prosecutions. This search used the keywords: inspection, compliance, violation, penalty, warning, fine and imprisonment for the period 2000–2013.

2 INSPECTIONS—IN THEORY

The objective of an inspection is that an industrial plant achieves regulatory compliance with

environmental regulations. Checks are usually carried out by the national environmental agency, whose staff are experts in their sector: for example, Control of Major Accident Hazard (COMAH) regulations are enforced by national agencies such as the Environment Agency for England and Wales and the Scottish Environment Protection Agency; the Environmental Protection Agency in the USA; and the Regional Department for Environment, Planning and Housing (*Direction Régionale de l'Environnement, de l'Aménagement et du Logement*—DREAL) in France.

DREAL comes under the authority of the local representative of the State (the *Préfet*), and is the competent authority in decisions concerning industrial plants (notably permits and administrative sanctions). The agency's inspectors are engineers, who have both a scientific and technical background and very good knowledge of the French environmental legal framework.

The procedure for inspections and the powers of inspectors are detailed in the Environmental Code, supplemented by directives from the Department of Ecology. The inspection procedure has changed: first in 2006 and then on 1 July 2013, which introduced a new mode of inspection, based more on transparency and negotiation (see below).

The inspection is led by environmental inspectors and takes place at several key moments in the industrial plant's history: before activity begins (through the assessment of the project proposal put forward by the future operator), during active operations, and when activity ends and the plant is closed down. At each of these times, the objective is to check that the plant complies with regulations and does not cause disturbance (noise, smell, etc.) or increase risk to the neighbourhood. The most interesting period is when the plant's activities may cause several types of damage; this is the most important inspection carried out by inspectors and the one we focus on in our study.

Generally, environmental legislation gives inspectors special powers to check regulatory compliance: they can enter an industrial site, grant or withdraw permits, enforce standards and if necessary, prosecute the operator of a non-compliant plant (Fineman 2000). There is a graduated scale of threats and sanctions, ranging from financial penalty notices, compliance notices and restoration notices to criminal charges, etc. In France, inspectors are sworn officers and this status gives them certain powers. To obstruct the work of an inspector is an offense, punishable by a fine (€150,000) and imprisonment (six months). To check regulatory compliance, inspectors may enter the plant at any time. The visit can be requested or unannounced. Most of the unannounced visits are due to complaints from neighbourhood residents. Inspectors can access any documents concerning the plant. They can also ask an external expert for their advice on the level of pollution or risks, which must be paid for by the plant's operator, if they consider the documentation to be insufficient or incomplete.

After an inspection, the inspector prepares a report (the *lettre de conclusion*), in which all the examples of non-compliance that have been observed are recorded. This report forms the basis for a prosecution in cases of non-compliance or failure to hold a permit. Before beginning a prosecution, the inspector can ask the *Préfet* to send a formal notice to the operator, which gives them time to rectify any deficiencies.

In principle, every case of non-compliance can be prosecuted, either once the notice's deadline has expired or, in serious cases immediately following the visit. Two types of sanctions can be applied: administrative and/or penal. Administrative sanctions are applied if the plant remains non-compliant after the notice's deadline has expired. The objective is to make the plant compliant. To that end, the *Préfet* can order that the sums needed to pay for the necessary works be deposited (the amount depends on the cost of the work to be carried out to achieve compliance); have the work done at the operator's expense; or suspend the plants activity until it is compliant.

Depending on the offenses committed, criminal sanctions can be applied to the operator. They can be fined for non-compliance with the applicable legislation or non-compliance with the formal notice (up to €100,000 and two years of imprisonment). If the reason for the non-compliance creates serious damage to the environment, or is a risk to health or safety, the sanction may be a €75,000 fine and a year of imprisonment. The operator can also be issued with a penalty (maximum €3000 per day) until the plant is compliant.

We saw earlier that in France there is a special environmental inspection agency that is dedicated to monitoring regulatory compliance. In theory, a prosecution can be launched each time an inspector notes a case of non-compliance.

However, does this theoretical scheme correspond to reality? Several sociological studies on the subject suggest that there are differences between what an inspection is supposed to be and what it really is.

3 INSPECTIONS—IN PRACTICE

First of all, it is important to note that the overall number of inspectors is not enough to monitor all industrial plants. No government has sufficient resources to check regulatory compliance in each

industrial plant and to prosecute every failure (Zaelke & Higdon 2006). The response to this situation is for environmental agencies to target their activities on those industrial plants that can cause serious pollution and damage to people and the environment, and those with the worst compliance records (Pedersen 2013).

In France, for example, there are about 500,000 Classified Installations (*Installations Classées*), but only 1, 250 full-time inspectors (as of 31 December 2012). It is clear that it is impossible to check the regulatory compliance of every industrial plant. For this reason, the plants to be checked are prioritized. The Department of Ecology provided a modernized inspection program for 2004–2007 and a Strategic Inspection Program for 2008–2012. These two programs outline the methodology to be used in the inspection, the organization of inspectors, information and training. Based on these programs, each year the Department of Ecology decides actions and inspection priorities. One of these priorities is to check the regulatory compliance of the most dangerous or polluting industrial plants.

In the United Kingdom, similar priorities are defined: the "risk based approach" reduces the administrative burden by organizing the work of national agencies, especially the Environment Agency. It focuses on major technological and emergent risks (Galland 2008). The same observation can be made in Belgium: a natural response to the shortage of resources is targeting, with inspection focused on those plants that are suspected to be non-compliant with environmental regulations and those that are the more dangerous or polluting (Rousseau 2007).

This first observation shows that, due to the lack of inspectors, checks of regulatory compliance cannot be as rigorous as they should be according to the legislation. Moreover, an indirect consequence of the lack of inspectors is to encourage a culture of "making arrangements": the inspector has no choice but to trust the operator to be compliant, as there are few ways to impose the regulations as they are prescribed in the legislation. This is a move away from command and control methods towards a self-regulatory approach (Pedersen 2013).

The approach to inspections is important as it determines how regulatory compliance is handled. French regulations concerning inspections take a "safety case" approach (Hale *et al*. 2002), which means that risk prevention is the responsibility of the operator of an industrial plant: they have to prove that they have identified and assessed the risks, and adopted appropriate prevention measures. In brief, they have to prove that the plant is safe for people and the environment. In this context, the plant, especially in large industrial groups, is a "self-regulated organization", to which officials can impose sanctions if self-regulation is insufficient (Dupré *et al*. 2009).

Furthermore, the Department of Ecology has directed inspectors to be more tolerant and promote industrial development. In 1995, a memo from the Department received by environmental inspectors confirmed this position: "It is clear that environmental inspectors must first establish a dialogue with the operators of inspected plants. It is not possible to prosecute each case of non-compliance" (Bonnaud 2002). Sometimes, inspectors have a dual role: to check regulatory compliance and also to advise the operator. This is the consequence of their specific technical knowledge, which can be used both to check regulatory compliance and to support prevention initiatives taken by operators (Strasser 1996).

This flexibility has an impact on the relationship between the "inspector" and the "inspected": inspectors are free to build a cooperative relationship with the inspected, and there is room for compromise (Ayres & Braithwaite 1991). Consequently, the regulatory compliance check is more based on negotiation. Etymologically, the Latin word "negotiation" means "trade or commerce". Specifically, it describes action to deal with an issue, the award of a contract and, by extension, various preliminary operations that are carried out in order to reach agreement. It also refers to discussions held before a contract is agreed or discussions concerning the settlement of a dispute (Cornu 2010).

In theory, there is no scope for negotiation in an administrative procedure that involves the inspection of an industrial plant, which may potentially lead to a prosecution in cases of non-compliance. However, sociological studies of regulatory compliance checks at industrial plants show that environmental inspectors negotiate their relationship with the entity they inspect. What is very interesting is that this conclusion is found not only in many French studies, but also in other countries (Hawkins 1984, Olsen 1992, Porter & Van der Linde 1995, Lowe *et al*. 1997, Smith 1997, Fineman 1998, 2000). In general, as White observes, "the mandate of most environmental agencies is not only to enforce compliance through use of criminal prosecutions, but to forge strategic alliances and working partnerships with industries, local governments and communities in support of environmental objectives" (White 2010). In the United Kingdom, maintaining a collaborative/negotiative relationship and a constructive dialogue with industries is crucial. Inspectors consider that without negotiation, the exercise becomes confrontational and while standards can be imposed, it is not sure they will be met (Fineman 2000).

In France, the sociologist Lascoumes carried out several surveys in the early 1990s of environmental

public policies and particularly environmental inspections. From his point of view, the purpose of environmental policies is not to protect nature (a sacrosanct value based on indisputable standards), as this would result in a prosecution each time there is environmental damage. Instead, his study of policies showed that they are more like strategic compromises between conflicting interests (environmental protection, the development of the industrial economy, urban planning, etc.) than real protection measures. Policies are more concerned with the modes of the relationship between different stakeholders, than the results to be achieved. In short, environmental policy is not a simple protection policy, but an organizational policy in which the purpose is to establish procedures for resolving problems. In this context, the main action principle for environmental inspectors is the regularization of non-compliant industrial plants. This regularization is not based on prosecutions, but on negotiation. Of course, the end goal is always compliance by industrial plants with the legal requirements. However, there are many ways to achieve this goal: visits to plants, emails, telephone calls, meetings, formal notices; prosecution is the ultimate action, which only taken when all other procedures have failed (Lascoumes 1994).

"Speak softly and carry a big stick" may be said to summarize the environmental inspector's position, without forgetting that the big stick can and will be used (White 2010). This shows that inspectors have an ambivalent role: "enforcer-as-helper" and "prosecutor-as-advisor" (Fineman 2000). With respect to sanctions, "prosecution ought to be an equal partner in the enforcement tool box" (White 2010): sanctions are necessary for the threat to be credible and to compel regulatory compliance (Zaelke & Higdon 2006). However, above all sanctions are an appropriate response to a particular set of circumstances (White 2010): this flexibility allows the inspector to tailor their response to the particular and distinct situation of each offender (Pedersen 2013). As Eckert (2004) notes in the case of Canadian and American inspectors, it is common for them to "respond to a detected violation by issuing a warning rather than prosecuting the violator". Eckert also noted that in cases of the inspection of petroleum storage facilities, the response to most violations has been a warning, with only a small number of prosecutions or fines. In this context, prosecution may be considered as a "poisoned chalice", which is unavoidable (Fineman 2000). However, the decision to prosecute depends on the size of the company, its previous performance and compliance record, the intent of the operator, and their degree of courtesy and respect for the inspector (Fineman 2000). Finally, prosecution remains a necessary last resort in the most serious cases (Pedersen 2013).

4 CONFIRMATION OF THE NEGOTIATION: THE FRENCH INSPECTION PROCEDURE

In French judicial procedures, the defendant's rights are based on the adversarial principle (the *principe du contradictoire)*, which means that both parties involved in a trial knows the arguments of their opponent.

In the context of the inspection of industrial plants, for many years administrative procedures did not provide any opportunity for the operator to be informed about developments and to present their own arguments. Prior to 2006, and the entry into law of the adversarial principle, the visit report was prepared by the inspector, working alone in their office. The plant's operator had no opportunity to make comments or to give their point of view. Moreover, the inspector was able to add new elements, which were not discussed during the visit. The time between the visit and the preparation of their conclusions was not clarified. This meant that in the time that elapsed between non-compliance being noted in the inspection and the formal notice sent by the *Préfet*, the operator was completely unaware of the subsequent procedures and administrative assessment of their case.

Little by little, the adversarial principle found in judicial procedures has influenced administrative procedures. In the following, we show that this principle forms the basis for a negotiation between the inspector and the operator of an industrial plant.

The French law that established citizens' rights in their dealings with the administration (12 April 2000) was the first to establish the principle of negotiation, by providing for "prior consultation" with the person who was the subject of a decision taken by an administrative authority; in this case the operator of the industrial plant.

At that time, the multiannual French environmental inspection program (2004–2007) had four main objectives. Two of them demonstrate the application of the adversarial principle: to increase the transparency of the actions of the inspector and to improve the coherency of all decisions taken on French territory. To achieve these objectives, the program provided easy access to information concerning the release of polluting materials, actions taken by the inspector to reduce industrial pollution and risks, and the results of the inspection, notably through the diffusion of information on the internet. This program has increased the visibility of inspection procedures and has allowed operators to be better informed of the procedures to be followed and how inspectors check industrial plants.

The Strategic Inspection Plan (2008–2012) confirmed the right of the general public to have access

to documents related to industrial plant regulation, especially those concerning the inspection visit. The 2006 modification to Article L 514-5 of the Environmental Code officially gives the operator the right to be informed of any follow-up subsequent to checks by the environmental inspector. The 2013 reform of environmental inspection confirmed this trend. Consequently, henceforth the adversarial principle is applied in post-visit procedures and before a formal notice is issued.

Transparency and the adversarial principle lead to the institutionalization of negotiations, both immediately following an inspection, and ex post, during prosecution procedures. Inspectors no longer prepare their visit report immediately after the inspection. First, they prepare a list of issues to be addressed or observations. This is written on-site, immediately following the visit, during a debriefing meeting. The document is signed by the inspectors and the plant's operator. The operator can add their own observations and comments concerning the list, by mail or e-mail, within three weeks of the visit. During this time they are expected to rectify any deficiencies.

This shows that the adversarial principle forms the basis for the procedure; the preparation of the list is the starting point for negotiations between inspectors and operators.

We have surveyed some of these lists, prepared by the environmental inspection agency in the *Provence-Alpes-Côte d'Azur* Region (in the south of France), which are available on the agency's website. This study shows that inspectors do not systematically demand compliance with the legislation. Most of the time, they indicate the issues that must be addressed within a certain timescale (usually three weeks). After the three-week deadline, the inspector updates the list with the following information: either the plant is compliant, or a formal notice is needed, or additional environmental measures are necessary. Next, they prepare their report (the *lettre de conclusion*), which summarizes the visit, the actions that were taken within the three weeks, or those which are planned and the time allowed to apply them. The same document also records any cases of previous non-compliance, which makes it possible to compare situations and see if the operator is making an effort to be compliant. The *lettre de conclusion* is send to the operator and can form the basis for a future formal notice.

This shows that the first part of the inspection procedure is based on negotiation; the objective is not to prosecute, but rather to find pragmatic solutions that address any deficiencies.

What happens in the case of non-compliance within the time indicated in the *lettre de conclusion*? The inspector, via the *Préfet*, can send a formal notice to the operator. In this notice, the *Préfet* reiterates the deficiencies that were found and gives a deadline for the operator to address them. According to a circular from the Department of Ecology (18 June 1998), this is a final warning and the deadline cannot exceed three months, except in special circumstances. However, in practice, this deadline is not always met. A study of court decisions shows that in some cases, a new deadline can be applied, notably when the plant is still non-compliant when the initial deadline expires. Moreover, several further deadlines can be applied, up to a period of two years (Baucomont & Gousset 1994)!

The second part of the inspection procedure is also based on negotiation, and allows the operator more time to make the plant compliant, beyond the deadline indicated in the legislation.

Since the 2013 reform to the Environmental Code, a new form of sanction has been introduced: "penal transaction". Before prosecution, and as a replacement to it, the *Préfet* can agree transaction with the operator, depending on the circumstances and the seriousness of the offense, the nature of the operator and its resources. In this case, the *Préfet* and the operator discuss the amount of the transactional fine and the operator's responsibilities; the idea is to both punish the operator and pay for any damages. The amount is limited to a third of the initial fine.

The introduction of penal transaction is final confirmation that the objectives of environmental policies are not to issue sanctions in cases of non-compliance, but to try to reconcile different interests, especially economic. With this kind of sanction available, public authorities may become less and less strict.

5 CONCLUSION

This study shows that the control of industrial plants is based on a negotiation between environmental inspectors and the operator. The negotiation demonstrates the real objective of environmental inspection: to try to reconcile conflicting interests and to protect the environment to the greatest extent possible without hindering the development of industrial activities. This leads to a compromise: the objective of control is not to prosecute but to find solutions that lead to compliance. The recent reform of the Environmental Code formalized the negotiation and the concept of the inspection.

What will be interesting in future work will be to examine the limit(s) of this concept of negotiation-based inspection. Are inspectors open to negotiation on any topics concerning the environment, including issues that relate to personal safety? How far can deadlines for compliance be extended? Are there some cases of non-compliance that do

not need to be prosecuted? What criteria should inspectors use to determine which cases of non-compliance should be prosecuted and those which should not?

In 1994, Pierre Lascoumes was doubtful about the limits of this kind of arrangement. Are repeated promises of compliance that are indefinitely postponed really tenable?

The answer has recently been given by the French administrative court, in the case of the AZF accident (*Cour Administrative d'Appel de Bordeaux*, January 24, 2013, n° 10BX02880, 10BX02881). The question revolved around whether or not environmental inspectors could be held responsible for the explosion of the industrial plant. Could it be argued that the inspection had failed and that this failure was one of the elements that contributed to the explosion? For the judges, the answer was "yes". They noted that the operator had committed numerous lapses in the management of the plant, which could be considered to be negligent; however, they pointed out that the inspection agency also made numerous mistakes. The plant was inspected eleven times between March 1995 and May 2001, without any formal notice being sent to the operator about poor management. It appears that the building where the explosion happened had never been inspected. The operator was never prosecuted, despite obvious and persistent failures. The judges noted that the negligence of the inspection agency was particularly serious, as the plant was located in an urban area, which should have justified harsh measures being taken against the operator. Consequently, the French State, because of the mistakes of the environmental inspection agency, was considered as responsible of a part of the accident.

The inspection of industrial plants may be based on negotiation, but the courts remind us that the application of environmental rules can only be negotiated up to a certain limit; and this limit is reached when safety is affected.

REFERENCES

Ayres, I. & Braithwaite, J., 1991. Tripartism: regulatory capture and empowerment. *Law and social enquiry* 16(3): 435–496.

Baucomont, M. & Gousset, P., 1994. *Traité de droit des installations classées*. Paris: Technique & Documentation, Lavoisier.

Bonnaud, L., 2002. Experts et contrôleurs d'État: les inspecteurs des installations classées de 1810 à nos jours (thesis). Cachan: École Normale Supérieure de Cachan.

Cornu, G. 2010. *Vocabulaire juridique*. Paris: Quadrige, PUF, 8th ed., 5th print.

Dupré, M. Etienne, J. & Le Coze, J.-C., 2009. L'interaction régulateur/régulé: considérations à partir du cas d'une entreprise Seveso II seuil haut. *Annales des Mines, Gérer et comprendre*, n° 97: 16–27.

Eckert, H., 2004. Inspections, warnings, and compliance: the case of petroleum storage regulation. *Journal of Environmental Economics and Management* 47: 232–259.

Fineman, S., 1998. Street level bureaucrats and the social construction of environmental control. *Organization Studies* 19(6): 953–974.

Fineman, S., 2000. Enforcing the environment: regulatory realities. *Business Strategy and the Environment Bus. Strat. Env.* 9: 62–72.

Galland, J.-P., 2008. La prévention des risques technologiques et professionnels en France et en Grande-Bretagne, des années 1970 à nos jours. *Revue française des affaires sociales* 2008/2, n° 2–3: 301–321.

Hale, A. Goossens, L. & Van de Poel, I., 2002. Oil and Gas Industry Regulation: from detailed technical inspection to assessment of safety management, *in Changing regulation: controlling risks in society*, ed. B. Kirwan, A. Hale, A. Hopkins, 79–106, Oxford: Pergamon.

Hawkins, K., 1984. *Environment and enforcement: regulation and the social definition of pollution*. Oxford University Press: Oxford.

Lascoumes, P., 1994. *L'éco-pouvoir. Environnements et politiques*. Paris: La Découverte.

Lowe, P. Clark, J. Seymour, S. & Ward, N., 1997. *Moralizing the environment*. UCL Press: London.

Olsen, P.B., 1992. *Six cultures of regulation*. Institute of Industrial Research and Social Development: Copenhagen Business School.

Pedersen, O.W., 2013. Environmental enforcement undertaking and possible implications: responsive, smarter or rent seeking? *The modern law review*, 76(2) MLR: 319–345.

Porter, M. & Van der Linde, C., 1995. Green and competitive. *Harvard Business Review* September-October: 120–134.

Rousseau, S., 2007. Timing of environmental inspections: survival of the compliant. *J. Regul. Econ.* 32: 17–36.

Smith, A., 1997. *Integrated pollution control*. Ashgate: Aldershot.

Strasser, K.A., 1996. Promoting pollution prevention and environmental technology in the United States traditional regulatory system. *Tilburg Law Review*, Vol 5, Issue 3:183–202.

White, R., 2010. Prosecution and sentencing in relation to environmental crime: Recent socio-legal developments. *Crime Law Soc Change*, 53: 365–381.

Zaelke, D. & Higdon, T., 2006. The role of compliance in the rule of law, good governance and sustainable development. *JFFP*, 5/2006: 376–384.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk assessment methods for improving urban security

C. Schoppe, J. Zehetner, J. Finger, D. Baumann, U. Siebold & I. Häring
Fraunhofer Ernst-Mach-Institut, Efringen-Kirchen, Germany

ABSTRACT: Risk management schemes have been applied to very diverse domains including logistics, health care, aviation, construction, defense, finance and security. Within common risk management processes the selection of dedicated risk assessment methods is crucial to fulfill the general requirements of such processes and some of the most critical risk management steps. There is a generic set of methods recommended by standards. These methods normally originate from a certain purpose but can be applied to systems and processes in general. The main goal of this article is to facilitate the selection of appropriate methods for risk assessment of issues occurring in the context of urban security and safety. Therefore we review and classify most of the risk assessment methods recommended by the generic standard ISO 31010 with respect to criteria relevant for their application in the urban security context, including estimated effort, needed data, expertise and technical support, specificity, and relevance.

1 INTRODUCTION

We understand urban security as prevention of and protection from unintentional and intentional harm resulting from crime or other deliberate human threats as well as anti-social behavior that take place in urban areas. Devising policies and deploying resources to enhance urban security is a complex task, in particular due to the high visibility of security issues to citizens and media and the many influences of urban security on everyday lives as well as economic prospects of citizens.

Considering the uncertainties that are involved in the rationales that determine devising policies and deploying resources there is a need for proper evidence bases that contain relevant information. Risk Assessment (RA) can be used to produce evidence bases for creating policies, for the prioritization of issues that need treatment and to assess situations with respect to the necessity to act. Therefore we propose to employ RA methods to create proper evidence bases to design security relevant policies.

There are many techniques that can be used to assess risks. The ISO standard (IEC/ISO 31010, 2009) alone lists over 30 RA techniques. The question that arises is: how to properly choose an appropriate RA technique that satisfies a given urban security need? Criteria for that can be the applicability with given constraints concerning personnel required, e.g., expert knowledge, timeframes and resources. To this end we review the methods presented in (IEC/ISO 31010, 2009).

The remainder of the article is structured as follows. In section 2 we anticipate urban security needs that RA methods are subject to. In section 3 we outline how needs are reflected within a defined taxonomy for indexing and selecting RA methods. In section 4, we briefly introduce the RA methods and classify them with respect to the taxonomy. In section 5 we conclude and give an outlook.

2 URBAN SECURITY NEEDS

In the following we list a few typical needs for organizations engaged in enhancing urban security. Decisions in urban environments usually take place in a very complex social system with very ambiguous and hardly quantifiable goals and values (Lewis and Hartley, 2001), (March and Olsen, 1989). Therefore we believe that sound explicit RA could support serious decisions and are expected to enhance the outcome of those decisions.

One reasonable need is prioritization of resources. Using RA can be a convenient way to plan resources in order to maintain security. In this way, the consequences of small capacities, e.g., limited monetary or personnel means, can be assessed and thus unforeseen negative consequences can be anticipated and mitigated.

As decisions tackling urban security often have high visibility and may trigger direct opposition, a credible and traceable narrative to justify also ongoing measures is often prerequisite. Here again RA can be of major impact as assessments of risks can be clearly communicated and often also have face validity, for example if bias-avoiding settings are used for generating qualitative assessments of consequences and frequencies.

Application of the presented methods is a complex task and should not be undertaken without proper training. Moreover note that it is not foreseen that solely one method should be applied but it is in many cases favorable to use several methods in a logical sequence.

To underpin the statements of this article we used the safety report of Luzern (Luzern 2013) to determine generic theoretical use cases in the domain of disturbances of the public (anti social behavior). We define case 1 as the generic topic disturbances of the public, case 2 as harassements in public areas, and case 3 as alcohol abuse in public areas. We will refer to these generic cases as Case 1, Case 2, and Case 3 throughout the method assesment.

3 CLASSIFICATION TAXONOMY

In this section we describe the developed taxonomy for classification of RA methods.

When choosing appropriate RA methods for urban security some aspects need consideration. Tight budgets are often a major issue in tackling urban insecurity, also see section 2. This holds true especially for proactive policies which nevertheless often have huge returns on investment. For example, in (Karoly et al., 2005) early childhood programs are evaluated regarding costs and benefits to society and found to have a good return on investment. For these reasons we select the criterion "resources" needed.

Another aspect to consider in regards to the assessment of risks in urban areas is the amount, type, and quality of data that is needed. Therefore we select the criteria "input" needed and the distinction between "qualitative" and "quantitative" for the input required.

A further criterion for using a method is the availability of supporting software, which we allocate to the criterion "software".

We try to estimate the effort that is needed to use a RA method in the field of urban security including the effort that is needed to adapt the method to particular urban security needs. We assume that the effort strongly depends on the focus of the method and the type of system it is usually applied in. So we selected the criterion "specificity". If a method is not focused on a certain aspect and is not intended for certain types of systems we rate the method as "generic". If a method is either focused on a certain aspect or it is intended for certain types of systems we rate it as "semi-specific". If a method is both focused on a certain aspect and is intended for certain types of systems we rate it "specific".

If a method is specific or semi-specific we qualify its specificity more in detail to support the assessment of the effort that is needed to apply the method in the field of urban security.

If a RA method can be used in the field of urban security in principle we determine the field within urban security in detail in the criterion "urban security field" and mention a possible benefit for above mentioned generic use cases (Case 1, Case 2 or Case 3) if applicable.

4 CATEGORIZATION OF RISK ASSESSMENT METHODS

In this section we categorize the RA methods. As proposed by (IEC/ISO 31010, 2009) RA methods can be distinguished in look-up methods, supporting methods, scenario analysis, function analysis, control assessment methods and statistical methods.

In sections 4.1–4.6 we briefly summarize the methods falling in these categories and their outstanding characteristics with respect to urban security. When discussing the methods, we use the taxonomy motivated and introduced in section 3. Table 1 sums up the classification of the RA methods according to the criterion "specificity" from the taxonomy. The values of the other taxonomies are given in the text along with the discussion of the applicability of the methods.

4.1 *Look-up methods*

In the following the look-up methods are described. These techniques present their output in lists in which the operator can look up the risk relevant entities.

4.1.1 *Check-lists*

A check-list is a collection of items (e.g. questions) which help to identify the current state of a system. Check-lists are usually developed by experts for a specific topic or system or reflect past experiences and can be used to identify hazards, risks or assess the effectiveness of a system or component (IEC/ISO 31010, 2009).

Check-lists are a generic method that can be applied in many fields within urban security. Particularly advantageous is that expert knowledge and knowledge from past experiences can be processed this way so that these check-lists can be used with relatively little experience and knowledge.

Check-lists can be applied, e.g., to assess levels of resistance of buildings against burglaries. A check-list for this application could contain questions like: Are there windows that can be seen by possible burglars? Accumulating answers to these kind of questions can help assessing resistance against burglaries. Also for pickpocketing risks rather short check-lists can be useful. In Case3 check-lists might be used to verify if a selected countermeasure was applied on every place where alcohol abuse was observed. The check-list then

Table 1. Specificity of risk assessment methods.

Section	Method name	Specificity
4.1.1	Check-lists	Generic
4.1.2	Preliminary Hazard Analysis (PHA)	Generic
4.2.1	Brainstorming	Generic
4.2.2	Structured or semi-structured interviews	Generic
4.2.3	Delphi technique	Generic
4.2.4	Structured "What if?" Technique (SWIFT)	Generic
4.2.5	Human Reliability Analysis (HRA)	Semi-specific
4.3.1	Root Cause Analysis (RCA)	Semi-specific
4.3.2	Business impact analysis	Generic
4.3.3	Fault Tree Analysis (FTA)	Semi-specific
4.3.4	Event tree analysis	Generic
4.3.5	Cause-Consequence Analysis (CCA)	Generic
4.3.6	Cause-and-effect analysis	Generic
4.4.1	Hazard And Operability Studies (HAZOP)	Specific
4.4.2	Hazard Analysis and Critical Control Points (HACCP)	Specific
4.4.3	Failure Modes and Effect Analysis (FMEA)	Specific
4.4.4	Reliability Centered Maintenance (RCM)	Specific
4.4.5	Sneak circuit analysis	Specific
4.5.1	Layer Of Protection Analysis (LOPA)	Semi-specific
4.5.2	Bow tie analysis	Semi-specific
4.6.1	Markov analysis	Specific
4.6.2	Monte Carlo simulation	Generic
4.6.3	Bayesian statistics and Bayes Nets	Generic
4.7.1	Decision tree analysis	Generic
4.7.2	FN curves	Semi-specific
4.7.3	Risk indices	Generic
4.7.4	Consequence/probability matrix	Generic

could contain names or geo-information of affected locations.

4.1.2 *Preliminary Hazard Analysis (PHA)*

PHA is conducted in several steps (Echterling, 2011) including hazards detection, preliminary classification into risk categories, assessing mitigation or reduction measures and checks if the applied measures comply with the expectations.

Aim is to appraise a preliminary risk category and to propose measures for mitigation using qualitative or quantitative techniques (Echterling, 2011).

Preliminary hazard analysis is a generic method that fits well to urban security issues. E.g. in Case 3 application of PHA could lead to the knowledge of probability and possible consequences of alcohol abuse to the public in the public. I.e. alcohol abuse takes place at certain places at certain times and can lead to a way of behaving that might compromise security of other people. Thus appropriate mitigation and response measures need to be planned and evaluated until the risk can be considered as mitigated.

4.2 *Supporting methods*

Supporting methods are techniques which are normally conducted with a survey manager who tries to educe knowledge or solution approaches from participants in interrogations. They can be applied during application of any of the described RA methods in the context of urban security.

4.2.1 *Brainstorming*

Brainstorming is a qualitative technique for generating ideas, clarifications and solutions (Gogus, 2013). It is a free flowing conversation amongst a group of knowledgeable people where ideas are proposed and discussed. It aims at inventions and the identification of failures and unnoticed hazards.

Brainstorming is a generic method and can be applied to almost any problem or assessment need. Note that results are qualitative in nature and that the analytical means of brainstorming are very limited. Usually no software is needed.

Brainstorming is appropriate for enhancing urban security. The fields of application are not restricted. It is a method that is well suited to be followed up by other methods, e.g. outcome of brainstorming can be further processed in a risk matrix. E.g. in Case1 Brainstorming could be applied at the very beginning to support identification of possible topics that have to be taken into account. In Case3 Brainstorming can be used as a supporting method within PHA to identify counter measures.

4.2.2 *Structured or semi-structured interviews*

This technique is a method to gain knowledge about a situation or a system and viewpoints of persons (Engle, 1998).

It is conducted by an interrogator who asks an interviewee a set of prepared open questions that can treat any themes (Cohen and Crabtree, 2006). Using this method a larger number of stakeholders can be involved because interviewees can be distributed over time and over location (Engle, 1998).

Interviews are a generic method and do not need additional software support. They are a proven methodology in the assessment of impacts and have in particular relevance when it comes to perceptions of risks. This has pitfalls as opportunistic policies should be prevented, nevertheless

interviews are of major use in urban security. E.g. in Case2 pedestrians could be interviewed to assess the impact of harassements in a certain area.

4.2.3 *Delphi technique*

Delphi technique is an iterative process to receive the most reliable consensus of opinions of a group of experts. It is used if there is a lack of appropriate information, for instance because of a lack of statistical/numerical data (Rowe and Wright, 1999).

In this technique multiple interrogations of different experts are conducted in a different way. Delphi techniques aim at untying the positive group effects while avoiding negative group effects. All participants contribute undisturbedly and during input collection implicit group dynamic effects are minimized. After several rounds, the group judgment is taken as the arithmetical mean of all rounds (Rowe and Wright, 1999).

Delphi is a generic method that fits perfect for utilization to enhance urban security. It is not bound to specific fields and is particularly useful to assess complex risks and larger scenarios. However, it needs dedicated time resources of all participants. E.g. in Case2 Delphi could be used to identify measures against harassment for people with different cultural background.

4.2.4 *Structured "What if?" Technique (SWIFT)*

SWIFT is a systematic team based study to identify risks and hazards (IEC/ISO 31010, 2009). It employs structured brainstorming and forms an alternative to hazard and operability studies technique (Card et al., 2012, IEC/ISO 31010, 2009).

SWIFT moderators use pre-developed guide words in combination with prompt words or phrases to stimulate participants to identify risks (Card et al., 2012, IEC/ISO 31010, 2009). 'What if' type phrases are used to investigate risk and how the further process differs from its normal behavior (IEC/ISO 31010, 2009). To identify hazards the facilitator typically asks 'How should' phrases.

SWIFT is a generic method that is useful in urban security and no software is needed for that technique. It is a straight forward approach to identify risks in almost all fields of urban security. E.g. in Case3 SWIFT could support the identification of effective countermeasures for alcohol abuse as the following: Raising alcohol prices in discos might lead to the phenomenon of pregaming as mentioned in (Luzern 2013).

4.2.5 *Human Reliability Analysis (HRA)*

Human reliability analysis is conducted in several steps. After the problem is defined the task is analyzed. During the next step the possible human errors are analyzed (event analysis). Factors that negatively influence human performance and error causes are immediately reduced and then quantified (frequency analysis). During screening in the next step it is estimated whether the error is significant or insignificant (consequence estimate). Significant errors and not screened errors are quantified in the next step. If the level of human reliability is achieved the process is documented. Otherwise the errors are reduced until the human reliability level is reached.

With regard to the aforementioned taxonomy human reliability analysis is a semi-specific method. This technique can be used to avoid faults and identify situations that are prone to induce inadequate actions. E.g. in Case 2 harassment might be encountered by explaining correct behavior to harassing people. HRA could then be used to analyze possible human errors in that task. One could then conclude that e.g. explanation should be performed by people with intercultural background as done in (Luzern 2013).

4.3 *Scenario analysis*

Under the term scenario analysis techniques are summarized, that try to assess a risk using scenarios. By defining a scenario, possible effects or possible causes of effects are analyzed. These techniques can be used to generate a solution which prevents the defined scenarios from taking undesirable turns.

4.3.1 *Root Cause Analysis (RCA)*

Root cause analysis is a technique to determine the root causes of failures in systems (Stapelberg, 2009). It can be used in multiple contexts like manufacturing improvements, safety projects, clinical accident, and crime reports (Reid and Smyth-Renshaw, 2012).

According to criteria given in section 3 RCA is a semi-specific method that focuses on failures in systems. RCA can therefore be used in urban security scenarios within the field of systems that can have failures, e.g. communication systems.

4.3.2 *Business impact analysis*

Business impact analysis is a technique to identify key disruption risks and how they affect operations and what resources are needed to manage them (IEC/ISO 31010, 2009).

This kind of technique involves several steps which are conducted by a team of knowledgeable members (Goldberg, 2008). Aim is to develop strategies for a quick recovery from unexpected incidents.

This generic method can be used in the field of urban security to assess processes and actions that are planned to mitigate risks, in particular after major disruptive events.

4.3.3 *Fault Tree Analysis (FTA)*

Fault Tree Analysis is a deductive process to identify casual factors which contribute to a specific undesired event (Modarres, 2006, IEC/ISO 31010, 2009). It is probably the most common assessment

technique in probabilistic RA to quantify the occurrence of failures in subsystems. To achieve this, it sub-divides a process into its basic components for which adequate data exist (Modarres, 2006).

Fault tree analysis has not to consider all possible failures, only these which lead to the top event (Modarres, 2006). The output is finally depicted in a directed tree diagram. The factors in the tree diagram can be hardware failures, software failures, human errors or pertinent events (IEC/ISO 31010, 2009).

The FTA focuses on the aspect of faults in every kind of system, so we classify it as semi-specific. If a top event is seen as an unintended event within the urban system FTA can be adapted with manageable effort. It should only be applied if combinations of events are crucial and necessary for understanding and improving urban security issues. E.g. in Case2 could be the negative impact on security for pedestrians. One possible failure that leads to the top event can be harassment. One failure that can lead to the aforementioned one could be alcohol abuse (which is in fact Case3). Harassment as consequence of alcohol abuse is also mentioned in (Luzern 2013).

4.3.4 *Event tree analysis*

Event tree analysis is a graphical technique following an inductive logic to represent events and consequences which can result from an initiating event. Additionally systems, functions and barriers can be considered (Stapelberg, 2009, IEC/ISO 31010, 2009).

This technique is a quite generic method to estimate consequences.

We rate this method as appropriate for use in the urban security domain, in particular for understanding and mitigating the spreading of security issues.

4.3.5 *Cause-Consequence Analysis (CCA)*

Cause consequence analysis was developed in Denmark to analyze risks in safety critical systems such as nuclear power stations (Stapelberg, 2009, IEC/ISO 31010, 2009). The difference to other tree analyses like "Decision tree analysis" is that cause-consequence is extended through the possibility to consider time delays.

CCA represents its output in a graphical way, starting from a critical event. Aim is to identify chains of events that can result in an unwanted event (Stapelberg, 2009). In this connection not every event has to be a failure event.

This technique regarding to the aforementioned taxonomy is a generic method that is able to estimate consequences of events. In the domain of urban security it is a valuable feature to take time delays into account. So we assume that this method is even more applicable in the urban security domain than event tree analysis. The drawback of ETA as well as CCA is that they inductively cover all chains of events rather than focusing from the very beginning on undesired security events, like FTA. E.g. in (Luzern 2013) it is mentioned that persons with mental issues or that are addicted to alcohol can be observed as problematic in the context of harassments, which refers to Case2. The application of CCA in Case2 can help to identify the linkage between harassments and people that are addicted to alcohol or have mental issues.

4.3.6 *Cause- and-effect analysis*

Cause and effect analysis is a qualitative method to identify possible causes of an unwanted event or problem.

Cause and effect analysis is a technique that can be used in the root cause analysis. Thereby this technique uses techniques like brainstorming, sometimes tree diagrams and mostly a fishbone diagram to structure a list of causes of a specific effect.

This generic method can be used in the domain of urban security to identify causes of events to counter reasons for unwanted events. This method could also be applied for Case2 with the same purpose as CCA.

4.4 *Function analysis*

These techniques deal with the functionality of a system. Aim is to develop an alternative technical solution to an existing problem.

4.4.1 *Hazard and operability studies (HAZOP)*

HAZOP is a structured and systematic examination of a planned or existing product, procedure or system (IEC/ISO 31010, 2009). The aim is to identify failure modes and their causes and consequences bearing the whole system in mind (IEC/ISO 31010, 2009, Dunjó et al., 2010).

This is achieved by exploring the effects of any deviation from its design condition. This way not only hazards can be identified but also operability problems (Dunjó et al., 2010).

HAZOP is a specific method that was developed for technical uses. Thus it cannot be easily adapted to urban security. Nevertheless the basic idea to identify failure modes and their causes and consequences could prove to be beneficial for urban security.

4.4.2 *Hazard Analysis and Critical Control Points (HACCP)*

HACCP is a method to protect a system against occurring hazards. Protection is achieved by putting controls in place at all relevant parts of the system, process or procedure (IEC/ISO 31010, 2009). It ensures that risks are minimized and possible contaminations are identified before they occur (Cusato et al., 2012).

In summary, HACCP is a technique in which critical key numbers in a system are defined to identify risks and hazards which can influence product quality (IEC/ISO 31010, 2009).

HACCP is a specific method that cannot readily be applied to assess urban security issues. HACCP is used to assess technical systems and thus the gap to urban security is not easily bridged. However, the idea of key sensitivities, observables and mitigation strategies could be a focusing starting point.

4.4.3 *Failure Modes and Effect Analysis (FMEA)*

Failure modes and effect analysis is a qualitative tabular technique to examine possible failure modes and solutions during system design which is conducted preventively to avoid errors and increase the technical dependability (Xiao et al., 2011, Ben-Daya, 2009).

FMEA is a specific technical method that is not particularly useful to assess urban security risks. This holds due to its technical specification.

4.4.4 *Reliability Centered Maintenance (RCM)*

RCM was developed for aircraft industry but quickly expanded in the last years to many other industries.

It is a technique to identify the policies that should be implemented to manage failures to achieve the required safety for a system or subsystem (IEC/ISO 31010, 2009). Thereby, this technique focuses on system functions not on hardware (Rausand, 1998). To analyze a system, RCM asks several questions e.g. concerning functions, causes of functional failures, modes of failures, and suitable proactive tasks (Siddiqui and Ben-Daya, 2009).

Aim of RCM is to reduce the occurrence of failures by focusing on the most important functions of the system and avoiding or removing maintenance actions that are dispensable (Rausand, 1998).

RCM analysis is a specific method. This method is specifically designed to maintain (and optimize) reliable processes. Therefore its key idea is suited for application in urban security: by using this technique strategies can be assessed with regard to their appropriateness.

4.4.5 *Sneak circuit analysis*

Sneak analysis is a technique for identifying latent hazards which arise from design or systematic errors but not from component caused failures (Whetton and Armstrong, 1994, IEC/ISO 31010, 2009).

Originally it was developed to verify design and to discover unintentional electronic circuit paths. Nowadays this technique is advanced to analyze failures in systems with complex workflows (Whetton and Armstrong, 1994). Usually it amends traditional methods such as HAZOP (Whetton and Armstrong, 1994). In this way failure points, unsuppressed inductive loads, unnecessary components, unnecessary software codes or inadequate redundancy provisions can be identified (NASA, 1995).

Sneak circuit analysis is a specific method that seems not to be useful for the enhancement of urban security due to its very technical specification.

4.5 *Control assessment methods*

These techniques assess risk by analyzing the layers of protection and how the risks harm them.

4.5.1 *Layer Of Protection Analysis (LOPA)*

Layer of protection analysis is a semi quantitative analytic tool developed for the chemical industry (Gowland, 2006, IEC/ISO 31010, 2009).

Aim is to develop independent layers of protection to prevent scenarios from changing in an undesirable scenario. Here it is important to ensure that all layers of protection are mutually independent. (Wei et al., 2008). Criteria for independency are given in (Gowland, 2006, Wei et al., 2008).

LOPA is a semi-specific method that can be used to assess the effectiveness of controls that have been put in place to mitigate urban security risks. LOPA offers a rather technical framework for performing such analyses. E.g. in Case3 one layer of protection could be the legal prohibition of selling alcohol in certain areas. A second layer of protection could be a number of social workers at the affected areas. LOPA can support the analysis of these protection layers.

4.5.2 *Bow tie analysis*

Bow tie analysis is a qualitative, iterative technique often conducted by a team. It unifies fault tree analysis and event tree analysis. This technique visualizes all effects leading to a top event and all consequences which result from the top event (Badreddine and Ben Amor, 2010).

Bow tie analysis is a semi-specific method. As it combines two methods which fit to the purpose of urban security enhancement, we believe it to be suitable for rather extensive analysis of specific security issues, e.g., terroristic events.

4.6 *Statistical methods*

Statistical methods use mathematical models to assess risks. These models use probabilities to predict the possible development of a process or system.

4.6.1 *Markov analysis*

Markov analysis is a technique which can be used when the assumption that the future state of a system depends only upon its present state holds (IEC/ISO 31010, 2009). Markov analysis assesses the reliability of a given system (Muthu and Petrou, 2007) by analyzing the transition probabilities, i.e. knowing the state the system is currently in, by the

means of Markov analysis the likelihood of transforming into another state is computed.

Markov analysis is a specific software-supported method. For many fields in urban security we deem it unlikely that the Markov property holds, i.e. that future events only depend on the present situation and are not influenced by past events.

4.6.2 *Monte Carlo simulation*

Monte Carlo simulation is a probabilistic technique conducted with software. It is applied where exact numerical methods cannot be reasonably used because of the complexity of the system (Pellicione and Lu, 2008). To cope with this complexity random distributions are estimated and the system is tested by using samples from the distributions as input.

Monte Carlo simulation is a generic RA method. Due to its complexity in calculation especially if many entities are involved we state that it can probably only be used to model very few and very particular aspects of urban security.

4.6.3 *Bayesian statistics and Bayes Nets*

Bayesian statistics are founded on the Bayes theorem that can be used to calculate conditional probabilities. Bayesian statistics are often represented as Bayesian Belief Networks (BBNs). BBNs are directed acyclic graphs that represent probabilistic dependency models. What distinguishes the BBNs from other casual belief networks is "the use of Bayesian calculus to determine the state probabilities of each node or variable from the predetermined conditional and prior probabilities" (Krieg, 2001), meaning that the probabilities can be based on a person's belief of the likelihood of an event.

Bayesian statistics are a generic method that is well suited for assessment of urban security related risks. In particular, with corresponding effort, BBNs can be applied to model severity of consequences for different scenarios based on expert opinion.

4.7 *Others*

All techniques that do not fit into one of the above categories are collected under this chapter.

4.7.1 *Decision tree analysis*

Decision tree analysis is a formal, structured and graphically supported technique used to simplify knowledgeable decision making. Branches in the diagram represent a classification rule and decision nodes indicate the value on target classes, (Doğanavşargil and Fattori, 2008). Big amounts of data and complex problems can be analyzed. Decision tree analysis helps to decompose unmanageable data volumes and problems into decision rules and to assess solutions (Doğanavşargil and Fattori, 2008).

Decision tree analysis is a generic method and should be applicable to urban security issues.

4.7.2 *FN curves*

FN curves are represented in diagrams that "are a graphical representation of the probability of events causing a specified level of harm to a specified population" (IEC/ISO 31010, 2009) or object class, e.g. built infrastructure. FN curves can be seen as continuous risk matrices and can be used to assess levels of risks by comparing the actual assessments of the risks with previously set thresholds.

FN curves are a semi-specific method and can be applied to urban security, e.g. for assessing explosive scenarios. FN curves can e.g. be applied to compare risks to levels of risk defined in standards (Suddle, 2003).

4.7.3 *Risk indices*

Risk index is a semi quantitative technique with the aim to rank different risks (IEC/ISO 31010, 2009).

After a detailed description of the monitored system, "scores are developed for each component in such a way that they can be combined to provide a composite index" (IEC/ISO 31010, 2009).

Risk indices are a generic method and can be applied for monitoring risks in urban environments.

4.7.4 *Consequence/probability matrix*

Consequence/probability matrices are also known as risk matrices. They present their output in a pictorial way in form of a matrix. Risk matrices are likewise used to rank different risks to determine which risks need further or more detailed analysis. They also create a common understanding for a level of risk (IEC/ISO 31010, 2009) and its communication.

With help of such matrices it is easy to assess risks in an intuitive way and arrange risks in damage classes. These damage classes can be of qualitative or quantitative nature. By coloring the different damage classes the risk matrix is even more intuitive understandable. Thereby the allocation of the damage classes is up to the user.

Risk matrices are a generic method that can be used intuitively and can be very convenient for a first assessment of risks to decide which risks should be considered in more detail. This way risk matrices are a very appropriate means for assessing risks in urban environments as can be seen, e.g. in Luzern (Luzern 2013).

5 CONCLUSION AND OUTLOOK

In this paper we briefly presented RA methods and assessed their relevance from the perspective of urban security. We proposed a categorization of the RA methods relevant for urban security.

In doing this we tried to extend present taxonomies as e.g. presented in (IEC/ISO 31010, 2009) for practical use in urban security. We demonstrated the practical relevance of the taxonomy for the selection of methods by giving application examples of the described methods where appropriate.

Future work could add more assessment methods and develop a software application that facilitates easy method selection for urban security practitioners. Moreover, we could refine the selection taxonomy or apply it to related domains, e.g. airport security.

This publication results from the BESECURE project (Best practice Enhancers for Security in Urban Environments, http://www.besecure-project.eu), funded by the European Union FP7 Security Programme under grant agreement number 285222.

REFERENCES

Badreddine, A. & Ben Amor, N. 2010. A New Approach to Construct Optimal Bow Tie Diagrams for Risk Analysis. *In:* García-pedrajas, N., Herrera, F., Fyfe, C., Benítez, J. & Ali, M. (eds.) *Trends in Applied Intelligent Systems.* Springer Berlin Heidelberg.

Ben-Daya, M. 2009. Failure Mode and Effect Analysis. *In:* Ben-Daya, M., Duffuaa, S.O., Raouf, A., Knezevic, J. & Ait-Kadi, D. (eds.) *Handbook of Maintenance Management and Engineering.* Springer London.

Card, A.J., Ward, J.R. & Clarkson, P.J. 2012. Beyond FMEA: The Structured What-If Technique (SWIFT). *Journal of Healthcare Risk Management,* 31, 23–29.

Cohen, D. & Crabtree, B. 2006. Qualitative Research Guidelines Project.

Cusato, S., Tavolaro, P. & Oliveira, C. 2012. Implementation of Hazard Analysis and Critical Control Points System in the Food Industry: Impact on Safety and the Environment. *In:* Mcelhatton, A. & Do Amaral Sobral, P.J. (eds.) *Novel Technologies in Food Science.* Springer New York.

Doğanavşargil, E. & Fattori, M. 2008. Decision tree analysis as a tool to optimise patent current awareness bulletins. *World Patent Information,* 30, 212–219.

Dunjó, J., Fthenakis, V., Vílchez, J.A. & Arnaldos, J. 2010. Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials,* 173, 19–32.

Echterling, N. 2011. Bericht E 17/11. Efringen-Kirchen: Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach Institut.

Engle, R. 1998. Multi-step, structured interviews to select sales representatives in Russia and Eastern Europe. *European Management Journal,* 16, 476–484.

Gogus, A. 2013. Brainstorming. *In:* Carayannis, E.G. (ed.) *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship.* Springer New York.

Goldberg, E.M. 2008. Sustainable Utility Business Continuity Planning: A Primer, an Overview and a Proven Culture-Based Approach. *The Electricity Journal,* 21, 67–74.

Gowland, R. 2006. The Accidental Risk Assessment Methodology for Industries (ARAMIS)/Layer Of Protection Analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment? *Journal of Hazardous Materials,* 130, 307–310.

IEC/ISO 31010 2009. International Electrotechnical Commission IEC/ISO 31010 Risk management—Risk assessment techniques. Geneva: International Electrotechnical Commission.

Karoly, L.A., Kilburn, M.R. & Cannon, J.S. 2005. Early Childhood Interventions—Proven Results, Future Promise. RAND Corporation.

Krieg, M.L. 2001. A Tutorial on Bayesian Belief Networks.

Lewis, M. & Hartley, J. 2001. Evolving forms of quality management in local government: lessons from the Best Value pilot programme *Policy & Politics,* 29, 477–496.

Luzern, City of. 2013. Sicherheitsbericht Stadt Luzern 2013.

March, J.G. & Olsen, J.P. 1989. *Rediscovering Institutions: The Organizational Basis of Politics* The Free Press.

Modarres, M. 2006. *Risk Analysis in Engineering: Techniques, Tools, and Trends*, Taylor & Francis Group.

Muthu, K. & Petrou, M. 2007. Landslide-Hazard Mapping Using an Expert System and a GIS. *Geoscience and Remote Sensing, IEEE Transactions on,* 45, 522–531.

NASA 1995. Sneak Circuit analysis guideline for electromechanical systems.

Pellicione, M. & Lu, T.-M. 2008. *Evolution of Thin Film Morphology*, Springer New York.

Rausand, M. 1998. Reliability centered maintenance. *Reliability Engineering & System Safety,* 60, 121–132.

Reid, I. & Smyth-Renshaw, J. 2012. Exploring the Fundamentals of Root Cause Analysis: Are We Asking the Right Questions in Defining the Problem? *Quality and Reliability Engineering International,* 28, 535–545.

Rowe, G. & Wright, G. 1999. The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting,* 15, 353–375.

Siddiqui, A.W. & Ben-Daya, M. 2009. Reliability Centered Maintenance. *In:* Ben-Daya, M., Duffuaa, S.O., Raouf, A., Knezevic, J. & Ait-Kadi, D. (eds.) *Handbook of Maintenance Management and Engineering.* Springer London.

Stapelberg, R.F. 2009. Safety and Risk in Engineering Design. *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design.* Springer London.

Suddle, S.I. 2003. A logarithmic approach for individual risk: the safety-index. *In:* Bedford, T. & Van Gelder, P.H.A.J.M. (eds.) *ESREL 2003.* Taylor & Francis.

Wei, C., Rogers, W.J. & Mannan, M.S. 2008. Layer of protection analysis for reactive chemical risk assessment. *Journal of Hazardous Materials,* 159, 19–24.

Whetton, C. & Armstrong, W. 1994. Sneak analysis of batch processes. *Journal of Hazardous Materials,* 38, 257–275.

Xiao, N., Huang, H.-Z., Li, Y., He, L. & Jin, T. 2011. Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. *Engineering Failure Analysis,* 18, 1162–1170.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Abstract representation of power system networks as a function of regularity properties

A.B. Svendsen, T. Tollefsen, R.F. Pedersen & K.P. Petursson
Goodtech Power, Bergen, Norway

D. Patel & O.D. Lampe
Christian Michelsen Research AS, Bergen, Norway

ABSTRACT: Goodtech and Statnett SF have developed an online regularity calculator with minimal delay between acquisition of process values and presentation of regularity indices for the power grid. The simulation tool calculates the probability of failure on every component in the system and combined with a flow model, the reliability of power supply for every load branch. In order to analyze and understand all risk and reliability changes every 10 minutes for the large network a new representation method must be developed and tested.

In this paper a new methodology for representation of how changing risk level can be presented for power system operators is introduced. By manipulating the geographical representation of the 7000 branched power system based on calculated risk levels and power flows, it should be possible to, by "one look at the screen", understand the current risk level and weigh the changes occurred.

1 INTRODUCTION

The fascinating, but very complex field concerning reliability analysis of power systems was opened by J. Endrenyi in his excellent textbook (Endrenyi, 1978) and later expanded by R. Billinton and R. N. Allan in their textbooks (Billinton, 1983) and (Billinton, 1996). Both these pioneers pointed out the efficiency of Markov models. However, lack of efficient tools for building large Markov models restricted practical application of this method and several publications has argued, incorrectly, that Markov models was not applicable in practical applications.

In a master's thesis carried out by Arne Brufladt Svendsen (Svendsen, 2002), thesis advisor Tørris Digernes discovered a method suitable for building large Markov models. A central clue in the calculation was the Kronecker matrix operators, (Sasty, 1999). The method was tested by Svendsen in his thesis and found to be very efficient for reliability analysis of power systems. Since then, various R&D projects concerning offline calculations of reliability of supply in complex meshed power grids have been carried out.

Although the simulation program Promaps was designed for offline analysis, it was early recognized that the concept also was suitable for online analysis. In 2009 an agreement between Goodtech Projects & Services and Statnett SF in Norway was signed concerning development of a computer program for online calculation of reliability of supply in the Norwegian main electrical power grid. The project was put in online operation October 2013 in Statnett's operational central.

The industry standard for visualizing the power system consists of nodes being positioned relative to each other, with respect to their geographical position, with straight lines representing cables and connections. During testing and verification of the online risk simulation tool, the need for new ways to visualize large networks rapidly became obvious.

More expressive and informative overviews over the power system may be produced by lessening these established constraints regarding visual representation.

In order to analyze and understand all the risk and reliability results every 10 minutes for the large net-work, a new representation of the changing risk level has been developed and tested.

Similar experiments on graphs in general have been heavily researched in the recent years (Landesberger, 2011). This is partly due to graphs of larger sizes appearing in several domains and due to more powerful processing capabilities on computers.

This document contains a presentation of the online risk tool Promaps Online, currently running simulation of the Norwegian power system. Furthermore in this paper we introduce some of

these latest graph visualization techniques into the realm of power system network analysis. In the following sections, we will present three different techniques applied on a power grid, edge bundling, focus and context visualization and non-geographic graph layout with clustering.

Section 2 presents the needs as seen from the grid owner's point of view. Section 3 presents the principles and background behind the reliability calculations. Section 4 describes how results are presented today, and how new techniques can be used to enhance visualization. A brief description of "non-electrical" applications is presented in section 5. The conclusions are presented in section 6.

2 THE TSO POINT OF VIEW

The Transmission System Operator (TSO) is faced with increasing requirements regarding the reliability of power delivery. The cost of not delivering agreed energy can be substantial.

In Norway there is a cost (CENS) connected to energy not being delivered. If a grid company has low continuity of supply, the company will experience a reduction in the allowed network charges every consumer pays.

The most important tools for power system operators are power flow calculations, dynamic analyses etc. To analyze the reliability of supply, additional tools are needed.

2.1 *Calculation tool*

It is easy for a TSO to recognize the need for simulation tools that can calculate the risk levels for different time horizons. Such a simulation tool should be useful for a TSO in online operations, day-ahead and intraday short-term grid planning:

Online operation:

- In online operation the risk level is calculated every minute and evaluated if risk indexes are out of boundary or out of planed and accepted risk level for the coming hours.

Day-ahead and intraday-planning:

- Short time planning of operation to perform detailed simulations for the next days based on planned power system parameters and grid configuration.

2.2 *Visualization*

With the new reliability calculation tools entering the industry, TSOs are for the first time able to get detailed information about the state of the power system every 10 minutes. However, it's not enough to receive the data, the operators must also be able to understand it, analyze it, and if necessary take precautionary actions.

This cannot be achieved in a satisfactory manner using tables and graphs, and conventional visualization techniques do not offer the necessary flexibility. Illustrating the state of the power system using fixed nodes and straight lines limits the amount of data that can be presented to just a few key parameters. In general, all information must be presented using only changing colors and numbers. There are several drawbacks to this approach.

1. Only a very limited amount of information can be shown at any given moment
2. In order to show the entire grid, a large number of big screens must be used, making it hard to get an overview

It is however not enough to create a new visualization technique. It's even more important to obtain and select the most relevant and useful information.

3 ONLINE RELIABILITY CALCULATIONS

Online calculations in Promaps consist of the following steps:

– Data acquisition
– Calculate probability and frequency of branch failure in power grid
– Calculate probability and frequency of all contingencies, and select a subset of contingencies with the highest probability of occurring
– Calculate consequences of the contingencies selected in previous step.
– Calculated aggregated risk indices based on probability and consequences of all selected contingencies
– Present results for users

These steps are then repeated every ten minutes, as new data is available, thus enabling trending of risk indices. A closer description of each step follows.

Data acquisition requires that Promaps is integrated in the TSO's SCADA-system. Necessary data are: an electric model of the power grid, process values, switch positions, information about protection schemes, and information about available spinning reserves. During online calculations only process data, switch positions and spinning reserves are necessary to update at every iteration.

Probability and frequency of branch failures are calculated by compositing Markov models and aggregation of states. Promaps represents each component, related to power flow properties, with a Markov model. Each model describes

possible states of the component and frequency of transition between states. Examples of states can be "functioning normal", "temporary error" and "sustained error". Markov models representing each branch in the power grid are then created through compositing models of all relevant components, and aggregating all resulting states with similar net effect on the power system. This enables Promaps to model every individual component in the power grid, thus making use of all available failure statistics. The full explanation of this methodology was presented in (Digernes, 2004).

A contingency consists of one or more branches failing at the same time. For a large power grid, the number of possible contingencies is infinite for all practical purposes. Therefore, consequence evaluation of all possible contingencies is not possible. Instead, Promaps calculates the probability of each contingency occurring, and select a subset of contingencies based on the probability. This subset typically consists of a few thousand contingencies, but will usually cover close to 99% of the complete probability space.

Each contingency has to be evaluated for consequences for the power grid. Consequences of interest are reduced ability of delivering power to load points. Promaps uses an economical load flow model, where different costs are assigned to production and spinning reserves, and load shedding are prioritized according to cost of not delivering energy. The methodology also supports different kinds of system protections.

Risk of the system not being able to deliver required energy to each load point can be calculated based on probability, expected frequency and consequences of all consistencies. Several risk indices can be derived from these results, the main risk index calculated in Promaps being *system minutes*, SMS. System minutes are the expected energy shortage normalized on the size of the power grid.

In the end the results are presented graphically to the users. Promaps has based its graphical view on TSOs SCADA pictures, adding a layer of risk indices.

4 PRESENTATION OF RESULTS

4.1 *Risk parameters*

To be able to quickly asses a power system's risk level, few key risk parameters should be presented. In Norway there is a cost for energy not being delivered to the customer (CENS). This cost is divided into different customer groups and time of day. When a TSO experience a loss of load, the TSO will get a reduction in next year income based on outage and the corresponding CENS cost.

The Promaps simulation tool calculates the power delivery reliability as a function of demand, the probability for undelivered energy for each load branch in the system and for the system as a whole. Therefore the CENS cost factor could easily be included in the results and are currently one of the system risk indicators used. In addition not delivered energy and corresponding CENS cost, System Minutes (SMS) is used as an online risk indicator.

4.2 *Standard operational view*

Currently the SMS index is being used to set the limits for the dynamic color indication for the risk level in the system. In the test evaluation phase that is ongoing, the following level is set for the total System Minute (SMS):

– 0–10 minutes, no color
– 10–15 minutes, yellow color
– >15 minutes, red color

The color indication is shown on a regional level in Figure 1. The colors represent the expected energy shortage normalized of the size of the respective region.

The color indication is shown on the single line diagram of Figure 3 for each load branch and for the total system. If there is yellow risk indication for the system the operator should evaluate possible action to be taken if the risk level further increases. If the system experience red indication the operator shall perform a power system action to reduce the risk.

The schematics in Figure 2, is based on the schematics currently being used by the TSOs in their operational central.

The TSOs need several such images in order to cover the entire grid. In addition, if a critical component lies on the boundary between two areas, it will be hard to get an overall picture of how actions carried out by the operator will impact the system in both regions.

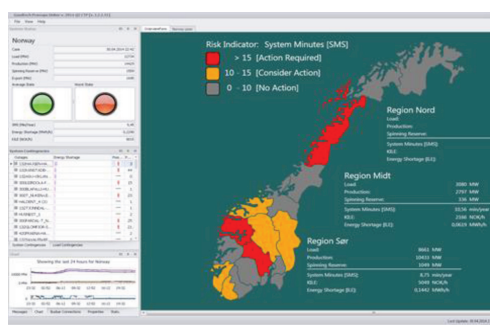


Figure 1. Overview of the risk level in each region.

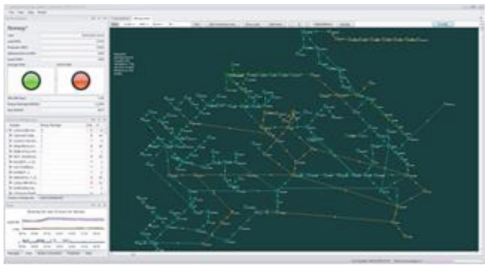


Figure 2. The standard operational view for one region.

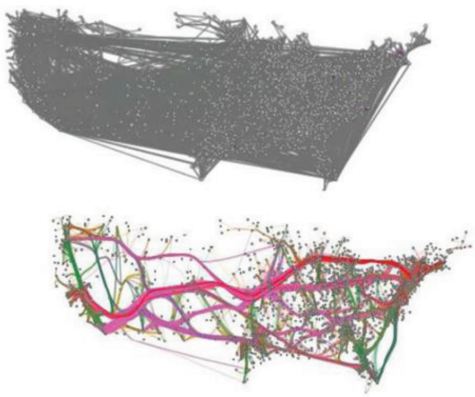


Figure 3. Edge-bundling. Naive visualization of migration between states in the US. Edge-bundling reduces clutter.

4.3 *Edge bundling*

Edge bundling is a technique where edges are attracted to each other so that edges that both move in the same direction and are next to each other bundle together into so called edge bundles. When the destination nodes are reached, the edges fan out from the bundles. The advantage of this method is most dominant in examples where the amount of edges is very high and connections are crossing each other in all directions. For such situations, normal straight edges will result in having the visual area overdrawn with edges so that none are discernible from each other. See Figure 3.

Bundle-thickness as well as color representing degree of flow adds extra information (right) (Cui, 2008).

To demonstrate this technique on the Norwegian power net, we have artificially added an extra amount of edges in the central part of the country and compared the result with original straight edge visualization (left) and edge bundling (right) in Figure 4.

The large square shows how edges are clustered into groups so it is easier to follow them. The small square shows a node with three edges going out in a similar direction and how the clustering of them before they fan out gives a more visually pleasing and easy-to-trace presentation. In general the visualization becomes more organic when using edge bundling. The technique could be particularly useful for power systems which have connectivity more similar to the one in Figure 1.

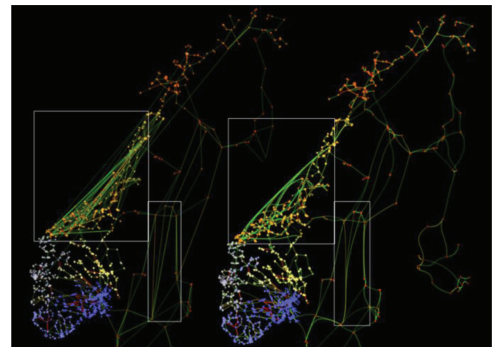


Figure 4. Demonstration of normal visualization (left) and edge bundling (right) on the power net of Norway. Extra edges have been added in the large box for demonstration purposes.

4.4 *Focus and context visualization*

Focus and context visualization is the technique of showing in the same visualization both details on the area of importance for a particular task (the focus area) and at the same time provide an overview so one can see the relations between the detail and the whole system (the context). The state of the art report (Herman, 2000) presents focus and context for the field of graph visualization.

Figure 5 shows three different views of the power system in Norway. SMS levels on nodes indicating capacity are colored from high to low with the color scale green-yellow-red. Edges are colored according to percentage of max flow with color scale blue-yellow-red where red is maximum. The smallest map to the left gives a compact overview. One can identify two areas being yellow and one being red. The center map has a higher zoom for better details while the rightmost map exhibits the focus and context property where the area which was red has been zoomed in on while displacing the nodes and edges around. One can imagine several such zoom-ins simultaneously on areas of particular importance.

Figure 5 shows such a focus and context example where the whole grid is shown as context while the area of maximum load is shown expanded in such a way that the neighboring nodes and edges

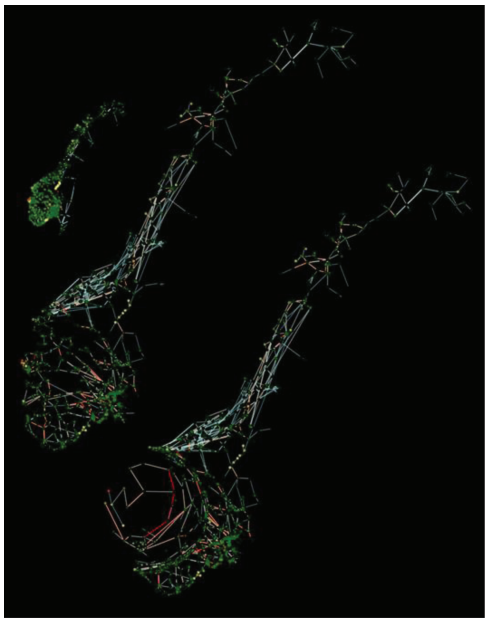


Figure 5. Three different views of the power net of Norway. SMS levels on nodes indicating capacity are colored from high to low with the color scale green-yellow-red.

are being pushed away. Such visualization can be made dynamic so that areas of importance get larger screen space while less important areas shrink, but still maintaining an overall correct geographic placement of the nodes.

4.5 *Non-geographic graph layout with clustering*

In this section we will demonstrate the effect of giving the network a new layout which is not based on geographic location, but on an abstract placement that distributes nodes and edges for reducing overlap and having a more even distance between nodes by spreading nodes that are very close to each other.

One of the main challenges of visualization of risk results is the complexity of causes and effect that comprises the results. The main contributing causes to the result might be located far from the load points affected, thus making it difficult to compress all relevant information into a single picture. For instance, a large industrial load can be greatly dependent on a few power lines supplying power to a greater topologic area. Usually the TSO are aware of these cuts, and monitor them, but new critical cuts might suddenly arise in if the total load of the system rises or maintenance work is performed on some parts of the power grid. It might thus be more appropriate to move away from the classical power grid views, and instead develop methodology for dynamic power grid view that do not focus on flow and topology, but instead highlights critical cuts and components. The idea is to make a picture of the power grid that hides away everything that is performing normal, and instead emphasizes on the few components that are critical for the reliability of the power grid. Such an approach might also lead operators to a better understanding of reliability in power grids.

Błąd! Nie można odnaleźć źródła odwołania. clearly illustrates how an abstract representation of the power grid can help emphasize the most important components.

In **Błąd! Nie można odnaleźć źródła odwołania.**, colors are added to easily differentiate the different geographic regions in the abstract network.

It can be seen that the abstract representation in Figure 7 clusters the region into parts that have weak connections in between. This can be helpful for identifying vulnerable connections and meaningful clusters.

In Figure 8 connections between clusters are shown only as single edges. The number on the



Figure 6. Figure on the left shows geographic layout while the one on the right shows abstract layout.

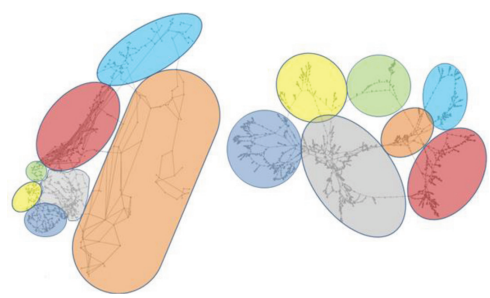


Figure 7. Figure on the left shows geographic layout while the one on the right shows abstract layout. Colors are added in order to easily identify the geograpic locations.

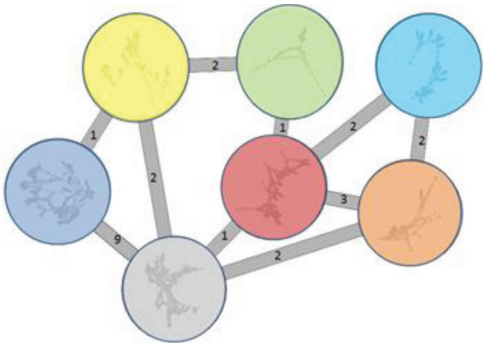


Figure 8. Regions shown as clusters, with single edges representing connections between clusters.



Figure 10. Splitting of clusters into subclusters.

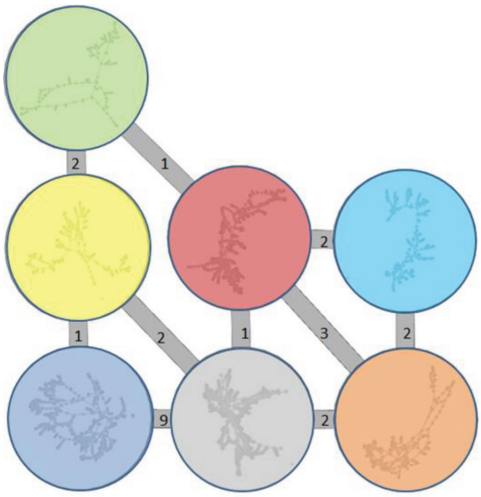


Figure 9. Regions shown as clusters, arranged in a regular grid.

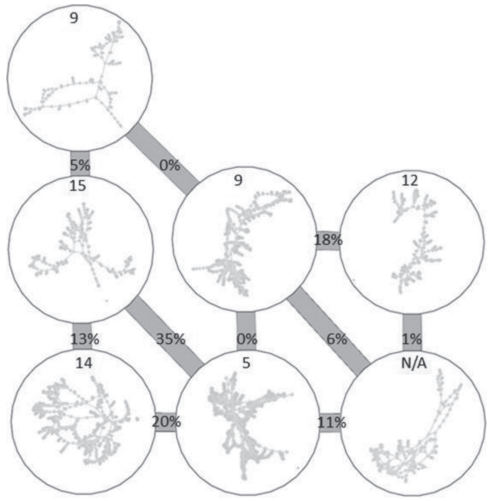


Figure 11. Values in supernodes represent SMS. Values on superedges represent percentage of maximum capacity.

edges tells how many actual branches there are between the clusters. As can be seen, few edges connect the clusters with each other. The color coding is identical to the image to the left in Figure 7.

Compared to Figure 7, the subgraphs in each cluster are represented in a more untangled way, as the connections are combined in superbranches instead of single edges. All clusters can easily be viewed in more detail by zooming in, with more information being included in the picture for each branch and node.

One of the main benefits of the clustering approach is that changes in network topology, as a result of outages or maintenance can easily be spotted, as the cuts are dynamic. If critical lines are out of operation, the entire representation will change, and new critical components will immediately be prominent.

Each of the clusters can be further split up into subclusters, that, when zoomed in on will show the most critical components within a given region, as shown in Figure 10.

Figure 11 shows how the system state can be shown in a very simple way using the clustering technique. The values in the supernodes show the SMS values, whereas the numbers on the superbranches represent the branch flows as a percentage of the maximum capacity.

Coloring of supernodes can be used to indicate information about energy surplus/deficiency in each area or the amount of spinning reserves in each area. These are important contributors to the overall risk calculation results.

5 "NON-ELECTRICAL" APPLICATIONS

Typical non-electrical applications are fluid flow systems including oil flow, and general material transport. Presumably also traffic and communication systems can be analyzed by this method. In these cases the power flow model is replaced by the actual system model. The principle based on unit models can also be used in general probability and reliability calculations to build extremely large models.

6 CONCLUSIONS

After installing the new simulation tool for reliability studies at Statnett SF, the need for a customized presentation method has become prominent.

Several approaches has been implemented and tested, some of which are included in this paper.

The most promising approach has been the graph layout with clustering. This approach gives the opportunity to, by a single look at the screen, identify the most critical cuts, and get an overview of the risk level in each area along with the state of the power system as a whole. By zooming in on a cluster, more information regarding the risk related to each individual branch and bus is shown.

The focus and context approach is particularly suitable if the operators want a complete overview of the power system, while still being able to identify individual critical components. It offers a great way of visualizing changes in a network over time, as different parts of the system will be prominent, depending on the current risk level in each area.

Edge bundling is suited to use in combination with the focus and context approach, as branches in areas of little interest can be bundled together, in order to simplify the presentation.

REFERENCES

Billinton, R. Allan, R.N. 1996. *Reliability Evaluation of Power Systems*. Plenum Press, New York.

Cui, W. Zhou, H. Qu, H. Wong, P. Li, X. 2008. Geometry-Based Edge Clustering for Graph Visualization. IEEE *Trans. on Vis. and Comp. Graphics (TVCG), Vol. 14 No. 6.*

Digernes, T. Svendsen, A.B. Aabø, Y. Hernandez, C. 2004. Analysis Including Reliability, Income and Cost for Power Systems. *PMAPS 2004.*

Endrenyi, J. 1978. Reliability modeling in Electric Power Systems. Wiley, New York.

Herman, I. Melancon, G. Marshall, M. 2000. Graph Visualization and Navigation in Information Visualization: A Survey. *IEEE Transactions on Visualization.*

Høyland, A. Rausand, M. 1994. *System Reliability Theory, Models and Statistical Methods*. John Wiley & Sons.

Landesberger, T. Kuijper, A. Schreck, T. Kohlhammer, J. van Wijk, J.J. Fekete, J.D. Fellner, D.W. 2011. Visual Analysis of Large Graphs: State-of-the-Art and Future Research Challenges. *Computer Graphics Forum, 2011.*

Rausand, M. Høyland A. 2004. *System Reliability Theory; Models, Statistical Methods, and Applications.* Jon Wiley & Sons.

Sasty, S. 1999. *Nonlinear Systems. Analysis, Stability, and Control. Springer.* New York.

Svendsen, A.B. 2002. *Pålitelighetsanalyse for vern- og kontrollutstyr i transformatorstasjoner.* Master thesis, NTNU, Norway.

Wang, X. McDonald, J.R. 1993. *Modern Power System Planning*. McGraw-Hill, London.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Drinking water quality aspect in ensuring the safety of water supply systems

I. Zimoch
Institute of Water and Sewage Engineering, Silesian University of Technology, Gliwice, Poland

E. Łobos
Institute of Mathematics, Silesian University of Technology, Gliwice, Poland

T. Żaba
Institute of Water Supply and Environmental Protection, Cracow University of Technology, Cracow, Poland

ABSTRACT: In the definition of safety states of water supply system the quality of drinking water plays an important role. Especially, trihalomethanes as disinfection by-products have to be taken into consideration, because they are dangerous for consumer's health and their concentration usually increase in water distribution subsystem. In this paper the method of determining the thresholds for water quality states (included in the comprehensive method of safety analysis) is presented. The states are based on chloroform because its share in total trihalomethanes is about 80%. Using the tools of mathematical statistics the relationships between chloroform and other quality and operational parameters of drinking water were analyzed and applied to an estimation of quality states. Additionally, the estimation of quality states was based on chloroform in drinking water flowing out from water treatment plant to water pipe network. The study was based on data obtained from the real water supply system.

1 THE PROBLEM OF TRIHALOMETHANES FORMATION IN WATER SUPPLY SYSTEMS

Decreasing water demand in water supply systems, that has been observed in last time, results in longer time of water delivery to consumers. This fact causes a health hazard because of water bacteriology contamination in pipe network. In order to maintain a high safety of exploitation of water supply system it is required to use monitoring system as a control process of water quality during its treatment and distribution. Testing for quality is crucial because the water's contents change constantly during its transport to the consumers. Many factors affect these changes, most importantly: chemical and biological stability of drinking water delivered into water pipe network, its temperature, water pipe's hydraulic exploitation conditions, its technical and sanitary condition, material from which the pipes are made, chemical and biological deposits and disinfectant presence.

Low concentration of disinfectant in the transported water is the cause of secondary growth of microorganisms, which leads to creation of a biofilm. Intensity of biofilm creation determines the lack of water's biological stability. Secondary growth of microorganisms is favored by high water temperature (above 15°C) and low water flow in the pipes (less then 0.1 m/s), which is the reason why water stays in the pipes even for several days (Gatel et al. 2000). The result of biofilm creation is the increase in water's color intensity, turbidity and the level of contamination with organic substances, ammonium nitrate, and corrosion products as well as bad smell and taste. Another consequence of the above phenomenon is the increase of the risk of creation in the water of heterotrophic organisms and bacteria (Okabe et al. 2002).

In order to avoid this threat the water chlorination is commonly applied in water treatment processes. This technology of water disinfection is popular in the whole world because of high efficiency and low price of chlorine. On the other hand, high chlorine concentration in water determines the formation of significant level of disinfection by-products mainly containing trihalomethanes. Trihalomethanes have toxic, carcinogenic and mutagenic character and they are dangerous for human health (WHO 2000, Krasner et al. 2006, Richardson et al. 2007, Goslan et al. 2009, Bull et al. 2009). During the water transport the chlorine react with humic substances, which are trihalomethanes precursors, and with

other organic substances of low compound mass (Rodriguez & Serodes 2001, Serodes et al. 2003, Golfinopoulos & Nokolaou 2005, Toroz & Uyak 2005, Wei et al. 2010). Also changing hydraulic conditions, caused by low demand, low flows and changing transport directions increase the trihalomethanes concentration (Francis et al. 2009, Tchórzewska-Cieślak & Rak 2010). The crucial problem is to study the kinetics of the trihalomethanes formation process. The literature review has shown many methods in which different factors are considered, however the problem has no unique solution (Baribeau et al. 2001, Lee et al. 2001, Gallard & Gunten 2002, Abdullah et al. 2003, Sadiq & Rodriguez 2004, Chowdhury et al. 2009, Shan et al. 2012, Villanueva et al. 2012).

The formation of trihalomethanes during the water transport in water pipe network is obvious considering present exploitation conditions. Disinfection by-products cause the decrease of water system safety so its monitoring is indispensable. The quality of drinking water is an important element of the comprehensive safety model (Zimoch 2011, Zimoch & Łobos 2012). They should be applicable in safety assessment which is the main matter of this paper.

2 CHARACTERISTIC OF CRACOW WATER SUPPLY SYSTEM

The current water supply system of Cracow city arise as a result of constructing the water treatment plants for over 100 years, their modernization and as well as the water-pipe network development resulting from building new housing at outskirts of the city. The system consists of two complex subsystems: water production subsystem and water distribution subsystem. The water production subsystem is built of water supply arrangements which create separated treatments lines feeding on surface water sources from Rudawa, Dłubnia, Sanka River, Dobczyce reservoir and underground water from intake in Mistrzejowice. Actual capacities of all water treatment plants cause that the Cracow water supply system is the system with excess, i.e. maximal system's reserve is about 74% of average twenty-four hours water demand.

The Raba Water Treatment Plant plays the most significant role in delivering water to the city; its average daily production is 80,760 m^3, which is approximately 48% of daily water demand. During emergency periods this water treatment production covers the full demand of citizens.

The Raba Water Treatment plant takes the raw water by tower-type water intake from reservoir Dobczyce, which has possibility of water intake from a level of the best quality parameters. The reservoir in Dobczyce is an unstable and non-homogeneous water resource. Its waters undergo typical qualitative and quantitative changes. The parameters that the most often reduce the season class of water quality are: total phosphorus, chlorophyll and oxygen sag. The eutrophication process results in domination of green algae and diatom phytoplankton that intensively develops from the spring to the late autumn. Late summer in the water depth there blue-green algae appears. These processes cause that the content of organic matter is high and its major part is precursors of trihalomethanes.

Raw water in Raba Water Treatment Plant is oxidized in the process of preliminary ozonization in contact tank with two chambers. Usually the dose of ozone is less than 4 g/m^3. Ozone is produced on the spot by system of PCI Ozone of capacity 30 kgO_3/h. Then water flows to the separation chamber where the coagulant (PAX or aluminum sulfate in dose 0–40 g/m^3), Magnaflok (in dose 0–0.5 g/m^3) and sometimes the active carbon (in dose 0–10 g/m^3) are added. In the next chamber the water jet is separated into two technological treatment lines: Raba I and Raba II.

Raba I contains a system of classic coagulation which consists of: three chambers of fast mixers, twelve flocculation chambers, and two coagulation horizontal settling tanks of capacity 8000 m^3. Then water is steered to 12 sand rapid filters of area 44 m^2 each and total capacity 1200–1300 m^3/h. The last step of technological process is disinfection using gas chlorine. Treated water is pressed by pumping station to water tanks in Gorzków, and then to water distribution subsystem.

The coagulation process in Raba II is realized in 4 accelerators of nominal capacity 2160 m^3/h. Next, water is steered to 16 fast sand filters of area 85 m^2 each and capacity 3800–4000 m^3/h. The final water treatment process is disinfection using chlorine dose 0.5–2 g/m^3. Drinking water, after disinfection, is also pressed to tanks in Gorzków.

Drinking water is transported from Raba Water Treatment Plant to the control station Piaski Wielkie (Cracow suburb) by system of transit waterpipes of diameters ∅1000 and ∅1400 and length about 17 km where water tanks in Gorzków (of capacity 22,500 m^3) and tanks complex in Siercza (4×34.000 m^3 and 3×7.500 m^3) are localized.

Drinking water in Cracow is delivered to consumers by main water-pipes (∅1200–∅350, length 282.72 km), distributing water-pipes (∅325–∅80, length 1100.21 km) and household terminals (∅100–∅25, length 466.27 km). Total length of the distribution subsystem on the city area serviced by City of Cracow Water and Sewage Utility Company is 1849.26 km. Over 100 years of functioning and continuous development of the water supply

system have resulted in great diversity of age and materials of various water-pipes. The main part of age structure is water-pipes made after 1975 (56% of total length). Majority of such water-pipes are made in 90's (26%), with application of new technologies and materials. The most significant part of water-pipes of water distribution subsystem is made of steel (32%), cast iron (26%), and PCV (23%). Inseparable elements of distribution subsystem are equalizing-reserve tanks. The Cracow water supply systems uses 11 water tanks of total capacity of over 276,200 m^3. These tanks capacities back up the level of 165% actual average twenty-four hour water demand in the city.

The complex structure of water supply system in Cracow, long distance from the main water treatment plant (Raba) and less water demand in the city result in increasing time of delivering drinking water to consumers. Additionally, the usage of chlorine in the disinfection process as well the presence of organic matter including significant part of trihalomethanes precursors in treated water cause the danger of harmful and carcinogenic disinfection by-products formation. Thus the higher concentrations of chloroform in drinking water are periodically observed.

3 RESEARCH DATA DESCRIPTION

Presented study is based on laboratory analyzes of various water quality parameters obtained by Central Water Quality Laboratory in Cracow Water Company. The analyzes were results of regular control monitoring procedures made by the company as well as additional study carried out within the framework of the project supported by Polish State Committee for Scientific Research under the contract No. 5T07E 044 25.

Data were collected from January 2007 to December 2013. Water samples were taken at Water Treatment Plant Raba and at selected 23 sampling points on water distribution network. Basic quality and operation parameters such as pH, residual chlorine, chlorine dose, chemical oxygen demand, UV absorbance in 272 nm, temperature were tested everyday at water treatment plant, but disinfection by-products parameters are analyzed once a month. Water quality parameters that characterize the process of disinfection by-products formation (such as pH, temperature, UV absorbance in 272 nm, total organic carbon, residual chlorine, chloroform, sum of trihalomethanes) in water pipes were analyzed on average once a month.

Additionally, in our research some important parameters were determined. They are: the distance from water treatment plant to sampling point, supply zone, efficiency parameter, and chlorine consumption. Each sampling point on the network was allocated to one of five supply zones dependently of its distance from water treatment plant (zones were designated every 5 km, i.e. the first zone was from 0 to 5 km, and the last zone—greater than 20 km). Efficiency parameter was defined as the ratio of zone and total production capacity. This parameter is a measure of contact time of drinking water in distribution subsystem with chlorine; it is also connected with daily water demand by consumers (the greater demand the greater production). Chlorine consumption is calculated as the difference between the total chlorine dose (the sum of chlorine doses in water treatment plant and water tank in Siercza) and the residual chlorine at sampling point.

Water samples were collected according to the Polish Standard PN-87/C-04632/01-04. The quality of water samples was specified according to the following procedures:

- pH [dimensionless]—PN-90/C-04540.01 (multifunction apparatus inoLab MultiLevel1),
- temperature [°C]—PN-77/C-04584 (mercury thermometer),
- chlorine [mg/dm^3]—PN-ISO 7393-2:1997 (photometer PC Compact Chlor),
- absorbance UV_{272} [cm^{-1}]—PN-84/C-05472 (spectrophotometer HACH DR 4000U),
- chemical oxygen demand [mgO_2/dm^3],—PB-NJL-W-15 (spectrofotometer HACH DR 4000U),
- total organic carbon [mgC/dm^3]—PN-EN-1484-1999 (analyzer TOC 5050 Shimadzu),
- chloroform and trihalomethanes [$\mu g/dm^3$]—75-PB-NJL-W-06 (gas chromatograph HP-5890GC/5970MSD).

Table 1 presents basic descriptive statistics of obtained data. Finally, the stochastic sample was consisting of 2838 cases and the total number of obtained cases of all considered variables was equal to 23,967. However, there are many missing data, so in further study the set of 333 cases was considered. This set consists of these sample points for which the chloroform concentration at network point and at water treatment plant were given (laboratory analyzes are made according to the monitoring plan which takes into account high costs of gas chromatography).

Although there was a large number of data (missing data were pairwise deleted) not all correlation coefficients between considered variables were found to be statistically significant. Statistically significant are coefficients of correlation between chloroform at network point and some variables measured at water distribution subsystem (residual chlorine, chlorine consumption) and measured at water treatment plant (total chlorine dose, chemi-

Table 1. Basic descriptive statistics of obtained data.

Variable	N	Mean	Min.	Max.	Standard deviation
Variables measured at water treatment plant					
Residual chlorine	2555	0.276	0.000	0.630	0.114
Total chlorine dose	2555	1.041	0.495	2.390	0.519
Chemical oxygen demand	2555	0.959	0.420	2.100	0.244
pH	2555	7.826	7.300	8.700	0.126
Total organic carbon	50	1.827	1.090	3.250	0.386
UV_{272}	2555	0.016	0.008	0.037	0.006
Temperature	2555	11.656	1.700	23.600	6.957
Chloroform	50	6.128	0.000	28.600	6.854
Trihalomethanes	50	7.468	0.000	31.500	7.998
Variables measured at network points					
Residual chlorine	333	0.109	0.000	0.500	0.064
Chlorine consumption	333	1.108	0.533	2.234	0.293
pH	333	7.773	7.200	8.400	0.144
Total organic carbon	314	1.671	0.640	4.680	0.478
UV_{272}	325	0.025	0.012	0.055	0.007
Distance	333	12.194	2.296	20.045	4.399
Zone*	333	3.021	1.000	5.000	0.949
Efficiency parameter**	333	3.527	1.003	6.983	1.147
Chloroform	333	14.927	0.000	41.900	8.536
Trihalomethanes	333	18.520	0.000	48.600	9.746

*zone [dimensionless], **efficiency parameter [$10^5 \cdot 24$ h/m^3].

Table 2. Statistically significant coefficients of correlation between chloroform at network point and listed variables.

Variable	Correlation coefficient
Residual chlorine*	–0.239
Total chlorine dose**	0.481
Chlorine consumption*	0.507
Chemical oxygen demand**	0.207
Total organic carbon**	0.258
Temperature**	0.702
Chloroform**	0.673

*at distribution subsystem, **at water treatment plant.

cal oxygen demand, total organic carbon, temperature, chloroform); their values are given in Table 2 and confirm known facts of disinfection by-products generation (Baribeau et al. 2001, Chowdhury et al. 2009, Villanueva et al. 2012).

One of important stage in our research on models of system safety is the selection of a valid parameter from the set of disinfection by-products. There are many papers (Lee 2001, Sadiq & Rodriguez 2004, Zimoch & Łobos 2008, Chowdhury et al. 2009) devoted to the problem of formation of trihalomethanes (THM) which are the sum of four

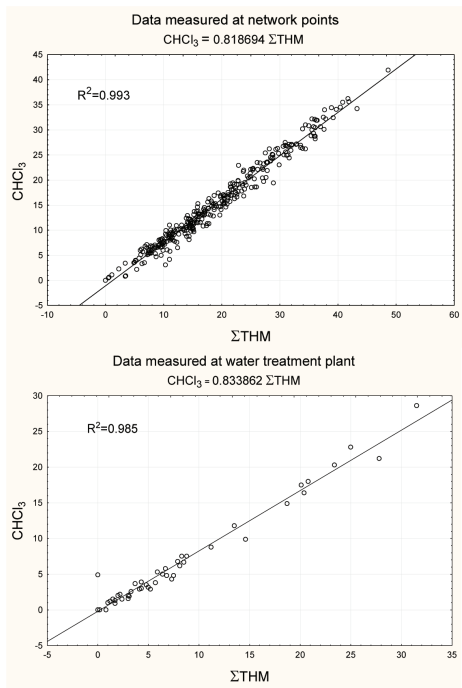


Figure 1. Relation between concentrations of total trihalomethanes and chloroform at network points (upper graph) and at water treatment plant (lower graph).

chemical compounds: chloroform ($CHCl_3$), bromodichloromethane ($CHCl_2Br$), dibromochloromethane ($CHClBr_2$), tribromomethane ($CHBr_3$). It is shown in some papers (Urbansky & Magnuson 2002, Richardson 2003) that chloroform has the largest share in total trihalomethanes. This fact was also observed in presented research in drinking water, both in water treatment plant and distribution subsystem (Fig. 1, it is worth to stress that for both obtained equations the determination coefficients are very close to 1).

Maximal allowable concentration of total trihalomethanes, established in Drinking Water Directive, is 100 μg/dm^3. The directive does not include allowable concentrations of specified compounds. Polish law imposes additionally the maximal allowable concentration of chloroform (30 μg/dm^3). Since the chloroform is about 80% of total trihalomethanes, it is possible that the total trihalomethanes satisfy the norm whereas the maximal allowable concentration of chloroform is exceeded. Therefore the concentration of chloroform is the better quality parameter to be considered in safety models of water supply systems and it is taken as the basic parameter in definitions of quality states in further study.

4 WATER QUALITY IN SAFETY STATES

4.1 *Safety states of water supply systems*

The comprehensive method of safety analysis of water supply systems described by Zimoch & Łobos (2012) takes into account drinking water quality, water production subsystem capacity and failures on water pipe network, which characterizes the operation conditions of water distribution subsystem. Depending on conditions listed above the four safety states were defined: full safety, acceptable safety menace, controlled safety menace, and safety loss.

The first of safety states is defined if delivered water is of good quality, in required quantity, under needed pressure. The second safety state includes exploitation events such that the system manager has to interfere only in one operation parameter in order to return to the full safety state. The acceptable safety menace state accepts the reduction of production capacity to 70% of full daily water demand. The third state is the consequence of essential decrement of all three parameters such that their co-occurrence influences on the secondary drinking water contamination. Thus this state forces an operator to undertake repair actions and increase the monitoring intensity of delivered water quality.

If the chloroform concentration in transported water is greater than or equal to triple maximal acceptable concentration, then the health risk is so large that the system is classified to be in the safety loss state. The complete safety loss occurs also in the situation of wrong hydraulic work of water distribution subsystem (for example if water main failure appears and water production subsystem capacity is less than 30% of water demand, the probability of water quality deterioration significantly increases and it is not acceptable by producer and consumer).

4.2 *Water quality criteria in safety model*

In the comprehensive method of safety analysis the concentration of disinfection by-products plays an important role. Therefore definitions of concrete safety states have to be strictly related to observed changes of water quality during its transport to consumers. Classes of water quality, based on chloroform concentration, were defined using its maximal allowable concentration given by Drinking Water Directive (1998) and Polish legal acts. Namely, the following three classes were presupposed:

- first quality state in which the concentration of chloroform belongs to the interval [0 μg/dm^3, 30 μg/dm^3]; such concentrations appear in the full safety and acceptable safety menace states, provided that the capacity of water production subsystem is equal to the daily water demand;
- second quality state which corresponds to water quality with chloroform concentration from interval (30 μg/dm^3, 90 μg/dm^3]; the class is mainly assigned to controlled safety menace state;
- third quality state where chloroform concentration exceeds 90 μg/dm^3, which always classifies the water supply system to be in the safety loss state.

In real water supply systems (Zimoch & Łobos 2008, Zimoch & Łobos 2011) the operation conditions usually cause the changes of water quality in the range of chloroform concentration from 0 to 60 μg/dm^3 whereas concentration greater than 90 μg/dm^3 are very rare and rather incidental random events. Mentioned facts indicate that searching more precise quality states (that characterize safety states of exploitation) are necessary.

It follows from detailed analysis of obtained data that almost all (precisely, more than 90%) items in the sample the chloroform concentration not exceeds the maximal allowable concentration, i.e. 30 μg/dm^3 (Fig. 2). From this reason the previous first quality state was divided into two new quality states, in which the concentration of chloroform belongs to the interval [0 μg/dm^3, 15 μg/dm^3] for the first quality state and to (15 μg/dm^3, 30 μg/dm^3]

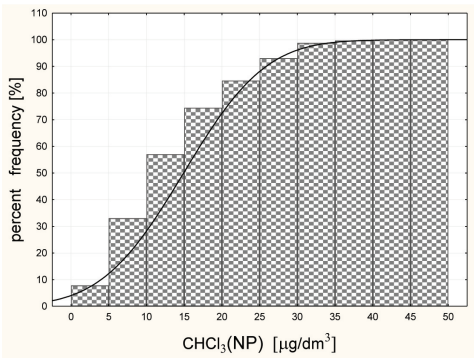


Figure 2. Empirical distribution function of chloroform concentration in drinking water at network points.

for the second quality state. Subsequently, the third quality state is determined by the interval (30 µg/dm^3, 60 µg/dm^3] and the forth one by chloroform concentrations greater than 60 µg/dm^3 which corresponds to the double maximal allowable concentration.

These newly specified thresholds for water quality states have been successfully proven in other research areas of water supply systems (in Wrocław city and several agglomerations in Silesia).

5 THE APPLICATION OF CHLOROFORM PREDICTION FUNCTIONS IN SAFETY MODELS

In these section we use the following notation for considered variables:

- $CHCl_3(NP)$ chloroform concentration at network point on the distribution subsystem,
- $CHCl_3(WTP)$ chloroform concentration at water treatment plant (in treated water),
- T temperature at water treatment plant,
- $D(Cl_2)$ total chlorine dose,
- $C(Cl_2)$ chlorine consumption,
- Z zone,
- $P(Q,Z) = 10^5 Z/Q$ efficiency parameter where Q denoted the production capacity.

Numerous predictive models obtained by multiple regression with various sets of independent variables, listed in Table 1, were tested. The dependent variable was always $CHCl_3(NP)$. The best models are following:

– model A

$$\ln\left[1+CHCl_3(NP)\right] = 1.411881 + 0.489433\ln\left[1+CHCl_3(WTP)\right] + 0.252920\ln T \quad (1)$$

– model B

$$\ln\left[1+CHCl_3(NP)\right] = 1.600953 + 0.458861\ln\left[1+CHCl_3(WTP)\right] + 0.180062\ln T + 0.314256\ln C(Cl_2) \quad (2)$$

– model C

$$\ln\left[1+CHCl_3(NP)\right] = 1.470181 + 0.459582\ln\left[1+CHCl_3(WTP)\right] + 0.170939\ln T + 0.350736\ln C(Cl_2) + 0.051175 Z \quad (3)$$

– model D

$$\ln\left[1+CHCl_3(NP)\right] = 1.451888 + 0.467855\ln\left[1+CHCl_3(WTP)\right] + 0.160356\ln T + 0.372107\ln C(Cl_2) + 0.053069\ P(Q,Z) \quad (4)$$

– model E

$$\ln\left[1+CHCl_3(NP)\right] = 1.374331 + 0.479503\ln\left[1+CHCl_3(WTP)\right] + 0.168612\ln T + 0.376004\ln D(Cl_2) + 0.053084\ P(Q,Z). \quad (5)$$

Model A is the best from the mathematical point of view. It is the result of both forward selection and backward elimination with $F_{enter} = 4$, $F_{delete} = 3$. All coefficients in this model are statistically significant. Other models have some coefficient which are not statistically significant but these models have better (i.e. greater) adjusted multiple coefficients of determination and better (i.e. less) standard estimation errors (Table 3). Basic statistical properties of discussed models are similar. The most important fact

Table 3. Comparison of statistical properties of discussed prediction models.

Model	Multiple coefficient of correlation	Adjusted multiple coefficient of determination	Standard estimation error
A	0.727	0.521	0.4284
B	0.733	0.526	0.4199
C	0.737	0.527	0.4193
D	0.738	0.529	0.4184
E	0.735	0.524	0.4208

is that all these models explain more than 52% of variability of dependent variable. One may notice that coefficients in the same variables are similar in all models. Moreover, the role of chlorine consumption (models B, C, and D) and total chlorine dose (model E) is comparable.

Prediction functions obtained by multiple regression have the following explicit forms:

– in model A

$$CHCl_3(NP) = 4.103696 \cdot \left[1 + CHCl_3(WTP)\right]^{0.489433} \cdot T^{0.252920} - 1 \quad (6)$$

– in model B

$$CHCl_3(NP) = 4.957755 \cdot \left[1 + CHCl_3(WTP)\right]^{0.458861} \cdot T^{0.180062} \cdot \left[C(Cl_2)\right]^{0.314256} - 1 \quad (7)$$

– in model C

$$CHCl_3(NP) = 4.350022 \cdot \left[1 + CHCl_3(WTP)\right]^{0.459582} \cdot T^{0.170939} \cdot \left[C(Cl_2)\right]^{0.350736} \cdot e^{0.051175\,Z} - 1 \quad (8)$$

– in model D

$$CHCl_3(NP) = 4.271171 \cdot \left[1 + CHCl_3(WTP)\right]^{0.467855} \cdot T^{0.160356} \cdot \left[C(Cl_2)\right]^{0.372107} \cdot e^{0.053069\,P(Q,Z)} - 1 \quad (9)$$

– in model E

$$CHCl_3(NP) = 3.952432 \cdot \left[1 + CHCl_3(WTP)\right]^{0.479503} \cdot T^{0.168612} \cdot \left[D(Cl_2)\right]^{0.376004} \cdot e^{0.053084\,P(Q,Z)} - 1. \quad (10)$$

For each of 333 sampling points the predicted value of variable $CHCl_3(NP)$ was calculated. Basing on this value, each point was classified to one of quality states and then the estimated quality state was compared with observed quality state.

Table 4 presents estimations of probabilities of proper and improper classifications. The use of prediction models forces an operator to make unnecessary laboratory analyzes if the estimated state is greater than the real one, which generate additional costs. The most undesirable situation is one where the estimation indicates the first or second quality state while the real chloroform concentration exceeds the maximal allowable concentration. For all models the probability of such improper classification is 0.069. Thus the best model is model B (it has the least probability of overestimation) and the worst is model E.

Table 4. Probabilities of proper and improper classifications to quality states (estimations are based on prediction functions of chloroform concentration at network points).

Model	Estimated state is equal to the real state	Estimated state is greater than the real state	Estimated state is less than the real state
A	0.679	0.171	0.150
B	0.682	0.162	0.156
C	0.676	0.165	0.159
D	0.673	0.168	0.159
E	0.661	0.174	0.165

6 RELATIONSHIP BETWEEN SAFETY STATES AND QUALITY OF TREATED WATER AT WATER TREATMENT PLANT

Since coefficients in variable $\ln[1 + CHCl_3(WTP)]$ in prediction model A-E (described in the previous section) are similar, a new question arises: is it possible to estimate quality safety states of network points using only the chloroform concentrations in treated water at water treatment plant?

In Figure 3 distributions of chloroform concentration at water treatment plant depending on quality states (defined by concentration of chloroform at network point) are shown. The analysis of data leads to the following definitions of quality safety states. In the first quality safety state the concentration of chloroform at water treatment plant belongs to interval [0 μg/dm^3, 3 μg/dm^3], in the second—to (3 μg/dm^3, 6 μg/dm^3], in the third—to (6 μg/dm^3, 12 μg/dm^3], and in the fourth—it is greater than 12 μg/dm^3.

Quality states determined at water treatment plant should correspond to appropriate quality states determined at network points. In Table 5 estimations of probabilities of proper and improper classifications (if quality states at water treatment plant are applied) are collected. On the one hand, this approach in comparison with method described in previous section is worse because it gives too much overestimations. On the over hand, there is less probability that estimated state is less

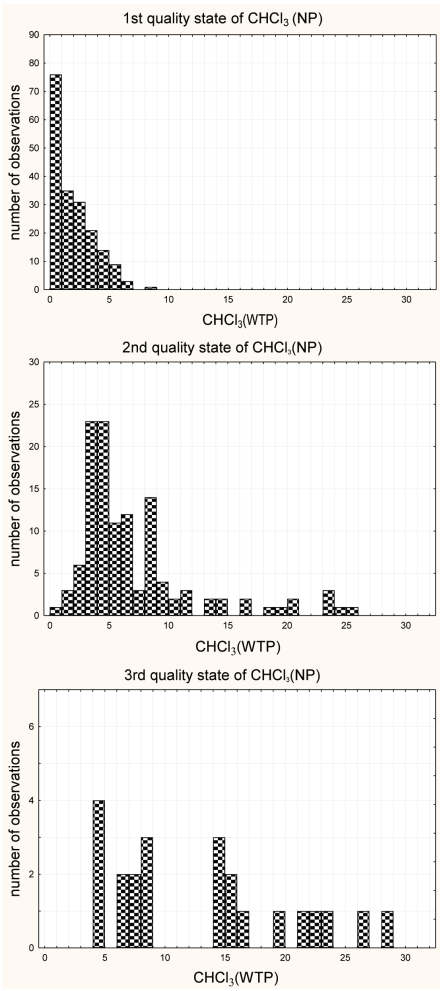


Figure 3. Distributions of chloroform concentration at water treatment plant depending on the quality states of chloroform at network points.

Table 5. Probabilities of proper and improper classifications to quality states in whole water pipe network assigned to particular zones (estimations are based on chloroform concentration at water treatment plant).

Zone	Estimated state is equal to the real state	Estimated state is greater than the real state	Estimated state is less than the real state
1	0.042	0.018	0.003
2	0.111	0.072	0.006
3	0.284	0.162	0.024
4	0.147	0.051	0.018
5	0.042	0.012	0.006
Sum	0.628	0.315	0.057

Table 6. Probabilities of proper and improper classifications to quality states in each zone (estimations are based on chloroform concentration at water treatment plant).

Zone	Estimated state is equal to the real state	Estimated state is greater than the real state	Estimated state is less than the real state
1	0.667	0.286	0.048
2	0.587	0.381	0.032
3	0.605	0.343	0.051
4	0.681	0.236	0.083
5	0.700	0.200	0.100

than the real one. Moreover, the probability that the estimation indicates the first or second quality state while the real chloroform concentration exceeds the maximal allowable concentration is very small (it is equal to 0.012 while for estimations with prediction models it is 0.069).

The level of concentration of newly formed chloroform is strictly connected with reaction time between chlorine and organic matter containing trihalomethanes precursors. The reaction time in presented models is represented by the zone. Since there are different numbers of water samples in defined five zones in water distribution subsystem, the probabilities of proper and improper classification were calculated for each separately. These probabilities are similar in all zones (Table 6) which confirms the correctness of the method.

7 CONCLUSION

Assumed in this paper new thresholds for quality safety states fit better to the range of variability of chloroform in real water supply system so they are more appropriate for consideration related to the comprehensive method of safety analysis.

Presented predictive models of chloroform concentration in drinking water delivered to consumer have not only scientific but also practical meaning. The use of them in monitoring process allows to decrease costs of laboratory analyzes. Considered models have acceptable determination coefficient about 52% because they are based on data collected in normal exploitation conditions of water supply system, during obligatory monitoring of treated and drinking water quality.

It was also shown that easier method of estimation of safety states works correctly. Namely, the quality safety state of network point may be estimated by the chloroform concentration in chlorinated water at water treatment plant. Such approach allows to optimize costs of monitoring and precisely analyze safety states of water qual-

ity in distribution subsystem. In 63% of analyzed network points (Table 5) the classification to particular safety state based on drinking water quality was the same as safety state determined by the chloroform concentration in chlorinated water in water treatment plant.

The application of described methods to the comprehensive method of safety analysis in order to develop Water Safety Plans is justified now, but study should be continued to obtain greater compatibility of quality safety states.

ACKNOWLEDGEMENT

The paper presented has been realized in frame of the research project co-financed by the European Union from the European Regional Development Fund, Sub-measure 1.3.1. "Development Projects"; project title: "IT system supporting the optimization and planning of production and distribution of water intended for human consumption in the sub-region of the central and western province of Silesia"; project ref. no. POIG.01.03.01-14-034/12.

REFERENCES

Abdullah, M., Yew, C., Ramli, M. 2003. Formation, modeling and validation of trihalomethanes (THM) in Malaysian drinking water: a case study in the districts of Tampin, Negeri Sembilan and Sabak Bernam, Selangor, Malaysia. *Water Research* 37: 4637–4644.

Baribeau, H., Prevost, M., Desjardins, R., Lafrance, P., 2001. Changes in chlorine and DOX concentration in distribution system. *Journal AWWA* 93: 102–114.

Bull, R., Rice, G., Teuschler, L., Feder, P. 2009. Chemical measures of similarity among disinfection by-product mixtures. *Journal of Toxicology and Environmental Health, Part A*. 72: 482–493.

Chowdhury, S., Champagne, P., McLellan, P. 2009. Models for predicting disinfection byproducts (DBP) formation in drinking waters: A chronological review. *Science of Total Environment* 407(14): 4189–4206.

Drinking Water Directive 98/83/EC, 1998. Council Directive of November 1998 on the quality of water intended for human consumption. *Official Journal of EC* (L 330.5.12.98): 32–54.

Francis, R., Small, M., VanBriesen, J. 2009. Multivariate distributions of disinfection by-products in chlorinated drinking water. *Water Research* 43: 3453–3468.

Gallard, H. & von-Gunten, U. 2002. Chlorination of natural organic matter: kinetics of chlorination and of THM formation. *Water Research* 36: 65–74.

Gatel, D., Sevais, P., Blocl, J., Bonne, P., Cavard, J. 2000. Microbial water quality management in the Paris suburbs distribution system. *Aqua* 49(5): 231–241.

Golfinopoulos, S. & Nikolaou, A. 2005. Survey of disinfection by-products in drinking water in Athens, Greece. *Desalination* 176: 13–24.

Goslan, E., Krasner, S., Bower, M., Rocks, S., Holmes, P., Levy, L., Parsons, S. 2009. A comparison of disinfection by-products found in chlorinated and chloraminated drinking waters in Scotland. *Water Research* 43: 4698–4706.

Krasner, S., Weinberg, H., Richardson, S., Pastor, S., Chinn, R., Sclimenti, M., Onstad, G., Thruston A. 2006. Occurrence of a new generation of disinfection byproducts. *Environmental Science & Technology* 40(23): 7175–7185.

Lee, K., Kim, B., Hong, J., Pyo, H., Park, S., Lee, D. 2001. A study on the distribution of chlorination by-products (CBPs) in treated water in Korea. *Water Research* 35: 2861–2872.

Okabe, S., Kokazi, T., Watanabe Y. 2002. Biofilm formation potential in drinking waters treated by different advanced treatment process. *Water Science and Technology: Water Supply* 2(4): 97–104.

Richardson, S. 2003. Disinfection by-products and other emerging contaminants in drinking water. *Trends in Analytical Chemistry* 22(10): 666–684.

Richardson, S., Plewa, M., Wagner, E., Schoeny, R., DeMarini, D. 2007. Occurrence, genotoxicity, and carcinogenicity of regulated and emerging disinfection by-products in drinking water: A review and roadmap for research. *Mutation Research* 636: 178–242.

Rodriguez, M.J. & Serodes, J.B. 2001. Spatial and temporal evolution of trihalomethanes in three water distribution systems. *Water Research* 35: 1572–1586.

Sadiq, R. & Rodriguez, M. 2004. Disinfection by-products (DBPs) in drinking water and predictive models for their occurrence: a review. *Science of the Total Environment* 321: 21–46.

Serodes, J.B. et al. 2003. Occurrence of THMs and HAAs in experimental chlorinated waters of the Quebec City area (Canada). *Chemosphere* 51: 253–263.

Shan, J., Hu, J., Kaplan-Bekaroglu, S., Song, H., Karanfil, T. 2012. The effects of pH, bromide and nitrite on halonitromethane and trihalonitromethane formation from amino acids and amino sugars. *Chemosphere* 86: 323–328.

Tchórzewska-Cieślak, B. & Rak, J. 2010. Method of identification of operational states of water supply system. In L.Pawłowski et al. (eds), *Environmental engineering III*: 521–526. London: CRC Press.

Toroz, I. & Uyak, V. 2005. Seasonal variations of trihalomethanes (THMs) in water distribution networks of Istanbul City. *Desalination* 176: 127–141.

Urbansky, E., Magnuson, M. 2002. Analyzing drinking water for disinfection byproducts. *Analytical Chemistry* 74(9): 260A–267A.

Villanueva, C., Castaño-Vinyals, G., Moreno, V., Carrasco-Turigas, G., Aragonés, N., Boldo, E., Ardanaz, E., Toledo, E., Altzibar, J., Zaldua, I., Azpiroz, L., Goñi, F., Tardón, A., Molina, A., Martín, V., López-Rojo, C., Jiménez-Moleón, J., Capelo, R., Gómez-Acebo, I., Peiró, R. 2012. Concentrations and correlations of disinfection by-products in municipal drinking water from an exposure assessment perspective. *Environmental Research* 114: 1–11.

Wei, J., Ye, B., Wang, W., Yang, L., Tao, J., Hang, Z. 2010. Spatial and temporal evaluations of disinfection by-products in drinking water distribution systems in Beijing, China. *Science of the Total Environment* 408: 4600–4606.

WHO, Disinfectants and disinfectant by-products. (2000). Environmental Health Criteria 216. Geneva: World Health Organization.

Zimoch, I. & Łobos, E. 2008. Analysis of spatial quality changes in water pipe network as a function that describes THM formation. *Polish Journal of Environmental Studies* 17(3A): 627–631.

Zimoch, I. & Łobos, E. 2011. Statistical approach to the THMs formation process in water treatment arrangements. *Inżynieria Ekologiczna* 26: 269–280.

Zimoch, I. 2011. Comprehensive method of reliability and safety analysis of water supply systems. Gliwice: Silesian University of Technology Press.

Zimoch, I. & Łobos, E. 2012. Method of safety analysis of water supply system. Proc. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, Helsinki 25–29 June (2012), vol. 7: 5816–5823. Helsinki: IAPSAM&ESRA.

Dynamic reliability

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Using dynamic risk modelling in Single European Sky Air Traffic Management Research (SESAR)

N. Fota
SESAR and Research—Performance and Method Unit, EUROCONTROL, France

M.H.C. Everdij & S.H. Stroeve
*National Aerospace Laboratory (NLR), The Netherlands**

T. Kråkenes & I. Herrera
SINTEF, Norway

J. Quiñones
Safety Directorate, AENA, Spain

T. Contarino & A. Manzo
SELEX and SICTA†, Italy

ABSTRACT: The SESAR research & development programme aims to drastically change Air Traffic Management (ATM) in the European airspace. The SESAR project "Develop techniques for Dynamic Risk Modelling (DRM)" aims at demonstrating the need for and potential added value of DRM in the safety assessment of new developments. The main deliverable is a DRM guideline that will help safety practitioners to decide whether DRM modelling is expected to provide added value, and how to conduct the assessment. The added value of DRM is being demonstrated by its application to a SESAR test case.

1 INTRODUCTION

1.1 *The need for dynamic risk modelling*

Today's challenge is that aviation systems are large-scale, complex and dynamic. New automated tools are developed to assist air traffic controllers and pilots to reduce separation. These technologies introduce a change in the human-machine interface and increase the complexity of Air Traffic Management (ATM) (Averty et al. 2009). New technology and new ways of interacting may have significant safety effects, which must be assessed by means of suitable methods.

Traditional methods such as fault trees and event trees have important limitations when it comes to capturing the dynamics and complexity of many sociotechnical systems and operations. Such "static" methods are often still adequate for some applications, but may be insufficient when faced with applications in which (Eurocontrol 2009):

a. There are multiple conditions affecting system response and operator behaviour.
b. There are different ways in which human operators may perform a task incorrectly, and there are multiple dynamic responses of the system and human operators to these different errors.
c. The physical status evolution has an influence on the stochastic discrete events related to failure and recovery.
d. There are multiple time-dependent interactions between the system and its environment, and between the system elements themselves.
e. There are uncertainties due to inherent randomness or unpredictable variability or due to the imperfect knowledge or incomplete information.

In the last decade, theories and methods have started to explicitly acknowledge dynamic sequencing and the need to address time-dependent interactions. In this paper, these methods are referred to as *Dynamic Risk Modelling (DRM)*. DRM is defined as the class of risk modelling techniques that explicitly represent the dynamic performance of the elements in the operation (people, equipment, procedures, environment) and their time-dependent interactions.

*On behalf of DFS Deutsche Flugsicherung, Germany.
†On behalf of ENAV.

1.2 *SESAR and the DRM project*

SESAR (Single European Sky ATM Research) aims to eliminate the fragmented approach to European ATM, transform the ATM system and synchronize all stakeholders. ATM systems delivered in the scope of SESAR are increasingly complex and integrated. There is a need for more advanced safety assessment approaches, taking into account the dynamic nature of events preceding an incident/accident within a SESAR Safety Assessment, and for complementary models that account for technical and human, context, interactions and dynamics. This is the focus of SESAR DRM project (DRM project, Herrera et al.), which considers existing and emerging developments in the area of dynamic risk modelling. The main objective of the DRM project is to provide guidelines for ***when*** and ***how*** to apply DRM techniques in real world analysis situations. These guidelines are aimed to be included in a future edition of the SESAR Safety Reference Material (SRM) (SESAR SRM 2012).

1.3 *Organisation of the paper*

This paper is organized as follows: Section 2 explains the criteria that have been developed by the DRM project for deciding whether a given SESAR application requires the use of DRM, and it explains how the DRM project has applied these criteria to select a SESAR test case application. Section 3 explains the process that led to the selection of one particular DRM method from a list of candidate methods. Section 4 briefly explains this DRM method in steps, and presents preliminary results of its application to the test case selected in Section 2. Section 5 presents concluding remarks.

2 CRITERIA FOR APPLYING DRM

The SESAR safety assessment approach typically uses static risk modelling techniques: safety criteria and objectives are identified based on accident incident models and further safety requirements are derived using Fault Trees, Failures Modes and Effects Analysis or similar techniques. This section presents criteria to identify specific cases where DRM application is required.

Criterion 1: In SESAR an initial risk evaluation using a conventional (static) method has been conducted and the level of uncertainty in the risk results is such that it cannot be conclusively argued whether the risk is acceptable or not.

Criterion 2: The system behaviour, when considering equipment functional variability, failures, human performance variability and errors, involves occurrences which cannot be considered in isolation, as they strongly depend on system status over time.

Criterion 3: The system behaviour when considering equipment functional variability, failures, human performance variability and errors depends on process variables.

If Criterion 1 is fulfilled together with at least one of Criteria 2 or 3, it is considered that the case is eligible to risk assessment with a DRM method. The anchoring points in a preceding conventional static analysis need to be clearly identified (i.e. the Operational Hazards that will be specifically modeled with DRM, their severities and associated safety objectives together with the justifications developed during the static safety risk assessment). This will serve as the basis for developing the Dynamic Risk Modelling cycle.

The DRM project applied these criteria to SESAR concepts and as a result it selected the use case "Land vs Line up" within the Conflicting ATC clearances project P06.07.01. Conflicting ATC Clearance (CATC) detection is a system that detects early situations of conflicting clearances that, if not corrected would end up in hazardous situations. The "land vs line up" use case considers one aircraft landing and another aircraft lining up to take off on the same runway used in mixed mode. For the detection to work, the controller needs to inform the system (input) each time he provides a clearance to an aircraft. In case of a "land vs line-up" CATC alert, the controller shall resolve the hazardous situation (i.e. avoid a runway collision) by immediately cancelling the line-up instruction and/or instructing a go around, as appropriate.

The static safety assessment initially performed within the SESAR project (SAR CATC 2012) identified a major uncertainty w.r.t. the efficiency of the operational use of "land vs line-up" CATC alert, in relation to the time required for the controller to interpret the alert and communicate the resolution instruction(s) to the involved aircraft and for the pilot(s) to implement the instruction(s). Therefore this case was selected as a suitable test case for DRM.

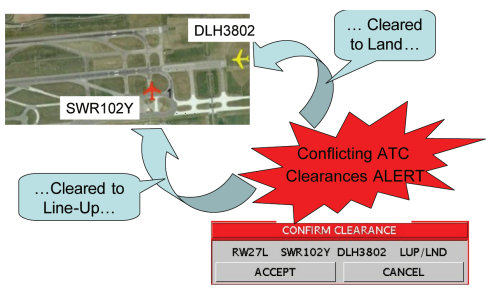


Figure 1. The land vs line-up CATC alert operation.

3 SURVEY OF POTENTIAL DRM METHODS

A variety of methods and tools for conducting DRM exist. Some methods have been in use for many years, while others are of newer date. The level of maturity of the methods varies a lot. The DRM project has identified and described a range of methods, and assessed the methods with regards to suitability for SESAR needs. In total 11 quantitative and qualitative methods have been studied. Priority has been given to methods that provide quantification of results.

The surveyed DRM methods are: Dynamic Event Trees; Dynamic Flowgraph Methodology; Discrete state-transition approaches (Markov chains, Petri Nets & extensions); Dynamic Bayesian Networks; Direct system simulation; DRM for aircraft certification; TOPAZ (Traffic Organization and Perturbation Analyzer); SoTeRia (Socio-Technical Risk Analysis); FRAM (Functional Resonance Analysis Method); STPA Hazard analysis (Systems-Theoretic Process Analysis); Collision Risk Modelling; Encounter-based model methodology. For references and brief descriptions of all these methods, refer to (DRM D04 2012).

By means of an analysis against several DRM-related criteria, the DRM project has selected TOPAZ as a suitable solution for the safety risk assessment of ATM operational scenarios. TOPAZ is an agent-based DRM method that uses Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of air traffic operations up to the level of collisions. For each application, the dynamics of the agents and the time-dependent interactions within and between the agents are modelled in the syntax of Dynamically Coloured Petri Nets (DCPN) (Everdij 2010). The compositional specification by DCPNs allows for the modelling of sociotechnical systems by its broad syntax, including stochastic differential equations (e.g. describing aircraft position and velocity), discrete state transitions (e.g. describing system states or human tasks), and interactions (e.g. describing the recognition of safety-relevant conditions by humans. Detailed descriptions of TOPAZ agent-based DRM and its application to ATM operations can be accessed in Blom et al. (2001, 2006), Stroeve et al. (2009) and Eurocontrol/FAA AP15 Safety (2014).

4 APPLICATION OF DRM METHOD TO TEST CASE

The TOPAZ-based DRM method follows 10 steps which are listed below.

1. Determine the scope of operation/system for DRM
2. Get a complete/consistent description of the operation/system
3. Get a complete list of hazards
4. Develop operational hazard scenarios
5. Develop a stochastic dynamic model
6. Develop risk decomposition
7. Implement the dynamic risk model into software
8. Run Monte Carlo simulations
9. Assess bias and uncertainty
10. Develop safety risks results

The following subsections briefly describe how to apply the steps, following the initial guidance developed by the DRM project in (DRM D07 2012), and provide preliminary results on the application to the test case operation of "land vs line-up" CATC alert developed in (DRM D09 2014).

4.1 *Determine the scope of operation/system for DRM*

DRM Method: In step 1, the scope and goal of the safety assessment are identified, as well as applicable safety criteria or objectives.

Scope: The scope includes a description of the boundaries of the operation and scenarios to be modelled, the types of functions or the types of equipment/procedures/people that are included.

Goal: The goal of the risk modelling is a description of what the DRM-based safety risk assessment aims to achieve in complement to the static safety assessment results.

Safety objectives: Safety criteria or safety objectives refer to target or acceptable levels of risk that are aimed to be achieved.

Application to Test Case: The scope considers mixed mode runway operations, with aircraft landing and taking off from a single runway. The operation is considered in three cases: (1) a baseline case without CATC system, (2) a CATC-OSED case as described in Section 2, and (3) a CATC-SAR case, which is the CATC-OSED operation plus an additional requirement for the controller to enter the clearance in the CATC system before communicating it to the pilots.

The main goal of the safety study is to obtain probability estimates for three types of safety events: (a) a collision between an aircraft landing with an aircraft taxiing to the runway to line-up, (b) the taxiing aircraft entering the Instrument Landing System (ILS) sensitive area, and (c) the taxiing aircraft entering the Obstacle-Free Zone (OFZ).

4.2 *Get a complete/consistent description of the operation/system*

DRM Method: In step 2, a complete and consistent description of the operation/system under

analysis is identified. This includes the operational context of the operation, the timeframe, the traffic characteristics, the geometric aspects of operation; the roles and responsibilities of the humans involved in the operation; the operational procedures, both on the ground and on board; and the logical description of the technical systems used in the operation, how they are operated and their overall performance.

Application to Test Case: Detailed information regarding operation of the system and implementation of the CATC was gathered. A short description of the CATC land versus line-up case is in Section 2.

4.3 *Get a complete list of hazards*

DRM Method: In step 3, a complete list of hazards is identified that are associated with the operation/system to be assessed. The list should include a large number and diversity of possible hazards. In addition to the Operational Hazards (identified at the level of the ATM service provided to Airspace Users) this includes hazards and conditions that may lead to a safety relevant situation (basic causes, root hazards), hazards and conditions that may hamper the resolution of the safety relevant situation (resolution hazards), and pre-existing hazards (those aviation hazards that are not caused by the ATM system but that are aimed to be prevented or mitigated by the ATM system). All the hazards identified here will be referred to in the following as 'hazards'.

Application to Test Case: The project used the material from the preceding static safety analysis, complemented by generic hazard database material from the DRM project partners, to collect a list of 42 hazards. A selection is provided below:

- Situation in which the intended trajectory of two a/c are in conflict on the Runway Protected Area.
- Failure to detect the conflicting clearances with the conflicting ATC clearances System.
- False alert of CATC system.
- Overload of pilot.
- Pilot fails to implement timely the ATCO resolution instruction following the CATC alert.

4.4 *Develop operational hazard scenarios*

DRM Method: In step 4, Operational Hazard Scenarios are constructed. Each such scenario aims to bring into account all relevant ways in which an operational hazard may develop and evolve, under influence of the related operational conditions (such as flight phase and location, level of traffic, environmental conditions), and the related hazards (i.e. basic causes, root hazards, resolution hazards, pre-existing hazards).

Application to test case: The hazards identified in the previous step have been clustered into groups of similar hazards. Next, the relations between these clusters have been depicted in the diagram shown below (ovals are hazard clusters). The clusters in the top describe hazards that may contribute to the causation of a conflict between a landing aircraft and a taxiing aircraft. The clusters in the bottom describe hazards that may hamper the recognition and resolution of the conflict via the CATC alert, the controller, and the pilots of both aircraft.

4.5 *Develop a stochastic dynamic model*

DRM Method: In step 5, a multi-agent stochastic dynamic model is developed, which describes the stochastic dynamic evolution through time of one or more Operational Hazard Scenarios. The model uses the syntax of Dynamically Coloured Petri Net (DCPN) (Everdij 2010) and is developed in 6 steps:

- Step 5.1: Identify the relevant Agents
- Step 5.2: Identify the relevant entities per Agent
- Step 5.3: Specify a Local DCPN (LPN) per entity
- Step 5.4: Interconnect the LPNs within each Agent
- Step 5.5: Interconnect the Agent models
- Step 5.6: Check how the operation and each hazard has been modelled, and iterate.

Application to Test Case: The DCPN-based model developed for the Test Case of "land vs line-up" CATC alert is too lengthy to be included in this paper; therefore, we restrict to a list of Agents and



Figure 2. Operational hazard scenario for conflict.

Agent entities (Table 1), and the specification of one LPN plus its inter-agent interactions.

Figure 3 presents the LPN graph for 'CATC alert', which is one of the agent entities in agent ATC System. The figure follows the syntax of DCPN, which consist of Places (circles), Transitions (squares) and Arcs (arrows) that connect the places with the transitions. The places represent the discrete modes of the entity, which in this case are *No alert* and *Alert*. At any given time, only one of these modes is the current one. A current mode holds a 'token' (not drawn below), which contains continuous valued information that further models the stochastic dynamic evolution of the model. The transitions model the switches between the modes. A switch can only be made if the transition has tokens in each of its input places, and if these tokens contain specific transition-dependent continuous-valued information.

Figure 4 presents the input interactions (Arrows) between the LPN 'CATC Alert' and the LPNs for the entities 'CATC Availability' and 'FDP/EFS'. The transition from *No alert* to *Alert* now has three input places rather than just one, and it needs tokens in each of these input places before the switch can be made. The figure shows that the 'CATC Alert' can only switch from *No Alert* to *Alert* if the 'CATC Availability' is *Up*

Table 1. Description of the agents in the DCPN-based model, and their agent entities.

Agent	Agent entities, plus what they model
Airport and environment	Visibility—The visibility range
	Runway—Layout of runway
	Wind—The actual wind
ATC system	Surveillance—Status of radar surveillance on ground and final approach
	VHF Com Runway Controller—Availability of the controller's VHF Com system
	FDP/EFS—Status of clearance input for both aircraft into the Flight Data Processing/Electronic Flight Strip system as well as status of the FDP/EFS system
	CATC Availability—Availability of CATC system
	CATC Alert—Whether CATC gives an alert
Runway controller	Situation awareness—The controller's situation awareness status and updating process, incl. position and intent of both aircraft, and awareness of CATC alerts
	Conflict action—Whether the controller gives conflict warnings to the pilots
	Clearance Specification—Status of clearance specifications by the controller to the pilots, in terms of having instructed the pilots and of having entered data into the FDP/EFS
	Workload—The current level of workload
	Skill—The level of skill of the controller
	Cognitive control mode—Whether controller is working in opportunistic or in tactical mode
Landing aircraft	Characteristics—Aircraft type, and final approach, landing, missed approach and taxiing characteristics of the aircraft
	Evolution—Position and velocity during final approach, landing and taxiing on the runway, or during missed approach
Avionics of landing aircraft	VHF Com Aircraft—Availability of the VHF Com system for the landing aircraft
Pilots of landing aircraft	Situation Awareness—Situation awareness status and updating process of the pilots of the landing aircraft, incl. position of the own aircraft and of the taxiing aircraft, and the awareness of controller instructions
	Flight Control—The control of the aircraft by the pilots, which may be normal operation or initiation of a missed approach
Taxiing aircraft	Characteristics—Aircraft type, taxiing and lining-up characteristics of the aircraft
	Evolution—Position and velocity during taxiing to the take-off position. As result of a conflict recognized, the aircraft may stop
	System Boundary—Whether the taxiing aircraft is inside or outside the system boundary, i.e. the area where a conflict may occur
Avionics of taxiing aircraft	VHF Com Aircraft—The availability of the VHF Com system for the taxiing aircraft
Pilots of taxiing aircraft	Situation Awareness—Situation awareness status and updating process of the pilots of the taxiing aircraft, incl. position of the own aircraft and of the landing aircraft, and situations requiring the aircraft to stop taxiing
	Flight Control—Control of the aircraft by the pilots, which may be normal operation, or stop taxiing

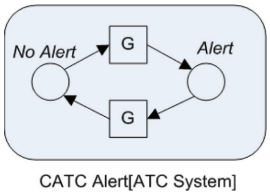


Figure 3. LPN graph for CATC alert.

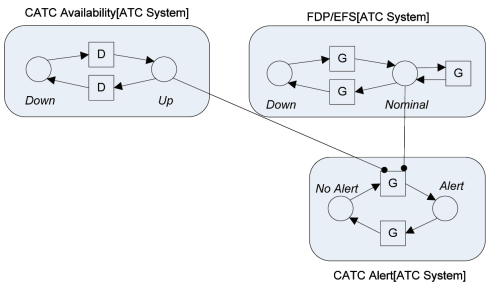


Figure 4. LPN graph for CATC alert, plus its input interactions with CATC availability and FDP/EFS.

and the 'FDP/EFS' is *Nominal*. A second condition for this switch to occur (but not visible in the figure) is that the value of the token in place *Nominal* in LPN FDP/EFS contains the information that the landing aircraft has been given the instruction to land and the taxiing aircraft has been given the instruction to line up; this should give rise to a conflicting ATC clearance alert.

The figures are further connected to other LPNs in a similar way. All figures are complemented by precise descriptions of the conditions and evolution of the LPNs and their interactions.

4.6 *Develop risk decomposition*

DRM Method: With a DCPN-based model now completed, it can next be used as basis of a Monte Carlo simulation to determine the probability of the outcome of the operational hazard, for instance an aircraft collision. To make these simulations more efficient, a risk decomposition is applied. This consists of decomposing accident risk simulations in a sequence of conditional Monte Carlo simulations and combining the results of these conditional simulations into the assessed collision risk value. The conditional runs are started from a conditional state, which is allowed due to the specific mathematic properties of DCPN-based models (Everdij 2010).

Application to Test Case: For the test case application, the probability of occurrence of a Safety Event (such as a Collision between the landing aircraft and the taxiing aircraft) is decomposed as follows:

$$P(Safety\ Event) = \sum_{k=1}^{M} P(Condition_k) \times P(Safety\ Event | Condition_k) \quad (1)$$

Here, the probabilities $P(Safety\ Event \mid Condition_k)$ are conditional probabilities of occurrence of the safety event given a certain well-defined condition *Condition_k* that occurs at a well-defined 'stopping time', and $P(Condition_k)$ is the probability of occurrence of this *Condition_k*. For the Test Case of "land vs line-up" CATC alert, the number of Conditions defined is $M = 192$, hence in the sum above, k is from 1 to 192. For example, *Condition_3* (i.e. $k = 3$) is the one where, at the stopping time: the LPN mode of the Surveillance tracking is Nominal, the LPN modes of the VHF Com for the controller and the landing aircraft are both Up, The VHF Com for the taxiing aircraft is Down, the controller intent for the taxiing aircraft is to Line-up, and the visibility condition is good.

The conditions have been chosen such that each $P(Condition_k)$ can be determined analytically as a function of one or more DCPN-based model parameter values. Hence, Monte Carlo simulations are only needed to determine the $P(Safety\ Event \mid Condition_k)$ for all k, after which all results are combined using the formula above. This significantly speeds up the Monte Carlo simulations by several orders of magnitude.

4.7 *Implement the dynamic risk model into software*

DRM method: In step 7, when the specification of the DCPN-based model and the risk decomposition are fully defined, they are implemented in software language in order to be able to run Monte Carlo simulations. Many software languages are suitable for this, as long as they accept all DCPN syntax principles. A major step in the software implementation is to test the code against all elements of the DCPN-based model and Risk decomposition.

Application to Test Case: The DCPN-based model and risk decomposition for "land vs line-up" CATC alert have been implemented in Delphi using Embarcadero RAD Studio XE3. It takes as input a list of model parameter values that can be set by the user, and that can be changed in order to determine risk values for various scenarios and parameter settings.

4.8 *Run Monte Carlo simulations*

DRM Method: In this step, the software implementation of the DCPN-based model is used to perform Monte Carlo simulations and compute safety risk results. Any Safety Event that can be observed in such simulation can be counted, and the number of counts, divided by the number of runs or the number of associated flight hours or movements, provides an estimate for the probability of occurrence of the Safety Event (e.g. a collision).

Application to Test Case: Risk results were produced by running a series of Monte Carlo simulations for three high-level CATC scenarios and for a set of parameters selected as being potentially representative for their impact on the safety event. Three parameter values were typically simulated in order to observe trends: a baseline value and a high and low value. At the time of writing of this paper, the application of this step was still ongoing. Some preliminary results are presented in the Figures 5 and 6.

In the Monte Carlo simulations the safety events defined in Step 1 were recorded: a collision between both aircraft, the taxiing aircraft entering the ILS sensitive area (150 m from the runway centerline), and the taxiing aircraft entering the OFZ (90 m from the runway centerline). The columns represent the safety event probability results for the three cases of the operation identified in Step 1: baseline without CATC, CATC-OSED, and CATC-SAR. The preliminary results indicate that the CATC system can largely reduce the collision risk, to a similar extent for the OSED and the SAR variants. The probability of entering the ILS sensitive area is hardly reduced by the CATC system. In contrast, the probability of entering the OFZ is reduced by the CATC system and notably more by the SAR variant.

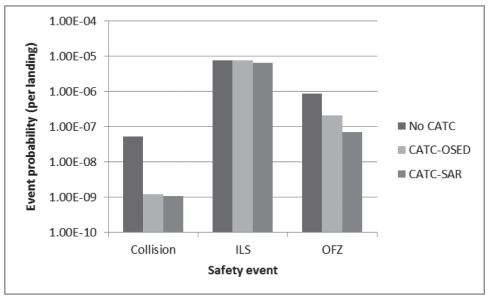


Figure 5. Event probability per landing.

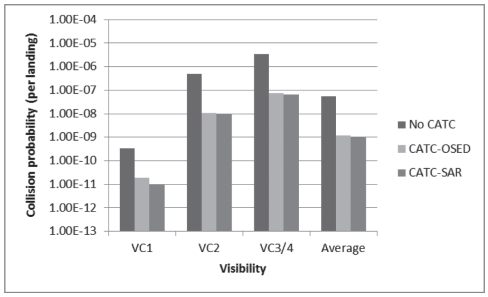


Figure 6. Collision probability per landing.

Figure 6 shows preliminary results for the conditional probability of a collision given three visibility conditions, i.e. VC1 (good visibility), VC2 (visibility range between 400 and 2450 m), and VC3/4 (visibility range between 0 and 400 m). These results show that the conditional collision risks are higher in the poorer visibility conditions, as the controller and the pilots have less opportunity to visually detect a conflict. Furthermore, the results indicate that the CATC system is effective to a similar extent in all visibility conditions.

4.9 *Assess bias and uncertainty*

DRM Method: By definition, any model is not the exact image of reality. The purpose of a bias and uncertainty assessment (Everdij et al. 2006) is to identify how the differences would impact on the evaluation of the risk level in terms of bias and uncertainty:

- Bias: the model-based accident risk is systematically higher or lower than the risk of the real operation.
- Uncertainty: the model-based accident risk lies in a range of credible values for the risk of the real operation (e.g. a 95% credibility interval).

Application to Test Case: At the time of writing of this paper, the application of this step was still ongoing. The initial results showed that:

- For all of the parameters in the DCPN-based model and risk decomposition, a credibility interval could be determined. This gives insight into which parameter values are reasonably certain, and for which more data might need to be collected.
- For most of the parameters in the DCPN-based model and risk decomposition, a sensitivity assessment could be determined. A parameter has a high sensitivity if changes to its value lead to significant changes to the collision risk result. For most parameters it appeared that they have a negligible sensitivity. For some parameters the sensitivity needs to be determined in more detail using dedicated Monte Carlo simulations.

4.10 *Develop safety risks results*

DRM Method: The results of the previous steps provide point estimates and credibility intervals for the probabilities of safety events in various conditions. Comparison of these results with safety criteria provides insight in risk acceptability and risk margins. Furthermore, these results can be used to identify safety bottlenecks (aspects of the operation that contribute to unacceptable risk levels) and they provide a basis to determine safety requirements and safety objectives.

Application to Test Case: The safety risk results achieved by the DRM approach will be compared with those of the static safety assessment initially performed for the CATC operation within the SESAR project. This comparison will be used to analyse the added value of the DRM approach.

5 DISCUSSION AND CONCLUDING REMARKS

The SESAR DRM project aims to show that consideration of dynamic aspects in the safety assessment of an operation is important when studying operational concepts in which multiple operators, technical systems, the environment, and their interactions play an important role. Within the context of SESAR, Dynamic Risk Modelling (DRM) is considered to be required if the level of uncertainty in the risk results of an initial risk evaluation using a conventional (static) method is such that it cannot be conclusively argued whether the risk is acceptable or not. In addition, at least one of the following criteria needs to hold true: a) The system behaviour, when considering equipment functional variability, failures, human performance variability and errors, involves occurrences which cannot be considered in isolation, as they strongly depend on system status over time. b) The system behaviour when consider-ing equipment functional variability, failures, human performance variability and errors depends on pro-cess variables.

By means of an analysis against several DRM-related criteria, the DRM project has selected TOPAZ from a list of candidate DRM methods as a suitable solution for the safety risk assessment of ATM operational scenarios. TOPAZ is an agent-based DRM method that uses Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of air traffic operations up to the level of collisions. The project produced guidelines for the application of this method in SESAR context, and applied the method to a SESAR Test Case of "Land vs Line-up" Conflicting ATC Clearances.

The Test Case has shown that DRM is able to model the stochastic dynamic aspects of an operation with more accuracy than is possible with static methods. Examples are the position and velocity of aircraft as they evolve through time, the stochastic dynamic behaviour of human operators in response to their environment, situation awareness differences between various actors, multiple scenarios that unfold under influence of hazards occurring, environmental changes, events occurring earlier or later than average, etc.

The preliminary DRM-based risk results show interesting differences with those of the preceding static safety assessment, which will be systematically studied in the remainder of the DRM project.

ACKNOWLEDGEMENTS AND DISCLAIMER

The work presented in this paper is financed by the SESAR Joint Undertaking (SESAR JU) programme. NLR contributes to the SESAR project on behalf of DFS Deutsche Flugsicherung GmbH. The authors thank project members AIRBUS (especially Joelle Monso, Eric Hannouz, Lionel Marie-Magdeleine), DFS (especially Viktoria Weigel), ENAV (especially Tiziana Russo) and SELEX (especially Angela Errico) for their contributions. This paper presents the authors' view only and is not intended to represent organizations or the SESAR JU position.

REFERENCES

Averty, P., Mehadhebi, K., Pirat, J.L. (009. Evaluation of ATC working practice from a safety and human factor perpective. Eight USA/Europe Air Traffic Management and Research Seminar.

Blom, H.A.P., Bakker, G.J., Blanker, P.J.G., Daams, J., Everdij, M.H.C., & Klompstra, M.B. 2001. Accident risk assessment for advanced air traffic management. In G.L. Donohue & A.G. Zellweger (Eds.), *Air Transport Systems Engineering* (pp. 463–480): AIAA.

Blom, H.A.P., Stroeve, S.H., & De Jong, H.H. 2006. Safety risk assessment by Monte Carlo simulation of complex safety critical operations. In F. Redmill & T. Anderson (Eds.), Developments in Risk-based Approaches to Safety: Proceedings of the Fourteenth Safety-critical Systems Symposium, Bristol, U.K., 7–9 February 2006: Springer.

DRM D04. 2012. SESAR P16.01.03 Deliverable D04: Identification of Dynamic Risk Modelling for SESAR needs, Selection of DRM solution for SESAR.

DRM D07. 2012. SESAR P16.01.03 Deliverable D07: Initial guidelines for Dynamic Risk Modelling (DRM) application.

DRM D09. 2014. SESAR P16.01.03 Deliverable D09: Dynamic Risk Modelling (DRM) Test Case application.

Eurocontrol/FAA AP15 Safety. 2014. Agent-based dynamic risk modelling for ATM: A white paper.

Eurocontrol 2009. 'Feasibility study on Dynamic Risk Modelling for ATM Applications', by M.H.C. Everdij, S.H. Stroeve.

Everdij, M.H.C., Blom, H.A.P., & Stroeve, S.H. 2006. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. *Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management*, New Orleans, USA.

Everdij, M.H.C. 2010. Compositional modelling using Petri nets with the analysis power of stochastic hybrid processes. PhD. Thesis, University of Twente. http://www.nlr-atsi.nl/eCache/ATS/15/060.pdf.

Herrera, et al. 2011. DRM project—Develop Techniques for Dynamic Risk Modelling. SESAR P16.01.03. Project Initiation report.

SESAR SRM. 2012. SESAR WP 16.06.01 Deliverable D06: SESAR Safety Reference Material, version 00-02-02.

SAR CATC. 2012. Safety Assessment Report for Conflicting ATC clearances SESAR P06.07.01, D17B, ed00.01.03.

Stroeve, S.H., Blom, H.A.P., & Bakker, G.J. 2009. Systemic accident risk assessment in air traffic by Monte Carlo simulation. *Safety Science, 47* (2), 238–249. doi:10.1016/j.ssci.2008. 04.003.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Modification of response spectra by probabilistic approach

V. Salajka, J. Kala, Z. Cada & P. Hradil
Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT: The paper deals with the seismic linear response spectrum modification based on a probabilistic approach. The modification improves the correctness of the deterministic seismic analysis of building structures using the response spectrum method. In that case, the structure response depends strongly on computed natural frequencies. The proposed response spectrum modification accounts for uncertainties in response due to uncertainties in frequencies caused by variances of computation model parameters. The response spectrum is modified so, that with a selected probability the given spectral values should not be exceeded. The variance of natural frequency values is obtained by modal analysis of a stochastic model of the structure.

1 INTRODUCTION

The dynamic behaviour of building structures subjected to seismic action is commonly analyzed using the deterministic approach. The computation model is designed using the finite element method. The time domain response to defined non-stationary ground motion can be computed using direct integration of structure equations of motion. For many reasons, procedures based on structure vibration mode superposition are preferred. The response spectrum method is very frequently applied (ASCE 2000, Braja 1984, Kala et al. 2012). The structure response depends strongly on computed natural frequencies. Due to variances of characteristic model parameters, particularly when soil-structure interaction is considered, high values of variance of computed frequency values could be expected. Hence, possible variation of the natural frequency value in relatively wide range must be respected in the response analysis. Consequently, responses of quite different levels could be obtained (see illustration in Fig. 1).

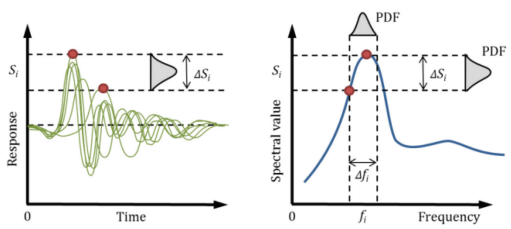


Figure 1. Variation of response spectrum values due to change of model frequency.

Uncertainties in computation of responses could be reduced by selecting appropriate configuration of parameters of the deterministic computation model. This way is lengthy and results are not guaranteed. Application of a stochastic model is limited due to pretentious computations. Another approach to account for uncertainties in response consists in modification of the given response spectrum. The modification of the response spectrum reduces e.g. the effects of random coincidences of computed frequencies with extremes of the spectrum course. Controlled broadening and lowering of the spectrum is recommended in (Cada et al. 2011, Holomek et al. 2012). The proposed response spectrum modification reduces effectively the uncertainties in response due to uncertainties in frequencies caused by variances of computation model parameters. The modification is based on the probabilistic description of natural frequencies of the analyzed structure, obtained by modal analysis of a stochastic model of the structure.

2 PROBABILISTIC DISTRIBUTION OF THE NATURAL FREQUENCY VALUE

The proposed response spectrum modification procedure will be explained using a case problem involving a thirteen-story panel building structure. The modal analysis has been performed applying an advanced finite element computation model (see Fig. 2). Solid and shell finite elements from the ANSYS program package have been used in modeling the structure. Solid massless elements have been used to model the layered subsoil. The characteristic parameters decisive for the analysis of first bending modes of vibration of the model have been selected

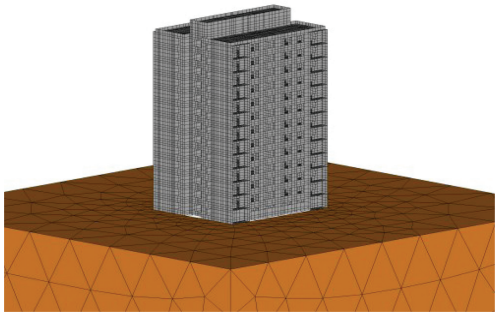


Figure 2. Finite element model of the panel building.

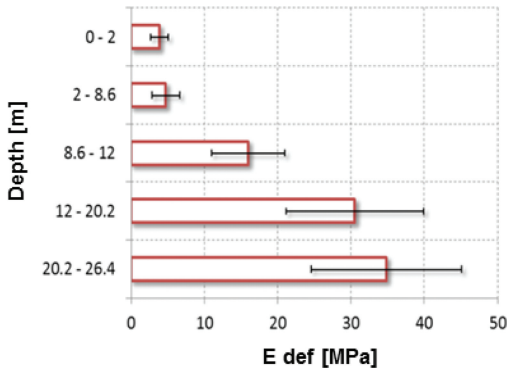


Figure 3. Modulus of elasticity of soil layers.

after performing a parametric study (Gupta 1992) of the dynamic behavior of the structure.

Moduli of elasticity of soil layers have been investigated experimentally. Effective densities of structure parts are based on the analysis of variations of masses of panels and those of floor live loads. Probability distribution types for all considered parameters have been determined (beta-type for soil, normal for panel densities, log-normal for live load). Corresponding mean values, standard deviations and coefficients of variation have been computed. Mean values of modulus of elasticity of soil layers with indicated standard deviations are shown in Figure 3 (Bajer et al. 2012).

Probability distributions of dominant horizontal bending frequencies f_x and f_y of the parametric model have been determined using the ANSYS program (ANSYS 2013) (modal analysis) in combination with the optiSlang program (Dynardo 2010) (LHS-method of generation of input parameters, analysis of output data) (Kala 2012, Kala et al. 2010, Kala et al. 2013). Results of computation are shown in Figure 4.

Stochastic analysis has been performed also at effective modal masses (m_{effx}, m_{effy}) and effective

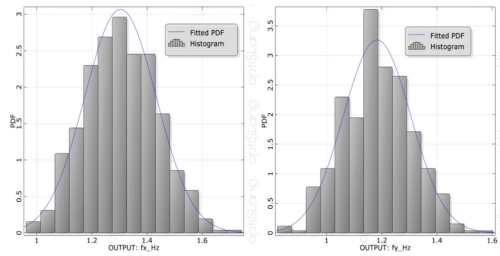


Figure 4. Probability distribution of dominant natural bending frequencies f_x and f_y of the model.

stiffnesses (k_{effx}, k_{effy}) computed from the relation in (Chopra 2001).

3 MODIFICATION OF RESPONSE SPECTRA

3.1 *The procedure description*

The procedure assumes, that the following is known:

- linear site-specific seismic response spectrum,
- probabilistic distribution of natural frequencies,
- position of the selected frequency in the probability function,
- required probability of non-exceedence of the spectral value.

3.2 *The repeated steps of the procedure*

The repeated steps of the procedure of modification are as follows (Kala et al. 2012):

1. selection of the frequency f_i,
2. construction of the probabilistic distribution function of f_i,
3. repeated steps for spectral values S_j in interval 0 to S_{max}:
   a. determination of frequency range where spectral values exceed S_j,
   b. computing area p_j under the probabilistic function of f_i,
   c. marking the point $[S_j, p_j]$ of the distribution function of exceedence of the spectral value S_i,
4. reading of the value S_i for the given probability of exceeding p from the distribution function,
5. fixing the point $[S_i, f_i]$ for the modified response spectrum,
6. return to step 1 to select next frequency.

For known probabilistic distribution of natural frequencies of the model, the modified response spectrum ensures no exceedence of spectral value at given probability p.

4 MODIFIED RESPONSE SPECTRA FEATURES

Selected cases of modified response spectra are shown in Figures 5 to 7. The parameter p is the probability of exceeding the distribution function and e is the exponent of the response change due to frequency change. Normal distribution of frequencies is assumed, with mean value corresponding to frequency f_i and with coefficient of variation v.

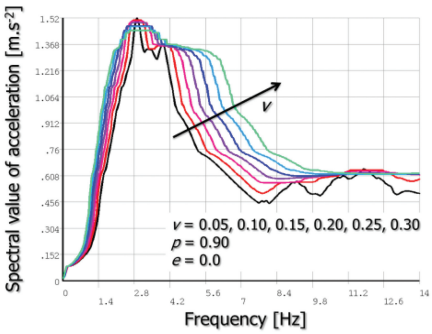


Figure 5a. Change of response due to change the frequency.

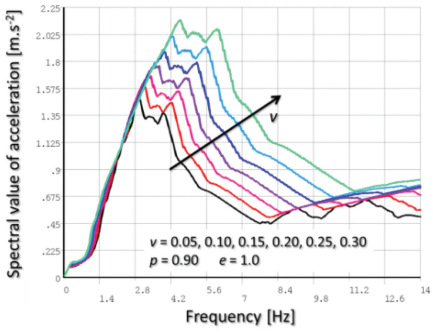


Figure 5b. Change of response due to change of model parameters.

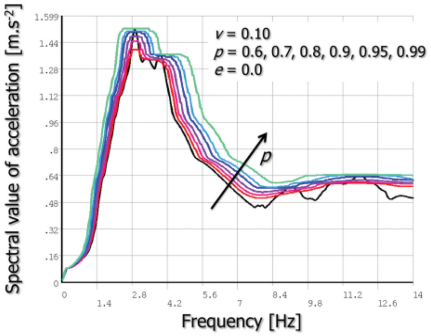


Figure 6a. Change of response due to change the frequency.

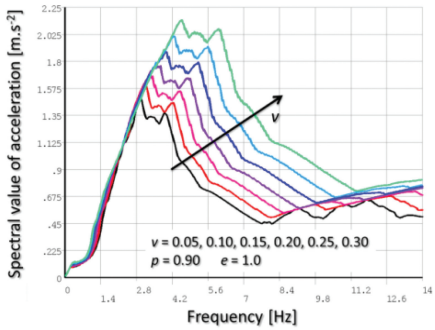


Figure 6b. Change of response due to change of model parameters.

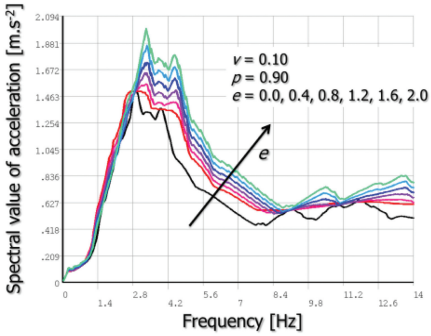


Figure 7a. Change of response due to change the frequency.

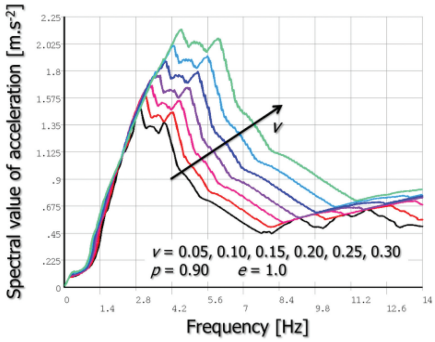


Figure 7b. Change of response due to change of model parameters.

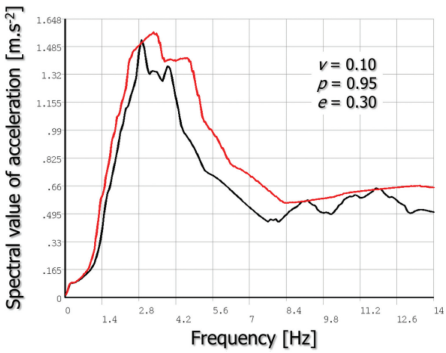


Figure 8. Response spectrum of the model as generated (black) and modified (red).

5 MODIFIED RESPONSE SPECTRUM FOR THE ANALYZED PANEL BUILDING

The modified response spectrum corresponding to parameters of the analyzed panel building is shown in Figure 8. The 95% probability of exceeding the distribution function has been selected.

6 CONCLUSION

The proposed response spectrum modification procedure ensures correctness of the deterministic seismic analysis of building structures using the response spectrum method. The modification reduces effectively the uncertainties in response due to uncertainties in frequencies causes by variances computation model parameters.

ACKNOWLEDGMENT

This outcome has been achieved with the financial support of the project of GACR 14-25320S "Aspects of the use of complex nonlinear material models".

REFERENCES

ASCE: ASCE 98-4 (2000) Seismic Analysis of Safety Related Nuclear Structures and Commentary. American Society of Civil Engineers.

ANSYS 2013, Inc. Release 15.0 Documentation for ANSYS. SAS IP, Inc.

Bajer, M. & Barnat, J. 2012 The Glue-Concrete Interface of Bonded Anchors. Construction and building materials, 34(9): 267–274, doi: 10.1016/j.conbuildmat.2012.02.030, ISSN 0950-0618.

Barnat, J. & Bajer, M. & Vyhnankova, M. 2012 Bond strength of chemical anchor in high-strength concrete, Procedia Engineering. 2012(40), pp. 38–43, ISSN 1877–7058, DOI: 10.1016/j.proeng.2012.07.052.

Braja, M.D. 1984 Fundamentals of Soil Dynamics. Elsevier, New York, Amsterdam, Oxford, ISBN 0-444-00705-9.

Čada, Z. & Hradil, P. & Mrózek, M. & Salajka, V. 2011 Parametric study on dynamic behaviour of a multi-storey building including soil-structure interaction. 17th International Conference, Engineering Mechanics, pp. 91–94.

Chopra A. 2001 Dynamics of structures. Theory and Applications to Earthquake Engineering. New Jersey: Prentice-Hall.

Dynardo GMBH 2010 OptiSlang 3.1.4 Documentation, Weimar, Germany.

Gupta A. 1992 Response Spectrum Method. In Seismic Analysis and Design of Structures. United States of America: CRC Press.

Holomek, J. & Bajer, M. 2012 Experimental and Numerical Investigation of Composite Action of Steel Concrete Slab. Procedia Engineering. 2012(40), pp. 143–147, ISSN 1877-7058, DOI: 10.1016/j.proeng.2012.07.070.

Kala, J. & Salajka, V. & Hradil. P. 2012 Sensitivity Investigation of eigenvalue problem of water tower construction interacting with fluid, *Journal of Vibroengineering*, 14(3): 1151–1159, ISSN 1392-8716.

Kala Z. & Kala J. 2010. Variance-based sensitivity analysis of stability problems of steel structures, *International Conference on Modelling and Simulation 2010; Proc. intern. conf., Prague, 22–25 June 2010*, Czech Republic.

Kala, Z. 2012. Geometrically non-linear finite element reliability analysis of steel plane frames with initial imperfections. *Journal of Civil Engineering and Management* 18(1): 81–90.

Kala, Z. & Kala, J. 2013. Uncertainty and sensitivity analysis of beam stability problems using shell finite elements and nonlinear computational approach. *Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures—Proceedings of the 11th International Conference on Structural Safety and Reliability, ICOSSAR 2013*; *Proc. intern. conf. New York, 16–20 June 2013*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dynamic Positioning systems with emphasis on harsh climate conditions

T. Li & O.T. Gudmestad
Department of Mechanical and Structural Engineering and Materials Science, University of Stavanger, Stavanger, Norway

A. Barabadi
Department of Engineering and Safety, University of Tromsø, Tromsø, Norway

ABSTRACT: Dynamic Positioning (DP) is becoming more and more popular as the reliability of DP systems is improving and as the oil and gas industry moves into deeper and harsher environments where other station keeping methods are inefficient and very costly. The most significant risk relevant to DP operations is loss of the position control ability. The environmental condition (e.g. wind, wave, and current) is one of the main influence factors on position keeping ability of the DP system which is more important in harsh environment such as Arctic and South China Sea. In this paper the operation of a DP vessel in harsh operational conditions will be discussed. Furthermore; hazard identification, consequences of loss of position and identification of robust barriers to avoid disastrous outcomes in such harsh operational conditions will also be discussed with emphasis on safe disconnection from the ongoing activity.

1 INTRODUCTION

Vessel operations in harsh climate conditions and deep-water require a closer review of the safety of the selected station keeping methods (Chen et al., 2008). Dynamic positioning is becoming more and more popular as the reliability of DP systems is improving and as the oil and gas industry moves into deeper and harsher environments where other station keeping methods are inefficient and very costly. The DP system contains a computer program which allows the motion components surge, sway and yaw to be automatic controlled, keeping the position of the vessel or installation (Faÿ, 1990). DP systems can provide rapid response to harsh weather such as hurricanes or tropical storms, emergency disconnection of the risers and self-navigate to a safe place. A DP system does not need to use large Anchor Handling Tug Supply vessel (AHTS) for anchor handling which can reduce the risk, cost and downtime that would occur during an anchor handling operation. Moreover there is no risk for the system to damage the subsea facilities without using the mooring line and anchors. However, the need for separate engine room, expensive electronic components and constant fuel consumption can increase the operational cost of the DP system, but using new technology we can reduce the operational cost of the DP system. For example, by using special hull designs (e.g. Bulb-bow, X-bow and Axe-bow) the resistance generated by the air and water will be minimized and consequently it can reduce the operational cost.

In harsh operational conditions environmental factors can affect the performance of DP which can lead to loss of the position control ability. For a Mobile Offshore Drilling Unit (MODU), loss of position without safe disconnection could result in critical damage not only to the well, but also to the subsea equipment. For an Offshore Support Vessel (OSV), loss of position could lead to collision with the nearby installation during operation or to damage to the subsea facilities. In order to increase the safety and reliability of a DP system, it is important to identify and quantify all influence factors and the way that they can affect the DP performance. For example "bad weather condition" is an effective factor on the position reference sensor or the local position reference system. Such operational conditions can vary from place to place and may have a dynamic nature in a specific location. Moreover, it is important to investigate safe recovery back to position, safe disconnection and reconnection when the loss of position is outside the safe operational range.

In this paper we review the application of DP in harsh climate conditions; more specifically we focuses on the Arctic conditions and the conditions in the South China Sea. Moreover, the paper deals with a preliminary hazard analysis of DP systems in such operational conditions. In this paper in section 2 the DP working conditions in Arctic

and South China Sea are discussed. Section 3 provides preliminary hazard analysis of a DP system in harsh climate condition and suggests risk reducing measures. Finally, section 4 presents the conclusions.

The objective of the paper is to communicate to those planning to apply DP in harsh environmental conditions a warning that loss of DP may be expected and that planning to implement mitigating measures is needed in such situations.

2 DP IN HARSH CLIMATE CONDITIONS

Dynamic Positioning is the technique to keep a floating structure stationary by means of controlling the magnitude and the direction of thrust, based on position feedback. In DP systems the computers will get the data from the references and sensors and compare them with the pre-set data. Then the DP control system will control the propulsion system to take action eliminating the difference between the actual positions and the heading data and the pre-set data (ISO19901-7, 2005). There are different types of sensors such as motion reference units, wind sensors and draught sensors which give feedback regarding such themes as the wind velocity or roll and pitch of the vessel.

2.1 *DP in the arctic condition*

In recent years, offshore oil and gas exploration and field development are increasingly focused on the Arctic waters. The U.S. Geological Survey has estimated that as much as 28 percent of all recoverable resources (oil, natural gas and natural gas liquids) yet to be discovered are to be found north of the Arctic Circle (Kayrbekova et al., 2011, Bird, 2008). At the same time, the Arctic also has the harshest environmental condition for offshore activities, for instance, the remoteness, the extreme cold, dangerous sea ice, and a fragile environment. There have been some examples of moored offshore installations in ice. However, there is very little operational experience regarding DP operations in ice.

There are several challenges for a dynamic positioning system to be used in ice. How to accurately predict the ice force is one of the most significant challenges (Jenssen et al., 2009). Ice thickness, concentration, size distribution of ice floes and drift velocity are known to be important factors regarding ice loads (Wilkman et al., 2009). The dynamics of the ice and the vessel's dynamics interact with each other, which makes the force of the ice on the vessel difficult to predict. In DP mode, and assuming the vessel is aligned with the ice drift direction, the thrust created by the propulsion of the vessel has to resist all the forces caused by the ice drift, which include not only the mean and oscillating force in the longitudinal x-direction, but also an oscillating force in the transverse y-direction and an oscillating yaw moment (Wilkman et al., 2009). That makes the vessel easily to drift off the position.

Another challenge for DP system operation in ice is that rotating the vessel on the spot is not possible. In order to turning a vessel in ice, the vessel has to move forward and backwards in order to rotate (Hals and Jenssen, 2012, Kuehnlein, 2009). Ice under the hull of the vessel is also a big challenge for DP system operations in ice. The ice floes propelled by the thrusters with high speed could create great harm to the hull of the vessel, as well as the equipment under the hull of the vessel, such as the acoustic transducers. Thus, the design of the hull is essential.

The cold temperature and the wind could damage the wind sensor and other equipment of the DP system on deck, which may lead to the holistic system being out of work. Those challenges disqualify the DP concept for continuous operation in. Ice conditions vary from light to heavy, both the speed and direction of drifting ice may change rapidly. These, as well as the challenges mentioned above, should be taken into account for a new concept DP system design. A new conceptual design includes the following features:

- Low ice resistance of the vessel at both bow and stern. This would be achieved by optimizing the icebreaking hull shape, similar to the ones found on icebreakers.
- High ability to turn the vessel in ice in order to follow changes in ice drift. This could be achieved by implementing a strong slope at the side of the vessel. This hull shape allows the vessel to break ice over the entire ship length. Azimuth propellers could deliver the required thrust for turning the drill ship.
- The vessel should be able to operate in ice without icebreaker assistance up to very severe ice conditions (Kuehnlein, 2009). With icebreaker assistance, the operational limits of the vessel should be extended even further.

A DP vessel's station keeping capability in the Arctic can be increased through ice management. The aim of ice management operation is to decrease the severity of the ice condition to a level where the DP system is operable. In practice, before the ice is approaching the DP vessel the ice blocks should be broken into small ones, which could prevent the DP vessel from drifting off position due to collision with big blocks of ice. The role of ice management is critical, because the station keeping capability of the DP vessel is limited in ice. In order to provide sufficient ice management intensity and

effect, normally more than one ice management vessel is needed. The bigger ice management vessel will be arranged further from the DP vessel, and the smaller or equally large ice management vessel will be arranged near the DP vessel. The ice management vessels cooperate to break the ice into smaller floes, and decrease the dynamical behavior of the ice against the DP vessel.

2.2 *DP in South China Sea*

South China Sea is the deepest and widest sea offshore China, with the richest oil and gas resource down below. The petroleum geological resources are estimated to be about 20–30 billion tons; gas resources are about 16 billion cubic meters contained in the South China Sea Basin, accounting for 1/3 of China's total oil gas resources of which 70% are in deep sea areas. However, the South China Sea is very famous for its hash environment. Oil and gas exploration activity in South China Sea can be challenging due to the weather and high seas, especially for the offshore facilities equipped with DP systems. Some of the most important weather challenges in South China Sea for DP are as follows:

Monsoon and the cold front*:* The general weather pattern is represented by the monsoon. During the monsoon the directionality of the environment changes and heavier rainfall occurs (Haveman et al., 2006). Besides, there is always strong wind accompanied. The cold fronts appearing in winter frequently bring wind with force at least 7–8; the wave height is around 3 meters during the winter. All of which generate a risk for the offshore installations positioned by DP systems to drift off position.

Soliton current*:* Soliton current caused by internal waves is a special phenomenon which occurs at several locations around the world, and also in the South China Sea during the summer season. The speed of the soliton current is usually up to 3–4 knots with the tide current, which will generate ripples on the sea surface. Generally, the soliton current is hundred meters width and 50 nautical miles long. Solitons occur all year round, especially in June and July. Large energy is contained in a soliton which increases the probability of offshore installation being forced off the position. If the forces acting on the hull of the installation exceed the power of the thrusters, then it will lose the keeping position ability. It also creates a significant risk that the position keeping ability is lost due to its high speed and rapid changing direction. The rapid change of speed and direction of the soliton will lead to a certain delay for the DP system to react to the environment, causing the installation to drift off the original position, even out of the warning limits. Thus, it is very important for the DP operator to detect the soliton early and take preactions to resist it from drift off position. Tide is the original cause for the generation of soliton. Thus the occurrence of solitons can be more or less predicted. Their intensity cannot be estimated but there may be measures to provide an advance warning of their impending arrival. With advance warning the facility activities can be scheduled until soliton passage is complete (Millmaker et al., 1997). Radar could also be used to detect the solitons. Solitons will generate ripples on the sea surface, so shipboard radar could be used to detect them. The speed and the wave length of the soliton could be accurately measured by radar and Acoustic Doppler Current Profiler (ADCP). In the case of Soliton:

– All generators should be kept at good working conditions to resist the effects of the soliton especially the ones that are not detected in time.
– After a soliton warning, the DP operator should ready all the thrusters and generators, in order to cope with the coming soliton impact.
– Adjust the heading of the installation directly against the soliton before the soliton arrival as far as possible to avoid soliton side attack.
– Adjust the DP system to quickly response to the changes of the environment. The quick mode could be used in this circumstance to cope with the rapid speed and direction changes of the soliton. Thus, enough time could be obtained for the thrusts to resist the external force before the rig is being forced off.

The typhoon: Most of the oil fields in the South China Sea will be affected during the typhoon season (around July to October) and there are some disasters related to the typhoons. For example in October 23rd 1983, the rig "Java Sea" was capsized due to the attack of a typhoon. All 81 people on board died, and the total economic loss was 350 million US dollars. Root cause for this disaster was that people in charge did not pay enough attention to the local typhoon, and it was too late when the actions were taken. In September 14th 2009, rig "West Hercules" operated in South China Sea. The rig was being forced off the original well position due to an attack of a typhoon. The root causes were that the people in charge were too confident about the ability of the rig to resist the typhoon attack. Typhoons are generated from east of Luzon Island, and are then moving into the South China Sea. The most predominant characteristics of this kind of typhoons are high strength, large affection area, but with enough warning time. There is another kind of typhoons named local typhoons. These develop from the tropical low pressure. The characteristics of this kind of

typhoons are less horizontal domain, low vertical height, and relatively low intensity. They are generated fast, are difficult to prevent and are usually destructive to the offshore facilities as strong wind and heavy seas are generated.

Typhoons increase the risk for the installation being forced off position, due to the external extremely high wave forces which may be exceeding the force generated by thrusters of the installation. Loss of position may occur as drift-off. Associated well damage, equipment damage, and even personnel injury accidents may occur. Additional measures should be taken to minimize the risk generated by typhoons, and make sure that the wind speed and wave do not exceed the rig's operational standards before disconnection.

The DP system accompanied by a mooring system for station keeping is a proven concept in typhoon areas. However, for some areas the mooring system could not be accompanied with DP system, because of the water depth. Much more additional actions should be taken to cope with the coming typhoon:

- The routine report will be more frequent when there is a typhoon. Then the installation management could decide whether to keep the original position or disconnect and navigate to safe area. Make sure that there is enough time to navigate to the safe area when deciding to disconnect;
- The installation should recover all the risers and subsea facilities timely before the approach of the typhoon near. All moving equipment or materials should be lashed tightly, and all the watertight openings should be checked. Enough maneuvering space should remain for the DP system to avoid collision with other installations nearby;
- Generators and thrusters should be used reasonably, avoid continuous use at full load condition. Reasonable heading should be adjusted to avoid that the rig is being directly exposed to the heavy wind and waves.
- Suitable navigation methods should be selected when deciding to disconnect. According to the moving path of the typhoon, the manager should justify the rig's relative position from the typhoon's eye;
- The location could shield the installation from exposing to the strong wind and waves. Hainan Island could provide an ideal shielding area for offshore DP installations. However, attention should be paid to a sudden direction change of the typhoon.

Offshore DP installations for the offshore oil and gas industry in the South China Sea must be outfitted with the ability to cope with unexpected coming of solitons, typhoons, cold fronts and other severe weather conditions. Successful operational experience of other DP installations in the South China Sea could be used for reference.

3 HAZARD IDENTIFICATION OF DP SYSTEM WITH EMPHASIS ON HARSH CLIMATE CONDITIONS

As mentioned the most significant risk relevant to DP operations is loss of the position control ability (Bakken and Smedvig, 2001, Fougere, 2005). Normally, there are two basic failure modes for loss of positions; they are drive-off and drift-off. For drive off, the OSV/MODUs go off position by their own thrusters' force, because inaccurate position data are received, which lead to that the DP system drives the installation to a wrong position. For drift-off, the force generated by thrusters could not resist the external environmental force; the installation will drift off its original position by the force of the wind, waves as well as the currents. Figure 1 shows the causes of the loss of position incidents from year 1994–2003 (Tjallema et al., 2007).

As Figure 1 shows the causes of loss of position, these can be categorized in three main groups including *i) environmental factors, ii) dynamic positioning system*, and *iii) DP operation associated personal*. As mentioned the environmental factors such as wind, wave, and current, directly influence DP vessels' resistance to loss of position. The possibility of sudden changes of wind and current direction, and the possibility of certain atmospheric conditions that influence the GPS, are the factors to evaluate (Chen et al., 2008, Chen et al., 2009). The characteristics of the dynamic positioning systems components (DP computer, power generation, position references, thrusters and electrical components) play significant contributions to resistance of loss of position. Using system redundancy is an effective way in order to increase the availability and reliability of the dynamic positioning system. Redundancy can reduce the probability of the DP installation's loss of position and protect the installation from dam-

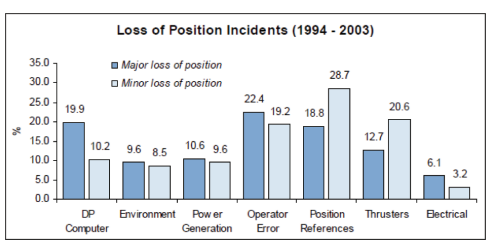


Figure 1. DP incidents causes (Tjallema et al., 2007).

Table 1. DP loss of position preliminary risk analysis.

Equipment node	Deviation	Failure causes	Consequence	Recommendation
Position reference	Total failed	1. Power supply off; 2. Satellite failure; 3. Device out of work; 4. Device damaged 5. *Positioning system inadequate (for example in the Arctic)*	1. Loss of position; 2. Environment pollution	1. More position reference; redundancy with different work principle; 2. Properly protect outer part of the device from damaging; 3. Emergency power supply 4. *Get ready for leaving location/abandon the operation*
	Position data with large error	1. Antenna signal damped; 2. Calculation part error; 3. Interrupted with each other	Moving out of limitation	1. Check the antenna regularly 2. Regularly system self-test; 3. Proper satellite or transponder position
	Do not get proper signal occasionally	1. Maintenance defect; 2. Transponder contaminated; 3. System disorders; 4. System setup error	1. Large thrusters load; 2. High fuel consumption; 3. Less position control accuracy; 4. Degradation of DP operation status	1. Regularly maintenance by specialist; 2. Check the satellite and transponder working condition; 3. Restart the system; 4. Properly system setup
Power station	No power supply	1. Fuel run out; 2. Fire alarm generate; 3. Switch-board burn out; 4. All generators out of work	1. Loss of position; 2. Collision with other installations; 3. Environment pollution	1. Enough fuel for daily consumption; 2. Establish emergency response procedure; 3. The emergency generator available at any moment
	Insufficient power supply	1. Damaged of power cable; 2. One of the generator shut down; 3. One or more power route blocked up	1. Moving out of limitation due to insufficient thrusters force; 2. Lower position keeping accuracy and reliability	1. Regularly power supply system checkup; 2. Generator maintenance regularly according to the PMS
Thruster	All thrusters shut down	1. No power supply; 2. Control station error; 3. Power switch board out of work; 4. Main power cable erosion	1. Loss of position; 2. Collision with other installations adjacent; 3. Environment damage	1. Regularly thruster system checkup; 2. Establish thruster working status monitoring system; 3. Redundancy power route setup
	One or two thruster out of work	1. Partly power route blocked up; 2. Electrical signal blocked from input to control station 3. *Repair has not been possible due to harsh environmental conditions*	1. Lower position keeping ability and reliability; 2. Loss of position may occur	1. Fulfill the check list before operation; 2. Redundancy power route setup; 3. Electrical signal checkup before input to DP control station
	Thrusters working abnormal	1. Mechanic part fail of the thruster itself 2. *Thruster power insufficient to keep up with environmental loading*	1. Out of work of the thruster; 2. Lower DP system position keeping capacity	1. Thruster maintenance according to the requirement; 2. Get ready of the spare part 3. *Ready for leaving location/abandon the operation*

(*Continued*)

Table 1. (*Continued*)

Equipment node	Deviation	Failure causes	Consequence	Recommendation
Sensor	1. Sensors not working in system	1. Failed of the sensors signal input	1. Lower DP position keeping ability	1. Regularly sensors working condition checkup
	2. Heading indicating error	2. Gyro compass working abnormally or failed	2. Loss of heading keeping ability	2. Redundancy of the gyro compass
	3. Thrusters force output hardly balance with the external force	3. *Sensors do not detect ice (Arctic) or solutions (South China Sea)*	3. Loss of position	3. Equip sensors with different working principles
	1. Wind sensor damaged	1. Hash external weather condition	1. Loss sensors signal occasionally	1. Proper sensor protection and examination
	2. Electrical signal could not receive by DP control station	2. Wrong sensor signal cable connection	2. DP system alarm sound out	2. Sensor restart, self-diagnose and test
	3. Sensors working disorder	3. Long time sensor working	3. Degradation of DP operation status	3. Replaced by new ones
Computer software	1. System paralysis	1. Original design problem	1. Loss the ability of system control	1. Software debug or redesign of the software
	2. Software incompatible with hardware	2. Old version software	2. Loss of position	2. Update the old software for the new one
	3. Wrong command for hardware	3. Wrong software for specific hardware drive	3. Degradation of DP operation status	
	1. Button input invalidation	1. Poor contact	1. System out of control	1. Computer system properly protected, and examination regularly according to maintenance plan
	2. Operation station shift invalidation	2. Software disorder	2. Emergency status may occur	
		3. Signal cable damaged	3. Degradation of DP operation status	2. Operation panel test timely
		4. Wrong software operation		

age (Li Jr, 2013). The minimum redundancy requirements of the DP systems are defined by different guide line such as Lloyd rules: Rules for classification and construction. Finally, the action of DP personnel may directly lead to loss of position of the DP system, or they may interact with the technical failure both contributing to loss of position. The following elements affect the human actions: training, certification, operation experiences, knowledge about the DP system, work attitude, teamwork spirit and so on. Besides, lack of competence may also lead to wrong system operation. HAZOP is one of the most commonly used techniques in the offshore industry (Khamidi and John, 2011). Dynamic positioning system can be analyzed through HAZOPs to identify the potential risk during a normal operation. Based on our experience related to risk analysis for harsh environment and experience from working in the South China Sea, we present a DP loss of position risk analysis in Table 1.

We review here the risk for "*DP loss of position*" by evaluating potential failure modes and their consequences. Mitigating measures are suggested. It should be noted that the Table 1 also specifies generic hazards; specific aspects for the harsh environment are highlighted in italic letters.

4 CONCLUSION

There is limited experience about using the DP system in harsh condition such as arctic condition and it is not a very mature technology being used in the harsh environment, such as the Arctic area. To have a safe operational, the resistance to loss of position and the robustness of the recovery as the key parameters for safe dynamic positioning operation of a drilling rig should be evaluated considering all influence factors. Loss of position when using DP systems in harsh operational condition is a major hazard and for a Mobile Offshore Drilling Unit (MODU), loss of position without safe disconnection could result in critical damage not only to the well, but also to the subsea equipment. Hence, the reliability of the DP methods should be considered by for example training and using the appropriate level of redundancy. Moreover, a well establish plan for safe disconnection and reconnection when the loss of position is occur should be established. To achieve this goal at first stage all influence operational conditions should be identified and their effect should be quantified.

REFERENCES

Bakken, B. & Smedvig, T. Risk Associated with Drive-Off/Drift-Off when Drilling on DP. Dynamic Positioning Conference in Norway, 2001.

Bird, K.J. 2008. *Circum-Arctic resource appraisal: Estimates of undiscovered oil and gas north of the Arctic Circle*, US Department of the Interior, US Geological Survey.

Chen, H., Moan, T. & Verhoeven, H. 2008. Safety of dynamic positioning operations on mobile offshore drilling units. *Reliability Engineering & System Safety,* 93, 1072–1090.

Chen, H., Moan, T. & Verhoeven, H. 2009. Effect of DGPS failures on dynamic positioning of mobile drilling units in the North Sea. *Accident Analysis & Prevention,* 41, 1164–1171.

Faÿ, H. 1990. *Dynamic positioning systems: Principles, design and applications*, Editions OPHRYS.

Fougere, P. Improving the Reliability and Availability of Dynamic Positioning Systems. SPE/IADC Drilling Conference, 2005. Society of Petroleum Engineers.

Hals, T. & Jenssen, N.A. DP Ice Model Test Of Arctic Drillship and Polar Research Vessel. ASME 2012 31st International Conference on Ocean, Offshore and Arctic Engineering, 2012. American Society of Mechanical Engineers, 467–472.

Haveman, C., Parliament, J., Sokol, J., Swenson, J. & Wagner, T. 2006. Design of a Floating, Production, Storage, and Offloading Vessel for Operation in The South China Sea. *Final Report, Texas A&M University*.

Jenssen, N.A., Muddesitti, S., Phillips, D. & Backstrom, K. DP in ice conditions. Dynamic Positioning Conference, 2009. 13–14.

Kayrbekova, D., Barabadi, A. & Markeset, T. 2011. Maintenance cost evaluation of a system to be used in Arctic conditions: a case study. *Journal of Quality in Maintenance Engineering,* 17, 320–336.

Khamidi, M.F. & John, K.V. Operational risk assessment framework of mobile mooring system. National Postgraduate Conference (NPC), 2011, 2011. IEEE, 1–6.

Kuehnlein, W. Philosophies for dynamic positioning in ice-covered waters. Offshore Technology Conference, OTC, 2009.

Li JR, T. 2013. DP systems for offshore vessel positioning in deep water.

Millmaker, A., Yu, L. & Adlam, J. The Challenges of Lufeng 22-1 Development. Offshore Technology Conference, 1997. Offshore Technology Conference.

Tjallema, A., Van Der Nat, C., Grimmelius, H. & Stapersma, D. The road to eliminating operator related dynamic positioning incidents. Dynamic Positioning Conference, 2007.

Wilkman, G., Suojanen, R.-A., Saarinen, S., Mattsson, T. & Leiviskä, T. DP in ice conditions—challenges and opportunities. Dynamic positioning conference, Houston, 2009.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Wear time-dependent reliability analysis using Bayesian inference

J. Feng, J. Zhang, J. Si & P. Wang
Science and Technology on Reliability and Environmental Engineering Laboratory, Beihang University, Beijing, China
School of Reliability and Systems Engineering, Beihang University, Beijing, China

ABSTRACT: Wear is one of the most important reasons for failures of mechanical systems and components. This paper presents a simulation approach for reducing the uncertainty in the wear time-dependent reliability analysis for a pin of a lifting mechanical system. The wear time-dependent reliability modeling of the pin is established based on Archard theory, and the material parameters, elastic modulus and Poisson's ratio are treated as uncertain variables. Then, Bayesian inference is used to incorporate the new information to update the probability density functions of elastic modulus and Poisson's ratio, and reduce the uncertainty. Wear time-dependent reliability of the pin before and after updating are evaluated using PHI2 method which is based on the up-crossing rate approach and allows to solve time-dependent problems using classical time-invariant reliability tools such as FORM/SORM methods.

1 INTRODUCTION

It is generally known that wear is one of three major causes of failures (wear, corrosion and fatigue) of mechanical systems and components. In general, wear is a gradual process, and the consequences of wear are not disastrous. Therefore people pay little attention to the importance of wear. In fact, the economic loss caused by the wear failure of mechanical equipment is enormous. Based on relevant data (Tung & McMillan 2004): about 70% of the mechanical equipment damage is caused by various forms of wear; US's annual economic loss caused by the wear is about 4 percent of its Gross National Product (GNP). Therefore, the wear reliability analysis and evaluation for mechanical systems and components is very important in scientific research and engineering.

Due to influences of measurement error, manufacturing, assembly and other factors, there is uncertainty in mechanical components' geometry size, material properties parameters (such as elastic modulus, Poisson's ratio), and so on. The uncertainty significantly affects the reliability of the mechanical components. Therefore, it is important to choose appropriate distributions of random variables before wear reliability analysis. The traditional probability theory method is one of common methods which are used to deal with the uncertainty of variables. However, the method of probability and statistics is subject to restrictions of sample size, sampling time and sample conditions. Sometimes, because sample size is too small, it is impossible to obtain the probability density functions of random variables.

When prior information about random variables is scarce, Bayesian inference method can reduce random variables uncertainty through integrating new information with prior information effectively. Based on Bayesian inference, we can obtain accurate reliability analysis results. Although Bayesian inference method has been widely used in some engineering fields (Rusk et al. 2011, Zhang & Mohammadian 2008, Zhang et al. 2009), few studies on its applications in mechanical time-dependent reliability area have been performed. A pin, the key component of a lifting mechanical system, is researched in this paper. Firstly, the elastic modulus and Poisson's ratio of the pin are considered as random variables; secondly, the wear time-dependent reliability model of the pin is established based on Archard wear theory; thirdly, the probability density functions of elastic modulus and Poisson's ratio are updated by Bayesian inference method in order to reduce the uncertainty; finally, based on PHI2 method, three examples about wear time-dependent reliability of the pin are analyzed: (i) updating elastic modulus only; (ii) updating Poisson's ratio only; (iii) updating both elastic modulus and Poisson's ratio.

2 WEAR MODEL OF THE PIN BASED ON ARCHARD THEORY

2.1 *Archard wear model*

The Archard model is one of the wear models which are widely accepted in engineering. It is firstly proposed by R. Holm, and then is developed

by Archard et al. The Archard model is given by (Archard 1953)

$$W = K\frac{PS}{H} \tag{1}$$

where W is the wear volume, K is the coefficient of wear, P is the normal load, S is the sliding distance, and H is Brinell hardness of materials.

2.2 *Weal model of the pin*

The diagram of a lifting mechanical system is shown in Figure 1. The lifting mechanical system consists of a lifting platform, 2 connecting rods, 2 cylinders, a pedestal, several hinges and so on. The lifting mechanical system is used to lifting the antenna. The pedestal is used to support the whole system, the lifting platform is used to install the antenna, the two connecting rods are used to transmit motion and force, and the cylinders are used to provide the driving force.

By Failure Mode, Effects and Criticality Analysis (FMECA) of the lifting mechanical system, it is found that the pin is one of the key components which have significant influence on system reliability, and the failure mechanism of the pin is wear. The finite element model of the lifting mechanical system shown in Figure 2 is established in ABAQUS. The ring in Figure 2 is the position that the pin is located in. During this process of lifting the antenna repeatedly, wear volume of the pin increases with an increasement in the number of lifting. According to Archard wear theory, after the lifting mechanical system lifting the antenna n times, the actual wear volume of the pin is given by:

$$W(n) = K\frac{PS}{H}n \tag{2}$$

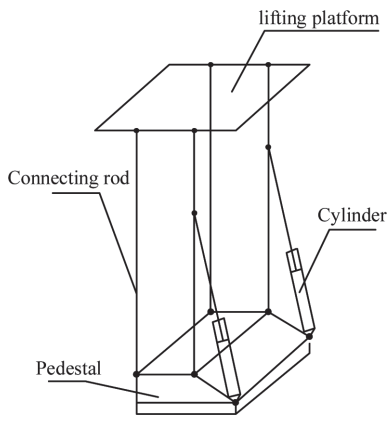


Figure 1. Diagram of the lifting mechanical system.

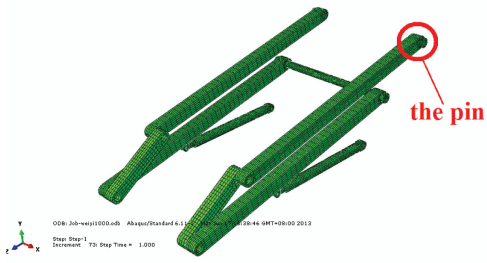


Figure 2. Finite element model of the lifting mechanical system.

where the sliding distance S is given as:

$$S = \frac{\pi}{2}r_1 \tag{3}$$

where r_1 is radius of curvature of the pin.

According to Hertz contact theory, the normal load P which the pin is subjected to, is given by:

$$P = \frac{\pi\sigma^2 r_1 r_2\left(\frac{1-\nu_1^2}{E_1}+\frac{1-\nu_2^2}{E_2}\right)L}{r_2 - r_1} \tag{4}$$

where σ is contact stress, r_1 is radius of curvature of the pin, r_2 is radius of curvature of the hole in the connecting rod, ν_1 is Poisson's ratio of the pin, ν_2 is Poisson's ratio of the connecting rod, E_1 is elastic modulus of the pin, E_2 is elastic modulus of the connecting rod, and L is the length of contact line, given by:

$$L = \pi r_1 \tag{5}$$

Substitute Eq. (3), Eq. (4) and Eq. (5) into Eq. (2) to obtain the wear model of the pin based on Archard wear theory:

$$W(n) = \frac{K}{2H}\frac{\pi^3\sigma^2 r_1^3 r_2\left(\frac{1-\nu_1^2}{E_1}+\frac{1-\nu_2^2}{E_2}\right)}{r_2 - r_1}n \tag{6}$$

3 BAYESIAN INFERENCE

Accurate estimates of the Probability Density Functions (PDFs) of random variables require large amount of data. However, in most engineering cases, the number of samples that can be obtained is ex-tremely limited, sometimes even cannot obtained. So the traditional probability statistical method is no longer applicable. In such circumstances, Bayesian inference method offers a workable solution, and

by integration of prior information with new information, it can be used to estimate the PDFs of random variables accurately.

Bayesian inference forms a normative and rational method for the probability updating when new information is made available (Karandikar et al. 2012). Considering a random variable X, let the prior PDF of X be $f(x)$, which expresses the uncertainty about X before the new information is taken into account. And let the likelihood function of X be $L(\theta|x)$, when new information θ is obtained. Then, the posterior PDF $f(x|\theta)$ of the random variable X can be obtained using the Bayes theorem (Zhu & Frangopol 2013):

$$f(x|\theta) = kL(\theta|x)f(x) \tag{7}$$

where k is a normalizing constant, given as (Zhu & Frangopol 2013):

$$k = \left(\int_{-\infty}^{+\infty} L(\theta|x)f(x)dx\right)^{-1} \tag{8}$$

It is noticed from Eq. (7) that the PDF of the random variable X is updated from the prior $f(x)$ to the posterior $f(x|\theta)$ by incorporating the new information θ. The posterior $f(x|\theta)$ expresses the uncertainty about X after the new information θ is taken into account.

4 TIME-DEPENDENT RELIABILITY ANALYSIS BASED ON PHI2 METHOD

Let us assume generalized stress to be $s(t)$, and generalized strength to be r. Mechanical products failure, when generalized stress exceeds general strength. The time-dependent limit state function of mechanical products is given by:

$$g(t, X) = r - s(t, X) \tag{9}$$

where X is the basic random variables, and t is time.

Let us define the instantaneous probability of failure of the mechanical products at time t by:

$$P_{f,i}(t) = \text{Prob}(g(t, X) \le 0) \tag{10}$$

This probability does not take into account what happened before t. It is independent of the previous states, i.e. it is not a conditional probability. It is computed by considering time as a fixed parameter in Eq. (10).

Let the up-crossing rate be $v(t)$. The key to time-dependent reliability analysis using PHI2 method is $v(t)$ (Andrieu-Renauda et al. 2004). Before computing $v(t)$, let us define two events:

$$\begin{cases} A = \{\exists t \in [0, T_f] | g(t, \boldsymbol{X}) > 0\} \\ B = \{\exists t \in [0, T_f] \,|\, g(t + \Delta t, \boldsymbol{X}) \le 0\} \end{cases} \tag{11}$$

where the two events are:
A = {mechanical products are in the safe domain at t}
B = {mechanical products are in the failure domain at $t + \Delta t$}

Then, the up-crossing rate $v(t)$ is defined by a limit formula (Andrieu-Renauda et al. 2004):

$$v(t) = \lim_{\Delta t \to 0} \frac{\text{Prob}(A \cap B)}{\Delta t} \tag{12}$$

According to Eq. (12), as long as we calculate the value of Prob($A \cap B$), we can obtain the value of $v(t)$. Figure 3 illustrates the probability of $A \cap B$ in FORM approximation (First Order Reliability Method) in the space of the standard variables $U = T(X)$ where T is an isoprobabilistic transformation. In this figure, $\beta(t)$ and $\beta(t + \Delta t)$ are respective the reliability indices of the events A and B. $\mathbf{n}(t)$ and $\mathbf{n}(t + \Delta t)$ are respective the unit normal vectors of A and B. ϕ_2 represents the probability density function of the binormal law. The probability $A \cap B$ is represented by the integral of ϕ_2 over the hatched volume.

Let us denote by ρ_t the correlation between A and B. The probability of $A \cap B$ is then, in FORM approximation (Andrieu-Renauda et al. 2004):

$$P(A \cap B) = \Phi_2(\beta(t), -\beta(t + \Delta t); \rho_t) \tag{13}$$

where Φ_2 is the binormal cumulative distribution function. And ρ_t is computed by (Mejri et al. 2010):

$$\rho_t = -\mathbf{n}(t) \cdot \mathbf{n}(t + \Delta t) = -\frac{\mathbf{x}^*(t)}{\beta(t)} \cdot \frac{\mathbf{x}^*(t + \Delta t)}{\beta(t + \Delta t)} \tag{14}$$

where $\mathbf{x}^*(t)$ and $\mathbf{x}^*(t + \Delta t)$ are respective Most Probable Point (MPP) at time t and $t + \Delta t$ in the standard normal space.

The reliability indices $\beta(t)$ and $\beta(t + \Delta t)$ are computed by considering time as a fixed parameter, i.e. using a time-invariant reliability analysis. Then the up-crossing rate is approximated by (Mejri et al. 2010):

$$v(t) \approx \frac{\Phi_2(\beta(t), -\beta(t + \Delta t); \rho_t)}{\Delta t} \tag{15}$$

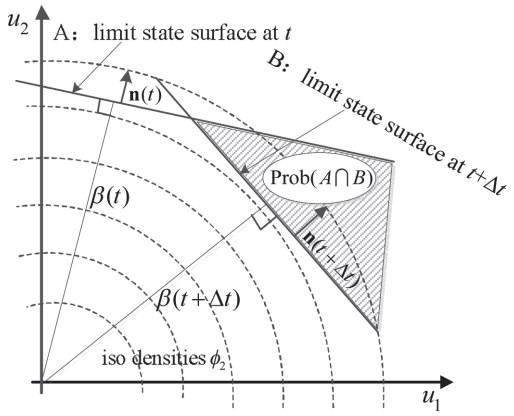


Figure 3. Computing $A \cap B$ based on FORM.

The binormal cumulative distribution function Φ_2 can be computed by using:

$$\Phi_2(\beta(t), -\beta(t+\Delta t); \rho_t) = \Phi(\beta(t))\Phi(-\beta(t+\Delta t)) + \int_0^{\rho_t} \frac{1}{2\pi\sqrt{1-z^2}} \exp\left\{-\frac{1}{2(1-z^2)}(\beta^2(t)+\beta^2(t+\Delta t) + 2z\beta(t)\beta(t+\Delta t))\right\} dz \quad (16)$$

Knowing the initial instantaneous probability of failure and the up-crossing rate $v(t)$, it is possible to compute an upper bound of the cumulative probability of failure of mechanical products within the time interval [0, T_f] by (Mejri et al. 2010):

$$P_{f,c}(0,T_f) \le P_{f,i}(0) + \int_0^{T_f} v(t)dt \quad (17)$$

5 TIME-DEPENDENT RELIABILITY ANALYSIS FOR THE PIN USING BAYESIAN INFERENCE

The lifting mechanical system discussed in this paper is made out of ASTM 1045 steel. And the values of parameters of the pin are given in Table 1.

In order to facilitate the calculation, only random variables of the pin are taken into account in this paper. The elastic modulus E_2 and Poisson's ratio ν_2 of the connecting rod are assumed to be deterministic, and the values of the two parameters are respective $E_2 = 206.000$ MPa, $\nu_2 = 0.269$.

In this paper, the finite element software ABAQUS is adopted to simulate and analyse the process of the lifting mechanical system lifting the antenna. The simulation shows that the ultimate stress of the pin during the process is $\sigma = 109.5$ MPa, and Figure 4 shows the stress nephogram of the pin.

Table 1. The values of parameters of the pin.

Parameters	Mean	Standard deviation
K	0.5×10^{-9}	–
H	286 HB	–
ρ_1	60 mm	–
E_1	200,000 MPa	11547 MPa
ν_1	0.26	0.01154

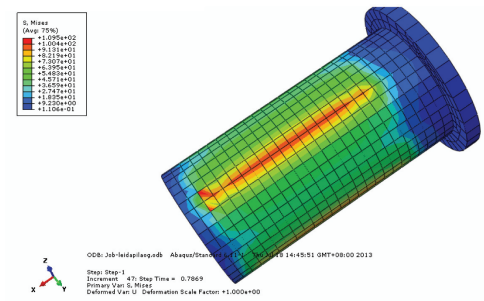


Figure 4. The stress nephogram of the pin.

Let the permitted value of the wear volume of the pin be W, and assume that W follow normal distribution with the mean of $\mu_W = 5$ mm^3 and the standard deviation $\sigma_W = 0.5$ mm^3. When the actual wear volume $W(n)$ exceeds W, the pin failures. According to Eq. (6) and Eq. (9), after the lifting mechanical system lifting the antenna n times, the time-dependent limit state function of the pin is

$$g(n,X) = W - \frac{K}{2H} \frac{\pi^3 \sigma^2 r_1^3 r_2 \left(\frac{1-\nu_1^2}{E_1} + \frac{1-\nu_2^2}{E_2}\right)}{r_2 - r_1} n \quad (18)$$

where X is the basic random variables of the wear model of the pin, and X is expressed as $[E_1, \nu_1]$.

5.1 *Wear time-dependent reliability analysis for the pin before Bayesian updating*

Assume that both of prior distributions of E_1 and ν_1 follow uniform distribution, and E_1 and ν_1 are independent of each other. Prior distributions for E_1 and ν_1 are selected as: $E_1 \sim U(a_1, b_1)$, $\nu_1 \sim U(a_2, b_2)$, where

$$\begin{cases} a_1 = \mu_{E_1} - \sqrt{3}\sigma_{E_1} = 180{,}000\,\text{MPa} \\ b_1 = \mu_{E_1} + \sqrt{3}\sigma_{E_1} = 220{,}000\,\text{MPa} \end{cases}$$

$$\begin{cases} a_2 = \mu_{\nu_1} - \sqrt{3}\sigma_{\nu_1} = 0.24 \\ b_2 = \mu_{\nu_1} + \sqrt{3}\sigma_{\nu_1} = 0.28 \end{cases}$$

and μ_{E_1} and σ_{E_1} are respective the mean and standard deviation of E_1; μ_{ν_1} and σ_{ν_1} are respective the mean and standard deviation of ν_1.

The prior PDFs of E_1 and ν_1 are respective:

$$f_{E_1}(x)=\begin{cases}\dfrac{1}{40000}, & 180,000\le x\le 220,000\\ 0, & otherwise\end{cases} \tag{19}$$

$$f_{\nu_1}(y)=\begin{cases}\dfrac{1}{0.04}, & 0.24\le y\le 0.28\\ 0, & otherwise\end{cases} \tag{20}$$

Before the PDFs of E_1 and ν_1 are updated, according to Eq. (18), the wear time-dependent reliability analysis results of the pin within the interval [0, n] is obtained using PHI2 method. The results are shown in Figure 5, where n is the number of the lifting mechanical system lifting the antenna, and $n = 4200$.

It is found from Figure 5 that: (i) the upper bound of cumulative probability of failure gradually increases with the increasement of n; (ii) the lower bound of the reliability of the pin gradually decreases with the increasement of n; (iii) the upper bound of cumulative probability of failure and the lower bound of the reliability are respective 0.4626 and 0.5374 within the interval [0, n].

5.2 *Wear time-dependent reliability analysis for the pin after Bayesian updating*

5.2.1 *Bayesian updating of random variables*

1. Update elastic modulus E_1

According to Bayesian inference method, the posterior distribution is proportional to the product of the prior distribution and likelihood functions. Under given the prior PDF of E_1, if we want to obtain the posterior PDF, we must firstly define the likelihood function. Based on the new information (Yu & Zhang 2011), the elastic modulus

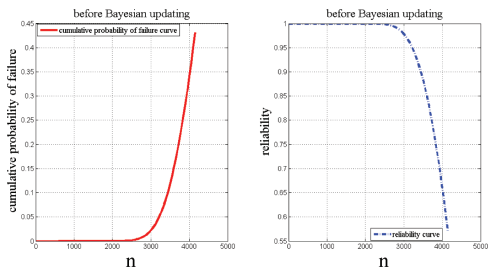


Figure 5. Reliability analysis results before Bayesian updating.

E of ASTM 1045 steel is subject to a normal distribution with the mean of 206,000 MPa and the variance of 6180^2 MPa^2. Therefore we can assume that the likelihood function of the elastic modulus E_1 is:

$$L_{E_1}(x)=\frac{1}{\sqrt{2\pi}\sigma_E}\exp\left(-\frac{(x-\mu_E)^2}{2\sigma_E^2}\right) \tag{21}$$

where, $\mu_E = 206{,}000$ MPa and $\sigma_E = 6180$ MPa.

Based on Eq. (7), the posterior PDF of E_1 is

$$f'_{E_1}(x)=\frac{1}{K_{E_1}}L_{E_1}(x)\quad 180,000\le x\le 220,000 \tag{22}$$

where K_{E_1} is a constant, given as (Christian 1995)

$$K_{E_1}=\int_{a_1}^{b_1}L_{E_1}(x)dx=\Phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)-\Phi\left(\frac{a_1-\mu_E}{\sigma_E}\right) \tag{23}$$

Therefore, the posterior PDF of E_1 follows a truncated normal distribution within the interval [a_1, b_1], and the cumulative distribution function of E_1 is (Christian 1995):

$$F'_{E_1}(x)=\frac{1}{K_{E_1}}\left(\Phi\left(\frac{x-\mu_E}{\sigma_E}\right)-\Phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)\right) \tag{24}$$

After Bayesian updating, the mean and variance of E_1 are respective (Christian 1995):

$$\mu'_{E_1}=\sigma_E\left(\frac{\phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)-\phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)}{\Phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)-\Phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)}\right)+\mu_E \tag{25}$$

$$\sigma'^{2}_{E_1}=\sigma_E^2\left(1+\frac{\frac{a_1-\mu_E}{\sigma_E}\phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)-\frac{b_1-\mu_E}{\sigma_E}\phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)}{\Phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)-\Phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)}\right)-\sigma_E^2\left(\frac{\phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)-\phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)}{\Phi\left(\frac{b_1-\mu_E}{\sigma_E}\right)-\Phi\left(\frac{a_1-\mu_E}{\sigma_E}\right)}\right)^2 \tag{26}$$

where ϕ represents the PDF of standard normal distribution.

Substituting values of a_1, b_1, μ_E, and σ_E back into Eq. (25) and Eq. (26) yields $\mu'_{E_1} = 206{,}190$ MPa and

$\sigma'_{E_1} = 5955$ MPa . After updating, the coefficient of variance of E_1 is $C.V'_{E_1} = \sigma'_{E_1}/\mu'_{E_1} = 0.0289$.

Comparing the posterior of E_1 with the prior, it is found that after Bayesian updating: (i) the distribution type of E_1 changes from the assumed uniform distribution to truncated normal distribution, as shown in Figure 6; (ii) the mean of E_1 increases, changing from 200,000 MPa to 206,190 MPa; (iii) the standard deviation of E_1 decreases significantly, changing from 11,547 MPa to 5955 MPa; (iv) the coefficient of variance also decreases significantly, changing from 0.0577 to 0.0289. We can see easily from the above point (ii) ~ point (iv): integration of the new information dramatically reduces the uncertainty of E_1.

2. Update Poisson's ratio ν_1

The updating process of ν_1 is the same as E_1. According to the new information (Yu & Zhang 2011), the Poisson's ratio of ASTM 1045 steel is subject to a normal distribution with the mean of 0.269 and the variance of 0.00807^2. So we can define the likelihood function of ν_1 of the pin as:

$$L_{\nu_1}(y) = \frac{1}{\sqrt{2\pi}\sigma_\nu}\exp\left(-\frac{(y-\mu_\nu)^2}{2\sigma_\nu^2}\right) \tag{27}$$

where, $\mu_\nu = 0.269$ and $\sigma_\nu = 0.00807$.

According to Eq. (7), the posterior PDF of ν_1 is:

$$f'_{\nu_1}(y) = \frac{1}{K_{\nu_1}} L_{\nu_1}(y) \quad 0.24 \le y \le 0.28 \tag{28}$$

where K_{ν_1} is a constant, given as (Christian 1995):

$$K_{\nu_1} = \int_{a_2}^{b_2} L_{\nu_1}(y)dy = \Phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right) - \Phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right) \tag{29}$$

Therefore the posterior PDF of ν_1 follows a truncated normal distribution within the interval $[a_2, b_2]$, and the cumulative distribution function of ν_1 is (Christian 1995):

$$F'_{\nu_1}(y) = \frac{1}{K_{\nu_1}}\left(\Phi\left(\frac{y-\mu_\nu}{\sigma_\nu}\right) - \Phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right)\right) \tag{30}$$

After Bayesian updating, the mean and variance of ν_1 are respective (Christian 1995):

$$\mu'_{\nu_1} = \sigma_\nu\left(\frac{\phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right) - \phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right)}{\Phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right) - \Phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right)}\right) + \mu_\nu \tag{31}$$

$$\sigma'^2_{\nu_1} = \sigma_\nu^2\left(1 + \frac{\frac{a_2-\mu_\nu}{\sigma_\nu}\phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right) - \frac{b_2-\mu_\nu}{\sigma_\nu}\phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right)}{\Phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right) - \Phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right)}\right) - \sigma_\nu^2\left(\frac{\phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right) - \phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right)}{\Phi\left(\frac{b_2-\mu_\nu}{\sigma_\nu}\right) - \Phi\left(\frac{a_2-\mu_\nu}{\sigma_\nu}\right)}\right)^2 \tag{32}$$

The coefficient of variance of ν_1 is $C.V'_{\nu_1} = \sigma'_{\nu_1}/\mu'_{\nu_1} = 0.0256$ after updating.

Comparing the posterior of ν_1 with the prior, it is found that after Bayesian updating: (i) the distribution type of ν_1 changes from the assumed uniform distribution to the truncated normal distribution, as shown in Figure 7; (ii) the mean of ν_1 increases, changing from 0.26 to 0.2704; (iii) the standard deviation of ν_1 decreases significantly, changing from 0.01154 to 0.00691; (iv) the coefficient of variance also decreases significantly, changing from 0.0444 to 0.0256. The trend in ν_1 is the same as E_1. Integration of the new information dramatically reduces the uncertainty of ν_1.

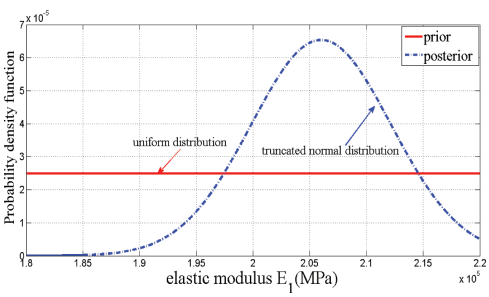


Figure 6. Prior and posterior PDFs of E_1.

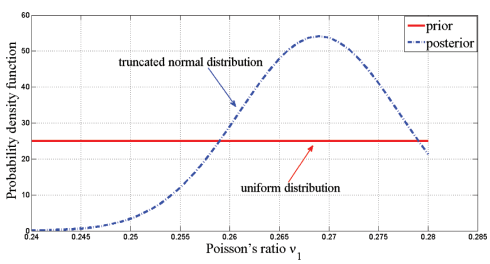


Figure 7. Prior and posterior PDFs of ν_1.

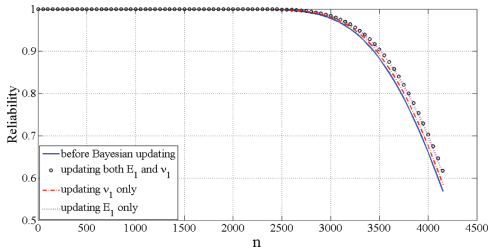


Figure 8. Reliability before and after Bayesian updating.

5.2.2 *Time-dependent reliability analysis for the pin after Bayesian updating*

After Bayesian updating, both of distribution types of E_1 and ν_1 change, which may lead to obvious changes in reliability results. Based on PHI2 method, three cases are analyzed herein: (i) ν_1 is treated as deterministic while E_1 is considered as a random variable to be updated; (ii) E_1 is treated as deterministic while ν_1 is considered as a random variable to be updated; (iii) update both E_1 and ν_1, assuming that they are statistically independent.

After Bayesian updating, the wear time-dependent reliability analysis results of the pin are shown in Figure 8.

We use the wear time-dependent reliability curve after updating both E_1 and ν_1 as the baseline, shown as the curve with circular makers in Figure 8, and we can see from Figure 8:

1. Based on prior distributions of E_1 and ν_1, the reliability result of the pin is conservative compared with the baseline;
2. Compared with ν_1, E_1 has greater influence on the reliability result. Because after updating E_1 only, the wear time-dependent reliability curve is more close to the baseline;
3. Under the condition of updating only one random variable (either updating E_1 or ν_1), the reliability result is conservative compared with the baseline. The accuracy of the reliability results depends on random variables. The more abundant the statistical information about random variables is, the higher the accuracy of the reliability result is.

6 CONCLUSION

This paper presents a simulation approach for reducing the uncertainty in the wear time-dependent reliability analysis for the pin of the lifting mechanical system. Bayesian inference is performed to update the PDFs of elastic modulus E_1 and Poisson's ratio ν_1. Then, based on PHI2 method, three examples about wear time-dependent reliability are analyzed: (i) updating E_1 only; (ii) updating ν_1 only; (iii) updating both E_1 and ν_1. The following conclusions are drawn:

1. In order to reduce uncertainty, Bayesian inference is proposed to incorporate the new information with the prior information. After Bayesian updating: (i) distributions of E_1 and ν_1 change; (ii) both the variances of E_1 and ν_1 decrease significantly; (iii) both the coefficients of variance of E_1 and ν_1 decrease significantly. So the uncertainty is reduced dramatically, and the random variables are more closer to their true statistical distributions;
2. It is not appropriate to deal with wear time-dependent reliability analysis based on prior information, and the reliability analysis result is conservative compared with the result after updating. The reason is that there is not enough information to describe the statistical nature of the random variables accurately;
3. The influences of different random variables on the reliability results are different;
4. If sufficient new information become available in the future, to ensure the accuracy of reliability results, the correlations among E_1 and ν_1 need to be taken into account.

ACKNOWLEDGEMENT

The authors express sincere appreciation to the editor and reviewers for their efforts to improve the quality of the paper. This work is supported by Space Mechanisms Reliability and its Dynamics and System Control, National Basic Research Program of China (2013CB733000).

REFERENCES

Andrieu-Renauda, C., Sudret, B., Lemaire, M., 2004. The PHI2 method: a way to compute time-variant reliability. *Reliability Engineering and System Safety,* 84(1): 75–86.

Archard, J.F., 1953. *Contact and Rubbing of Flat Surface*. J. Appl. Phis. 24(8): 981–988.

Christian, P.R., 1995. Simulation of truncated normal variables. *Statistics & Computing,* 5(2): 121–125.

Karandikar, J.M., Kim, N.H., Schmitz, T.L., 2012. Prediction of remaining useful life for fatigue-damaged structures. *Engineering Fracture Mechanics,* 18(96): 588–605.

Mejri, M., Cazuguel, M., Cognard, J.Y., 2010. A time-variant reliability approach for ageing marine structures with non-linear behavior. *Computers & Structures,* 89(19): 1743–1753.

Rusk, D.T., Lin, K.Y., Swartz, D.D., Ridgeway, G.K., 2011. Bayesian updating of damage size probabilities for aircraft structural life-cycle management. *J Aircraft,* 39(4): 689–96.

Tung, S.C. & McMillan, M.L., 2004. Automotive tribology overview of current advances and challenges for the future. *Tribology International,* 37(7): 517–536.

Yu, M. & Zhang, C., 2011. *Handbook of Steel Products*. Beijing: Chemical Industry Press. (in Chinese).

Zhang, J., Zhang, L.M., Tang, W.H., 2009. Bayesian framework for characterizing geotechnical model uncertainty. *J Geotech Geoenviron Eng,* 135(7): 932–40.

Zhang, Y. & Mohammadian, A., 2008. Bayesian updating of transferred household travel data. *Transportation Research Record,* 2049: 111–118.

Zhu, B.J. & Frangopol, D.M., 2013. Reliability assessment of ship structures using Bayesian updating. *Engineering Structures,* 56: 1836–1847.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

RAVEN and dynamic probabilistic risk assessment: Software overview

Andrea Alfonsi, Cristian Rabiti, Diego Mandelli, Joshua Cogliati & Robert Kinoshita
Idaho National Laboratory, Idaho Falls, USA

Antonio Naviglio
University "La Sapienza", Rome, Italy

ABSTRACT: Risk Analysis Virtual Environment (RAVEN) is a generic software framework to perform parametric and probabilistic analysis based on the response of complex system codes. The initial development was aimed at providing dynamic risk analysis capabilities to the Reactor Excursion and Leak Analysis Program v.7 (RELAP-7) Thermo-Hydraulic code, currently under development at the Idaho National Laboratory (INL). Although the initial goal has been fully accomplished, RAVEN is now a multi-purpose probabilistic and uncertainty quantification platform, capable to agnostically communicate with any system code. This agnosticism includes providing Application Programming Interfaces (APIs). These APIs are used to allow RAVEN to interact with any code as long as all the parameters that need to be perturbed are accessible through input files or via python interfaces. RAVEN is capable of investigating the system response as well as the input space using Monte Carlo, Grid, or Latin Hyper Cube sampling schemes, but its strength is focused toward system feature discovery, such as limit surfaces, separating regions of the input space leading to system failure, using dynamic supervised learning techniques. The paper presents an overview of the software capabilities and their implementation schemes followed by some application examples.

1 INTRODUCTION

1.1 *Initial development*

The development of RAVEN (Alfonsi, Rabiti, Mandelli, Cogliati, & Kinoshita 2013) started in 2012, when, within the Nuclear Energy Advanced Modeling and Simulation (NEAMS) program, the need to provide a modern risk evaluation framework became stronger. RAVEN's principal assignment is to provide the necessary software and algorithms in order to employ the concept developed by the Risk Informed Safety Margin Characterization (RISMC) (Smith, Rabiti, et al. 2012) program. RISMC is one of the pathways defined within the Light Water Reactor Sustainability (LWRS) program. In the RISMC approach, the goal is not just specifically identifying the frequency of an event potentially leading to a system failure, but the closeness (or not) to key safety-related events. This approach may be used in identifying and increasing the safety margins related to those events. A safety margin is a numerical value quantifying the probability that a safety metric (e.g. as peak pressure in a pipe) is exceeded under certain conditions.

The initial development of RAVEN has been focused on providing dynamic risk assessment capability to RELAP-7, currently under development at the INL and, likely, future replacement of the RELAP5-3D (RELAP5-3D Team, 2009) code.

Most of the capabilities implemented having RELAP-7 as principal focus are easily deployable for other system codes. For this reason, several side activities are currently ongoing for coupling RAVEN with software such as BISON, fuel performance, (Williamson, Hales, et al. 2012), RELAP5-3D. This paper is focused on the RAVEN software infrastructure and its functionality.

2 SOFTWARE INFRASTRUCTURE

2.1 *Outlines*

RAVEN has been developed in a highly modular and pluggable way in order to enable easy integration of different programming languages (i.e., C++, Python) and, as already mentioned, coupling with any system code.

RAVEN is composed of three main software systems that can operate either in coupled or stand-alone mode:

- Control Logic System
- Graphical User Interface
- Probabilistic and Parametric framework

The control logic system and the Graphical User Interface are currently available for RELAP-7 only. For this reason, attention is focused on the probabilistic and parametric framework.

2.2 *Probabilistic and parametric framework*

The probabilistic and parametric framework represents the core of the RAVEN analysis capabilities. The main idea behind the design of the system is the creation of a multi-purpose framework characterized by high flexibility with respect to the possible performable analysis. The framework must be capable of constructing the analysis/calculation flow at run-time, interpreting the user-defined instructions and assembling the different analysis tasks following a user specified scheme.

In order to achieve such flexibility, combined with reasonably fast development, a programming language naturally suitable for this kind of approach was needed: Python.

Hence, RAVEN is coded in Python and is characterized by an object-oriented design. The core of the analysis performable through RAVEN is represented by a set of basic components (objects) the user can combine, in order to create a custom analysis flow. A list of these components and a summary of their most important functionalities are reported as follows:

- *Distribution*: In order to explore the input/output space, RAVEN requires the capability to perturb the input space (initial conditions of a system code). The initial conditions, that represent the uncertain space, are generally characterized by Probability Distribution Functions (PDFs), which need to be considered when a perturbation is applied. In this respect, a large library of PDFs is available.
- *Sampler*: A proper approach to sample the input space is fundamental for the optimization of the computational time. In RAVEN, a "sampler" employs a unique perturbation strategy that is applied to the input space of a system. The input space is defined through the connection of uncertain variables and their relative probability distributions.
- *Model*: A model is the representation of a physical system (e.g. Nuclear Power Plant); it is therefore capable of predicting the evolution of a system given a coordinate set in the input space.
- *Reduced Order Model (ROM)*: The evaluation of the system response, as a function of the coordinates in the input space, is very computationally expensive, especially when brute-force approaches (e.g. Monte Carlo methods) are chosen as the sampling strategy. ROMs are used to lower this cost, reducing the number of needed points and prioritizing the area of the input space that needs to be explored. They can be considered as an artificial representation of the link between the input and output spaces for a particular system.

The list above is not comprehensive of all the RAVEN framework components (visualization and storage infrastructure).

2.2.1 *Distribution*

As already mentioned, the perturbation of the input space, through the initial conditions (parameters) affected by uncertainties, needs to be performed by the proper distribution functions. RAVEN provides, through an interface to the BOOST library, the following univariate (truncated and not) distributions: Bernoulli, Binomial, Exponential, Logistic, Lognormal, Normal, Poisson, Triangular, Uniform, Weibull, Gamma, and Beta.

The usage of univariate distributions for sampling initial conditions is based on the assumption that the uncertain parameters are not correlated with each other. Quite often uncertain parameters are subject to correlations and thus the univariate approach is not applicable. This happens when a generic outcome is dependent on different phenomena simultaneously (i.e. the outcome dependency description can not be collapsed to a function of a single variable). RAVEN currently supports both N-Dimensional (N-D) PDFs. The user can provide the distribution values on either Cartesian or sparse grid, which determines the interpolation algorithm used in the evaluation of the imported CDF/PDF:

- N-Dimensional Spline (Habermann, & Kindermann 2007), for Cartesian grids
- Inverse weight (Gordon & Wixom 1978), for sparse grids

Internally, RAVEN provides the needed N-D differentiation and integration algorithms to compute the PDF from the CDF and vice versa.

As already mentioned, the sampling methods use the distributions in order to perform probability-weighted perturbations. For example, in the Monte Carlo approach, a random number $\in [0,1]$ is generated (probability threshold) and the CDF, corresponding to that probability, is inverted in order to retrieve the parameter value usable in the simulation. The existence of the inverse for univariate distributions is guaranteed by the monotonicity of the CDF. For N-D distributions this condition is not sufficient since the $CDF(X) \rightarrow [0,1]$, $X \in R^N$ and therefore it could not be a bijective function. From an application point of view, this means the inverse of a N-D CDF is not unique.

As an example, the Figure 1 shows a multivariate normal distribution for a pipe failure as

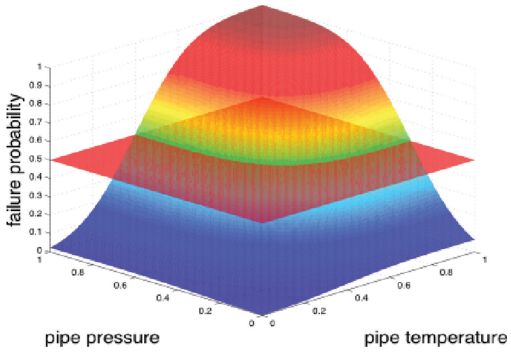


Figure 1. 2-D CDF, function of pressure and temperature.

function of the pressure and temperature. The plane identifies an iso-probability surface (in this case, a line) that represents a probability threshold of 50% in this example. Hence, the inverse of this CDF is an infinite number of points.

As easily inferable, the standard sampling approach cannot directly be employed. When multivariate distributions are used, RAVEN implements a surface search algorithm for identifying the iso-probability surface location. Once the location of the surface has been found, RAVEN chooses, randomly, one point on it.

2.2.2 *Sampler*

The sampler is probably the most important entity in the RAVEN framework. Indeed, it performs the driving of the specific sampling strategy and, hence, determines the effectiveness of the analysis, from both an accuracy and computational point of view. The samplers, that are available in RAVEN, can be categorized in three main classes:

- Once-through
- Dynamic Event Tree (DET)
- Adaptive

2.2.2.1 *Once-through samplers*

The once-through sampler category collects all the strategies that perform the sampling of the input space without exploiting, through dynamic learning approaches, the information made available from the outcomes of calculation previously performed (adaptive sampling) and the common system evolution (patterns) that different sampled calculations can generate in the phase space (dynamic event tree).

In the RAVEN framework, three different and well-known "once-through" samplers are available:

- Monte Carlo (MC)
- Latin Hyper Cube (LHS)
- Grid Based

As already mentioned, all these sampling strategies are well known, as well as their properties. Therefore, a detailed investigation of their application is not provided.

2.2.2.2 *Dynamic event tree sampler*

In order to clarify the idea behind the DET Sampler currently available in RAVEN, a small overview is needed.

In technological complex systems, as nuclear power plants, an accident scenario begins with an initiating event and then evolves over time through the interaction of dynamics and stochastic events. This mutual action leads to the production of infinitely many different scenarios, which define a continuous dynamic event tree with infinite branches. At each time point, the stochastic variability of the accident outcomes is determined by a multivariate probability distribution. The PRA analysis needs an approximation to this distribution for selected consequence variables. A way to achieve this goal is an Event Tree approach. In dynamic PRA analysis, conventional Event Tree (Alfonsi, Rabiti, Mandelli, Cogliati, Kinoshita, & Naviglio 2013) sequences are run simultaneously starting from a single initiating event. The branches occur at user specified times and/or when an action is required by the operator and/or the system, creating a deterministic sequence of events based on the time of their occurrence. One of the disadvantages of this method is that the timing/sequencing of events and system dynamics is not explicitly accounted for in the analysis. In order to overcome these limitations a "dynamic" approach is needed. The DET (Alfonsi, Rabiti, Mandelli, Cogliati, Kinoshita, & Naviglio 2013) technique brings several advantages, among which is the fact that it simulates probabilistic system evolution in a way that is consistent with the severe accident model. This leads to a more realistic and mechanistically consistent analysis of the system taken into consideration. The dynamic PRA, in general, and the DET methodologies in particular, are designed to take the timing of events explicitly into account, which can become very important especially when uncertainties in complex phenomena are considered. Hence, the main idea of this methodology is to let a system code determine the pathway of an accident scenario within a probabilistic "environment".

From an application point of view, a N-D grid is built on the CDF space. A single simulation is spawned and a set of triggers is added to the system code control logic. Every time a trigger gets activated (one of the CDF thresholds in the grid is overpassed), a new set of simulations (branches) is spawned. Each branch carries its own conditional probability.

As expected, a continuous monitoring of the system evolution in the phase space is needed.

Figure 2 shows a practical example. In this particular case, it is assumed that the probability failure of a pipe depends on the fluid pressure magnitude. Three probability thresholds are defined on the cumulative distribution function. One simulation is spawned (0). As soon as the pressure of the fluid reaches a value corresponding to a 33% probability (CDF), a stop signal is sent and the framework starts two new simulations (branches). The branch in which the system evolved to the newer condition (pipe failed, red line) carries 33% of the probability, while the other the complementary amount. The same procedure is repeated at point 2.

Generally, not all the input space can be explored using a DET approach. For instance, usually the parameters affected by aleatory uncertainty are sampled using a dynamic event tree approach, while the ones characterized by epistemic uncertainty are sampled through "once-through" sampling strategies. At the moment a hybrid approach ("once-through" sampling of initial conditions followed by a dynamic event tree strategy) is currently under development.

As already mentioned, this strategy requires a tight interaction between the system code and the sampling driver (i.e., RAVEN framework). In addition, the system code must have a control logic capability (i.e. trigger system). For these reasons, the application of this sampling approach to a generic code needs a bigger effort when compared to the other Samplers available in RAVEN. Currently, the DET is fully available for the thermal-hydraulic codes RELAP-7 and RELAP5-3D.

2.2.2.3 *Adaptive samplers*

A recent feature available within RAVEN is the possibility to perform smart sampling (also known as adaptive sampling) as an alternative to classical "once-through" techniques.

The motivation is that nuclear simulations are often computationally expensive, time-consuming, and high dimensional with respect to the number of input parameters. Thus, exploring the space of all possible simulation outcomes is infeasible using finite computing resources. During simulation-based probabilistic risk analysis, it is important to discover the relationship between a potentially large number of input parameters and the output of a simulation using as few simulation trials as possible.

This is a typical context for performing adaptive sampling where a few observations are obtained from the simulation, a Reduced Order Model (ROM) is built to represent the simulation space, and new samples are selected based on the model constructed. The ROM, discussed in section 2.2.4, is then updated based on the simulation results of the sampled points (see Fig. 3). In this way, it is attempted to gain the most information possible with a small number of carefully selected sampled points, limiting the number of expensive trials needed to understand features of the system space.

In the following, the specific use case of identifying the limit surface, i.e. the boundaries in the simulation space between system failure and system success (see Fig. 4) is analyzed.

For this scope two classes of algorithms are considered:

- Model-based algorithms
- Data-based algorithms

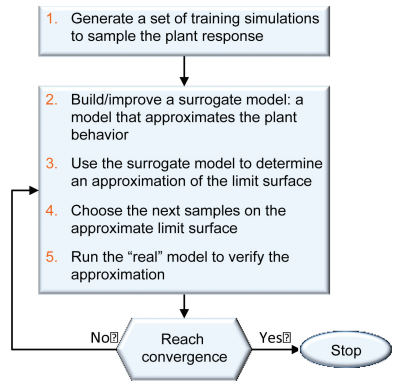


Figure 3. Adaptive sampling algorithm.

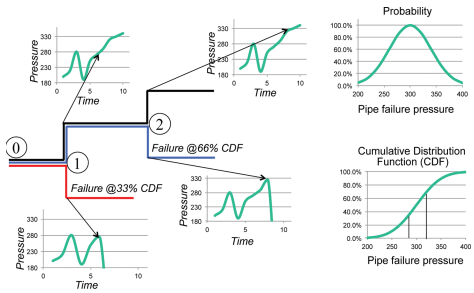


Figure 2. Dynamic event tree simulation pattern.

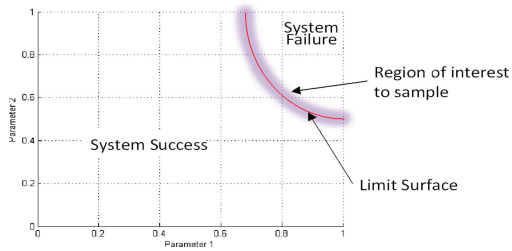


Figure 4. Graphical representation of the limit surface.

In the first class, the created ROM aims at approximating the real response function of the system as function of the input parameters. Once it is built, it is used to search for the points that are in the proximity of the limit surface using contour reconstruction based algorithms. Response function can be built using Support Vector Machines (SVM) (Mandelli & Smith 2012) or Kriging based interpolators (Mandelli, Smith, Rabiti, Alfonsi, et al. 2013).

On the other side, data-based algorithms do not build a response function based ROM but determine the location of the limit surface directly from the neighborhood graph constructed from the training data, without any dependencies on a particular prediction model.

These algorithms begin the search of the limit surface by directly building a neighborhood structure as the ROM (e.g. a relaxed Gabriel graph) (Mandelli, Smith, Rabiti, Alfonsi, et al. 2013) on the initial training data. It then creates a candidate set by first obtaining linearly interpolated points along spanning edges (i.e. edge of the graph that connect points having different outcomes) of the graph, and introducing a random perturbation along all dimensions to these points.

2.2.3 *Models*

The Model entity, in the RAVEN environment, represents a "connection pipeline" between the input and the output space. The RAVEN framework does not own any physical model (i.e. it does not posses the equations needed to simulate a generic system), but implements APIs by which any generic model can be integrated and interrogated. The RAVEN framework provides APIs for three different model categories: Codes, Externals and ROMs.

The Code model represents the communication pipe between the RAVEN and any system code. Currently, RAVEN has APIs for RELAP5-3D, RELAP-7 and any MOOSE (Gaston, Hansen, et al. 2009) based application.

The External model allows the user to create, in a Python file (imported, at run-time, in the RAVEN framework), its own model (e.g. set of equations representing a physical model, connection to another code, control logic, etc.). This model will be interpreted/used by the framework and, at run-time, will become part of RAVEN itself.

The data exchange between RAVEN and the system code can be performed either by direct software interface or by files. If the system code is parallelized, the data exchanging by files is generally the way to follow since it can be much more optimized in large clusters.

Figure 5 shows a schematic representation of the whole framework, highlighting the communication pipes among the different modules and engines. As can be seen, in the figure all the components discussed so far are reported. In addition the data management, mining and processing modules are shown.

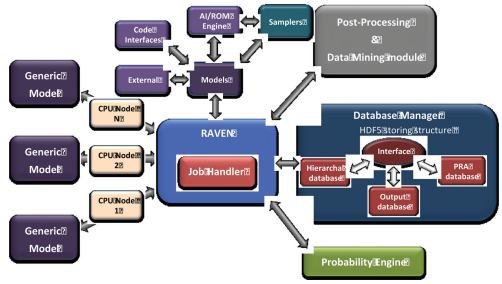


Figure 5. RAVEN probabilistic and parametric framework.

2.2.4 *Reduced order models*

As briefly mentioned, a ROM is a mathematical representation of a system, used to predict a selected output space of a physical system.

The "training" is a process that uses sampling of the physical model to improve the prediction capability (capability to predict the status of the system given a realization of the input space) of the ROM. More specifically, in RAVEN the reduced order model is trained to emulate a high fidelity numerical representation (system codes) of the physical system. Two general characteristics of these models can be generally assumed (even if exceptions are possible):

1. The higher the number of realizations in the training sets, the higher is the accuracy of the prediction performed by the reduced order model. This statement is true for most of the cases although some ROMs might be subject to the over-fitting issues. The over-fitting phenomenon is not discussed here, since its occurrence is highly dependent on the algorithm type, (and there is large number of ROM options available in RAVEN). Every time the user chooses a particular reduced order model algorithm to use, he should consult the relative literature.
2. The smaller the size of the input domain with respect to the variability of the system response, the more likely the surrogate model will be able to represent the system output space.

In most of the cases of interest, the information that is sought is related to defining the failure boundaries of a system with respect to perturbations in the input space. For this reason, in the development of RAVEN, it has been given priority to the introduction of a class of supervised learning algorithms, which are usually referred to as classifiers. A classifier is a reduced order model that is capable of representing the system behavior through a binary response (failure/success).

The first class of classifier introduced has been the SVM (Mandelli & Smith 2012) with several different kernels (polynomial of arbitrary integer order, radial basis function kernel, sigmoid) followed by a nearest-neighbor based classification using a K-D tree search algorithm. All these supervised learning algorithms have been imported via an API from the scikit-learn (Pedregosa et al. 2011) library. In addition, the N-D spline and the inverse weight methods, that are currently available for the interpolation of N-D PDF/CDF, can also be used as ROMs.

2.2.5 *Simulation environment*

RAVEN is perceived by the user as a pool of tools and data. Any action in which the tools are applied to the data is considered a 'step' in the RAVEN environment. For the scope of this paper, "multiRun" type of step will be described, since all others are either closely related (single run and adaptive run) or just used to perform data management and visualization. Firstly, the RAVEN input file associates the variable definition syntax to a set of PDFs and to a sampling strategy. The "multiRun" step is used to perform several runs (sampling) in a block of a model (e.g. in a MC sampling).

At the beginning of each sub sequential run, the sampler provides the new values of the variables to be modified. The code API places those values properly in the input file. At this point the code API generates the run command and asks to be queued by the job handler. The job handler manages the parallel execution of as many runs as possible within a user prescribed range and communicates with the step controller when a new set of output files are ready to be processed. The code API receives the new input files and collects the data in the RAVEN internal format. The sampler is queried to assess if the sequence of runs is ended, if not, the step controller asks for a new set of values from the sampler and the sequence is restarted as described in Figure 6.

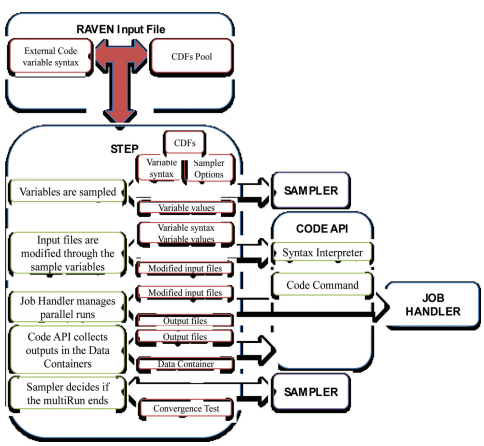


Figure 6. Calculation flow for a multi-run sampling.

The job handler is currently capable to run different run instances of the code in parallel and can also handle codes that are multi threaded or using any form of MPI parallel implementation.

RAVEN also has the capability to plot the simulation outcomes while the set of sampling is performed and to store the data for later recovery.

3 EXAMPLES

This section shows examples of analyses performed using RAVEN with three different codes: RELAP-7 (Section 3.1), RELAP5-3D (Section 3.2) and an external model (Section 3.3).

3.1 *RELAP-7 analysis*

As already mentioned, the first system code that has been driven by RAVEN is RELAP-7. This section shows a station blackout analysis on a simplified Pressurized Water Reactor using RELAP-7 as system code. The plant response has been analyzed using the Monte Carlo and DET approach.

3.1.1 *Monte Carlo analysis*

Once the plant is in Station Black-Out (SBO) condition, the probability of recovering the emergency cooling system is set dependent from the recovery of any of the following systems:

- Diesel Generators (DGs): the power is restored when two of the three DG trains are recovered. The recovery time t_{DG1} of the first train is characterized by a normal distribution (σ = 200 s, μ = 800 s). The recovery time of the second train t_{DG2} is characterized by a uniform distribution (min = 0.5, max = 1.0) and driven by the relation: pdf (t_{DG2}) = pdf (t_{DG1}) · U (x).
- The Reserve Station Service Transformer and the main AC line recovery times t_{RSST} and t_{138} are described by normal distributions ($\sigma_{RSST/138}$ = 500 s, μ_{RSST} = 1400 s, μ_{138} = 2000 s).

The simulation scope is to assess the failure/success ratio of the plant. The goal function associated is: $\theta_f(T_{c\,MAX}, t) = \delta(T - T_{fC})$.

Where $T_{c\,MAX}$ and T_{fC} are the maximum and the failure clad temperatures, respectively. The failure temperature of the clad is also a stochastic variable characterized by a triangular distribution (min = 1255 K, max = 1700 K, peak = 1477 K).

Note that the time at which both diesel generators are available needs to be treated as a multidimensional distribution function unless the recovery of the second train is computed inside the system control logic once the recovery time of the first

train is already known. For this analysis, 4000 MC samples were performed.

3.1.2 *Dynamic event tree analysis*

The situation considered is exactly the one presented in the MC analysis (see Section 3.1.1) and the details of the analysis can be found in (Alfonsi, Rabiti, Mandelli, Cogliati, Kinoshita, & Naviglio 2013). Figure 7 shows the time evolution of the clad temperature and a projection of the sampling grid pattern generated by the dynamic event trees approach. The green lines are the simulation continuing while the red dots signal a point where a simulation was stopped when reaching the maximum clad temperature. It could be noticed that there are simulations being stopped at a level of temperature that is exceeded in other simulations. The reason is of course the random value of the clad failure temperature. On the bottom, the plot shows a projection of the threshold triggered by the DET simulation of the transient. The projection is performed by defining the recovery time of the auxiliary system $\mathbf{t_{AC} = min(t_{DG2}, t_{138}, t_{RSST})}$. It is clear how the competing variable (max clad temperature and AC recovery time) are alternatively moved towards higher values of their CDF until a transition point between success and failure is reached. This pattern is generated by contemporaneously sampling two antagonist variables (or in a terminology more familiar in the RISMC framework, contemporaneously sampling capacity and load).

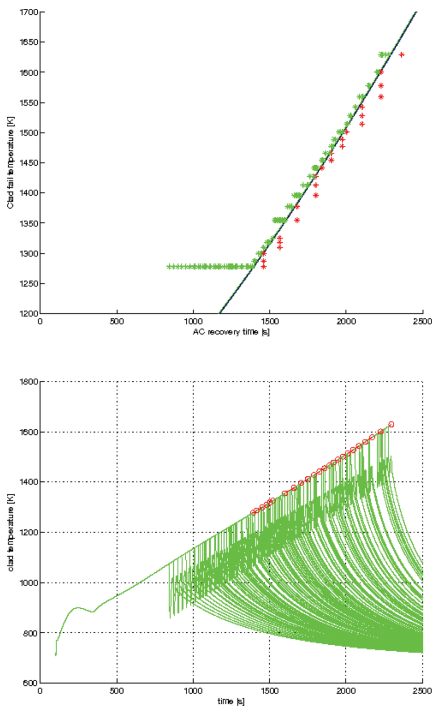


Figure 7. Top: DET a-posteriori limit surface. Bottom: clad temperature evolution.

3.2 *RELAP5-3D BWR SBO analysis*

For the RISMC project, we employed RAVEN and RELAP5-3D to analyze a Station Black-Out (SBO) accident scenario for a Boiling Water Reactor (Mandelli, Smith, Alfonsi, Rabiti, et al. 2014). In particular, we employed both classical statistical tools, i.e. MC, and more advanced machine learning based algorithms to perform uncertainty quantification in order to quantify changes in system performance and limitations as a consequence of power uprate.

In one of these analyses we focused on considering a 2-dimensional state space: Firewater (FW) availability time (measured after ADS activation) and battery life. By randomly changing these two parameters we observed the outcome of each simulation (failure or success) and, by using a SVM based classifier, we were able to determine the limit surface.

Results are shown in Figure 8 for two different values of power: 100%, and 120%. As expected, a longer battery life and a shorter firewater injection alignment time lead to success, while a short battery life and long firewater alignment time failed.

3.3 *Space propulsion system*

For the PSAM conference, a benchmark problem, a space propulsion system, was issued in

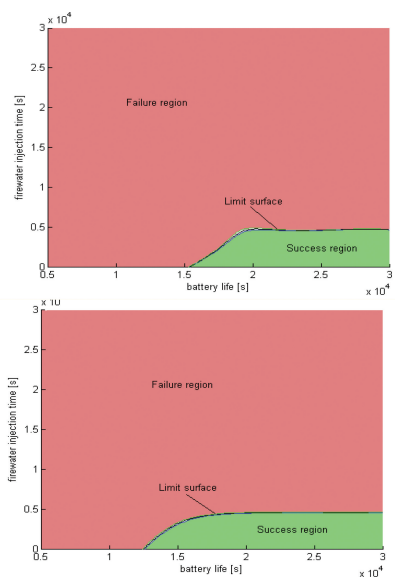


Figure 8. FW availability time vs. battery life: limit surface for 100% (top) and 120% (bottom) power.

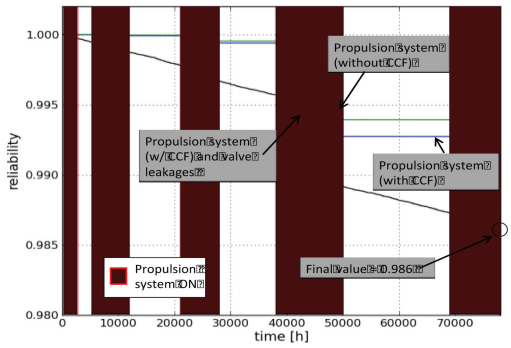


Figure 9. Temporal profile of the PSAM 2014 space propulsion system reliability.

order to compare Dynamic PRA methods. In this respect, the RAVEN team proposed a solution to this benchmark problem using RAVEN coupled with an external model that mimics both the dynamic (deterministic) and stochastic (e.g., failure on demands, damage accumulation, common cause failures) behavior of the propulsion system (Mandelli, Smith, Alfonsi & Rabiti 2014). The goal was to measure the temporal profile of the system reliability over the design life (78,000 hours, approximately 9 years). Results are shown in Figure 9 for two different cases: propulsion system only (with and without common cause failures) and propulsion system coupled with valve leakages.

4 CONCLUSIONS

RAVEN is reaching a level of maturity that merits its release of the code for testing outside of Idaho National Laboratory. The statistical analysis framework based on grids and Monte Carlo relies on very well assessed methodologies, and has been performing well during internal testing. The integration of those methodologies with the data handling flexibility, the visualization capabilities and the ease of coupling with different physical model simulators show how RAVEN can be a powerful tool for PRA analysis. The DET implementation allows also a rapid turnaround time for the coupling with other codes as long as access to the simulator's control logic is provided. DETs have been identified as one of the most promising approaches for PRA. Thus, the development is currently focused on making the DET an adaptive approach.

Moreover, the coming release will let the PRA community familiarize itself with these enhanced techniques like limit surface or ROM construction for identifying the leading mechanisms of system failure.

REFERENCES

Alfonsi, A., Rabiti, C., Mandelli, D., Cogliati, J. & Kinoshita, R. 2013. Raven as a tool for dynamic probabilistic risk assessment: Software overview. *Proceedings of International Conference of mathematics and Computational Methods Applied to Nuclear Science and Engineering,* 1247–1261, San Valley (USA).

Alfonsi, A., Rabiti, C., Mandelli, D., Cogliati, J., Kinoshita, R., & Naviglio, A. 2013. Dynamic event tree analysis through Raven, In *Proceedings of ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis.*

Anders, D., Berry, R. et al., 2012. Relap-7 level 2 milestone report: Demonstration of a steady state single phase PWR simulation with relap-7. Tech. Rep. INL/EXT-12-25924, Idaho National Laboratory.

Gaston, D., Hansen, G. et al. 2009. Parallel multiphysics algorithms and software for computational nuclear engineering, Journal of Physics: Conference Series 180(1).

Gordon, W.J., & Wixom, J.A. 1978. Shepard's Method of "Metric Interpolation" to Bivariate and Multivariate Interpolation, in *Mathematics and Computation* 32 (141): 253–264.

Habermann, C. & Kindermann, F. 2007. Multidimensional Spline Interpolation: Theory and Applications. *Computational Economics* 30(2): 153–169.

Mandelli, D. & Smith C. 2012. Adaptive sampling using support vector machines, in *Proceeding of American Nuclear Society* 107: 736–738.

Mandelli, D., Smith, C., Rabiti, C., Alfonsi, A., et al. 2013. Dynamic PRA: an overview of new algorithms to generate, analyze and visualize data. In *Proceeding of American Nuclear Society.*

Mandelli, D., Smith, C., Alfonsi, A., Rabiti, C., et al. 2014. Overview of New Tools to Perform Safety Analysis: BWR Station Black Out Test Case. In *Proceeding of International Conference on Probabilistic Safety Assessment and Management—PSAM.*

Mandelli, D., Smith, C., Alfonsi, A. & Rabiti, C. 2014. Analysis of the Space Propulsion System Problem Using RAVEN, In *Proceeding of International Conference on Probabilistic Safety Assessment and Management—PSAM.*

Pedregosa F., et al. 2011. Scikit-learn: Machine Learning in Python, *Journal of Machine Learning Research,* 2825–2830.

Rabiti, C., Mandelli, D., et al. 2012. Reactor analysis and virtual control environment (Raven) FY12 report. Tech. Rep. INL/EXT-1227351, Idaho National Laboratory.

RELAP5-3D Team, 2009. RELAP5-3D Code Manual. Tech. Rep. INEEL-EXT-98-00834, Idaho National Laboratory.

Smith, C., Rabiti, C., et al. 2012. Risk Informed Safety Margins Characterization (RISMC) Pathway Technical Program Plan. Tech. Rep. INL/EXT-11-22977, Idaho National Laboratory.

Williamson, R.L., Hales, J.D. et al 2012. Multidimensional multiphysics simulation of nuclear fuel behavior, *Journal of Nuclear Materials* 423: 149–163.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Integrated Deterministic Probabilistic Safety Analysis (IDPSA) of a fire scenario

M. Kloos & J. Peschke
GRS mbH, Garching, Germany

B. Forell
GRS mbH, Cologne, Germany

ABSTRACT: A research project at GRS aimed at demonstrating how a combination of the MCDET tool and the FDS code can be used to perform an IDPSA in the frame of a probabilistic fire safety analysis. The mixture of MCDET and FDS provided a sample of dynamic event trees comprising many different time series of quantities of the fire evolution associated with corresponding conditional occurrence probabilities. These results were used to derive exemplary probabilistic fire safety assessments from criteria such as the temperatures of targets or the time periods with target temperatures exceeding critical values. The paper gives an overview on the fire scenario investigated, outlines the steps of the analysis and presents a selection of results including a quantification of the influence of epistemic uncertainties. Lessons learned from the analysis are discussed.

1 INTRODUCTION

IDPSA—frequently also called Dynamic PSA—can be regarded as a complementary analysis to the classical Deterministic (DSA) and Probabilistic (PSA) Safety Analyses (Adolfsson et al. 2011, Adolfsson et al. 2012). It makes extensive use of a deterministic dynamics code and applies advanced methods for an improved modeling and probabilistic assessment of complex systems with significant process/hardware/software/firmware/human interaction (Aldemir 2013). An IDPSA is particularly suitable in the frame of a fire PSA, since it can more realistically model and assess the interaction of the fire dynamics with the performance of technical systems and human actions.

A useful software tool for performing an IDPSA is the MCDET tool which applies a combination of Monte Carlo (MC) simulation and the Dynamic Event Tree (DET) approach (Kloos & Peschke 2006, Kloos et al. 2013b). The first tool proposed in literature which applied the DET approach is DYLAM (Dynamical Logical Methodology; Amendola and Reina 1984; Cojazzi 1996). Other software tools using the DET approach are, for instance, ADS-IDAC (Hsueh & Mosleh 1996, Chang & Mosleh 1998), SCAIS-TSD (Izquierdo J.M. et al. 1994, Munoz et al. 1999) or ADAPT (Catalyurek et al. 2010).

Since the MCDET tool can in principal be coupled with any deterministic dynamics code, the FDS (Fire Dynamics Simulator) code from NIST (McGrattan K. et al. 2013) was selected to be applied for fire simulation. What makes the MCDET tool particularly useful for a fire safety analysis is its Crew Module which allows for considering the human actions performed for fire fighting as a dynamic process (Kloos & Peschke 2008).

The fire scenario selected to be analyzed deals with the fire fighting means designated to be applied in a reference NPP once a fire occurs for any reason. One major assumption is the failure of the automatic actuation of the fixed fire extinguishing system in the compartment where the fire is supposed to start. This implies that fire fighting mainly depends on the operability of the fire detection and alarm system, the performance of human actions as well as on the operability of active fire barrier elements (e.g. fire dampers and fire doors) and of the fire extinguishing systems which can be manually actuated.

The first steps of the analysis which were already presented in Kloos et al. (2013a) mainly focused on the performance of the human actions to be applied for fire fighting without running the FDS code. In those situations where human actions had to be considered as dependent on the fire evolution, case-by-case analyses were performed on conditions defined by decisive states of the fire evolution (e.g. smoke in front of the door visible or not, when fire fighters reach the fire compartment). The computational effort of those case-by-case analyses was negligible, since the MCDET tool making use just of the Crew Module without applying a

dynamics code (such as FDS, for instance) runs very fast. Results of the analyses were conditional distributions referring to the timing of human actions. These distributions were used as input to the analysis presented in this paper.

Main subject of the analysis presented here was the fire dynamics as simulated by the FDS code in interaction with stochastic factors affecting the fire over time. The mixture of MCDET and FDS was used to simulate many different time series of quantities of the fire dynamics associated with corresponding conditional occurrence probabilities. From these results, distributions referring to the temporal evolution of target temperatures and quantifications of the influence of epistemic uncertainties could be derived.

Chapter 2 of this paper gives a short overview on the MCDET method. Information on the fire scenario including the scenario-specific fire model and the fire fighting procedures investigated can be found in chapter 3. The steps of the analysis and a selection of results are described in chapter 4. Conclusions and lessons learned from the analysis are presented in chapter 5.

2 MCDET METHOD

Coupled with a deterministic dynamics code such as FDS, the MCDET tool performs a combination of Monte Carlo (MC) simulation and the Dynamic Event Tree (DET) approach (Kloos & Peschke 2006, Kloos et al. 2013b). This combination is able to treat any kind of uncertainty. Aleatory uncertainties due to stochastic influences referring to discrete quantities (e.g. success/failure of the fire detection and alarm system to operate; success/error of human actions) are handled by the DET approach, whereas aleatory uncertainties referring to continuous quantities (e.g. time periods for carrying out human actions) are handled by MC simulation. MC simulation is also applied to consider epistemic uncertainties (due to lack of knowledge). The sampling of values for continuous aleatory variables is not performed a priori, i.e. before the calculation of a DET is launched. It is performed when needed in the course of the calculation. In this way, it is possible to treat the influence of the dynamic process on aleatory uncertainties and to consider, for instance, a higher failure rate of a component, if a high temperature seriously aggravates the condition of the component.

Output of the simulations with the MCDET tool coupled to a dynamics code is a large spectrum of different sequences, for instance, of the evolution of the fire. It can be considered as a sample of individual DETs, each constructed from a set of values sampled for the continuous aleatory variables. From the time series of output quantities of the dynamics code (e.g. the temperature inside the jacket of cable targets provided by FDS) and the corresponding likelihoods available for each sequence, conditional DET-specific and, by the application of statistical methods, unconditional scenario-specific likelihoods of damage states can be calculated.

3 FIRE SCENARIO

Main subject of the analysis presented here are the fire fighting means designated to be applied in a German reference Nuclear Power Plant (NPP) in case of a fire. The fire was assumed to initially occur in a compartment with cooling and filtering equipment for pump lubrication oil. Besides this process equipment, the compartment is equipped with electrical cables routed below the ceiling. These cables partly carry out safety related functions.

It was assumed that malfunction of the oil-heating system designated to heat up the pump lubrication oil in the start-up phase of the NPP causes an ignition of the oil. The evolution of the fire was considered to depend on the leakage rate of the oil. The heat release rate may be limited by the oxygen available in the compartment.

The dimensions of the compartment are about $w \times l \times h = 8\ m \times 6.2\ m \times 6\ m$. Compartment walls are from concrete. The compartment is divided into a lower and an upper level by a steel platform at 2.4 m height. The steel platform can be reached by steel stairs. The three compartment doors lead to the lower level of the compartment. It was assumed that one of these doors was left in open position with a reference probability of 0.005 (see Table 1). The mechanical air exchange by an air intake and an exhaust vent was assumed to be 800 m^3/h. The fire damper at the exhaust vent was supposed to close after melting of a fusible link at 72 °C. This mechanism was supposed to fail with a reference probability of 0.01 (see Table 1). If the outlet damper is closed, the mechanical air supply into the room was assumed to be reduced to 400 m^3/h. This value was chosen to account for increased pressure losses, if the inlet air leaves the room via other leakages.

The fire was supposed to start on the steel platform at the electrical oil heater. The evolution of the fire was considered as being linear over time. The characteristic time to reach 1 MW heat release rate was varied from 250 s to 700 s (see Table 1). In the upper layer cable tray, the cable targets were exposed to hot smoke and radiation.

3.1 *Scenario specific model*

The fire simulation was performed with the Fire Dynamics Simulator (FDS) 6.0 (McGrattan K.

Table 1. Epistemic uncertainties.

Epistemic variables	Refer. value	Distrib. type	Distribution parameters
Value of optical density at which emerging smoke is visible under door [1/m]	0.3	Uniform	Min = 0.2, Max = 0.4
Response time index for activation temperature of fire dampers [$\sqrt{m \cdot s}$]	125	Uniform	Min = 50, Max = 200
Threshold of optical density D below which fire compartment can be entered [1/m]	0.4	Uniform	Min = 0.3, Max = 0.5
Fraction of fuel mass (oil) converted into smoke	0.097	Uniform	Min = 0.095, Max = 0.099
Time to reach 1 MW heat release rate [s]	425	Uniform	Min = 250, Max = 700
Cable Conductivity [W/m*K]	0.275	Uniform	Min = 0.15, Max = 0.4
Specific heat of cable [kJ/kg*K]	1.225	Uniform	Min = 0.95, Max = 1.5
Depth of cable isolation [m]	0.0016	Uniform	Min = 0.0012, Max = 0.002
Cable density [kg/m^3]	1131	Uniform	Min = 833, Max = 1430
Specific heat of concrete [kJ/kg*K]	0.65	Uniform	Min = 0.5, Max = 0.8
Conductivity of concrete [W/m*K]	1.75	Uniform	Min = 1.4, Max = 2.1
Thickness of concrete walls in the compartment [m]	0.37	Uniform	Min = 0.32, Max = 0.42
Probability that fire door falsely stays open	0.005	Beta	$\alpha = 1.5$, $\beta = 236.5$
Probability that fire damper fails to close	0.01	Beta	$\alpha = 1.5$, $\beta = 117.5$
Failure temperature of I&C cables [°C]	170	Uniform	Min = 145, Max = 195
Critical time periods [s] with I&C cable temperatures:			
≥145 °C	420	Uniform	Min = 360, Max = 480
≥150 °C	300	Uniform	Min = 240, Max = 360
≥160 °C	215	Uniform	Min = 180, Max = 250
≥170 °C	160	Uniform	Min = 120, Max = 200
≥180 °C	80	Uniform	Min = 40, Max = 120

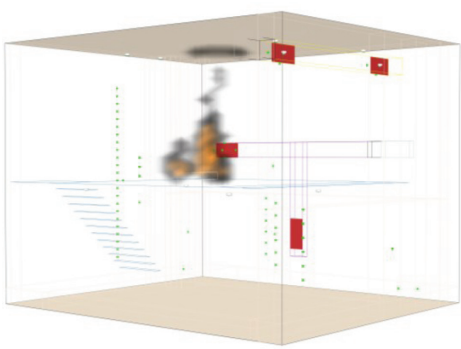


Figure 1. Snapshot of the compartment layout by FDS.

et al. 2013). The compartment was discretized in one mesh with a grid solution of 0.2 m in all three directions (see Fig. 1).

The air inlet duct (violet in Fig. 1) has one diffusor above the fire and one to the lower level. The outlet duct (yellow) sucks air from the upper layer by two diffusors which can be closed by the fire damper. The mechanical air supply was assumed to allow for a heat release rate of about 800 kW inside the compartment that is reduced to 400 kW after closing the damper. The inlet air damper was supposed not to close, because the fusible link is kept cold.

The thermal penetration of the cable material was described by the model for Thermally Induced Electrical Failure (THIEF) implemented in FDS. The THIEF model predicts the temperature of the inner cable jacket under the assumption that the cable is a homogeneous cylinder with one-dimensional heat transfer. The thermal properties—conductivity, specific heat, and density—of the assumed cable are independent of the temperature. In reality, both the thermal conductivity and the specific heat of polymers are temperature-dependent. In the analysis, conductivity, specific heat, density, and the depth of the cable insolation were considered as uncertain parameters with relevant influence (see Table 1).

The local optical density D of the smoke at 3.20 m height of the fire compartment was assumed to be an important factor affecting the time needed to suppress the fire. For optical densities below D = 0.1 m^{-1}, it was assumed that the personnel in charge of fire fighting can detect the fire and start to suppress it by means of a portable fire extinguisher after a delay of 10 s. For 0.1 m^{-1} < D < 0.4 m^{-1}, it is assumed that the delay time until

the fire source is detected and the suppression can be started increases, when the optical density rises. The delay time was assumed to be D times 100 seconds. For $D \geq 0.4\ m^{-1}$, fire suppression with a portable fire extinguisher and without any personal protective equipment was supposed to be impossible. More details are given in section 3.2. The threshold value of $0.4\ m^{-1}$ for the optical density was considered as a relevant parameter subjected to epistemic uncertainty (Table 1).

Once the fire suppression had started in a sequence, the simulation of the fire dynamics was stopped as soon as the temperature inside the cable jacket fell below 120 °C. Otherwise, a sequence was calculated up to 1800s after ignition.

3.2 *Fire fighting means*

If equipment and procedures work as intended, fire fighting is a rather short process, because the compartment where the fire is assumed to occur is equipped with a fixed fire extinguishing system which suppresses the fire with a sufficiently large amount of water after actuation by the fire detection and alarm system. However, one major assumption of the analysis presented here was the failure of the automatic actuation of the fixed fire extinguishing system. This implies that the fire has to be extinguished by manual fire fighting means performed by the plant personnel in charge.

Three states of the fire detection and alarm system can be assumed as decisive for the human actions to be performed for fire fighting, namely at least two detectors, only one detector or none of the detectors indicating an alarm signal to the control room. If at least two fire detectors send an alarm signal, the control room operator (shift leader) immediately instructs the shift fire patrol and the on-site fire brigade to inspect the compartment and to perform the necessary steps for fire suppression. If there is a signal by only one detector, the signal might be a faulty or spurious one (e.g. due to dust, steam, etc.). This is why the fire patrol trained for fighting incipient fires is instructed to inspect the fire compartment and to verify the fire. Suppose the fire patrol verifies the fire, the shift leader, who is immediately informed, calls the on-site fire brigade. In the meantime, the fire patrol tries to suppress the fire either by a portable fire extinguisher or by manually actuating the fixed fire extinguishing system from outside the fire compartment. If none of the fire detectors sends an alarm, the detection of the fire depends on the shift patrol inspecting the compartment at a random time once during a shift.

The fire patrol usually is the first person who arrives at the fire compartment. His/her success of suppressing the fire with a portable fire extinguisher was assumed to be depending on the local optical density D of the smoke at 3.20 m height (0.80 m above the level of the platform). If the optical density is too high (see section 3.1), fire suppression by the fire patrol inside the compartment is assumed to be impossible due to reduced visibility and irritant smoke effects on eyes and breathing organs. The fire patrol does not wear personal protective equipment. In this case, his/her only chance of successfully fighting the fire is to manually actuate the fixed fire extinguishing system. If the fire extinguishing system does not operate as intended, the fire brigade has to extinguish the fire with their equipment.

Besides the reliability of the fire detection and alarm system and the performance of human actions, the success of fire fighting mainly depends on the reliability of active fire barrier elements such as fire dampers or doors and of the fire extinguishing systems which can be manually actuated.

4 EXEMPLARY ANALYSIS

4.1 *Analysis steps*

In the first analysis steps, the human actions applied during the fire scenario were investigated in detail (Kloos et al. 2013a). The dynamic model of these actions was constructed on the basis of documents from the reference NPP and walk-talk-throughs at locations relevant for fire fighting. After the model was encoded in corresponding datasets of the Crew Module, the parameters of the Crew Module subjected to epistemic or aleatory uncertainty and considered as relevant for the analysis results were identified and the probabilistic information used to express the uncertainty (distributions and branching information) was specified. The corresponding data were entered as input to the Probabilistic Module of the MCDET tool.

The simulation runs of the first analysis steps were performed without running the FDS code. They were performed just by the combination of Crew Module, Probabilistic Module and the Scheduler of MCDET. That combination ran very fast and provided more than 100 Dynamic Event Trees (DETs) for each of several conditions. Those conditions identified as being decisive to the human actions of the fire fighting process were given by the relevant states of the fire detection and alarm system (none, only one or at least two of the detectors operate as required) as well as by the fire progression (e. g. visibility of smoke in front of the door when shift personnel reaches the fire compartment or production of smoke in the fire compartment).

From the DETs resulting from the simulations of the MCDET modules, various conditional distributions could be derived by using the

corresponding post-processing module of the MCDET tool. The distributions refer to the timing of human actions such as the time period between fire alarm and the arrival of fire fighters at the fire compartment door or the time period between the arrival at the fire compartment door and the beginning of fire extinguishing. They express stochastic variability and were used as input to the simulations performed in the subsequent analysis steps. Those analysis steps dealt with the modelling, simulation and evaluation of the interaction of the fire dynamics with relevant stochastic factors affecting the fire dynamics.

The stochastic factors taken into account refer to the timing and outcome (success/error) of tasks of human actions affecting the fire evolution, the operability of the fire detection and alarm system as well as to the functioning of active fire barrier elements (i.e. fire dampers and fire doors) and of the fire extinguishing systems which could be manually activated. Modelling information on the dynamics-stochastics interaction was specified as input to the FDS code as well as to the Probabilistic Module of the MCDET tool. The input file of the Probabilistic Module included a listing of the parameters subjected to stochastic variability (aleatory uncertainty) as well as the corresponding distributions and branching information expressing the stochastic variability. It also comprised information on the relevant parameters subjected to epistemic uncertainty. Corresponding information is given in Table 1.

The simulations of the FDS code and those of the Probabilistic Module were supervised by the old version of the MCDET Scheduler which allowed for calculating each DET in one process. The simulation approach made extensive use of the restart capabilities of the FDS code. The fire scenario was calculated up to 1800s (0.5 hours) after ignition.

The output of the simulations comprised data of about 2400 different fire sequences from a sample of 120 individual DETs. These data were evaluated by using corresponding post-processing modules of the MCDET tool.

4.2 *Consideration of epistemic uncertainties*

Like with continuous aleatory uncertainties, the influence of epistemic uncertainties is considered by Monte Carlo (MC) simulation (see chapter 2). The approach applied to account for both types of uncertainties is a double loop nested MC simulation: Sets of values of the parameters subjected to epistemic uncertainty (epistemic variables) are sampled in the outer loop. For each of these sets, different sets of values for the continuous aleatory variables are sampled and contribute to the generation of different Dynamic Event Trees (DETs) in the inner loop. That means a sample of DETs is constructed per set of epistemic variable values.

The approach applied to quantify the influence of epistemic uncertainties at least needs two distinct DETs per set of epistemic variable values. The results from all DETs generated for all sets of epistemic variable values can be used to estimate the mean $E(P_{Ep})$ and variance $Var(P_{Ep})$ of output quantity P_{Ep} subjected to epistemic uncertainty only:

$$P_{Ep} = E(P|Ep) \tag{1}$$

$$E(P_{Ep}) = E(E(P|Ep)) = E(P) \tag{2}$$

$$Var(P_{Ep}) = Var(E(P|Ep)) = Var(P) - E(Var(P|Ep)) \tag{3}$$

where P_{Ep} is, for instance, the (mean) likelihood of a damage state as a function of epistemic parameters. P_{Ep} can be estimated from the corresponding damage state likelihoods P derived from each DET per set of epistemic variable values.

An expression of the epistemic uncertainty of P_{Ep} can be obtained by applying the estimators for the mean $E(P_{Ep})$ and variance $Var(P_{Ep})$, for instance, to derive the parameters of a distribution supposed to be appropriate for P_{Ep} (e.g. Log. Normal or Beta distribution). The estimators for the mean $E(P_{Ep})$ and variance $Var(P_{Ep})$ can also be applied in the unequation of Cantelli to get a conservative estimator of the 95%-quantile of P_{Ep}:

$$P(P_{Ep} \geq E(P_{Ep}) + t) \leq \frac{Var(P_{Ep})}{Var(P_{Ep}) + t^2}, t \geq 0 \tag{4}$$

Another alternative to express the epistemic uncertainty of P_{Ep} is the calculation of the one-sided upper (95%; 95%) tolerance limit of P_{Ep} (Wilks 1942). The only requirement of this alternative is that at least 59 values of P_{Ep} are available (Wilks 1941). In the analysis presented here, 60 different sets of values were sampled for the epistemic variables. Information on the parameters subjected to epistemic uncertainty and with relevant influence on the output quantities (e.g. temperatures of cable targets) to be investigated is given in Table 1.

4.3 *Analysis results*

The safety related targets which could be damaged and, therefore, were selected to be considered in this analysis, are I&C cables routed below the ceiling of the fire compartment. The fire was regarded as successfully suppressed as soon as the temperature inside the cable jacket fell below 120 °C after the fire fighters started to extinguish the fire.

The temporal evolution of the temperature inside the cable jacket was already presented in Kloos et al.

(2014). For comparison, Figure 2 shows the evolution of the gas temperature at a height of 5.4 m of the compartment where the fire occurred. Differences between the sequences are due to the combined influence of aleatory and epistemic uncertainties. Distinct colors used in Figure 2 make clear which sequences lead to successful fire suppression (green, red and blue curves) and which not (black curves). The fire can be successfully suppressed either by the fire patrol (green curves) or by the fire brigade (red curves).

The value estimated for the mean conditional probability that the fire patrol is able to suppress the fire within 1800s after ignition is 0.994. If the fire patrol fails to suppress the fire (this is usually the case if he/she is not able to manually activate the fixed fire extinguishing system), the mean conditional probability that the fire brigade is able to extinguish the fire is estimated to be 0.999. The fire brigade arrives at the fire compartment about 3 to 16 minutes later than the fire patrol with a probability of 0.95. The mean conditional probability that neither the fire patrol nor the fire brigade is able to suppress the fire within 1800s was calculated to be 5.97 E-06.

Figure 3 compares distributions of the maximum temperatures of the gas layer at a height of 5.4 m and of the inner jacket of the I&C cables routed below the ceiling of the compartment where the fire occurred. The two dotted curves are the conditional distributions of the maximum temperatures of the gas layer and of the inner cable jacket, if the fire is not successfully extinguished within 1800s after ignition. The distributions under the condition of successful fire suppression are shown by the solid curves. The overall unconditional distributions are not shown separately. They are nearly identical with the corresponding conditional distributions, if the fire is successfully suppressed. This is due to the very high conditional probability for

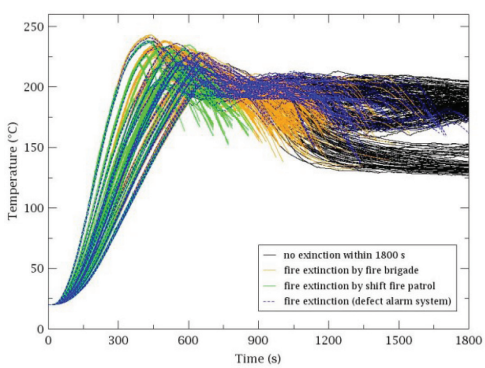


Figure 2. Temporal evolution of the gas temperature at a height of 5.4 m of the fire compartment.

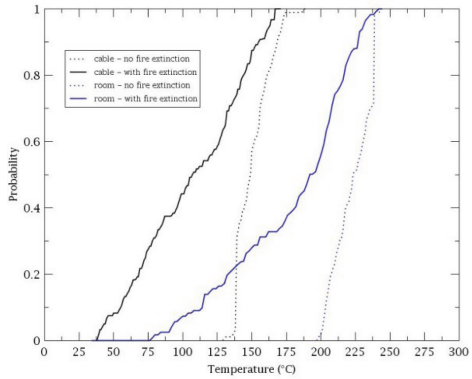


Figure 3. Conditional distributions of the maximum temperatures of the gas layer at a height of 5.4 m and of the inner jacket of I&C cables routed below the ceiling of the fire compartment.

successful fire suppression within 1800s. The mean value that fire suppression within 1800s is not successful was estimated to be 5.97 E-06.

From Figure 3, it can be concluded that the maximum gas temperature at a compartment height of 5.4 m does not exceed 230 °C, and the maximum temperature inside the cable jacket does not exceed 163 °C with a mean probability of 0.95. What is interesting and what cannot be concluded from Figure 2 is the mean probability of approx. 0.3 that the maximum gas temperature is between 75 °C and 155 °C. The corresponding range of the maximum temperature inside the cable jacket is between 30 °C and 75 °C. Reason for the low maximum temperatures is early successful fire extinguishing by the fire patrol. The mean probability that the fire patrol successfully suppresses the fire within 450 s after ignition is approx. 0.5.

Distributions referring to the time period with the temperature exceeding 160 °C inside the cable jacket are shown in Figure 4. They indicate, for instance, that this time period is not longer than approx. 113 s with a mean probability of 0.95, if the fire can be successfully suppressed. This result is also applicable to the overall unconditional distribution because of the very high conditional probability for successful fire suppression. If the fire cannot be suppressed within 1800s, the 95%-quantile of the time period with the temperature exceeding 160 °C inside the cable jacket is 192 s. The differences between the two conditional time distributions in Figure 4 seem to be not very large. Nevertheless, these differences might be relevant, if the time period with a high temperature inside the cable jacket is a relevant criterion for cable failure.

Estimates of the probability of I&C cables to be damaged by the fire were derived on the basis of

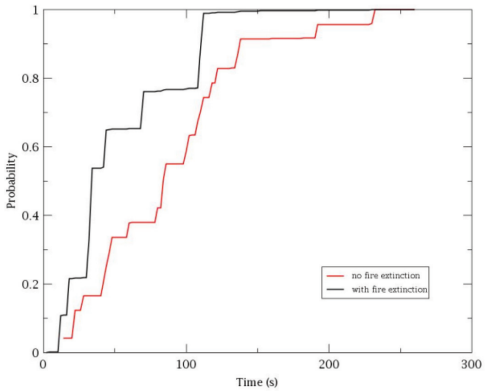


Figure 4. Conditional distributions of the time period with the temperature exceeding 160 °C inside the cable jacket.

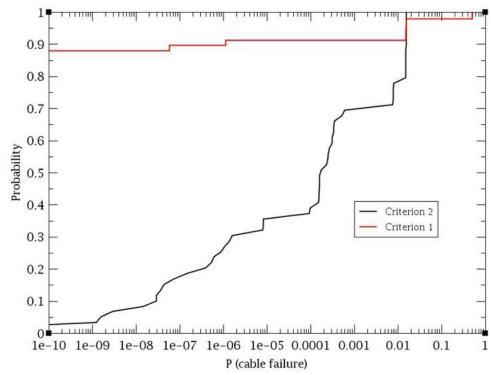


Figure 5. Epistemic uncertainty of the conditional probability of damaged I&C cables.

two different failure criteria. According to failure criterion 1, the cables were assumed to be damaged, if the temperature inside the cable jacket exceeds a critical value. With criterion 2, the failure of a cable was supposed to be determined by both a high level of the temperature inside the cable jacket and a critical time period with the inner cable temperature on a high level (see Fig. 4). Reference values and uncertainty quantifications referring to the failure temperature (criterion 1) and the critical time periods (criterion 2) are specified in Table 1. It is emphasized that the specifications are used only for demonstration purposes. They were derived from available experimental data on failure temperatures of I&C cables (Babst et al. 2011) and should be checked for real applications, in particular, with respect to the critical time periods for given temperature levels.

The mean conditional probability that an I&C cable in the fire compartment is damaged during the fire scenario was estimated to be 1.76 E-02 based on failure criterion 1 and 4.10 E-03 based on criterion 2. Figure 5 shows the epistemic uncertainty of the cable damage probability for each criterion. It can be seen that the epistemic probability distributions due to both criteria differ significantly. Since just a sample of 60 values is available from the simulations of MCDET and FDS, the one-sided upper (95%, 95%) tolerance limit was calculated to quantify the epistemic uncertainty of the cable damage probability (see section 3.2). With failure criterion 1, the (95%, 95%) tolerance limit is 0.5. The (95%, 95%) tolerance limit based on criterion 2 is 1.53 E-02.

The results clearly show the effect of different failure criteria on the calculated cable damage probability. They underline what intuitively seems to be more realistic, namely to consider both high temperature and the exposure time to high temperature as a criterion for assessing targets as deteriorated or damaged. To this purpose, corresponding data should be made available. As demonstrated, the MCDET method can use these data in order to provide corresponding risk assessments.

5 CONCLUSIONS

An exemplary IDPSA of a fire scenario was performed to demonstrate its modelling capacity and evaluation options in the frame of a probabilistic fire safety analysis. The simulations were carried out by a combination of the MCDET tool and the FDS code. This combination allowed for a quite realistic simulation of the interaction between the fire dynamics and relevant stochastic influencing factors over time.

What made the MCDET tool particularly useful for the analysis was its extra Crew Module which permitted to consider the human actions designated to be performed for fire fighting as a dynamic process. MCDET simulations performed just with the Crew Module without running FDS provided a huge amount of data for generating conditional distributions of the timings of human actions. Those distributions were used as input to the IDPSA performed with the combination of FDS and MCDET.

Besides the timings of human actions, the individual performances of all systems and components designated to be applied for fire detection, alarm, confinement and suppression were considered as subjected to aleatory uncertainty. Epistemic uncertainties were taken into account as well. Those ones which were considered as potentially important refer to parameters of the FDS code and failure criteria specified for cable targets.

From the huge amount of output data provided by the FDS-MCDET simulations, distributions referring to the temporal evolution of target temperatures could be calculated. Based on these distributions, quantifications useful for fire safety assessment were derived.

The main lesson learned from the analysis was the importance of having a well validated dynamics model when performing an IDPSA. Since a scenario-specific model was not available as input to FDS, it had to be created just in the course of the IDPSA project. The amount of work necessary to make that model applicable in combination with the MCDET tool was higher than initially expected. A lot of activities had to be spent to find a way of how to handle the limited restart capabilities of FDS in order to make the code running in combination with MCDET while simultaneously avoiding extensive calculation time and data storage.

ACKNOWLEDGEMENTS

The work presented in this paper was sponsored by the Ministry of Economics and Technology (BMWi) within the frame of the Research and Development Project RS1198.

REFERENCES

Adolfsson, Y. et al. (eds) 2011. In Proceedings of the Deterministic/Probabilistic Safety Analysis Workshop. October 2011. VTT-R-07266-11, VTT, Espoo, Finland.

Adolfsson, Y. et al. 2012 (eds). In IDPSA-Integrated Deterministic-Probabilistic Safety Assessment, 2nd workshop, November 19–21, 2012, KTH, Stockholm, Sweden.

Aldemir, T. 2013. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Annals of Nuclear Energy* 52: 113–124.

Amendola, A. & Reina, G. 1984. DYLAM-1, A Software Package for Event Sequence and Consequence Spectrum Methodology. EUR-924, CEC-JRC ISPRA, Commission of the European Communities, Ispra, Italy.

Babst, S. et al. 2011. Methoden zur Durchführung von Brand-PSA im Nichtleistungsbetrieb. GRS-A-3579, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, in German.

Catalyurek, U. et al. 2010. Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees. *Reliability Engineering and System Safety* 95: 278–304.

Chang, Y.H. & Mosleh, A. 1998. Dynamic PRA using ADS with RELAP5 code as its thermal hydraulic module. In Mosleh, A. & Bari, R. (eds.), *PSAM 4*. Springer-Verlag, New York: 2468–2473.

Cojazzi, G. 1996. The DYLAM approach to the dynamic reliability analysis of systems. *Reliability Engineering and System Safety* 52: 279–296.

Hsueh, K.S. & Mosleh, A. 1996. The Development and Application of the Accident Dynamic Simulator ADS For Dynamic Probabilistic Risk Assessment of Nuclear Power Plants. *Reliability Engineering and System Safety* 52: 297–314.

Izquierdo, J.M. et al. 1994. Automatic generation of dynamic event trees: a tool for integrated safety assessment. In Aldemir, T., Siu, N., Mosleh, A., Cacciabue, P.C., Goktepe, B.G. (eds.). *Reliability and Safety Assessment of Dynamic Process Systems*. NATO ASI Series F, vol. 120. Springer-Verlag, Heidelberg: 135–150.

Kloos, M. & Peschke, J. 2006, MCDET—A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach. *Nuclear Science and Engineering* 153: 137–156.

Kloos, M. & Peschke, J. 2008. Consideration of Human Actions in Combination with the Probabilistic Dynamics Method MCDET. *Journal of Risk and Reliability* 222: 303–313.

Kloos, M. et al. 2013a. Advanced probabilistic dynamics analysis of fire fighting actions in a nuclear power plant with the MCDET tool. In *Proceeding of European Safety and Reliability Conference ESREL 2013*. Amsterdam, Netherlands.

Kloos, M. et al. 2013b. Updates and current application of the MCDET simulation tool for Dynamic PSA. In *Proceedings of ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis*. Columbia, SC.

Kloos, M. et al. 2014. Insights from an integrated Deterministic Probabilistic Safety Analysis (IDPSA) of a Fire Scenario. To be published in *Proceedings of PSAM 12 Conference, Honolulu, Hawaii, 22–27 June 2014*.

McGrattan, K. et al. 2013. Fire Dynamics Simulator. Technical Reference Guide Volume I: Mathematical Model. *NIST Special Pub.* 1018, Sixth Edition.

Munoz, R. et al. 1999. DENDROS: a second generation scheduler for dynamic event trees. In Aragones, J.M., Ahnert, C., Cabellos, O. (eds.), *M&C'99—Madrid*: 1358–1367.

Wilks, S. 1941. Determination of sample sizes for setting tolerance limits. *Annals of Mathematical Statistics* 1 (1): 91–96.

Wilks, S. 1942. Statistical prediction with special reference to the problem of tolerance limits. *Annals of Mathematical Statistics* 13(4): 400–409.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dynamic reliability models for multiple dependent competing degradation processes

Y.H. Lin & Y.F. Li
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy—Electricité de France, at École Centrale Paris—Supelec, France

E. Zio
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy—Electricité de France, at École Centrale Paris—Supelec, France
Energy Department, Politecnico di Milano, Milan, Italy

ABSTRACT: This paper presents a holistic treatment to multiple dependent competing degradation processes, by employing the Piecewise-Deterministic Markov Process (PDMP) modeling framework. The proposed method can handle the dependencies between physics-based models, between multi-state models and between these two types of models. A Monte Carlo simulation algorithm is developed to compute the components/systems reliability. A case study on one subsystem of the Residual Heat Removal System (RHRS) of a nuclear power plant is illustrated.

1 INTRODUCTION

Physics-based models and multi-state models are widely used to model the degradation processes of components/systems. A physics-based model aims at developing an integrated mechanistic description of the component/system life consistent with the underlying real degradation mechanisms (e.g. wear, stress corrosion, shocks, cracking, fatigue, etc.) by using physics knowledge and equations (Chookah et al. 2011), whereas a multi-state model describes the degradation process in a discrete way, supported by material science knowledge (Li et al. 2012), degradation and/or failure data (Giorgio et al. 2011) from historical field collection or degradation tests.

Components/systems are often subject to multiple competing degradation processes and any of them may cause failure (Wang & Pham 2012). The dependences among these processes need to be considered under certain circumstances, e.g. when the degradation state of some components/systems can influence the degradation state dynamics or lifetime distribution of other components/systems (Rasmekomen & Parlikad 2013), or/and the various degradation processes within one component/system are physically not independent (Wang & Pham 2012). This makes the analysis and prediction of the components/systems reliability a challenging problem (Peng et al. 2010). Wang and Pham (Wang & Pham 2012) applied time-varying copulas for describing the dependencies between the degradation processes modeled by statistical distributions. Straub (Straub 2009) used a dynamic Bayesian network to represent the dependencies between degradation processes modeled by multi-state models. For some highly reliable components (e.g. pumps and valves in nuclear power plants, light-emitting diodes, etc.), degradation and/or failure data are often limited and do not allow building their lifetime distributions. Physics-based models are an alternative for characterizing the degradation processes (Fan et al. 2011).

In this work, we extend the existing modeling approaches to a more general setting, whereby the components degradations are modeled by physics-based models or multi-state models and dependencies exist among the components and the degradation processes within one component. To treat various dependencies, we employ the Piecewise-Deterministic Markov Process (PDMP) (Davis 1984, Cocozza-Thivent 2011) for components and system modeling.

The remainder of this article is organized as follows. Section 2 presents the proposed degradation model for systems with degradation dependency. Monte Carlo simulation procedures to solve the model are presented in Section 3. Section 4 presents one case study on one subsystem of a residual heat removal system (Coudray & Mattei 1984) from Électricité de France (EDF). Numerical results and analysis are presented in Section 5. Section 6 concludes the work.

2 DEGRADATION MODELING WITH DEGRADATION DEPENDENCY

Based on the available information/data about components degradations and failures, two main types of models are used to represent the degradation processes of components: physics-based model and multi-state model.

2.1 *Physics-based model*

The time-dependent evolution of continuous variables is often used to describe the degradation processes of components. The continuous variables

$$\vec{X}(t) = \begin{pmatrix} \vec{x}(t) \\ \vec{y}(t) \end{pmatrix} \tag{1}$$

may represent: 1. degradation variables $\vec{x}(t)$ such as crack length (Keedy & Feng 2012), which describe the components degradation condition; 2. physical variables $\vec{y}(t)$ such as operation time, velocity and force (Daigle & Goebel 2011a), which influence the evolution of degradation variables. Physics equations, mathematically written as differential equations (which are often a set of first-order ordinary differential equations), are then used to describe the variation of $\vec{x}(t)$ in time, considering external influencing factors $\vec{\theta}_L$, such as temperature and pressure (Jacobsen 2006), whose behaviors are not modeled by the physics equations.

We assume that there are M components in the system, $\vec{L} = (L_1, L_2, \ldots, L_M)$, whose degradation processes are modeled by physics-based models. Let

$$\overrightarrow{X_{L_m}}(t) = \left(\overrightarrow{x_{L_m}}(t), \overrightarrow{y_{L_m}}(t)\right) \in \mathbb{R}^{d_{Lm}}, m = 1, 2, \ldots, M \tag{2}$$

denote the vector containing all d_{Lm} time-dependent variables for component L_m; their evolutions are described by the following first-order ordinary differential equations:

$$\overrightarrow{\dot{X}_{L_m}}(t) = \overrightarrow{f_{L_m}}\left(\overrightarrow{X_{L_m}}(t), t \mid \overrightarrow{a_{L_m}}\right) \tag{3}$$

where $\overrightarrow{a_{L_m}}$ represents the parameters in the physics equations, including external influencing factors $\overrightarrow{\theta_{L_m}}$.

To consider the dependences between the components, let

$$\vec{X}(t) = \left(\overrightarrow{X_{L_1}}(t), \overrightarrow{X_{L_2}}(t), \ldots, \overrightarrow{X_{L_m}}(t)\right) \in \mathbb{R}^{d_L} = \mathbb{R}^{d_{L1} + d_{L2} + \cdots + d_{LM}} \tag{4}$$

denote the overall degradation condition of all the M components. We extend the set of differential equations in (3) by including the variables of the other $M - 1$ components:

$$\overrightarrow{\dot{X}_{L_m}}(t) = \overrightarrow{f_{L_m}}\left(\vec{X}(t), t \mid \overrightarrow{a_{L_m}}, \overrightarrow{b_{L_m}}\right) \tag{5}$$

where $\overrightarrow{b_{L_m}}$ is the vector of parameters characterizing the influence of the other components on the degradation processes of component L_m.

For any component L_m, the degradation variables

$$\overrightarrow{x_{L_m}}(t) = \left(x^1_{L_m}(t), x^2_{L_m}(t), \ldots, x^{d^1_{L_m}}_{L_m}(t)\right) \tag{6}$$

have the critical values (thresholds):

$$\overrightarrow{x_{L_m}}^*(t) = \left(x^{1\,*}_{L_m}, x^{2\,*}_{L_m}, \ldots, x^{d^1_{L_m}\,*}_{L_m}\right) \tag{7}$$

Component L_m fails when one of the degradation variables exceeds the corresponding critical value. The failure time t_f of component L_m is defined as follows:

$$t_f = Min_{\arg t} \left[x^1_{L_m}(t) = x^{1\,*}_{L_m}, \ldots, x^{d^1_{L_m}}_{L_m}(t) = x^{d^1_{L_m}\,*}_{L_m}\right] \tag{8}$$

2.2 *Multi-state model*

Under the situation that there is not any available physics-based model for the degradation processes of the components, a multi-state model (Lisnianski & Levitin 2003) can be built using historical degradation and/or failure data of components. Markov processes (Giorgio et al. 2011) and semi-Markov processes (Chryssaphinou et al. 2011) are widely used in practice as multi-state models, where the degradation conditions of the components are represented by a limited number of states describing the degradation severity. The transition rates (estimated from historical data) between two different degradation states are used to describe the speed of reaching another degradation state.

We assume that there are N components in the system, $\vec{K} = (K_1, K_2, \ldots, K_N)$, whose degradation processes are modeled by multi-state models. The component K_n has $d_{Kn} + 1$ states, $S_{Kn} = \{0, 1, \ldots, d_{Kn}\}$, ranging from perfect functioning state 'd_{kn}' to complete failure state '0'. The component is partially functioning in all generic intermediate states.

To consider the dependences between the components and the influencing factors, let

$$\vec{Y}(t) = (Y_{K_1}(t), Y_{K_2}(t), \ldots, Y_{K_N}(t)) \in S = S_{K_1} \times S_{K_2} \ldots \times S_{K_N} \tag{9}$$

denote the overall degradation condition of all the N components, where $Y_{Kn}(t)$, $n = 1, 2, \ldots, N$, indicates the degradation state of component K_n at time t. Let $\{\vec{Y}_k, T_k\} \in S \times \mathbb{R}^+$, $k \in \mathbb{N}$ denote the degradation processes of the N components, where $\vec{Y}_k$ denotes the state of the N components after k transitions (a transition occurs as long as any one of the N components changes its state) and T_k denotes the time of arrival at state $\vec{Y}_k$. Then, the state of the N components at time t can be defined as follows:

$$\vec{Y}(t) = \vec{Y}_k, \forall t \in [T_k, T_{k+1}[\tag{10}$$

We assume that $\{\vec{Y}_k, T_k\}$, $k \geq 0$ follows a Markov renewal process which generalizes the notion of Markov jump process. Then, the probability that the N components will step to state $\vec{J}$ from state $\vec{i}$ in the time interval $[T_n, T_n + \Delta t]$, given $\{\vec{Y}_k, T_k\}$, $k \leq n$, is defined as follows:

$$\begin{aligned} &P[\vec{Y}_{n+1} = \vec{J}, T_{n+1} \in [T_n, T_n + \Delta t] \,|\, \{\vec{Y}_k, T_k\}_{k \leq n}, \vec{\theta}_K] \\ &= P[\vec{Y}_{n+1} = \vec{J}, T_{n+1} \in [T_n, T_n + \Delta t] \,|\, \vec{Y}_n = \vec{i}, \vec{\theta}_K] \\ &\forall n \geq 0, \Delta t \geq 0, \vec{i}, \vec{J} \in S, \vec{i} \neq \vec{J} \end{aligned} \tag{11}$$

where $\vec{\theta}_K$ represents the external influencing factors. The process $\vec{Y}(t)$ is a continuous time Markov process if the holding time at any state $\vec{i} \in S$ is exponentially distributed according to state $\vec{i}$ and the system total running time t, denoting by the transition rate $\lambda_{\vec{i}}(t, \vec{\theta}_K)$. Otherwise, it is a semi-Markov process. The system fails if one of the N components reaches its complete failure state. The reliability of such system at time t can be calculated as follows:

$$\begin{aligned} R(t) = P[&Y_{K_1}(s) \neq d_{K_1}, Y_{K_2}(s) \neq d_{K_2}, \ldots, Y_{K_N}(s) \\ &\neq d_{K_N} \forall s \leq t] \end{aligned} \tag{12}$$

2.3 *PDMP for systems with degradation dependency*

In this section, we consider that the system contains M components described by physics-based models and N components described by multi-state models. The interdependencies between the two groups of components are taken into account. We assume that the degradation levels of the components in the first group may influence the transition times and transition directions of the degradation processes of the second group, and the degradation states of the second group may influence the evolution trajectories of the continuous variables in the first group. We employ PDMP to model this type of interdependence. Let

$$\vec{Z}(t) = \begin{pmatrix} \vec{X}_{L_1}(t) \\ \vec{X}_{L_2}(t) \\ \vdots \\ \vec{X}_{L_M}(t) \\ \vec{Y}(t) \end{pmatrix} = \begin{pmatrix} \vec{X}(t) \\ \vec{Y}(t) \end{pmatrix} \in E = \mathbb{R}^{d_L} \times S \tag{13}$$

represent the degradation condition of the whole system defined on E, a hybrid space of $\mathbb{R}^{d_L}$ and S. $(\vec{Z}_t = \vec{Z}(t))$ $t \geq 0$ is a stochastic process with values in the probability space (E, ε) where ε is a σ-algebra of E (Cocozza-Thivent 2011). Let

$$\vec{Z}_k = \vec{Z}(T_k) = \begin{pmatrix} \vec{X}(T_k) \\ \vec{Y}_k \end{pmatrix} \in E, k \in \mathbb{N} \tag{14}$$

denote the degradation state of the whole system at the transition time T_k of the process $\vec{Y}(t)$. $\{\vec{Z}_k, T_k\}$, $k \geq 0$ is then a Markov renewal process defined on the space $E \times \mathbb{R}^+$, since the probability that the whole system will step to state $\vec{J}'$ from state $\vec{i}'$ in the time interval $[T_n, T_n + \Delta t]$, given $\{\vec{Z}_k, T_k\}$, $k \leq n$ is as follows:

$$\begin{aligned} &P\left[\vec{Z}_{n+1} = \vec{J}', T_{n+1} \in [T_n, T_n + \Delta t] \,\middle|\, \left\{\vec{Z}_k, T_k\right\}_{k \leq n}, \vec{\theta}_K\right] \\ &= P\left[\vec{Z}_{n+1} = \vec{J}', T_{n+1} \in [T_n, T_n + \Delta t] \,\middle|\, \vec{Z}_n = \vec{i}', \vec{\theta}_K\right] \\ &\forall n \geq 0, \vec{i}', \vec{J}' \in E, \vec{i}' \neq \vec{J}' \end{aligned} \tag{15}$$

where the transition probability depends also on the variables of the M components from the first group. The evolution of the whole system between two consequent jumps of process $\vec{Z}(t)$, when $t \in [T_k, T_{k+1}[$, $k \in \mathbb{N}$ is defined as follows:

$$\dot{\vec{Z}}(t) = \begin{pmatrix} \dot{\vec{X}}_{L_1}(t) \\ \dot{\vec{X}}_{L_2}(t) \\ \vdots \\ \dot{\vec{X}}_{L_M}(t) \\ \vec{0} \end{pmatrix} = \begin{pmatrix} \vec{f}_{L_1}^{\vec{Y}_k}\left(\vec{X}(t), t \,|\, a_{L_1}, b_{L_1},\right) \\ \vec{f}_{L_2}^{\vec{Y}_k}\left(\vec{X}(t), t \,|\, a_{L_2}, b_{L_2},\right) \\ \vdots \\ \vec{f}_{L_M}^{\vec{Y}_k}\left(\vec{X}(t), t \,|\, a_{L_M}, b_{L_M},\right) \\ \vec{0} \end{pmatrix} \tag{16}$$

where $\vec{f}_{L_M}^{\vec{Y}_k}$, $n = 1, 2, \ldots, M$ are the physics equations, given the influence of the degradation state $\vec{Y}_k$ of the N components from the second group. The process $\vec{Z}(t)$ that takes values in E is a Piecewise-Deterministic Process (PDP) since it can be written as follows [Lorton et al. 2013]:

$$\vec{Z}(t) = \varphi(\vec{Z}_k, t - T_k), \quad for \quad t \in [T_k, T_{k+1}], \forall k \in \mathbb{N} \tag{17}$$

and $\overline{Z}(t)$ is a PDMP on the condition that φ satisfies the following [Cocozza-Thivent. 2011]:

$$\varphi(\vec{y},t+s)=\varphi(\varphi(\vec{y},t),s),\forall t,s\geq 0,\vec{y}\in E \tag{18}$$

This is especially true in our case, as φ is the solution of a first-order ordinary differential equations system [Lorton et al. 2013].

Let $\mathcal{F}=\mathcal{F}_{\overline{X}}\times\mathcal{F}_{\overline{Y}}\subsetneq E$ denote the space of the failure states of $\vec{Z}(t)$, where $\mathcal{F}_{\overline{X}}$ denotes the sub-space of the failure states for $\vec{X}(t)$ and $\mathcal{F}_{\overline{Y}}$ denote the sub-space of the failure states for $\vec{Y}(t)$; then, the reliability of the system at time t can be calculated as follows:

$$R(t)=P[\vec{Z}(s)\notin\mathcal{F},\forall s\leq t] \tag{19}$$

3 RELIABILITY ESTIMATION

Analytically solving the PDMP is a difficult task due to the complex behavior of the system (Marseguerra & Zio 1996), which contains the stochasticities in the components modeled by multi-state models and the time-dependent evolutions of the components modeled by physics-based models. On the other hand, Monte Carlo simulation methods are suited for the reliability estimation of the system.

3.1 *The simulation procedure*

The procedure of the MC simulation is represented as follows:

Set N_{max} (the maximum number of replications) and $k=0$ (index of replication)
Set $k'=0$ (number of trials that end in the failure state)
While $k<N_{max}$
  Initialize the system by setting $\overrightarrow{Z'}$ (initial state), and the time $T=0$ (initial system time)
  Set $t'=0$ (state holding time)
  While $T<T_{miss}$
    Sample a t' through the probability density function
    Sample an arrival state $\overrightarrow{Y'}$ for stochastic process $\vec{Y}(t)$ from all the possible states through the conditional probability function
    Set $T=T+t'$
    Calculate $\vec{X}(T)$ by using the physics equations (16)
    Set

$$\overrightarrow{Z'}=\begin{pmatrix}\overrightarrow{X}(T)\\ \overrightarrow{Y'}\end{pmatrix}$$

    If $T\leq T_{miss}$
      Calculate all the extreme values $(\overline{X}_n^0, n\in\mathbb{N})$ of $\overline{X}(t)$ in the interval $[T-t', T]$ by using the physics equation (16)
      If $(\exists m\in\mathbb{N}, \overline{X}_m^o\in\mathcal{F}_X)\vee(\overrightarrow{Z'}\in\mathcal{F})$
        Set $k'=k'+1$
        Break
      End if
    Else (when $T>T_{miss}$)
      Calculate all the extreme values $(\overline{X}_n^o, n\in\mathbb{N})$ of $\overline{X}(t)$ in the interval $[T-t', T_{miss}]$ by using the physics equations (16)
      If $\exists m\in\mathbb{N}, \overline{X}_m^o\in\mathcal{F}_X$
        Set $k'=k'+1$
        Break
      End if
    End if
  End While
  Set $k=k+1$
End While

Since the first derivative of $\overline{X}(t)$ on the interval $[T_k, T_{k+1}]$, $k\in\mathbb{N}$ exists, $\overline{X}(t)$ is continuous on such interval. If $\overline{X}(t)$ is monotonous in the interval $[T_k, T_{k+1}]$, the extreme values of $\overline{X}(t)$ are reached at the boundary points of the interval. Otherwise, the extreme values of $\overline{X}(t)$ can be obtained by comparing all the local extreme values found by Fermat theorem (Bronshtein et al. 1985). To calculate the value of $\overline{X}(t)$, Runge-Kutta methods can be applied for the numerical solution of the ordinary differential equations (Hairer et al. 1993, Hairer et al. 1996).

The estimated component reliability at time T_{miss} can be obtained by

$$\hat{R}(T_{miss})=1-k'/N_{max} \tag{20}$$

where k' represents the number of trials that end in the failure state of the system, and the sample variance is (Lewis & Böhm 1984):

$$var_{\hat{R}(T_{miss})}=\hat{R}(T_{miss})(1-\hat{R}(T_{miss}))/(N_{max}-1) \tag{21}$$

4 ILLUSTRATIVE CASE

In this section, one important subsystem of a residual heat removal system (Coudray & Mattei 1984) has been considered to illustrate the proposed method. This subsystem consists of a pneumatic valve and a centrifugal pump, which are used in conjunction in a variety of domains for fluid delivery. The degradation model of the pump is modified from the one originally supplied by EDF, while that of the valve is an existent physics-based model presented in (Daigle & Goebel 2010, Lorton

et al. 2013). Two types of dependence have been considered, as follows:

1. Common degradation cause: the abrasive particles in the fluid which can aggravate the degradation processes of both components (Wierman et al. 2007).
2. Degradation dependency: the degradation of the pump can lead it to vibrate (Zhang et al. 2006), which will, in turn, cause the vibration of the valve and therefore aggravate the degradation process of the latter (Moussou et al. 2001).

The common degradation cause and degradation dependency leads us to resort to our proposed method to assess the reliability of this two-component series system.

4.1 *Pneumatic valve*

The pneumatic valve refers to a normally-closed and gas-actuated valve with a linear cylinder actuator which has been studied by Daigle and Goebel (Daigle & Goebel 2010) and Lorton et al. (Lorton et al. 2013) by using physics-based modeling. A simplified scheme of the valve is shown in Figure 1.

The valve contains a top chamber (above the piston) and a bottom chamber (below the piston), which are respectively connected to a top pneumatic port and a bottom pneumatic port. The position of the piston (between fully closed position '0' and fully open position 'L_s') is controlled by filling or evacuating the chambers by regulating the pressure of the pneumatic ports. A return spring is linked with the piston to ensure the closure of the valve when pressure is lost due to the spring force.

One of the most common degradation mechanisms of the valve is the internal leak at the seal surrounding the piston (Lorton et al. 2013). Owing to the internal leak of the piston, the pneumatic gas can flow between the two chambers therefore influencing the response time and the behavior of the valve. The degradation variable of the valve is then the equivalent orifice area of the internal leak of the piston, denoted by $L(t)$. At the initial stage, the valve is set to the fully closed position.

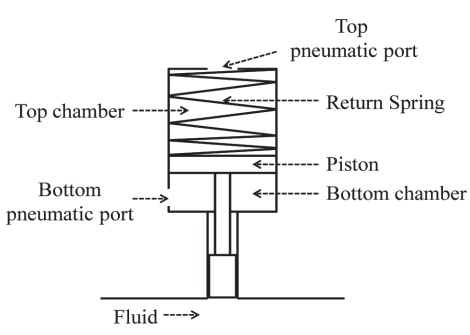


Figure 1. Simplified scheme of the pneumatic valve (Daigle & Goebel 2010).

The degradation process of the valve at time t is described by the following vector:

$$\overrightarrow{X_v}(t) = \begin{pmatrix} L(t) \\ x(t) \\ v(t) \\ m_t(t) \\ m_b(t) \\ t \end{pmatrix} \tag{22}$$

where $x(t)$ is the position of the valve, $v(t)$ is the velocity of the valve, $m_t(t)$ is the mass of the gas in the top chamber, $m_b(t)$ is the mass of the gas in the bottom chamber and t is the running time of the valve. The derivatives of these variables are represented by:

$$\overrightarrow{\dot{X}_v}(t) = \begin{pmatrix} \dot{L}(t) \\ v(t) \\ a(t) \\ f_t(t) \\ f_b(t) \\ 1 \end{pmatrix} \tag{23}$$

where $a(t)$ is the valve acceleration, $f_t(t)$ and $f_b(t)$ are the mass flows going into the top and bottom chambers, respectively. The development of the internal leak is defined as follows:

$$\dot{L}(t) = w(1+\alpha_v)rv(t)^2 \tag{24}$$

where $v(t)$ is the velocity of the valve, w is the wear coefficient without the consideration of abrasive particles in the fluid, and α_v is a constant to characterize the relative increment of the developing rate of the internal leak influenced by the abrasive particles in the fluid. All the other physics equations of the valve and the parameter definitions and values can be founded in (Daigle & Goebel 2010).

The critical value L^* for the internal leak of the piston $L(t)$ is defined as the value above which ($L(0) > L^*$) the valve cannot reach the fully open position within the 15 s time limit after an opening command is executed at time $t = 0$s. The size of the internal leak is assumed to be constant during the opening procedure ($\dot{L}(t) = 0$, $0 \le t \le 15$) (Lorton et al. 2013) to obtain a conservative critical value

that $L^* = 3.20e-6$ m^2 in this case. The behavior of the valve within 15 s with different values of $L(0)$ is shown in Figure 2.

4.2 *Centrifugal pump*

We assume that the degradation process of the centrifugal pump is modeled by a continuous-time homogeneous Markov chain with constant transition rates as shown in Figure 3.

The perfect functioning state is denoted with the label '3' and '0' is the label of the complete failure state. At the initial stage, the valve is set to the perfect functioning state. The vibration of the pump caused by degradation is classified into two levels: 'smooth' and 'rough' (Vlok et al. 2002) corresponding to the degradation states '2' and '1', respectively. Let $Y_p(t)$ denote the degradation state of the pump at time t and $S_p = \{0, 1, 2, 3\}$ denote the degradation states set. The formulations of transition rates are assumed as follows:

$$\begin{cases} \lambda_{32} = \lambda'_{32}(1+\alpha_{p32}) \\ \lambda_{21} = \lambda'_{21}(1+\alpha_{p21}) \\ \lambda_{10} = \lambda'_{10}(1+\alpha_{p10}) \end{cases} \tag{25}$$

where λ'_{32}, λ'_{21} and λ'_{10} are the original transition rates without the consideration of abrasive particles in the fluid. The constants α_{p32}, α_{p21} and αp_{10} represent the relative increments of transition rates caused by the abrasive particles in the fluid.

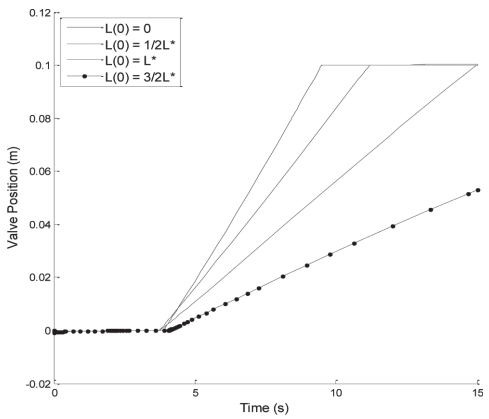


Figure 2. Valve behavior with different sizes of the internal leak.

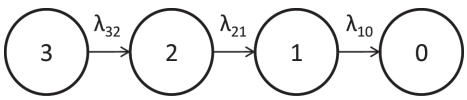


Figure 3. Degradation process of the pump.

4.3 *PDMP for the degradation processes of the system*

The degradation processes of the whole system are modeled by PDMP as follows:

$$\vec{Z}(t) = \begin{pmatrix} \overrightarrow{X_v}(t) \\ Y_p(t) \end{pmatrix} = \begin{pmatrix} L(t) \\ x(t) \\ v(t) \\ m_t(t) \\ m_b(t) \\ t \\ Y_p(t) \end{pmatrix} \in R^6 \times S_p \tag{26}$$

and

$$\dot{\vec{Z}}(t) = \begin{pmatrix} \overrightarrow{\dot{X}_v}(t) \\ 0 \end{pmatrix} = \begin{pmatrix} \dot{L}'(t, Y_p(t)) \\ v(t) \\ a(t) \\ f_t(t) \\ f_b(t) \\ 1 \\ 0 \end{pmatrix} \tag{27}$$

where $\dot{L}'(t, Y_p(t))$ is the derivative of the internal leak of the valve with the consideration of the degradation dependency between the valve and the pump while the development of the internal leak of the valve is dependent on the degradation state of the pump, we have

$$\dot{L}'(t, Y_p(t)) = w(1+\alpha_v)(1+\beta_{Y_p(t)})rv(t)^2 \tag{28}$$

where $\beta_{Yp}(t)$ is the relative increment of the developing rate of the internal leak caused by the vibration of the pump (if we ignore the degradation dependency, then $\beta_{Yp}(t) = 0$). The times between two consequent jumps of PDMP follow the exponential distribution with constant transition rates determined by equation (25). The space of the failure states of $\vec{Z}(t)$ is $\mathcal{F} = \mathcal{F}_{\overrightarrow{Xv}} \times \mathcal{F}_{Yp} = [L^*, +\infty] \times \{0\}$.

5 RESULTS AND ANALYSIS

Due to the high reliability of the components, it is typically computationally expensive to simulate the failures or certain degradations. The values of the parameters of the pump and of the parameters

characterizing the degradation dependency are shown in Table 1. We set them in a way to simulate the system functioning under an accelerated aging condition.

At the initial stage, the two components are both in perfect state and the valve is in the fully closed position. The command of the valve is a 30 s-periodic-signal and the valve is commanded to open in the first half-period and to close in the second half. The pump is functioning until it reaches the failure state '0'.

A Monte Carlo simulation over a time horizon of $T_{miss} = 700$ s is run $N_{max} = 10^5$ times. In Figure 4, we compare the reliability of the whole system

Table 1. The values of the parameters of the pump and of the parameters characterizing the degradation dependency.

Parameter	Value
w	5e-9 m/N
α_v	20%
λ'_{32}	5.00e-3/s
λ'_{21}	5.00e-3/s
λ'_{10}	5.00e-3/s
α_{p32}	20%
α_{p21}	20%
α_{p10}	20%
β_3	0
β_2	10%
β_1	20%
β_0	0

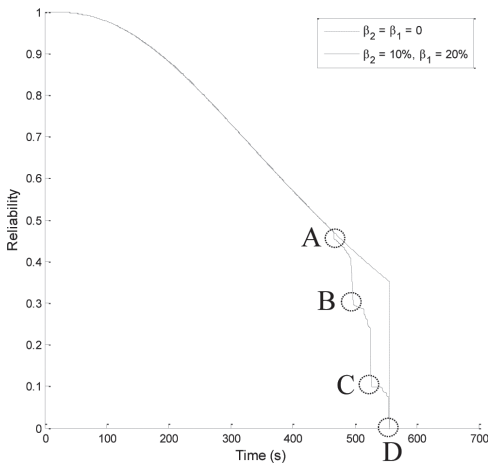


Figure 4. System reliability with common degradation cause and w/o degradation dependency.

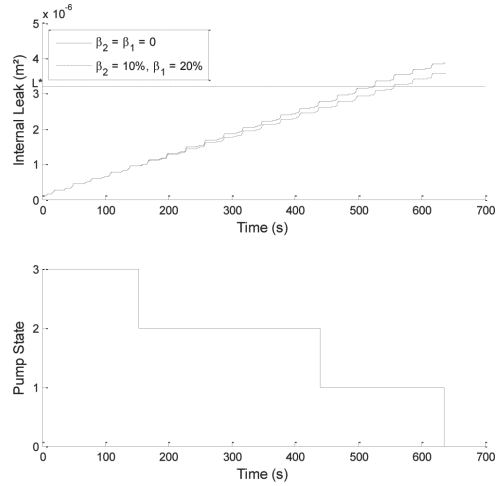


Figure 5. Development of the internal leak of the valve in one simulation trial with common degradation cause and w/o degradation dependency.

with common degradation cause and degradation dependency to that with only common degradation cause. From the Figure, we can see that before 465.67 s (point A) the two curves coincide and the system reliability is equal to the reliability of the pump. After that time, the valve begins to fail in some simulation trials, which corresponds to the situation when the pump jumps to state '1' very quickly and stays there until the valve fails. The system reliability, then, experiences three sharp decreases at around 497.39 s (point B), 526.77 s (point C) and 556.45 s (point D) respectively, and the system is definitely failed afterwards. The longest failure time of the valve is at point D, corresponding to the situation when the pump stays in the initial state '1' from the beginning until the failure of the valve.

The development of the internal leak of the valve during one simulation trial is presented in Figure 5, where the pump is seen to reach state '2' at 152.83 s, state '1' at 439.92 s and failure state '0' at 635.78 s. The valve fails at 525.03 s which is 31.28 s earlier than the failure time without degradation dependency.

6 CONCLUSION

We employ the PDMP approach to develop a new method for modeling multiple dependent competing degradation processes. The significance of the proposed method lies in its capability to describe the degradation dependency between physics-based models, between multi-state models and between

the two types of models. A Monte Carlo simulation algorithm is designed to compute the components/systems reliability. The results of a illustrative case study have shown the effectiveness and capabilities of our modeling and simulation framework.

ACKNOWLEDGEMENT

The authors would like to thank Mrs. Dominique VASSEUR, Mr. Antoine DESPUJOLS and Mr. Emmanuel ARDILLON from the Department Industrial Risks Management (MRI), Electricité de France R&D for their insightful comments. The work was supported by Electricité de France Contract No. 8610-5910112096.

REFERENCES

Bronshtein, I.N., Semendiaev, K.A. & Hirsch, K.A. 1985. *Handbook of mathematics*, Van Nostrand Reinhold New York.

Chookah, M., Nuhi, M. & Modarres, M. 2011. A probabilistic physics-of-failure model for prognostic health management of structures subject to pitting and corrosion-fatigue. *Reliability Engineering & System Safety,* 96, 1601–1610.

Chryssaphinou, O., Limnios, N. & Malefaki, S. 2011. Multi-state reliability systems under discrete time semi-Markovian hypothesis. *Reliability, Ieee Transactions on,* 60, 80–87.

Cocozza-Thivent, C. 2011. Processus de renouvellement markovien, Processus de Markov déterministes par morceaux. *Online book available on the webpage: http://perso-math. univ-mlv. fr/users/cocozza. christiane/recherche-pageperso/PresentationRMetPDMP. html.*

Coudray, R. & Mattei, J. 1984. System reliability: An example of nuclear reactor system analysis. *Reliability Engineering,* 7, 89–121.

Daigle, M. & Goebel, K. Model-based prognostics under limited sensing. Aerospace Conference, 2010 IEEE, 2010. IEEE, 1–12.

Daigle, M. & Goebel, K. 2011a. A model-based prognostics approach applied to pneumatic valves. *International Journal of Prognostics and Health Management,* 2, 1–16.

Davis, M.H. 1984. Piecewise-deterministic Markov processes: A general class of non-diffusion stochastic models. *Journal of the Royal Statistical Society. Series B (Methodological)*, 353–388.

Fan, J., Yung, K. & Pecht, M. 2011. Physics-of-failure-based prognostics and health management for high-power white light-emitting diode lighting. *Device and Materials Reliability, IEEE Transactions on,* 11, 407–416.

Giorgio, M., Guida, M. & Pulcini, G. 2011. An age-and state-dependent Markov model for degradation processes. *IIE Transactions,* 43, 621–632.

Hairer, E., Nørsett, S.P. & Wanner, G. 1993. *Solving Ordinary Differential Equations I: Nonstiff Problems,* Springer.

Hairer, E., Nørsett, S.P. & Wanner, G. 1996. *Solving Ordinary Differential Equations II: Stiff and Differential-Algebraic Problems,* Springer.

Jacobsen, M. 2006. Point process theory and applications: marked point and piecewise deterministic processes, Springer.

Keedy, E. & Feng, Q. 2012. A physics-of-failure based reliability and maintenance modeling framework for stent deployment and operation. *Reliability Engineering & System Safety,* 103, 94–101.

Lewis, E. & Böhm, F. 1984. Monte Carlo simulation of Markov unreliability models. *Nuclear Engineering and Design,* 77, 49–62.

Li, Y.-F., Zio, E. & Lin, Y.-H. 2012. A Multistate Physics Model of Component Degradation Based on Stochastic Petri Nets and Simulation. *Reliability, IEEE Transactions on,* 61, 921–931.

Lisnianski, A. & Levitin, G. 2003. *Multi-state system reliability: assessment, optimization and applications*, World scientific.

Lorton, A., Fouladirad, M. & Grall, A. 2013. Computation of remaining useful life on a physic-based model and impact of a prognosis on the maintenance process. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*.

Marseguerra, M. & Zio, E. 1996. Monte Carlo approach to PSA for dynamic process systems. *Reliability Engineering & System Safety,* 52, 227–241.

Moussou, P., Cambier, S., Lachene, D., Longarini, S., Paulhiac, L. & Villouvier, V. 2001. Vibration investigation of a French PWR power plant piping system caused by cavitating butterfly valves. *ASME-PUBLICATIONS-PVP,* 420, 99–106.

Peng, H., Feng, Q. & Coit, D.W. 2010. Reliability and maintenance modeling for systems subject to multiple dependent competing failure processes. *IIE transactions,* 43, 12–22.

Rasmekomen, N. & Parlikad, A.K. 2013. Maintenance Optimization for Asset Systems With Dependent Performance Degradation. *Reliability, IEEE Transactions on,* 62, 362–367.

Straub, D. 2009. Stochastic modeling of deterioration processes through dynamic Bayesian networks. *Journal of Engineering Mechanics,* 135, 1089–1099.

Vlok, P., Coetzee, J., Banjevic, D., Jardine, A. & Makis, V. 2002. Optimal component replacement decisions using vibration monitoring and the proportional-hazards model. *Journal of the operational research society*, 193–202.

Wang, Y. & Pham, H. 2012. Modeling the dependent competing risks with multiple degradation processes and random shock using time-varying copulas. *Reliability, IEEE Transactions on,* 61, 13–22.

Wierman, T., Rasmuson, D.M. & Mosleh, A. 2007. *Common-cause failure database and analysis system: event data collection, classification, and coding*, Division of Risk Assessment and Special Projects, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission.

Zhang, S., Hodkiewicz, M., Ma, L. & Mathew, J. 2006. Machinery condition prognosis using multivariate analysis. *Engineering Asset Management*. Springer.

Expert methods in system safety and reliability

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Development of a new algorithm for optimal multi-level redundancy allocation

M.A. Farsi
Astronautic Research Institute, Iranian Space Research Center, Tehran, Iran

ABSTRACT: Nowadays, the Redundancy Allocation Problem (RAP) is increasingly becoming an important tool in the initial stages of or prior to planning, designing, and control of systems. The Multi-Level Redundancy Allocation Problem (MLRAP) is an extension of the traditional RAP such that all available items for redundancy (system, module and component) can be simultaneously chosen. Although, RAP has been considered by several researchers, attention to MLRAP is little. In this paper, we focus on this subject and develop a new method to solve MLRAP. In this paper, the total cost is assumed as the most important constraint. A new meta-heuristic optimization algorithm, called Hybrid Bat Algorithm (HBA), to solve constrained optimization problem (MLRAP) is developed. This method based on bat behavior to detect a prey. To demonstrate this method capability, a multi level system redundancy allocation is described. This method results are comprised with HGA, MA and Two Dimensional Arrays encoding and Hybrid Genetic Algorithm (TDA-HGA). For this system, optimal results are same as TDA-HGA and better than HGA and MA in all cases. Thus, proposed method is a simple and powerful tool to determine the optimal multi-level redundancy allocation.

1 INTRODUCTION

One of the most important steps to design a new system is reliability modeling and prediction. In this step, usually reliability allocation is done to achieve a desired reliability value. The typical reliability allocation problem may be stated as maximization of system reliability subject to some budget constraint, or minimization of system cost subject to the attainment of some specified level of system reliability. Nowadays, the Redundancy Allocation Problem (RAP) is increasingly becoming an important tool in the initial stages of or prior to achieve a desired reliability value and predefined performance. The industrial systems include several modules and subsystems. Each subsystem is divided to several units and finally several components (parts) are used to build a unit. The RAP is one of the most important reliability optimization problems with regards to improving the reliability of real-world systems in the design phase. The most optimal redundancy allocation methods try to solve a problem in system level and other items are ignored. In real-world systems (for example, communication systems, computing systems, control systems, and critical power systems), the influence of subsystems and components on system reliability cannot be ignored, therefore all available items for redundancy (system, module and component) should be considered. The Multi-Level Redundancy Allocation Problem (MLRAP) is an extension of the traditional RAP such that all available items for redundancy can be simultaneously chosen. Although, RAP has been considered by several researchers [1–4], attention to MLRAP is little.

The RAP has been proved to be an NP-hard problem. Thus, how to find effective approaches to it is a hot topic. There are many approaches proposed to cope with RAPs, including exact methods, max-min approaches, dynamic programming, heuristic methods, and meta-heuristic algorithms. Among them, meta-heuristic methods, especially Genetic Algorithms (GAs), are widely, successfully utilized due to their robustness, and strong ability of global search, even though sometimes they are time-consuming. From these reviews, it can be observed that, in spite of its importance in the real world, the MLRAP has rarely been investigated.

G. Levitin (2003) proposed an algorithm based on a GA framework with a universal generating function technique for the system survivability evaluation. This method aims to solve multi-level protection cost minimization problems subject to survivability constraints. Later, Yun and Kim (2004) proposed a restricted multi-level redundancy allocation model, and addressed a tri-level RAP using a customized GA. However, the customized GA employs a fixed-length vector to represent the solution to the MLRAP, and thus redundancy is

required to be allocated to only one unit in a direct line, which is defined as a set of units from the system-level unit down to one component unit. Though, both introduced methods were designed to cope with MLRAPs, they were based on strong assumptions or rigid rules that do not accord with reality. Recently, Kumar et al. (2008 and 2009) reformulated MLRAPs so that redundancy allocation can be carried out at any level of a multi-level system. In this work, a solution to an MLRAP was represented by a hierarchical structure, and a simple GA was adopted to tackle the MLRAP involved. He et al. (2013) proposed Two Dimensional Arrays encoding and Hybrid Genetic Algorithm (TDA-HGA). Their method is very useful to determine the best structure of system. Although these researches have been shown to be effective via empirical studies, its effectiveness on the MLRAP can still be improved significantly.

In this paper, we proposed a new heuristic method (hybrid Bat Algorithm) to solve MLRAP. This method use bat movement principle to find prey. This method is simple and very fast to find the best result. This method described in the next section.

2 BAT ALGORITHM

Bats are fascinating animals. Microbats are a type of bats that they use a type of sonar, called echolocation, to detect prey, avoid obstacles, and locate their roosting crevices in the dark. If we idealize some of the echolocation characteristics of microbats, we can develop various bat inspired algorithms or Bat Algorithms (BA). In echolocation, each pulse only lasts a few thousandths of a second (up to about 8–10 ms). However, it has a constant frequency which is usually in the region of 25–150 kHz corresponding to the wavelengths of 2–14 mm. In BA, the echolocation characteristics of microbats can be idealized as the following rules (Yang, Xin-She et al. 2011 and 2012):

1. All bats use echolocation to sense distance, and they also "know" the difference between food/prey and background barriers in some magical way;
2. Bats randomly fly with velocity v_i at position x_i with a fixed frequency f_{min}, varying wavelength and loudness A_0 to search for prey. They can automatically adjust the frequency (or wavelength) of their emitted pulses and adjust the rate of pulse emission r ϵ [0,1], depending on the proximity of their target;
3. Although the loudness can vary in many ways, it is assumed that the loudness varies from a large (positive) A_0 to a minimum constant value A_{min}. A_0 in this research (optimal reliability allocation) is 1 and A_{min} is zero. The basic steps of BA can be summarized as the pseudo code shown in Figure 1.

For each bat (i), its position x_i and velocity v_i in a N-dimensional search space should be specified. x_i and v_i should be subsequently updated during the iterations, since bat should be moved to target (prey). The new solutions x_i^t and velocities v_i^t at time step t are determined by:

$$f_i = f_{\min} + \left(f_{\max-} - f_{\min} \right) \beta \tag{1}$$

$$v_i^t = v_i^{t-1} + \left(x_i^{t-1} - x^* \right) f_i \tag{2}$$

$$x_i^t = x_i^{t-1} + v_i^t \tag{3}$$

where β in the range of [0,1] is a random vector drawn from a uniform distribution. Here, x^* is the current global best location (solution), which is located after comparing all the solutions among all the n bats. As the product $\left(x_i^{t-1} - x^* \right) f_i$ is the velocity increment. For implementation, $f_{min} = 0$ and $f_{max} = 1.0$ are used in this research. Initially, each bat is randomly assigned a frequency that is drawn uniformly from [0, 1].

For the local search part, once a solution is selected among the current best solutions, a new solution for each bat is generated locally using a local random walk:

Bat Algorithm

Objective function f(x), x=(x_1,x_2,…,x_n)
Initialize the bat population x_i and v_i
Define plus frequency f_i at x_i
Initialize pulse rates r_i and the loudness A_i
While (t<max number of iterations)
Generate new solution by adjusting frequency,
And updating velocities and locations/solutions (eq. 2 to 4)
If rand > r_i
Select a solution among the best solutions randomly
Generate a local solution around the selected best solution by a local random walk
End if
If (rand<A_i and f(x_i)<f(x*))
Accept the new solutions
Increase r_i and decrease A_i
End if
Rank the bats at each iteration and find their current best x*
End while
Post process results and visualization

Figure 1. Pseudo code of BA.

$$x_{new} = x_{old} + \varepsilon A^t \quad (4)$$

where, the random number ε is drawn from [–1, 1], while A^t is the average loudness of all the bats at this time step.

The update of the velocities and positions of bats has some similarities to the procedure in the standard particle swarm optimization (Kennedy et al. 1995) as f_i essentially controls the pace and range of the movement of the swarming particles. To a degree, BA can be considered as a balanced combination of the standard particle swarm optimization and the intensive local search controlled by the loudness and pulse rate.

Furthermore, the loudness A_i and the rate r_i of pulse emission have to be updated accordingly as the iterations proceed. Once a bat has found its prey, the loudness usually decreases and the rate of pulse emission increases. The loudness can be chosen as any value of convenience. In this paper, $A_0 = 1$ and $A_{min} = 0$ is used. Assuming $A_{min} = 0$ means that a bat has just found the prey and temporarily stop emitting any sound, we have:

$$A_i^{t+1} = \delta A_i^t, \quad r_i^{t+1} = r_i^0 \left[1 - \exp(-\gamma t) \right] \quad (5)$$

where δ and γ are constants. In fact, δ is similar to the cooling factor of a cooling schedule in the simulated annealing (kirkatrick et al., 1983). For any $\delta > 0$ and $\gamma < 1$:

$$A_i^t \to 0, \quad r_i^t \to r_i^0, \quad as \quad t \to \infty \quad (6)$$

According to our study and simulation results, $\delta = \gamma =$ 06–0.9 can be used for reliability allocation problem modeling.

2.1 *Modified bat algorithm*

Original bat algorithm has been proposed for continues variable. In this paper we develop this algorithm for discrete variable. Therefore, this algorithm should be modified. In proposed algorithm, the random walking and random fly are used and the next location (solution) is determined according to predefined data (or available values). In this condition, the closest state is selected as the next location for each bat. For example, a bat is characterized with A, B and C parameters, in random fly; all these parameters are calculated using equations 3 and 4. Then, distances between this new value and predefined values are compared. The closest value to determined value is selected as the next value. After this step, this new location is checked by problem constraint such as cost. If this location can satisfy constraint, this value is accepted. Some bats are motivated to better search and increase convergence speed to find the best solution. In each iteration, some of bat position and location is changed randomly. We call it motivation. In this process, some bats (5% of bats) are selected according to their position (out of the best zone particle). Then, their positions are changed randomly. Thus, modified and proposed method in this paper, it is called Hybrid Bat Algorithm (HBA). This algorithm is applied via a developed Visual Basic.Net Program.

Problem modeling and handling of constraints to MLRAP is explained in the following sections.

3 PROBLEM DESCRIPTIONS

In this section, we will first present the background description of MLRAP and then provide the formulation of this problem. To avoid confusion, the differences between the three most commonly used words in this paper are first presented below:

– Component: the elementary part of a system, at the lowest level.
– Unit: any part of a system either refers to the system, subsystems, or the components.

Also, the MLRAP investigated in this paper is formulated based on multi-level serial systems with the following assumptions.

- *Assumption 1*: The redundancy can be allocated to the units on any level.
- *Assumption 2*: The quality (reliability, cost) of each component is predefined. If one unit is not a component, its reliability, and cost are calculated based on its child units.

3.1 *Multi level serial system*

A multilevel serial system is defined as a hierarchical system with the entire system at the topmost level, the subsystems at lower levels, and the components at the lowest level. The system, subsystems, and components are all referred to as units. Child units of one unit refer to a fixed number of serial units at its immediately lower level while parent unit refer to the unit at the immediately higher level. Figure 2 shows an example of multilevel serial systems. As Figure 2 shows, U1 is a system unit with three serial child units U11; U12 and U13. U11 is the parent unit of three units: U111; U112 and U113. This structure applies to all of the units except for the component units, which have no child units.

3.2 *Multilevel series redundancy allocation model*

Redundancy could be configured to any unit from system level to component level. Once the

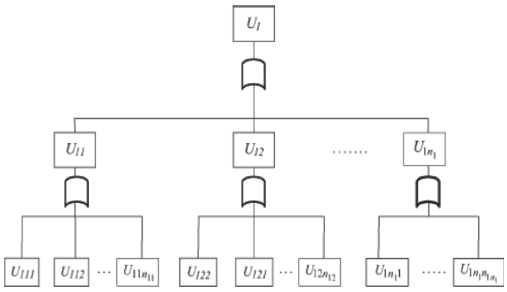


Figure 2. A general multi level series system.

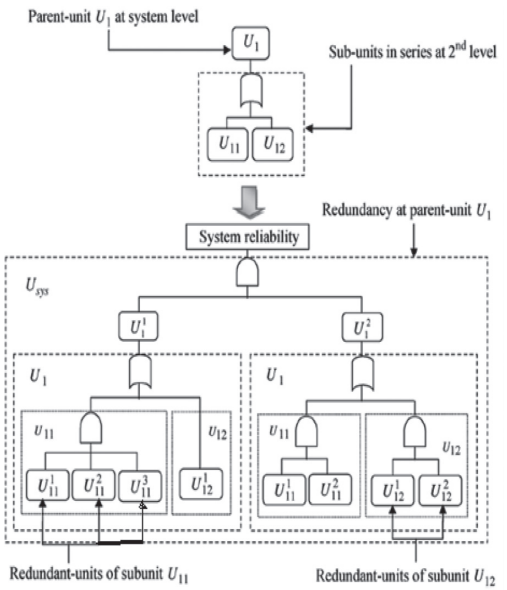


Figure 3. An example of redundancy allocation in bi-level series configuration.

redundancy is allocated to units at parent level, there will be multiple child units at lower levels. Figure 3 illustrates an example of multilevel redundancy allocation model to a bi-level serial system. Figure 3 consists of one system unit and two component units. The redundancy of unit U_1 is 2, so there are two groups of child units under U_1^1 and U_1^2 respectively. Under parent unit U_1^1 and U_1^2, the redundancy for unit U_{11} and U_{12} is (3,1) and (2,2) respectively. Example in Figure 3 indicates that it might be difficult to represent the redundancy information in one multilevel system, because the overall number of the replica of one unit in the child level is determined by the redundancy of its parent unit and the redundancy of itself. For example, the redundancy of unit U_1 is 2, so there are two groups of child units U_{11}. The redundancy of child units U_{11} belonging to different parent unit U_1^1 and U_1^2 is 3 and 2 respectively. So the overall number of replica of U_{11} is 3 + 2 = 5.

3.3 *Redundancy allocation optimization problem*

In a multilevel serial system after redundancy allocation, the reliability of the higher level units could be obtained from the reliability of all its child units including all replicas. In general, a given unit U_i in the multilevel system has n_i subunits, U_{i1}; U_{i2}; . . .; U_{in_i}, which must be connected either in series or in parallel. When x_i is the number of U_i redundant units, there are $n_i x_i$ sub-units in the level below U_i. A unit in the jth redundant unit of the mth sub-unit of U_i is denoted $U_{i,m}^j$. Thus, the reliability R_i of unit U_i for multilevel series and parallel configurations can be calculated using the following equations:

$$R_i = \prod_{m}^{n_i}\left[1 - \prod_{j}^{x_i}\left(1 - R_{i,m}^{j}\right)\right] \tag{7}$$

$$R_i = 1 - \prod_{m}^{n_i}\left[\prod_{j}^{x_i}\left(1 - R_{i,m}^{j}\right)\right] \tag{8}$$

where $R_{i,m}^j$ are reliability values of the sub-unit $U_{i,m}^j$. Each $R_{i,m}^j$ value is calculated using the above equation at the level immediately below the unit, and these calculations are recursively iterated to the level just above the very lowest hierarchical level.

Using Eq. (7, 8), the reliability of the system could be calculated. For example, the reliability of the system shown in Figure 2 is calculated as Eq. (9).

$$R = 1 - \left(1 - \left[\left(1 - \prod_{j=1}^{3}\left(1 - R_{11}^{j}\right)\right)\left(R_{12}^{1}\right)\right]\right) \times \left(1 - \left[\left(1 - \prod_{j=1}^{2}\left(1 - R_{11}^{j}\right)\right)\left(1 - \prod_{j=1}^{2}\left(1 - R_{12}^{j}\right)\right)\right]\right) \tag{9}$$

In a multi lenvel system, the cost can be calculated as the sum of its child units and some additional cost. Wang et al. (2010) sugessted following Eq. for the system cost calculation. This equation has been used by the most of research to cost modeling, we also use this equation.

$$C_i = \sum_{m=1}^{n_1}\left(\prod_{j=1}^{x_{1m}} C_{im}^{j} + \left(\lambda_{im}\right)^{x_{im}}\right) \tag{10}$$

As shown by Eq. (10), the cost C_i of unit U_i may be calculated from $C_{i,m}^j$, the cost of jth replica of mth child unit and λ_{im}, the additional cost of mth child unit when configuring redundancy. x_{im} also denotes the number of redundant units in the mth

serial child unit and n_i denotes the number of child units under U_i. Wang et al. (2010) specified that to reflect the hierarchical structure, additional cost is only introduced in the component level. In our model, we do not specify it but allow different value of kim for each unit. We only need to set $\lambda_{im} = 0$ for all the units except for the component units to meet the assumptions made by Wang et al. (2010).

For the system illustrated in Figure 2, using this equation, the system cost is calculated as Eq. 11.

$$C_{sys} = \left[\left(\sum_{j=1}^{3} C_{11}^{j} + (\lambda_{11})^3\right) + (C_{12} + \lambda_{12})\right] + \left[\left(\sum_{j=1}^{2} C_{11}^{j} + (\lambda_{11})^2\right) + \left(\sum_{j=1}^{2} C_{12}^{j} + (\lambda_{12})^2\right)\right] + (\lambda_1)^2 \tag{11}$$

MLRAP is an NP-hard problem. To find optimal state, we use a hybrid BA. In real-world problems, the several constraints such as cost, volume, mass, and etc impress the optimal solution. Cost is an important constraint and often, its influence is more than other constraints. Thus, the typical MLRAP may be stated as maximization of system reliability subject to some cost constraint. In this paper, MLRP is formulated as shown by Eq. 6.

4 EXPERIMENTAL STUDY

In this section, the performance of our TDA-HGA is evaluated on two MLRAP examples. The results are compared with MA (Wang et al., 2010) and IMA (He et al., 2012), which are the most recent algorithms in the literature and outperform other algorithms such as HGA (Kumar et al., 2008). The structures of the multilevel serial systems are illustrated in Figure 4 This system comprises three levels.

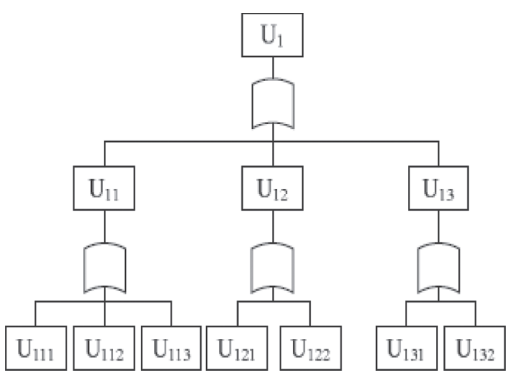


Figure 4. Experimental study.

The MLRAP for this system has been used by He et al. (2013), Wang et al. (2010), and Kumar et al. (2008) to evaluate the performance of TDA-HGA, HGA, MA. To make a fair comparison between other algorithms and HBA, the control parameters set for MA by Wang et al. (2010) were also used in experiments for HBA.

Specifically, the population size was set to 100, the maximum generation was 500, the crossover rate was set to 0.8, and the mutation rate was set to 0.1. In our algorithm, the local search rate was set to 0.2. For this system, the redundancy that can be allocated to a single unit was set between 1 and 5. The input parameters for the units in the two systems are shown in Table 1.

In this experiment, we aim to evaluate the convergence behavior of our HBA on a case study. The same group of input parameters used by Wang et al. (2010) was also used here. The cost constraint value was set to 300, and the parameters of the components of the system were given in Table 1. The best solution obtained in each generation was recorded, and the reliability of the corresponding system was calculated. The convergence curves of HBA shows that this method is very fast to find the best result. The detailed comparison of HBA and TDA-HGA, MA and HGA will be given in next sub-sections.

4.1 *Performance over different constraint values*

The previous experiment only provides a case study on which the HBA outperformed, and further comparisons between the four methods subject to different cost constraint values were carried out in this experiment. Seven cost constraint values were sampled between the intervals 150–340. All the system parameters were kept the same as the previous sub-section.

For each cost constraint value, HBA, TDA-HGA, HGA and MA were carried for 10 times. Table 2 summarizes the results of this experiment including the best reliability and cost obtained. For each cost constraint value, the reliability that is significantly better than the others is highlighted in boldface. From Table 2, we can observe that the proposed

Table 1. Input parameters.

Unit	Reliability	Cost	λ
U_{111}	0.9000	5	3
U_{112}	0.9500	6	4
U_{113}	0.8500	5	4
U_{121}	0.8500	7	4
U_{122}	0.9000	6	4
U_{131}	0.9000	8	3
U_{132}	0.8000	7	4

Table 2. MLRAP results.

Cost con.	Best solutions							
	MA		HGA		TDA-HGA		HBA	
	Reli	Cost	Reli	Cost	Reli	Cost	Reli	Cost
150	0.8005	141	0.764	148	0.8057	140	0.8057	140
180	0.8781	179	0.8617	173	0.8826	179	0.8826	179
200	0.9032	198	0.8899	198	0.9220	200	0.9220	200
250	0.9628	249	0.947	250	0.9689	249	0.9689	249
280	0.9729	278	0.9647	279	0.9853	280	0.9853	280
300	0.9849	299	0.9730	292	0.9884	299	0.9884	299
340	0.993	338	0.9835	337	0.9943	340	0.9943	340

HBA outperformed original MA and HGA on all the cases, in terms of both the quality of the best solutions, and overall performance. In particular, the best solutions found by our HBA are always better than those found by MA and HGA. HBA performed similar to TDA-HGA on best reliability in all of the test cases. TDA-HGA is a method that it is improved in several version, but our algorithm is a first version of HBA, therefore, we hope, the capability of this method is improved by developing of the proposed algorithm in next, specially, we focus on local search method in the next work.

5 CONCLUSION

In this paper, the RAP on multi-level systems is investigated. A novel Hybrid Bat algorithm (HBA) is proposed to solve this problem. This algorithm is based on micro bat fly to find prey. This method is improved and modified in this paper to determine the best result in a MLRAP. Fundamental of this method is described and capability of this method id demonstrated using a practical problem. This problem has been solved using Genetic Algorithm and Memetic Algorithm, our study shows that the proposed method is very fast and powerful to solve MLRAP. The best solutions found by our HBA are always better than those found by MA and HGA. HBA performed similar to TDA-HGA on best reliability in all of the test cases. Therefore, we hope the capability of this method is improved by developing of the proposed algorithm in next, especially; we focus on local search method in the next work.

REFERENCES

He Pan, Kaigui Wu, Jie Xu, Junhao Wen, Zhuo Jiang, 2013, "Multilevel redundancy allocation using two dimensional arrays encoding and hybrid genetic algorithm", computer and industrial engineering, vol. 64, pp. 69–83.

Kennedy, J. and Eberhart, R. 1995, "Particle swarm optimization", Proceeding of IEEE Int. Conference Neural Networks, Perth, Australia, pp. 1942–1945.

Kirkpatrick, S., Gelatt, C.D., and Vecchi, M.P. 1983, "Optimization by simulated annealing", Science, New Series, vol. 220, No.4598, pp. 671–680.

Kumar R., K. Izui, M. Yoshimura, and S. Nishiwaki, 2008, "Multilevel redundancy allocation optimization using hierarchical genetic algorithm", IEEE Trans. Reliability, vol. 57, no. 4, pp. 650–661.

Kumar, R., Izui, K., Masataka, Y., et al. 2009, "Optimal multilevel redundancy allocation in series and series–parallel systems", Computers and Industrial Engineering, vol. 57, pp. 169–180.

Levitin G., 2003, "Optimal multilevel protection in series-parallel systems," Reliability Engineering and System Safety, vol. 81, no. 1, pp. 93–102.

Wang, Z., Tang, K., & Yao, X.,2010. "A memetic algorithm for multi-level redundancy allocation". IEEE Transaction on Reliability, vol. 59, pp. 754–765.

Yang, Xin-She. 2011, "Bat algorithm for multi-objective optimization", International Journal of Bio-Inspired Computation, Vol. 3, No. 5, pp. 267–274.

Yang, Xin-She, and Amir Hossein Gandomi. 2012, "Bat algorithm: a novel approach for global engineering optimization", Engineering Computations, vol. 29, No. 5, pp. 464–483.

Yun W.Y. and J.W. kim, 2004, "Multilevel redundancy optimization in series systems," Computers and Industrial Engineering, vol. 46, pp. 337–346.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Aircraft crew escape system assistant

N. Grzesik & R. Czapla
Aviation Faculty, Polish Air Force Academy, Dęblin, Poland

ABSTRACT: In this publication the authors presented a proposal to use fuzzy expert systems in crew escape onboard pilot decision making systems. The subject of research is to ensure the ability of those systems to adapt to changing environmental conditions and, in consequence, their reliable operation (support and ensure pilots' safety. The authors use fuzzy logic to present advanced work in this field. The development of fuzzy expert aircraft onboard pilot decision making system assistant projects used by a pilot in emergency situations is referred to in the study. One of the projects was presented in the publication. It has been developed on the basis of Matlab Fuzzy Logic Toolbox and Simulink software. Complexity of the problem cause imposed restrictions. This publication is an integral part of the author's scientific researches.

1 INTRODUCTION

In this publication the authors presented a proposal to use fuzzy expert pilot decision making system assistant for determining the ejection seats mode in emergency situation during air task.

The subject of research is to ensure their ability to adapt the crew escape system to changing environmental and aircraft conditions, reliable operation and pilots' safety improvements. Advanced work in this area the authors present using of fuzzy logic.

Described the occurrences and imprecise defined terms, using classical mathematical apparatus, based on the methods required to be strictly limits or decisions such as binary logic, in which the elements belong to the set or not, Grzesik (2012); Piegat (1999); Yager & Filev (1995). Natural language operates inaccurate and quality concepts, such as "flight speed is low" or "flight altitude is high". Those concepts are very difficult to translate into machine language without losing of their nature. The values of quality, like a description of the world through words, are more natural to man. For example, determine the aircraft altitude with the words: too small, quite low, medium or too high is more natural and simpler than the estimation in meters or feet. Qualitative description is less precise and depends on the person describing it. Hence the proposal to use fuzzy expert system, where experts determine the criteria and principles of operation of these systems (base of inference rules). Proper selection of the experts is one of the most important procedures in the design process of such systems, Żurek & Grzesik (2014). The experts could be not only pilots (very experienced—a lot of flight hours on under consideration type of aircraft) but also engineers (specialized in under consideration type of aircraft ejection seats and crew escape systems), Smykla & Adamski & Burek & Walczak (2006).

Conducting extensive analysis and preliminary studies and very wide range of applications of fuzzy logic (also in safety and reliability systems), Grzesik (2006); Kacprzyk & Yager (1985); Mulawka (1996); Piegat (1999); Yager (2004); Zio (2009); Żurek & Grzesik (2014), the authors found that its properties can also be used in aircraft onboard safety systems like crew escape. For example in military aircraft equipped with ejection seats. Most of used ejection seats work in several modes. In emergency situation pilot must choose proper work mode for safe escape. All modes depend on aircraft flight parameters like flight altitude and velocity (sometimes position of an aircraft in the air is also crucial). Flight parameters data have ranges for emergency systems work. The ranges of work are divided into sets of data which determine the mode of emergency systems work. Example is presented on Figure 1.

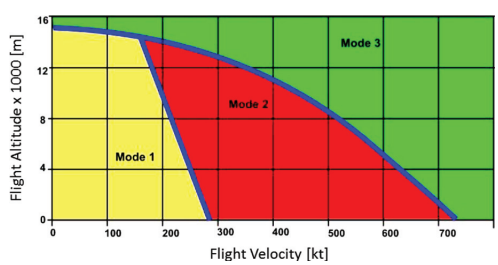


Figure 1. Ejection seat work modes, Lockheed Martin (2006).

Those sets and ranges are characteristic for fuzzy logic and provide opportunity to use the data in fuzzy inference systems. According to those facts authors made an effort to develop of fuzzy expert aircraft crew escape onboard pilot decision making system assistant projects which can be used by pilot (or work autonomously—in case of emergency situations concerns pilots unconsciousness) during the air task. One of the projects was presented in the publication. It has been developed based on Matlab Fuzzy Logic Toolbox and Simulink software, Mrozek & Mrozek (1998, 2001).

Complexity of the problem cause imposed restrictions. This publication is an integral part of the author's scientific researches.

2 PROJECT OF FUZZY EXPERT AIRCRAFT ONBOARD PILOT DECISION MAKING SYSTEM

Project is Mamdani type non-adaptive fuzzy inference system with two inputs and one output (MISO—many inputs—single output), Wrona (2013). The project is shown on Figure 2.

Speed in knots („SPEED (kt)") and pressure height in feet („ALTITUDE (ft)") are input variables. Output variable is required ejection mode („MODE").

Ejection mode selection analysis provided information about number of fuzzy sets in specific variables. „SPEED (kt)" input should consist of three fuzzy sets (membership functions—small, moderate and high). „ALTITUDE (ft)" input should consist of two fuzzy sets (membership functions—small and high). "MODE" output variable should consist of three fuzzy sets assigned to specific ejection modes (Mode 1, Mode 2 and Mode 3). However, the system work precision was unsatisfactory. To improve it more fuzzy sets in inputs should be added. Changes are presented on Figures 3–4.

Rules base consist of sixteen „If-Then" rules (Fig. 6). Premises (speed and altitude) are connected with „and" operator. Conclusions describe specific ejection modes.

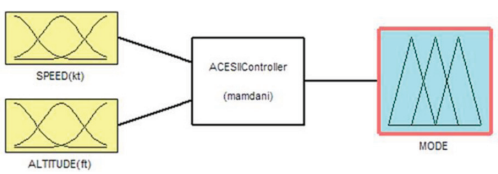


Figure 2. Fuzzy expert aircraft onboard pilot decision making system for ACES II ejection seats mode selection.

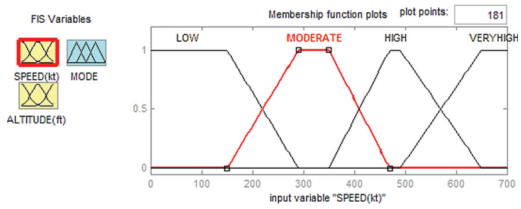


Figure 3. Fuzzy sets, shapes and ranges of membership function for SPEED input variable.

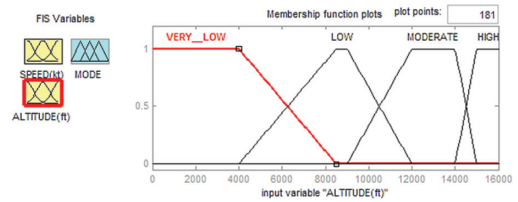


Figure 4. Fuzzy sets and shapes and ranges of membership function for ALTITUDE input variable.

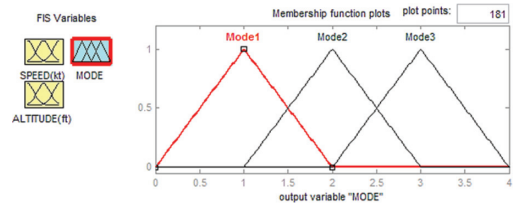


Figure 5. Fuzzy sets and shapes and ranges of membership function for MODE output variable.

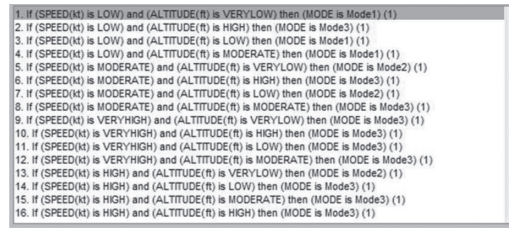


Figure 6. „If-Then" rules base.

Implication was made with „PROD" operator and aggregation with „MAX" operator.

Center of gravity method (*„Centroid"* name is used in Matlab software) was used in output variables defuzzification process (because all active rules are used in defuzzification process). It improved model sensitivity on input parameters change. Disadvantage of center of gravity method is large amount of calculation (because irregular shaped

surface, like Gausses' functions, surface integration difficulty). This disadvantage was eliminated by using polygonal membership functions.

Examples of membership functions and output variables defuzzification for specific speed and altitude data were presented on Figure 7.

For aircraft speed 100 kt, flight altitude 3000 ft, aircraft crew escape system assistant calculated that optimal ejection mode is 1. For aircraft speed 350 kt, flight altitude 8000 ft, aircraft crew escape system assistant calculated that optimal ejection mode is 2. And finally, for aircraft speed 600 kt, flight altitude 12000 ft, aircraft crew escape system assistant calculated that optimal ejection mode is 3.

Examples of control surface for specific speed and altitude data were presented on Figure 8.

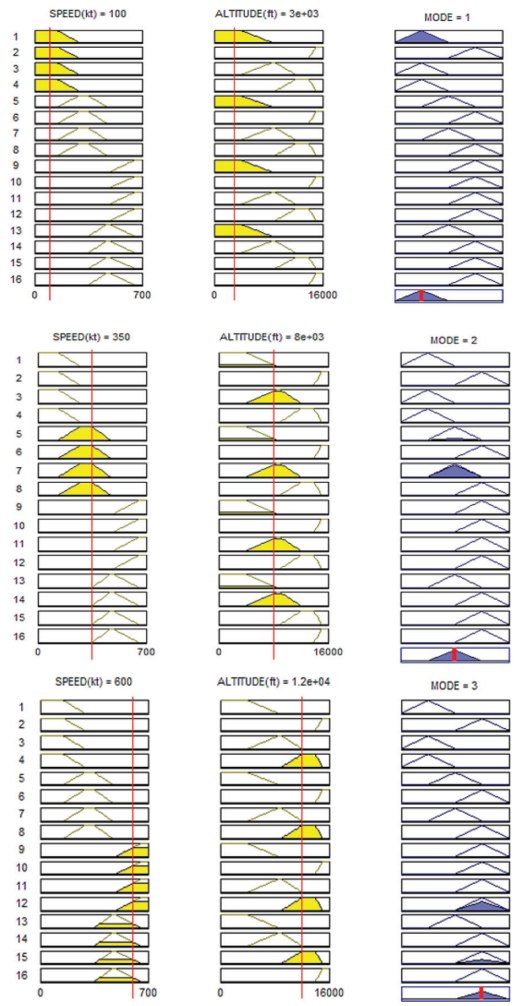


Figure 7. Rules base and defuzzification for specific speed and altitude data.

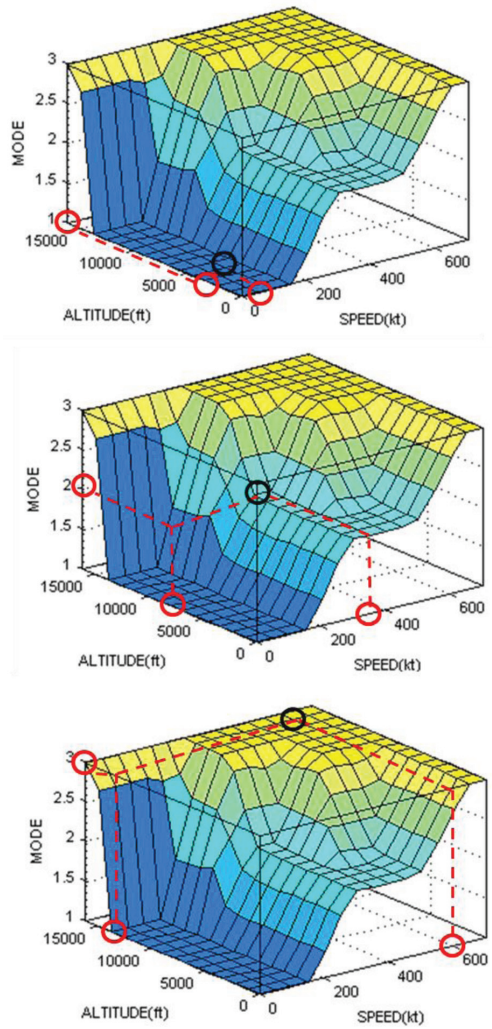


Figure 8. Control surface for specific speed and altitude data.

3 FUZZY EXPERT AIRCRAFT ONBOARD PILOT DECISION MAKING SYSTEM EXPERIMENTAL WORK VERIFICATION

Experimental system work verification is presented in Table 1. Table includes aircraft speed, altitude and ejection modes calculated by fuzzy expert inference system, Wrona (2013).

For fuzzy expert inference system and aircraft onboard crew escape data comparison, selected samples points were placed on ejection modes diagram (Fig. 9). The samples for ejection mode number 1 are yellow, for mode 2—red and finally

Table 1. Experimental system work verification for ACES II ejection seat data.

Number of samples	Speed [kt]	Altitude [ft]	Output data after defuzzification	Ejection mode
1	100	2500	1	Mode 1
2	100	5000	1	Mode 1
3	100	7500	1	Mode 1
4	100	10000	1	Mode 1
5	100	12500	1	Mode 1
6	100	15000	1	Mode 3
7	200	2500	1,33	Mode 1
8	200	5000	1,33	Mode 1
9	200	7500	1,33	Mode 1
10	200	10000	1,73	Mode 2
11	200	12500	1,71	Mode 2
12	200	15000	3	Mode 3
13	300	2500	2	Mode 2
14	300	5000	2	Mode 2
15	300	7500	2	Mode 2
16	300	10000	2,31	Mode 2
17	300	12500	3	Mode 3
18	400	2500	2	Mode 2
19	400	5000	2,14	Mode 2
20	400	7500	2,4	Mode 2
21	400	10000	2,4	Mode 2
22	400	12500	3	Mode 3
23	500	2500	2,1	Mode 2
24	500	5000	2,1	Mode 3
25	500	7500	2,78	Mode 2
26	500	10000	3	Mode 2
27	600	2500	2,72	Mode 3
28	600	5000	2,72	Mode 3
29	150	3000	1	Mode 1
30	150	6000	1	Mode 1
31	150	9000	2,4	Mode 1
32	150	12000	1	Mode 1
33	350	3000	2	Mode 2
34	350	6000	2	Mode 2
35	350	9000	2	Mode 2
36	350	12000	3	Mode 3
37	550	3000	2,35	Mode 2
38	550	6000	2,43	Mode 2
39	550	9000	3	Mode 3
40	285	680	1,98	Mode 2
41	275	850	1,92	Mode 2
42	265	1025	1,86	Mode 2
43	255	1200	1,78	Mode 2
44	245	1370	1,71	Mode 2
45	232	1550	1,6	Mode 2
46	220	1730	1,5	Mode 1
47	210	1870	1,42	Mode 1
48	200	2015	1,33	Mode 1
49	190	2160	1,25	Mode 1
50	180	2300	1,18	Mode 1

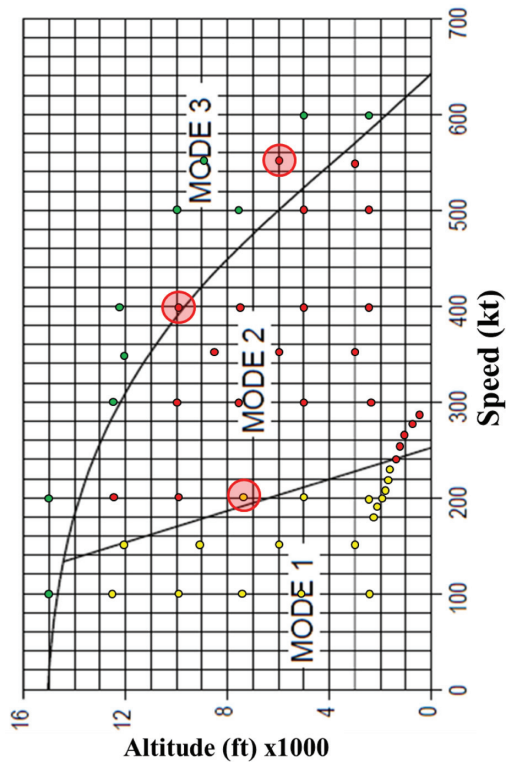


Figure 9. Experimental research results.

mode 3—green. Additionally, wrong ejection modes selected by the fuzzy expert system were marked as red circles (3 of 50 samples had wrong ejection modes selected). Due to real work of crew escape system, the mistakes of data values are insignificant. Small aircraft speed increasing solves the problem and fuzzy expert inference system work properly.

That is why further research and analysis of the system are indispensable (like: changing shapes of membership functions could eliminate the mistakes).

4 FUZZY EXPERT AIRCRAFT ONBOARD PILOT DECISION MAKING SYSTEM SIMULATION WORK VERIFICATION

Simulink software was used to verify of fuzzy expert aircraft onboard pilot decision making system work. Simulation data came from F-16 training manuals and emergency situation conducted by F-16 pilot on aircraft simulator. Designed in Simulink software ACES II fuzzy controller consists of two kinds of blocks: Signal Builder and Fuzzy Logic

Controller, Mrozek & Mrozek (1998, 2001). Signal builders (one for aircraft speed and one for aircraft altitude) present a full range of speed and altitude changes during selected air task. Data from fuzzy expert aircraft onboard pilot decision making system designed in Matlab Fuzzy Logic Toolbox are transferred to Simulink Fuzzy Logic Controller. In addition, to observe a calculation in the real time, Scope was connected to each block (to inputs and to the output).

To verify of proper system work one of emergency situation was considered. It was aircraft engine malfunction (shortly after takeoff). For that kind of F-16 malfunction pilot emergency procedure is as follows:

– pull up the aircraft to increase altitude (speed is decreased);
– drop all stores (inventory);
– eject from the aircraft.

According to simulation assumptions engine malfunctions occurs at 68 feet of altitude with 285 kt of speed (aircraft landing gear retracted). Pilot needs to confirm the malfunction. Then aircraft altitude required to be increased (to 2300 feet) speed is decreased (to 180 kt), stores dropped and at the end pilot ejects. All procedure lasts approximately 10 seconds. During that time 11 samples were received.

Emergency situation simulation input data for the samples are presented in Table 2. Inputs and output diagrams are presented on Figures 11–13.

If the emergency ejection procedure started before 6-th second after malfunction occurs,

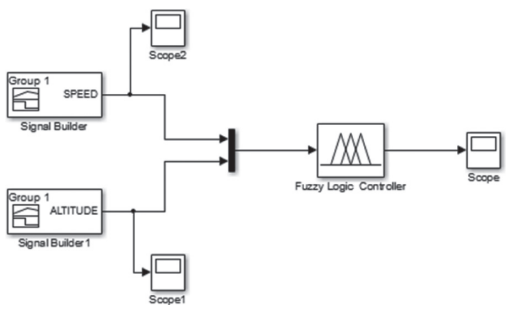


Figure 10. Project of fuzzy expert aircraft onboard pilot decision making system in Simulink software.

Table 2. Emergency situation simulation input data for the samples.

Number of samples	Speed [kt]	Altitude [ft]
1	285	680
2	275	850
3	265	1025
4	255	1200
5	245	1370
6	232	1550
7	220	1730
8	210	1870
9	200	2015
10	190	2160
11	180	2300

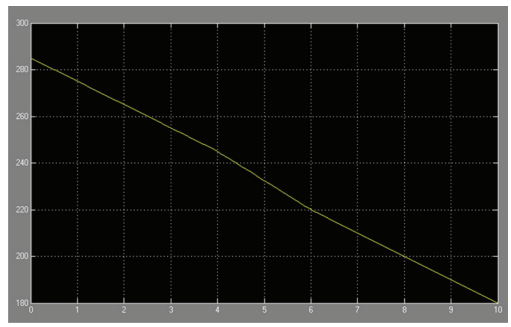


Figure 11. Speed diagram.

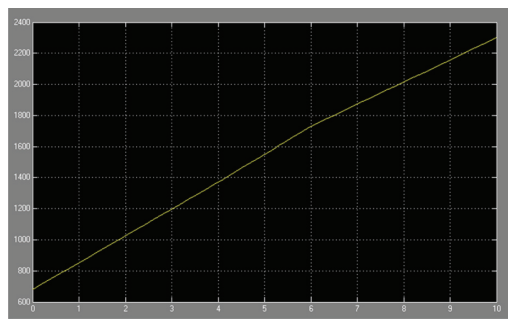


Figure 12. Altitude diagram.

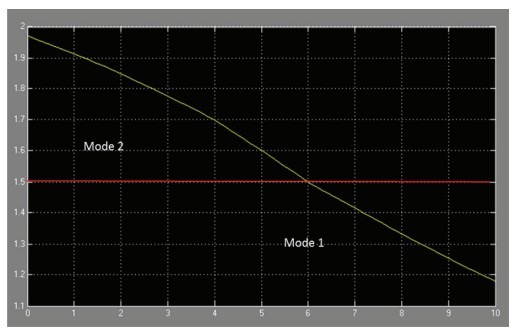


Figure 13. Mode diagram.

the fuzzy expert system would select ejection mode 2. While if the emergency ejection procedure started after 6-th second when malfunction occurs, the fuzzy expert system would select ejection mode 1.

Comparing simulation results with F-16 crew escape system, authors concluded that wrong ejection mode was selected by fuzzy expert system only once, but error value was negligible. That is why authors recognize fuzzy expert system work accurately and correctly at the system design level.

5 CONCLUSIONS

According to research results authors concluded that make full use of non-adaptive Fuzzy expert systems in emergency situations concerning use of ejection seats is possible. It is advisable to continue the research because fuzzy system work error range was minor. What is a more, dynamic change of flight parameters and measurement systems inaccuracies can be liable for errors occurrence. Nevertheless fuzzy expert aircraft onboard pilot decision making system work correctly and use it in emergency situation is possible and reasonable.

It is real time working system with high level of accuracy of ejection mode selection. However, increase a number of fuzzy sets was necessary to reach the required precision system work level. Increasing the number of fuzzy sets can lead to designing difficulties (mathematical calculations enlargement).

What is more, because of the heuristic nature of the fuzzy logic methodology there is no guarantee that the project will operationally well perform. One of the most important aspects therefore is testing and validation of the system performance. Full testing is crucial factor for those kinds of safety systems.

As a result authors propose take under consideration to use in future projects Takagi-Sugeno models or neutral network.

Use of fuzzy expert systems in aircraft emergency situation (ejection) is pioneering and never found before in the world literature.

REFERENCES

Grzesik N. 2006. Badanie efektywności eksploatacyjnej samolotu wyposażonego w układ wspomagająco decyzyjny. Rzeszów: Politechnika Rzeszowska.

Grzesik N. 2012. Podstawy sterowania rozmytego. Dęblin: Wyższa Szkoła Oficerska Sił Powietrznych.

Kacprzyk J., Yager R.R. 1985. Emergency-Oriented expert systems: A fuzzy approach. Information Sciences, Volume 37, Issues 1–3, December, Pages 143–155.

Mrozek B.; Mrozek Z. 1998. Matlab 5.x Simulink 2.x—Poradnik użytkowania. Warszawa: Wydawnictwo PLJ.

Mrozek B.; Mrozek Z. 2001. Matlab 6—Poradnik użytkowania. Warszawa: Wydawnictwo PLJ.

Mulawka J.J. 1996. Systemy ekspertowe. Warszawa: Wydawnictwo Naukowo—Techniczne.

Piegat A. 1999. Modelowanie i sterowanie rozmyte. Warszawa: Akademicka Oficyna Wydawnicza EXIT.

Smykla I.; Adamski M.; Burek M.; Walczak W. 2006. Opuszczanie samolotu w sytuacjach awaryjnych—zagrożenie bezpieczeństwa załogi. Dęblin: Wyższa Szkoła Oficerska Sił Powietrznych.

Students Training Manuals STM-410. 2006. Fort Worth: Lockheed Martin.

Wrona O. 2013. Analiza możliwości wykorzystania nieadaptacyjnych sterowników rozmytych podczas sytuacji awaryjnych w lotnictwie. Dęblin: Wyższa Szkoła Oficerska Sił Powietrznych.

Yager R.R. 2004. Uncertainty modeling and decision suport, Reliability Engineering & System Safety, Volume 85, Issues 1–3, July–September: Pages 341–354.

Yager R.R., Filev D. 1995. Podstawy modelowania i sterowania rozmytego. Warszawa: WNT.

Zio E. 2009. Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety. Volume 94, Issue 2, February: Pages 125–141.

Żurek J., Grzesik N. 2014. Fuzzy expert aircraft onboard control systems assistant. Safety reliability and risk analysis: Beyond the horizon. ESREL conference proceedings. London: Taylor & Francis Group: Pages 250–251.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A fuzzy system for evaluation of baggage screening devices at an airport

J. Skorupski
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

P. Uchroński
Upper Silesian Aviation Group, Poland

ABSTRACT: An airport is a complex engineering system; it is composed of many elements interconnected with numerous internal relations with a strongly pronounced role of the human factor. One of the specific tasks carried out by the Airport Managing Entity (AME) is to configure the Airport Security System (ApSS) so that to attain the expected level of confidence in the airport safety and security. This task consists in selection of infrastructure, technical equipment, allocation of personnel and financial means that are necessary to perform all functions of the ApSS. One of the aspects of the configuration of the ApSS is the allocation of available x-ray baggage screening devices searching for items prohibited for transportation. To make this allocation, we need to know how effective these devices are (in terms of detecting prohibited items). This assessment is dependent on several factors which are treated as linguistic variables and are input to fuzzy inference system: the ability to detect explosives (linguistic variable *Detectability*), the number of detection lines (linguistic variable *Number of detection lines*), the effectiveness of the TIP (Threat Image Projection) system (linguistic variable *TIP evaluation*) and the age of the machine (linguistic variable *Device age*). Some of these elements are difficult to objective assessment, as they are heavily dependent on the human factor or the information is uncertain and incomplete. So fuzzy ApSS analysis is proposed. The output from the fuzzy inference system is linguistic variable *Device evaluation*. The meaning of this variable is the ability to protect the aircraft against prohibited items. The proposed new method of assessing the airport baggage screening system involves the construction of a hierarchical fuzzy inference system. Such a system has been built with the use of the compositional fuzzy inference rule. The usefulness of the method is exemplified for Katowice-Pyrzowice international airport, for which an assessment of devices has been performed. The results show that not only allocation of specific devices for specific control points is important for the security of passengers. Also important are the locally accepted principles of their work, which so far are not specified by international regulations. This applies for instance to the selection of the number (frequency) of TIP images. Preliminary analyzes show that the proposed approach can be effective as part of an expert system for supporting the airport operator in configuring ApSS.

1 INTRODUCTION

An airport consists of numerous elements which are linked with various internal relations with a strong impact of the human factor. It is therefore a complicated socio-technical system. The correct operation of an airport requires providing the appropriate level of security by the Airport Managing Entity (AME). One of the aspects involved in providing security is protection against the acts of unlawful interference (ICAO 2010). The research related to providing the continuity of operation of an airport conducted so far focused mainly on the problem of operational availability i.e. the reliability of various technical components of the airport system considered together with their structural reliability as well as the external factors e.g. weather conditions (Kozłowski 2004). Among papers that are strictly related to the problems of airport security it is worth to note the work of (Gkritza et al. 2006), which indicates the need to provide the proper security level at an airport but at the same time minimize the nuisance caused by the security control process to the passengers. The new way of meeting the requirements for security control were suggested in (de Lange et al. 2013), where considerable savings were found by using the "virtual queues".

Airport Managing Entity (AME) is responsible for keeping the airport in operation availability. One of the specific tasks performed by the AME is configuring the Airport Security System (ApSS) so that the required level of trustworthiness regarding its safety is reached (Kirschenbaum et al. 2012). This

task requires the selection of infrastructure, technical equipment and personnel allocation (Soukour et al. 2013) and assigning the financial means required for the implementation of all ApSS functions. Configuring the ApSS in a rational manner requires the knowledge on how the different elements of the complicated structure affect the final security level of an airport (Gerstenfeld & Berger 2011).

Review of literature indicates that there are no effective methods for the evaluation of airport security. With this in mind, we suggest a mathematical model based on the theory of fuzzy reasoning whose output would be an evaluation of the airport security system as a factor for providing the continuity of operation of an airport. This evaluation will be expressed as linguistic variable value and the method used to obtain it will involve all the required factors related to airport security: screening baggage, control of passengers, perimeter security and security culture. It will also include the impact of the environment in the form of the organisational and operational characteristics.

In this work we present the idea of evaluation the entire ApSS, however, we will concentrate on more detailed description of the local model for evaluating of the x-ray equipment used for scanning of the checked and hand luggage. The developed model, together with its computerised implementation in the SciLab environment may be treated as an expert system supporting the decision making process for persons who are in practice responsible for selecting infrastructure components, technical equipment and personnel required by the airport security system.

2 AIRPORT SECURITY SYSTEM

An Airport Security System (ApSS) is used to prevent acts of unlawful interference. This notion is defined in (ICAO 2010) as an unlawful and purposeful act involving e.g.:

- destruction of an aircraft or causing damage to it,
- placing objects, devices or substances on-board an aircraft which may cause the destruction of the aircraft,
- hijacking an aircraft,
- destruction of ground or on board equipment or causing interference in their operation,
- providing false information which causes hazard for people and their belongings in aviation communication,
- destruction or severely damaging devices at an airport.

A practical method of achieving the goals of the ApSS is to perform a security control of the persons and their baggage before they are boarded on an aircraft. On the other hand it also involves the so called perimeter security i.e. the prevention of unlawful access to the airport area.

There are numerous structures related to security control which are discussed in detail in (Uchroński 2011). The security control is performed at the Security Control Points (SCP) and is a complex process that involves numerous devices whose effectiveness and pace of operation has a big impact on the ability of the ApSS to perform its functions (Hainen et al. 2013). The following devices are used:

- metal detector gates,
- manual metal detectors,
- x-ray baggage screening equipment used for detecting explosives and other prohibited items (Wetter 2013),
- radioactive material detectors.

This paper analyses the effectiveness of equipment (x-ray devices) used to detect prohibited items in registered and hand baggage.

3 MODEL OF THE AIRPORT SECURITY SYSTEM

Four basic factors which influence the airport security level may be defined. These are: the baggage screening system, the passenger control system, external security and security culture. A general schematic of relations between these factors is presented in Figure 1.

Each of the elements (rectangles) presented in Figure 1 is a complex structure. The internal relations are highly dependent on the human factor and other factors which are not subject to precise description. As a result, they will be treated as representations of fuzzy hierarchical local models with numerous inputs. Establishing the values of linguistic variables *Baggage Screening*, *Person Control*, *External Security* and *Security Culture* requires a further development of the diagram. Due to the limited volume of the paper it is impossible to present the entire diagram structure. In order to illustrate the essence of the method, Section 5 discusses a local model used for the evaluation of devices used for registered and hand baggage screening.

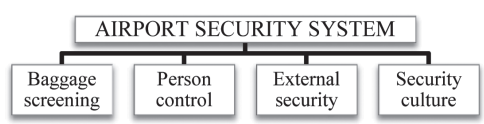


Figure 1. Diagram of a fuzzy model of main factors influencing the security level at an airport.

4 CONCEPT FOR THE EVALUATION OF AN AIRPORT SECURITY SYSTEM

This paper suggests an evaluation of an airport security system based on a hierarchical model of fuzzy reasoning. This approach results from the fact that the tested system is heavily influenced by the human factor and other elements, which are not subject to unequivocal and precise description. It is impossible to detect the functional relationships between the various factors which influence the effectiveness of the security system and an evaluation of the security level. In such cases it is required to use expert opinions. As we have to deal with expert opinions, it is a known fact that very often they are formulated in a descriptive and an imprecise way. We must therefore view the decision making problem in context of uncertainty related to decision making (Dubois & Prade 1992). All this locates the decision making problem in an area described by e.g. the theory of fuzzy sets or rough sets (Greco et al. 2001).

This paper focuses on fuzzy reasoning. A similar approach, although related to the evaluation of an aircrew status, was presented in the work by (Skorupski & Wiktorowski 2013). This paper is a follow up to the work by (Skorupski & Uchroński 2014), where the general structure of interaction model in the airport security model is discussed in detail.

A fuzzy set A will denote a set of

$$A = \left\{ \left(x, \mu_A(x)\right) : x \in X, \mu_A(x) \in [0,1] \right\} \tag{1}$$

where μ_A is the membership function of this set and X is a set of considerations.

A linguistic variable is a variable whose values are words or sentences in a natural or artificial language. These words or sentences will be called the linguistic values of a linguistic variable.

Our models will most often assume that the membership functions of linguistic variable values have a trapezoidal shape and that a typical membership function with the parameters (a,b,c,d) is as follows:

$$\mu_i(x;a,b,c,d) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a < x \le b \\ 1, & b < x \le c \\ \dfrac{d-x}{d-c}, & c < x \le d \\ 0, & x > d \end{cases} \tag{2}$$

Within the scope of the reasoning process we will use the input value fuzzification block, reasoning block using a number of rules and the defuzzification block. The rule sets will be created using experts' opinions, in particular those presented by persons responsible for organising a Security Management Systems (SeMS) at airports. Such set may contain classic non-fuzzy implications as well as fuzzy implications. In the second case we will use the so called compositional method of reasoning introduced by Zadeh (1973) which uses a generalised "modus ponens" fuzzy reasoning rule. This results in the following reasoning scheme (Kacprzyk 1986), where P, P', Q, Q', S are fuzzy relations.

$$\begin{aligned} &I : P \Rightarrow Q \\ &P : P' \\ &C : P' \circ (P \Rightarrow Q) \end{aligned} \tag{3}$$

where I denotes implication, P—premise, C—conclusion, while "$\circ$" is a max-min composition, defined on the sets X, Y, Z, whose result for fuzzy relations $A \subset X \times Y$ and $B \subset Y \times Z$ is a fuzzy relation $A \circ B \subset X \times Z$ with a membership function:

$$\mu_{A \circ B}(x,z) = \vee_{y \in Y} (\mu_A(x,y) \wedge \mu_B(y,z)), \quad \forall x \in X, \forall z \in Z \tag{4}$$

Relations P and P' are often constructed on the basis of the AND operator, as in Tables 1 and 2. We will use implications in the form of fuzzy conditional sentences (rules) i.e.

$$IF\ P\ THEN\ Q\ ELSE\ S \tag{5}$$

The conditional sentence is equal to a certain fuzzy relation $R \subset X \times Y$; we will use the max-min rule that was selected from the numerous definitions of such fuzzy relations found in the literature

$$R = (P \times Q) + (\sim P \times S) \tag{6}$$

which is expressed in the form of the following membership function

$$\mu_R(x,z) = \left(\mu_P(x) \wedge \mu_Q(y)\right) \vee \left(\left(1 - \mu_P(x)\right) \wedge \mu_S(y)\right), \quad \forall x \in X, \forall y \in Y \tag{7}$$

If we write down the reasoning scheme (3) in the form of a fuzzy reasoning system we will reach the following form

$$\begin{aligned} &I : IF\ P\ THEN\ Q \\ &P : x\ IS\ P' \\ &C : y\ IS\ Q' \end{aligned} \tag{8}$$

where $P, P' \subset X$, $Q, Q' \subset Y$

Table 1. Fuzzy reasoning rules for the *TIP Evaluation* local model.

Rule	Premise	Conclusion
R1	TIP_Number IS very_low AND TIP_Frequency IS very_high	TIP_Evaluation IS very_low
R2	TIP_Number IS low AND TIP_Frequency IS high	TIP_Evaluation IS low
R3	TIP_Number IS medium AND TIP_Frequency IS medium	TIP_Evaluation IS medium
R4	TIP_Number IS high AND TIP_Frequency IS low	TIP_Evaluation IS high
R5	TIP_Number IS very_high AND TIP_Frequency IS very_low	TIP_Evaluation IS very_high

Table 2. Fuzzy reasoning rules for the *Device evaluation* local model.

Rule	Premise	Conclusion
R1	Detectability IS very_low	Device_evaluation IS very_low
R32	Detectability IS low AND TIP_Evaluation IS medium AND Number_of_detection_lines IS low AND Device_age IS very_low Detectability IS medium AND	Device_evaluation IS low
R102	TIP_Evaluation IS low AND Number_of_detection_lines IS high AND Device_age IS very_low Detectability IS high AND	Device_evaluation IS medium
R193	TIP_Evaluation IS medium AND Number_of_detection_lines IS high AND Device_age IS low Detectability IS very_high AND	Device_evaluation IS high
R292	TIP_Evaluation IS very_high AND Number_of_detection_lines IS medium AND Device_age IS very_low	Device_evaluation IS high

The result of reasoning Q' is specified according to the compositional rule of inference as

$$\mu_{Q'}(y) = \bigvee_{x \in X} \left(\mu_{P'}(x) \wedge \mu_R(x,y)\right), \forall y \in Y \tag{9}$$

where $R \subset X \times Y$ is a fuzzy relation specified by the formulas (6–7). In such cases the membership function of the result has the final form of

$$\mu_{Q'}(y) = \bigvee_{x \in X} \left(\mu_{P'}(x) \wedge \left(\left(\mu_P(x) \wedge \mu_Q(y)\right) \vee \left(1 - \mu_P(x)\right)\right)\right), \quad \forall y \in Y \tag{10}$$

A fuzzy reasoning system implemented in the SciLab package and applied in Section 5 uses the above inference reasoning method specified in formulas (8–10).

5 A FUZZY MODEL FOR THE EVALUATION OF X-RAY BAGGAGE SCREENING DEVICES AT AN AIRPORT

5.1 *General structure of the fuzzy model "Device evaluation"*

Figure 1 presents a general diagram of interactions in the *Airport Security System* model. As mentioned before it is a complex hierarchical structure. One of its elements is the *Screening baggage* local model. It consists of two local sub-models: *Hand baggage* and *Registered baggage*. Each of these is further composed of three sub-models: *Device evaluation*, *Personnel evaluation* and *Control procedure*.

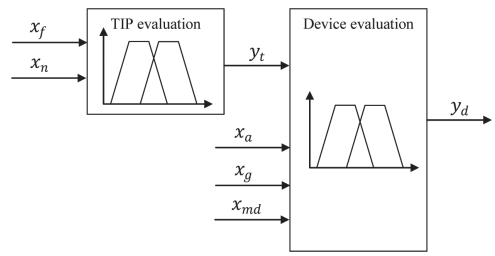


Figure 2. Diagram of the *Device evaluation* fuzzy model.

The subject of analysis in this section is the *Device evaluation* fuzzy model. Its diagram is presented in Figure 2. The output of the fuzzy reasoning system (y_d) associated with this fuzzy model is dependent on four input variables: *Detectability*(x_{md}), *TIP evaluation* (y_t), *Number of detection lines* (x_g), *Device age* (x_a).

5.1.1 *"Detectability" input variable*

The *Detectability* linguistic variable characterises the technical parameters of the x-ray devices which determine the effectiveness of the entire security control process. This category encompasses the conventional RTG devices and EDS (Explosive Detection System) devices. The latter are more

advanced as they are able to detect explosives on their own. In case of conventional RTG devices the effectiveness of security control rests in the most part on the abilities of the Security Screener (SS). EDS devices, apart from the parameters of conventional equipment, also allow:

– detecting explosive materials located in the baggage or other parcels irrespective of their shape, location and position and signalling their presence using an alarm,
– sending an alarm signal in case of: detecting an object that is used to prevent the detection of explosive materials, contents of the baggage or parcel are too dense to perform an control.

The values assumed by the *Detectability* linguistic variable are: *very small*, *small*, *medium*, *big* and *very big*. It is assumed that the membership functions of given fuzzy sets will have a trapezoidal shape. To establish them we will use a standard procedure for the evaluation of the device that is performed during every start-up. This calls for using a standard test sample that help verify if the device meets the minimum values related to set requirements (European Commission 2010):

1. resolution of a single wire,
2. useable penetration,
3. spatial resolution,
4. singular penetration (thin material),
5. singular penetration (dense material),
6. differentiating materials,
7. detection of explosive material and signalling,
8. signalling the detection of an item preventing the detection of explosive materials,
9. signalling if the contents of the baggage or parcel are too dense to perform an control,
10. indicating the location of the item that triggered the alarm.

The end result of the test is a filled record form which specifies the number of requirements being met. For a standard, fully functional RTG device this number is 6 (requirements 1–6) and for an EDS class device—10 (additional requirements 7–10). Other values are possible for devices which are partially damaged during operation which is not noticed by the technical personnel. The representation of the *Detectability* linguistic variable is shown in Figure 3.

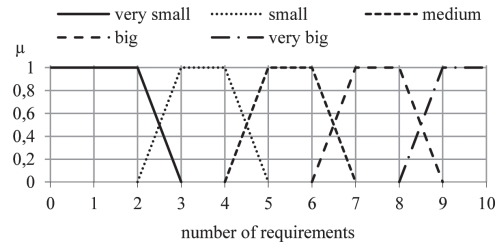


Figure 3. Membership functions of the *Detectability* linguistic variable values.

5.1.2 *"TIP Evaluation" local model*

The second input variable in the device evaluation model is the variable specifying the TIP (Threat Image Projection) system effectiveness. In reality this variable is an output of another local model with *TIP number* (x_n) and *TIP frequency* (x_f) being the fuzzy input variables. The TIP system used for projection of virtual threat images is one of the tools which allow for constant improvement of the operator's skill. Its idea is to project a virtual prohibited item on the image of the piece of baggage being screened. The task of the operator is to detect the virtual object in the image and confirm this fact by pressing the button on the RTG device. This increases the awareness of screening personnel who are forced to search for prohibited items in the baggage image more often than is the case when the TIP system is not used. The effectiveness of the TIP system depends on two parameters:

– number of dedicated TIP images (number of TIPs), which must be numerous enough to prevent memorising their configuration, shape, type etc.; the greater the number of virtual images available in the device the more effective it is at screening baggage,
– frequency at which the TIP images are projected on the real screen image (TIP frequency); in this case, too high frequency of the TIP images in relation to the number of baggage items being screened may cause automatic indications of suspect baggage without an in-depth analysis of the reviewed baggage image.

TIP frequency is established based on individual practice at every airport and this value is kept secret. The *TIP number* and *TIP frequency* input variables assumed for this model are shown in Figures 4–5.

The output variable of the local fuzzy reasoning model for TIP evaluation is presented in Figure 6. This variable is at the same time the input variable for the device evaluation model. The example assumed fuzzy reasoning rules are shown in Table 1.

5.1.3 *"Number of detection lines" input variable*

The x-ray devices differ with the number of generators creating the image. Each generator creates one detection line which allows for creating an image seen from one set direction (angle). In a multiple generator variant, the screened baggage (as it passes through the device's tunnel) is inspected

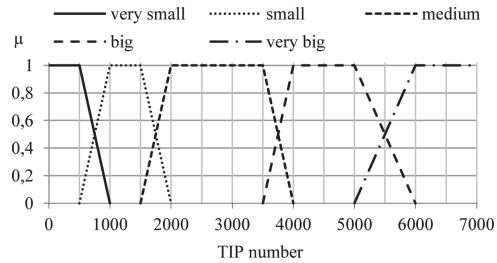


Figure 4. Membership functions of the *TIP Number* linguistic variable.

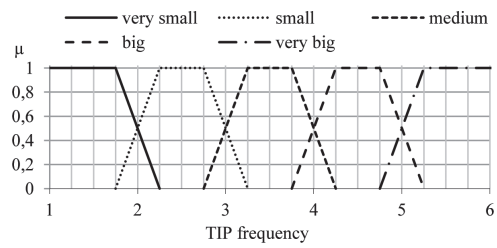


Figure 5. Membership functions of the *TIP Frequency* linguistic variable.

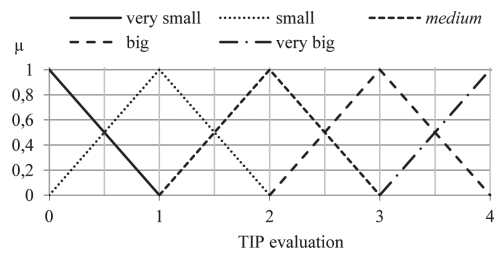


Figure 6. Membership functions of the *TIP Evaluation* linguistic variable.

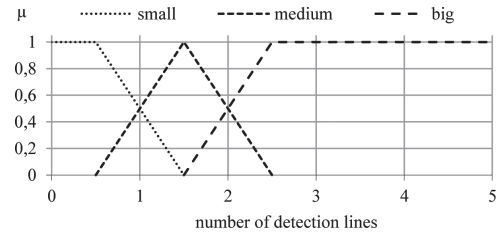


Figure 7. Membership functions for the *Number of detection lines* linguistic variable.

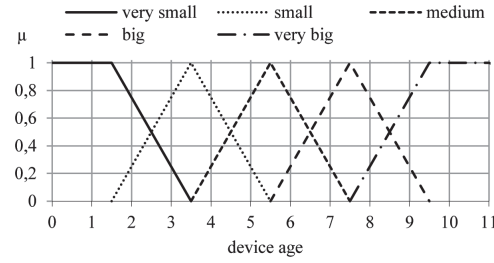


Figure 8. Membership functions of the *Device age* linguistic variable.

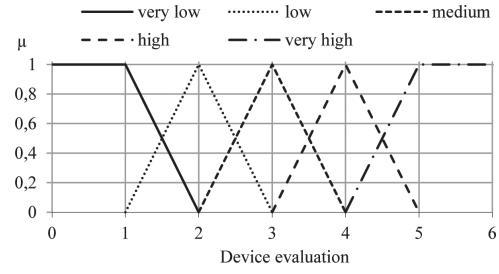


Figure 9. Membership functions of the *Device evaluation* output variable.

by several beams of Roentgen radiation which generates signals in multiple detectors installed in the device at various angles. This allows to obtain images as seen from different directions. Therefore, the probability of detecting a prohibited item hidden in the baggage is much greater if a device with several radiation generators is used during security control. The membership functions for the *Number of detection lines* linguistic variable are shown in Figure 7.

5.1.4 *"Device age" linguistic variable*

The fourth factor taken into account in the analysis is the device age. It influences the probability of failure of the device during operation. Due to frequent reliability checks of the device (at every start-up) the possible time of operation at less the full operational capability is relatively limited. Thus, the age of the device will also be considered a minor factor in the evaluation. The assumed membership functions for different values of the *Device age* linguistic variable are shown in Figure 8.

5.1.5 *Output variable of the "Device evaluation" local model*

The *Device evaluation* local model assumes a five-level scale of linguistic variable values. This is shown in Figure 9.

The fuzzy reasoning system is completed by 301 fuzzy rules defined by expert practitioners; some examples are shown in Table 2.

Table 3. List of baggage x-ray devices at the Katowice-Pyrzowice International Airport.

No.	Manufacturer/model	x_n	x_f [%]	x_{md}	x_g	x_a	y_d
1	Heimann 6040 aTiX	6000	2.8	10	4	6	5.2
2	Heimann 6046 si	6000	2.8	6	1	7–8	2.8–3.1
3	Heimann 6040 i	6000	2.8	6	1	9–10	2.1–2.5
4	Heimann 100100 T	0	0	6	1	7	1.4
5	Smiths 10080 EDX-2is	904	2.8	10	2	8	4.4
6	Smiths 100100 T-2is	599	2.8	6	2	4	3.5
7	Smiths 100100 V-2is	0	0	6	2	3	2.7

5.2 *Example of device evaluation for Katowice-Pyrzowice International Airport*

The Katowice-Pyrzowice International Airport has almost 2.5 million passengers per year with 1.7 million passenger in scheduled traffic and about 0.8 million in charter. In the years 2011–2013 about 30 thousand air operations per year were performed (GTL, 2014a). The Upper Silesian Aviation Group, the entity managing the airport has developed and implemented its own security policy. One of its elements is to perform effective and proactive corrective actions in order to minimise the risk (GTL, 2014b). One of the elements of such actions is the evaluation of x-ray devices presented below.

At the Katowice-Pyrzowice International Airport baggage screening is performed using standard commercially available equipment listed in Table 3. Using the hierarchical fuzzy model described above and a calculation tool created using the SciLab package utilising the max-min compositional inference rule based on relations (8–10) the following results were achieved which are specified in the last column of Table 3. It contains defuzzified values of the *Device evaluation* linguistic variable (see Fig. 9).

Analysis of the results shows that the devices operating in the EDS standard ($x_{md} = 10$) are evaluated as *very high* or *high* (see Fig. 9). The evaluation of the device without the EDS function ($x_{md} = 6$) depends mostly on the number of detection lines. In case of devices with two lines the evaluation results are close to *medium* even though these devices have very few TIP images or do not have such function at all (no 6–7). Devices with a single detection line are rated in the scope from *very low* for a x-ray without TIP image function (no 4), through *low* for older device (no 3), to *medium* for newer devices of this class (no 2).

6 METHOD FOR SELECTING EQUIPMENT AND WORK TECHNOLOGY FOR A X-RAY DEVICES AT AN AIRPORT

It is obvious that the most beneficial solution would involve using only new, modern EDS devices with numerous detection lines and equipped with many TIPs. However, this is a very costly solution, which is often hardly justified by the volume of air traffic.

The presented method for the evaluation of a x-ray devices allows us to present an interesting solution in the field of work technology. This solution is a result of analysis of impact of increasing the frequency of TIPs. A model of relation between the *Device Evaluation* output variable and *TIP Frequency* input variable has been analysed by changing the x_f value in the scope between 0 and 6%. Figure 10 shows the results for an EDS standard device but with a small number of TIPs using the Smiths Detection 10080 EDX-2is as an example.

As we can see the x-ray devices's evaluation result depends on the frequency of TIP images. The borderline values which guarantee the highest evaluation values for the device reaching 4.4, which is the intermediate zone between the *high* and *very high* result, are values 1% and 2.8%. Exceeding those values would result in lowering the effectiveness of the baggage screen system to as low as level 3.1 i.e. *medium* value. The decrease of the result is explained by the low number of TIPs available in the x-ray machine. High frequency of images not only lowers the alertness of the SIO but also allows him to memorise the TIPs, thus decreasing the effectiveness of the control.

In case of a standard RTG device, the selection of the correct TIP frequency may also result in increased work effectiveness (Fig. 11).

As we can see the evaluation result for this device is not affected very much by the TIP display frequency. This is understandable as they are very numerous and the SIO is unable to memorise them. Yet, the remark made in the chapter describing input variables still applies—too high TIP frequency lowers the alertness of the operator. Assuming a work technology which displays more than 3% of TIPs results in an evaluation result of about 3.0, which is equal to the *medium* value. Lowering the TIP frequency to about 1.6–1.8% allows slightly improve the effectiveness of the system (to 3.3).

Taking into consideration the borderline frequencies for device with a low number of TIPs and

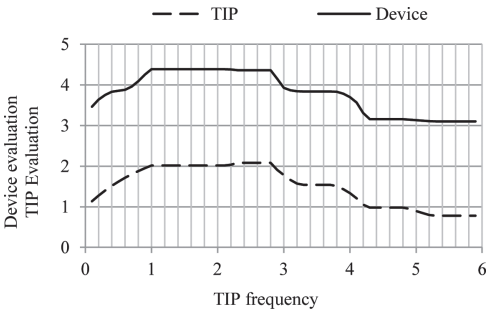


Figure 10. Relation between the *TIP Evaluation* and *Device Evaluation* variables and the *TIP Frequency* variable for the Smiths Detection 10080 EDX-2is.

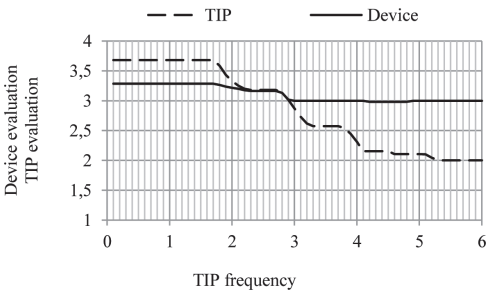


Figure 11. Relation between the *TIP Evaluation* and *Device Evaluation* variables and the *TIP Frequency* variable for the Heimann Smiths 6046 si device.

for devices with a high number of TIP we suggest assuming the *TIP Frequency* parameter value at about 1.8% as a simple and cost-free method of improving the effectiveness of baggage screening system at the airport.

7 SUMMARY AND CONCLUSIONS

The method for the evaluation of effectiveness of x-ray devices at an airport suggested in this paper allows for simple evaluation of individual devices. The developed *Device Evaluation* fuzzy model is part of a bigger model constructed in order to improve the effectiveness of the airport's entire security system.

The evaluation of effectiveness, although important, needs not to be a goal by itself. The suggested approach allows for researching the possible changes in equipment and work technology in order to find solutions that are better than those currently in use. The presented practical example of the Katowice-Pyrzowice International Airport shows that this is not only possible but also does not necessarily require any expenditure.

REFERENCES

de Lange, R., Samoilovich, I. & van der Rhee, B. 2013. Virtual queuing at airport security lanes, *European Journal of Operational Research* 225(1): 153–165.

Dubois, D. & Prade, H. 1992. On the relevance of non-standard theories of uncertainty in modelling and pooling expert opinions. *Reliability Engineering & System Safety* 36: 95–107.

European Commission 2010. *Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security*, EU Official Journal, L55/1, Brussels.

Gerstenfeld, A. & Berger, P.D. 2011. A decision-analysis approach for optimal airport security, *International Journal of Critical Infrastructure Protection* 4(1): 14–21.

Gkritza, K., Niemeier, D. & Mannering, F. 2006. Airport security screening and changing passenger satisfaction: An exploratory assessment, *Journal of Air Transport Management* 12(5): 213–219.

Greco, S., Matarazzo, B., & Slowinski, R. 2001. Rough sets theory for multicriteria decision analysis, *European Journal of Operational Research* 129: 1–47.

GTL 2014a. http://www.katowice-airport.com/pl/lotnisko/statys tyki-roczne (access on 3.1.2014).

GTL 2014b. http://www.katowice-airport.com/pl/lotnisko/polity ka-bezpieczenstwa (access on 3.1.2014).

Hainen, A.M., Remias, S.M., Bullock, D.M. & Mannering, F.L. 2013. A hazard-based analysis of airport security transit times, *Journal of Air Transport Management* 32(0): 32–38.

ICAO 2010. *Civil Aviation Security Manual—Protection Against Unlawful Interference, International Civil Aviation Organization*, Doc. 8973.

Kacprzyk J. 1986. *Fuzzy sets in system analysis*, Państwowe Wydawnictwo Naukowe, Warsaw.

Kirschenbaum, A., Mariani, M., Van Gulijk, C., Rapaport, C. & Lubasz, S. 2012. Trusting technology: Security decision making at airports, *Journal of Air Transport Management* 25(0): 57–60.

Kozłowski M. 2004. *Method for evaluation of an airport's operational availability*, PhD thesis, Faculty of Transport, Warsaw University of Technology, Warsaw.

Skorupski, J. & Uchroński, P. 2014. Model for the evaluation of the airport security system, *Zeszyty Naukowe. Transport / Politechnika Śląska* 83: 251–260.

Skorupski, J. & Wiktorowski, M. 2013. The problem of crew status assessment in the context of air traffic safety, *Prace Naukowe Politechniki Warszawskiej. Transport* 96: 401–411.

Soukour, A., Devendeville, L., Lucet, C. & Moukrim, A. 2013. A Memetic Algorithm for staff scheduling problem in airport security service, *Expert Systems with Applications* 40(18): 7504–7512.

Uchroński P. 2011. Impact of terminal infrastructure on the security of civil aviation, *Zeszyty Naukowe. Transport / Politechnika Śląska* 72: 101–108.

Wetter, O.E., 2013. Imaging in airport security: Past, present, future, and the link to forensic and clinical radiology, *Journal of Forensic Radiology and Imaging* 1(4): 152–160.

Zadeh, L.A., 1973. Outline of a new approach to the analysis of complex systems and decision processes, *IEEE Transactions on Systems Man and Cybernetics* 3: 28–44.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantification and modelling of epistemic uncertainties for availability risk of future offshore wind farms using expert judgment

A. Zitrou, T. Bedford & L. Walls
Department of Management Science, University of Strathclyde, Glasgow, Scotland

ABSTRACT: We develop a model to capture state-of-knowledge, as well as aleatory, uncertainties associated with off-shore wind farm technologies, processes and environments. Our goal is to better understand systemic technology risks and support investment decisions for effective, efficient risk management. Typical epistemic uncertainties present in the offshore wind context are articulated. A protocol for eliciting expert judgment to quantify variables representing epistemic uncertainties and other relevant model parameters is presented. We discuss the elicitation of judgments from an expert panel of energy company technical specialists and show an application of our model to a generic new design offshore wind farm.

1 INTRODUCTION

The UK government has set ambitious renewable energy targets to address the issue of increased carbon emissions (Department of Energy & Climate Change, 2013). To meet these targets, capacity is being increased by, for example, building offshore wind farms which use novel large-scale, complex technology and are sited further from shore. However, deploying innovative technology in partially understood environments introduces the potential for systemic weaknesses associated with the design, manufacturing and operation of wind farm systems. Since weaknesses increase the perceived levels of risk related to offshore wind projects they inhibit capacity growth and act as a barrier to investment.

Understanding of the level of control one has over risk is important in the context of financial decision-making associated with new offshore wind farm projects. Effective risk management requires a new model to adequately address systemic risk, which is important for two reasons. First, if systemic risk, which impacts across all turbines, is ignored then overall farm performance will be over-estimated. Second, the epistemic uncertainty associated with systemic risk can be reduced by as we learn from relevant data and information gathered from, for example, relevant testing.

We have developed a novel availability growth model that takes into account the sources of systemic risk to provide a more accurate estimation of farm performance over early life (Zitrou & al, to appear). Our model focuses on early operating life, which usually covers the first five years of operation, because the impact of systemic risk is more prevalent when teething problems arise and are resolved through remedial actions at the price of additional investment. Our model can be used to understand the scale of uncertainties involved in wind farm development and, thus, inform decisions to grow availability and buy-down risk. In particular, the farm performance estimates obtained through modelling can be used to support assessment of the risk-return profile of offshore wind projects at a pre-construction phase. Our model has a general structure that can be adjusted to reflect a particular application and requires to be populated using an appropriate mix of expert judgment and empirical data.

In this paper we explain how we have designed and implemented a structured expert judgment elicitation process to identify the key uncertainties for a particular offshore wind farm context and to quantify selected model parameters associated with epistemic uncertainties. In Section 2 we overview our contextual model to set the scene before describing the mathematical approach to modelling the epistemic uncertainties. In Section 3 we explain our general protocol of expert judgment elicitation, while in Section 4 we discuss how we gathered judgmental data from a panel of experts with experience in wind farm engineering, technology and operations for a UK Round III wind farm application. In Section 5 we show how the subjective assessments of epistemic uncertainties made by our expert panel can be used to instantiate the model and present selected outputs of modelling. We conclude in Section 6 by discussing the methodological and practical implications of our results.

2 MODELLING FARM PERFORMANCE

2.1 *Conceptual framework*

Our model is designed to represent the key sources of epistemic uncertainties from a risk-management perspective. The model captures the specific effect of epistemic issues on the wind farm subassemblies, as well as their aggregated effect on overall farm performance. Compared to the standard uncertainty analysis, where epistemic uncertainty is represented by varying the model parameters over intervals, the output from our model has a practical interpretation and, therefore, can be used meaningfully to inform decision-making.

Figure 1 provides a diagrammatic representation of our model framework. Farm performance is measured in terms of its availability-informed capability. We introduce this measure to merge farm energy capacity with the technical availability because we believe that this better supports uncertainty analysis. Availability informed capability is a function of the uptime, whether full or partially operating states, and downtime performance. Oval nodes represent the uncertainties affecting performance, with shaded nodes being specifically the epistemic uncertainties affecting reliability and hence uptime performance. That is, design inadequacy, operation error and manufacturing fault, which we collectively refer to as "triggers" because they act as initiators of failure events that will reduce reliability and they represent factors about which we shall gain knowledge through experience. Other uncertainties, such as waiting and repair times, are treated as aleatory. The boxes represent interventions taken to grow performance and reduce uncertainty, and include major innovations such as design changes as well as minor adaptations such as refinements of operational procedures.

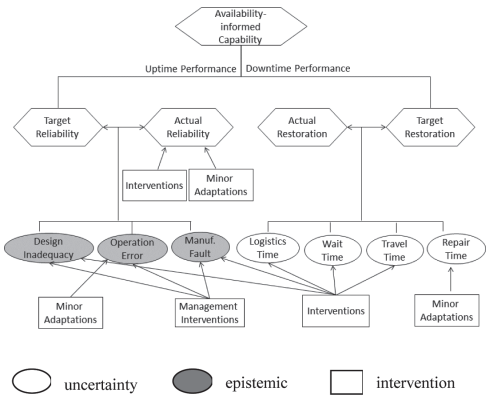


Figure 1. Conceptual model framework of model.

2.2 *Mathematical foundations*

We represent uncertainties in our model at the level of the farm subassemblies, such as gearboxes, generators, blades. The combined effects of uncertainties at the subassembly level are then aggregated to the wind farm level through the model structure.

2.2.1 *Failure intensity function*

The failure intensity $\lambda(t)$ is a function of the inherent reliability properties of the subassembly at start of life, $t = 0$, denoted by the hazard rate, $h(t)$, and the modification of these properties through maintenance and other interventions prior to some time, t, which can be represented by the virtual age, v_t. Therefore by combining the hazard rate with the virtual age, the failure intensity of the subassembly at time t is given by:

$$\lambda(t) = h(v_t), \quad t > 0 \tag{1}$$

2.2.2 *Parametric model for hazard rate*

We assume two classes of subassembly failure mechanism, shock and wearout, which occur in sequential phases. During the first phase shock failures occur at a constant rate, ρ. The second phase relates to wearout which, for the purposes of this paper, we assume to have a Weibull rate, with scale parameter a and shape parameter b. We assume that the transition between the first and second phases occurs at time w. Thus the parametric form of the hazard rate at time s is given by:

$$\begin{aligned} &\rho \text{ if } s \le w \\ &\rho + ab(s-w)^{b-1} \text{ if } s > w. \end{aligned} \tag{2}$$

Extending our reasoning to capture the additional risk due to triggers, we write the hazard rate as:

$$h(v_t) = \tilde{h}(v_t \mid \underline{\theta}) + \sum_{j=1}^{3} X_j(t) h_j(v_t \mid \underline{\theta}_j) \tag{3}$$

where components $h_j(\cdot)$ for $j = 1, 2, 3$ represent the risk added to the subassembly due to their exposure to triggers and the parameters are represented by θ. We assume that triggers cause affected subassemblies to fail more frequently due to shocks and/or age prematurely. We also assume that hazards $\tilde{h}(\cdot)$ and $h_j(\cdot)$ ($j = 1, 2, 3$) have the same parametric model as in Equation (2). To represent epistemic uncertainty, variables $X_j(t)$ in Equation (3), and also the parameters, are assumed to be uncertain. This allows hazard $h(\cdot)$ to be take alternative formulations, allowing for the possibility of different (epistemic) scenarios.

Triggers can have different properties in terms of the way they impact on subassembly reliability.

For example, design inadequacies and manufacturing faults might affect subassemblies from the moment turbines start operating, implying:

$$X_1(t) = X_1, \forall t \text{ and } X_2(t) = X_2, \forall t \quad (4)$$

Bernoulli distributions with parameters p_1 and p_2 can be used to model the variables $X_1(t)$ and $X_2(t)$ respectively. In contrast, an operational error may manifest itself after a maintenance operation at any time during operational life implying that $X_3(t)$ has again a Bernoulli distribution, but is "switched on" with a given probability after a maintenance action. In the model, design triggers simultaneously impact all turbines, manufacturing triggers impact independently on individual turbines subassemblies, and (maintenance) operational triggers occur independently at each subassembly maintenance event.

2.2.3 *Trigger probabilities*

We discuss a functional relationship that allows us to assess what trigger probabilities we should adopt for a given subassembly class. We assume that the susceptibility of subassemblies to a trigger depends on a number of factors relating to design, operational and environmental characteristics. We call these attributes, denoted by A_i for $i = 1, \ldots, n$, and assign to each one a scale. For example, the chance of a manufacturing fault developing may depend quality control processes applied during manufacturing (i.e. Quality Control), the degree to which novel process principles are used in the manufacturing process (i.e. Process Novelty) and the track record of the manufacturer (i.e. Manufacturer Status) as depicted in Figure 2. Each of these attributes has a number of levels which have been defined in conjunction with domain experts. For example, Manufacturer status has five levels, ranging from a new manufacturer with lack of relevant track record through to an established manufacture with a long positive track record producing a given subassembly.

To assess a trigger probability, the analyst chooses the appropriate level for each attribute that influences the particular trigger. The probability

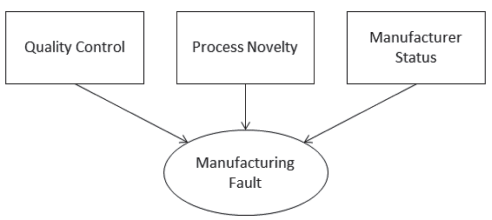


Figure 2. Attributes influencing manufacturing fault trigger.

can then be determined by using a log-linear model, viz:

$$p_j(x_1, \ldots, x_n) = q_j r_1^{x_1 - 1} \ldots r_n^{x_n - 1} \quad (5)$$

where x_i is the level of attribute A_j, q_j is the trigger probability for the worst case scenario (i.e. attribute levels are at the minimum) and r_i is the proportion by which the trigger probability changes when A_j moves by one level whilst the levels of A_k for $k \neq j$ remain fixed.

2.3 *Quantification and model implementation*

Expert judgment is a key source of data especially in relation to the failure process and the quantification of epistemic uncertainties. For example, we need to specify and to determine the values of target variables, such as the baseline probability and risk reduction proportions, which we assume are fixed. The shock rate, wear-out parameters and onset of premature wear-out also require to be assessed. For the epistemically uncertain parameters, such as the onset of aging, we use the whole uncertainty distribution as assessed by experts.

To run our model we also need to specify farm features, such as the number of turbines, rated power, farm layout, time horizon, entry into service times. The details of the maintenance strategy, such as the restoration rates under different degrees of repair, the impact on virtual age, the times and durations of anticipated overhauls, the effect of de-rating on turbine energy output and the characteristics of the logistics operations such as waiting times. Historical experience data can be used, where appropriate, to provide estimates of repair rates and waiting times, conditional on weather. Sources of experience data include Reliawind.

The model has been coded in MATLAB and is implemented as a two-loop Monte Carlo simulation (Bier & Lin, 2013; Wu & Tsang, 2004). The outer loop determines realizations of the epistemically uncertain parameters, whereas the inner loop is a nested loop that performs iterations given the parameters determined in the outer-loop. This code configuration allows us to distinguish between the epistemic and aleatory uncertainty: variation within the inner loop is linked to aleatory uncertainty whereas variation across the outer loop is a representation of epistemic uncertainty.

3 PROTOCOL FOR EXPERT JUDGEMENT

A formal expert judgment elicitation comprises of the stages of motivating (i.e. establishing rapport between the experts and the analyst), structuring (i.e. clarify the objects and events

that are the subjects of the elicitation process), conditioning (i.e. explaining to the experts how to coherently assess their degree of belief), encoding (i.e. obtaining expert assessments) and verifying (i.e. ensuring that the assessments made by the experts reflect their true belief) (Morgan and Henrion, 1990; Merkhofer, 1987; Spetzler and von Holsteins, 1975).

In our protocol, motivating, structuring and conditioning are undertaken during a qualitative stage involving a workshop with the selected experts to identify key uncertainties and to prepare experts for encoding. Encoding of subjective probability assessments are conducted during a follow-up quantitative stage when experts are asked individually to complete questionnaires with questions associated with the parameters associated with epistemic uncertainties. Figure 3 summarizes our protocol.

3.1 *Qualitative stage*

The aims of the qualitative stage are two-fold: to agree the structure the general model for the specific application; and to identify the key uncertainties relevant to the application. A facilitated, semi-structured workshop provides a suitable mechanism for achieving these aims because it allows experts to share their knowledge and reasons for articulating uncertainties and to be made aware of the issues to consider when expressing their later judgments probabilistically. For example, the potential for biases such as representativeness and anchoring (Tversky, 1974) can be explained to improve the quality of expert assessments. The qualitative stage is extremely important because the insights gained can be used to simplify the model complexity and reduce the requirements from the quantitative stage.

A key workshop activity will be the identification of key subassemblies whose reliability estimates are subject to large or moderate epistemic uncertainty for the farm under consideration. In other words, these are subassemblies that are exposed to triggers and can potentially have a worse than expected reliability. Thus we first identify the key subassemblies and secondly we identify for each key subassembly the relevant failure mechanisms in a typical situation, as expected, or when a trigger is present.

The selection of key subassemblies potentially subject to epistemic uncertainties is done both to reduce the quantitative elicitation burden on experts and to ensure that the computations will run faster. The cost of this is some loss of variance in the overall computed epistemic uncertainty in the model, but it is judged that this is relatively small. Furthermore, the kind of decisions that we wish to consider will be around the subassemblies with larger epistemic uncertainties.

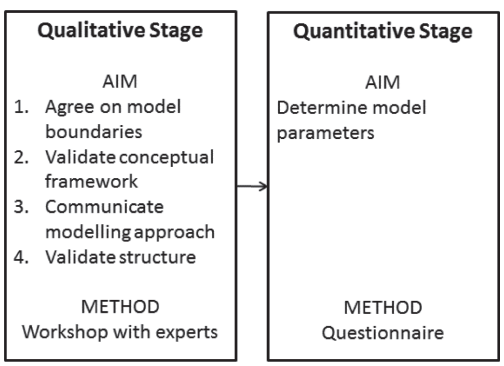


Figure 3. Two-stage expert judgment elicitation protocol.

3.2 *Quantitative stage*

Prior to quantification, the analyst determines the model parameters on the basis of expert judgment gained at the qualitative stage. Typically we might expect to want to elicit probabilities related to the trigger probabilities and the reliability of subassemblies under different scenarios. We choose a questionnaire as the data collection method because it gives experts the time and freedom to consult other sources of information (e.g. past data, event reports, etc), in order to form a probability assessment with which they feel comfortable.

A number of techniques are reported that allow the analyst to associate expert assessments to target variables (Merkhofer, 1987; Meyer & Booker, 1991; Kadane & Wolfson, 1998). We use the quantile method, according to which experts assess, for example, the 5%, 50% and the 95% quantiles of their uncertainty distribution on the target variable. We subsequently use the classical method with equal weights (Cooke, 1991) to aggregate the expert responses. For epistemically uncertain parameters the output of the elicitation exercise is an uncertainty distribution. For the remaining parameters, the output is a median value. Let us consider two examples in relation to the elicitation of the trigger probabilities and their reliability profiles.

3.2.1 *Eliciting trigger reliability profiles*

The trigger reliability profiles questionnaire supports elicitation of the uncertainty distributions on the parameters of the trigger-induced hazard functions h_j for each key subassembly. The hazard parameters are not directly observable quantities and so it is hard for experts to assess their values. To facilitate elicitation, experts are asked to assess the times by which a certain number of

Table 1. Example question on quantile assessment of wear-out onset from trigger reliability profiles questionnaire.

Consider a turbine that operates under normal conditions. Assume that the turbine is affected by a design inadequacy in the gearbox but by no other triggers. The design inadequacy causes the gearbox to age prematurely (over early life).			
After how many months of operation (since installation) will initial signs of degradation be observed?	Lower value (5%-ile)	Upper value (95%-ile)	Central value (50%-ile)

Table 2. Example question from the trigger probabilities questionnaire. *Central value corresponds to the 50% quantile of the expert's uncertainty distribution.*

Suppose that the subassembly has the worst possible configuration across Quality Control, Process Novelty and Manufacturer Status i.e. vector of attribute levels (1, 1, 1), which means no existing process standards, new manufacturer, no quality control. This configuration results in the highest probability of a manufacturing fault.	
Please provide your assessments of this probability.	Central value

subassemblies in a group behave in a certain way (e.g. fail or exhibit premature wear-out). Responses are subsequently linked to the parameters based on the distributional assumptions made within the model framework (i.e. shocks occur according to an exponential distribution). Table 1 shows an example question relating to the assessment of the times of wear-out onset. Since these are epistemic uncertainties, we elicit three quantiles to determine an uncertainty distribution.

3.2.2 *Eliciting trigger probabilities*

The trigger probabilities questionnaire supports elicitation of the information necessary to determine the parameters of the model given in Equation (5). In effect we are assessing the relative weights of the influencing factors. To determine the parameters, experts are asked to state the median of their individual, internal uncertainty distribution on relative risk reductions. Table 2 provides an example of such a question. Assuming the validity of Equation (5), we can then restrict the number of questions we have to ask of experts, because the impact of a specific factor can be determined by holding the other factors constant. Hence the experts are asked to answer a set of questions in which one factor at a time is changed.

4 ELICITATION WITH ENERGY EXPERTS

We have worked with a panel of eight experts with experience in wind farm engineering, technology and operations to conduct a formal elicitation following the protocol explained in Section 3. All experts were employed by the same renewable energy company and had many years of experience in the sector or in the relevant technologies. Experts were selected in collaboration with a lead technical specialist to ensure all were suitably qualified to provide probability assessments. The purpose of our study was primarily to trial our elicitation process and to challenge our modelling approach. Hence the wind farm under consideration was a typical UK Round III Offshore Wind Farm.

4.1 *Workshop insights*

We found that it was very important to carefully explain the difference between state-of-knowledge uncertainty and the aleatory uncertainties associated to lifetimes of the subassemblies: our experience was that after some initial confusion the experts quickly understood. It was the explanations of epistemic uncertainties as arising through triggers that helped to create this understanding.

Figure 4 shows the set of key subassemblies and the triggers to which they are believed to be susceptible as elicited during the workshop. This diagram is particularly important because it illustrates where the experts believe there is no significant epistemic uncertainty arising from the triggers. This qualitative step therefore justifies a simplification in modelling.

4.2 *Quantitative expert subjective assessments*

Quantitative elicitation used the two questionnaires on reliability profiles and trigger probabilities. The former was used to determine the form of the hazard when the trigger is present, and the latter was used to assess the weights in the trigger model.

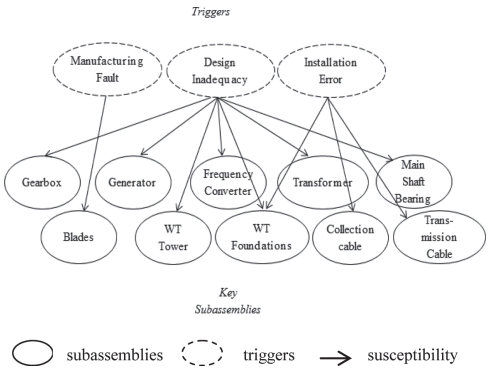


Figure 4. Illustrative output of qualitative elicitation stage.

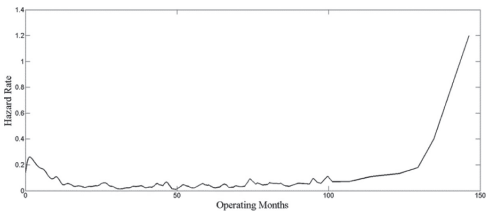


Figure 5. Hazard rate of gearboxes affected by a design inadequacy consistent with the elicited judgments of expert panel.

For example, each expert in our panel provided their own subjective probability assessment of the number of months of operation, since installation, will initial signs of degradation be observed for a type of turbine affected by a design inadequacy in the gearbox but by no other triggers; the example question shown in Table 1. On analysis of the elicited judgmental data we found that a lognormal distribution gave the best fit on the distributions aggregated across experts.

Figure 5 shows the hazard rate, $h(v_t)$ computed from Equation (3), for the population of gearboxes affected by a design inadequacy, consistent with the questionnaire data collected. During the first months of operation, the hazard rate decreases due to infant mortality failures but then the hazard rate levels out. Since design inadequacy issues cause gearboxes to age prematurely, the first signs of ageing start as early as after 100 operating months.

Our expert panel also provided individual probability judgments about the chance of each of the trigger probabilities such as a manufacturing fault for a subassembly produced by a new manufacturer who had not employed process standards and not used any form of quality control. That is, a worst case scenario as shown in Table 2.

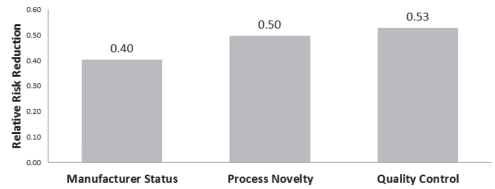


Figure 6. Relative risk reduction achieved by moving each attribute affecting the Manufacturing Fault trigger from the best to the worst level configuration, whilst the other attributes remain fixed to a mid-level.

By using the aggregated probability assessments of the expert panel for each trigger scenario within the model given in Equation (5), we can obtain the relative risk reduction of each attribute as illustrated in the bar chart in Figure 6. Interpreting the relative risks we find that improving the configuration of a subassembly across Manufacturer Status from new manufacturer (i.e. worst level) to established manufacturer (i.e. best level) will be reduced to 40% of its original value. The bar chart shows that Manufacturer Status is the most important attribute in terms of exposing the subassembly to the trigger and, in the context of our data for this application, Quality Control of the least important attribute.

5 EXAMPLE MODELLING OF EPISTEMIC UNCERTAINTY ON FARM AVAILABILITY

To illustrate how the expert judgment elicited from our panel of experts for a typical UK Round III wind farm might be used within our availability informed capability model depicted in Figure 1 and explained in Section 2, let us consider the following example situation.

Our interest lies in assessing the early-life technical performance of the large-scale offshore wind farm at a pre-construction stage. The farm comprises 100 5 MW turbines of a new design and its target performance is 97% availability. The turbines will be subject to both corrective and preventive maintenance, and the effect of maintenance is expected to vary from perfect to imperfect, depending on the type of failure and maintenance action. The maintenance strategy setting is similar to the one considered in (Zitrou et al, 2013).

Each turbine has the key subassemblies shown in Figure 4 and these represent the subassemblies likely to have large or moderate epistemic uncertainties in their reliability estimates. We also create a further generic subassembly category that collectively represents the other non-key subassemblies for which it is anticipated to have small epistemic

uncertainties in their reliability estimates. We assume that this generic subassembly will be subject to shock failures only over early life and will achieve target reliability.

Using Equation (5) we can determine the exposure of key subassemblies to triggers. Specifically, we assume that gearboxes are the main source of epistemic risk, with a design inadequacy probability as high as 0.8. The generator follows with a 0.5 probability of a design inadequacy, whereas blades have a 50% chance of having manufacturing faults.

As well as populating our availability model using the elicited expert judgment from our panel, we also used sources such as Reliawind (REF) to provide generic data for this example. We make additional assumptions about the timing of major interventions to address the realization of weaknesses that trigger a drop in reliability to illustrate their effect on availability estimates and their uncertainties. We have run the Matlab model as a simulation with 50 outer-loop (i.e. epistemic uncertainties) and 50 inner-loop iterations (i.e. aleatory uncertainties).

5.1 *Selected results*

Figure 7 shows weekly farm availability-informed capability during early life when the simulation results across all 2500 iterations are combined. The output is summarized in terms of the median weekly capability, together with the 5% and 95% quantiles. These uncertainty bounds represent a mix of epistemic and aleatory uncertainties. Farm performance appears to deteriorate over the first two years dropping to near 85% in the worst case around year 2. Major innovations to replace the original gearboxes which possess a design inadequacy being in year 2 allow farm performance to gradually reach the target levels, close to 97%.

We can focus on the effect of epistemic uncertainty only by calculating the mean farm availability averaged over the whole early life from the inner-loop iterations of the model. Figure 8 shows the empirical probability distribution of this mean.

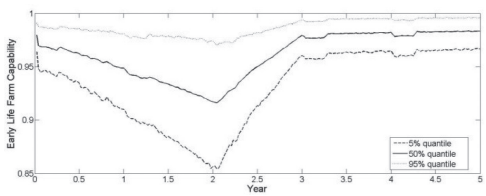


Figure 7. Estimated weekly farm availability-informed capability with 95% combined epistemic and aleatory uncertainties from simulation model of example scenario.

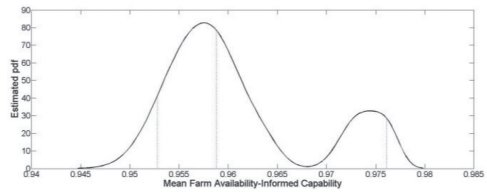


Figure 8. Epistemic probability distribution function on the mean farm availability-informed capability averaged over first 5 years of operation.

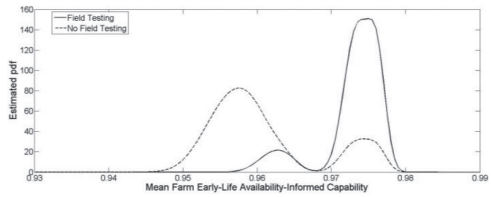


Figure 9. Epistemic probability distribution function on the mean farm capability averaged over first 5 years of operation under the two decision scenarios with and without field testing.

The variance of this distribution is a representation of the effect of epistemic uncertainty.

Now, suppose that extensive testing can reduce the chance of design inadequacy in gearboxes to 15%. This value has been obtained by modulating the Field Testing attribute from the worst to the best level and is, thus, consistent with Equation (5). Our model can then provide insight into the impact of this decision on farm performance and, at the same time, on our ability to assess this at a pre-construction stage. Figure 9 compares the distributions of the mean early-life farm availability-informed capability under the two decision scenarios: with and without field testing. Our outputs suggest that, in the worst case scenario, the mean farm capability might drop to 95% if no field testing is undertaken. However, if field testing is undertaken, this capability will increase to 96%.

6 CONCLUSIONS

New offshore wind farms deploy novel large-scale and complex technology. Such high degree of innovation brings the potential for systemic weaknesses in, for example, design, manufacturing and operational processes. As farms accumulate experience such weaknesses should be resolved, although most likely at the cost of additional investment. Our goal is to support pre-construction stage modelling to capture our

state-of-knowledge uncertainties so that we might better understand systemic technology risks and make good decisions to buy down these uncertainties in a timely manner.

Throughout our research we have worked with engineering experts with experience with the offshore wind technology, environment and business to ground our model in the real decision-making context. In this article we focus on the role played by a panel of experts from a particular company to provide judgments about their epistemic uncertainties on selected variables and parameters. Through their engagement our experts also played a role in validating our model structure and allowing us to test our expert judgment elicitation protocol.

In this paper we have presented elements of our mathematical model relevant to the representation of epistemic uncertainty and show how the model can be used with the expert judgment elicited from the panel of engineers from the company. We have sought to explain the rationale for our elicitation protocol and provide insight into elements of the judgmental data collected and its analysis.

Our model requires further validation study to mature our framework for practical implementation. Equally there are technical improvements required for the simulation model to speed computation, for which either parallelization of the code, or use of statistical code emulators, may provide useful approaches. Also, we have designed the modelling software in a modular manner so that the richness of the set of, for example, degradation models and so on, can be increased beyond those already reported.

ACKNOWLEDGEMENTS

This research was supported by EPSRC grant EP/I017380/1. We gratefully acknowledge support and contributions of colleagues from the Department of Electronic and Electrical Engineering of University of Strathclyde, Scotland.

REFERENCES

Bier, V.M. and Lin, S-W. 2013. On the treatment of uncertainty and variability in making decisions about risk. Risk Analysis, 33(12):2126–2139.

Cooke, R. 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press.

Department of Energy & Climate Change. UK renewable energy roadmap update: 2013. Technical report, 2013.

Kadane, J.B. and Wolfson, L.J. 1998. Experiences in elicitation, The Statistician, 47, 3–19.

Merkhofer, M.W. 1987. Quantifying judgmental uncertainty: methodology, experiences and insights. IEEE Transactions on Systems, Man, and Cybernetics, 17, 741–752.

Meyer, M.A. and Booker, J.M. 1991. Eliciting and Analysing Expert Judgment: A Practical Guide, American Statistical Association and the Society of Industrial and Applied Mathematics.

Morgan, M. and Henrion, M.G. 1990. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge University Press. http://www.reliawind.eu/.

Spetzler, C.S. and von Holsteins, C.-A.S.S. 1975. Probability encoding in decision analysis. Management Science, 22(3): 340–358.

Tversky, A. 1974. Assessing uncertainty. Journal of the Royal Statistical Society. Series B, Methodology, 36(2):148–159.

Wu, F.-C. and Tsang, Y.-P. 2004. Second-order Monte Carlo uncertainty/variability analysis using correlated model parameters: application to salmonid embryo survival risk assessment. Ecological Modelling, 177:393–414.

Zitrou, A., Bedford, T. and L. Walls, 2013. "Availability growth and state of knowledge uncertainty simulation for offshore wind farms", In Safety, Reliability and Risk Analysis: Beyond the Horizon, R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia, and A.C.W.M. Vrouwenvelder (eds), CRC Press, 743–750.

Zitrou, A., Bedford, T. and L. Walls, to appear. "A Model for Availability Growth to Support Decisions in the Presence of Systemic Risk for New Generation Offshore Wind FarmsAvailability growth and state of knowledge uncertainty simulation for offshore wind farms", under review.

Zitrou, A., Bedford, T. and L. Walls, to appear. "Modelling Epistemic Uncertainties in Early Life Wind Farm Performance to Support Risk Reduction Decisons", under review.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Expert method and real time simulation in navigational safety analysis

T. Abramowicz-Gerigk
Gdynia Maritime University, Poland

ABSTRACT: The navigational analysis is the important part of the design process of new port facilities as well as development and reconstruction of existed ports. A significant amount of effort is devoted to predicting and reducing the navigational risk. Recently due to the growing number of big container vessels many ports conduct the accessibility studies to determine the possibility of operation of the vessels bigger than the design ship for the particular port. The methods traditionally used to determine the navigational risk in restricted areas are based on fast time and real time simulations. The comparison of the navigational safety analyses based on the real time simulation and expert judgement using the interview questionnaires gives a new insight into the problem of safety margin. The accessibility study of the container vessel bigger than the design ship for the particular port has been presented as an example.

1 INTRODUCTION

1.1 *Background*

Navigational safety analysis is a usual task in the design process of a navigational area. In the tasks related to the new design of a manoeuvring area all the factors affecting safety of ship navigation in restricted waters should be investigated (Abramowicz-Gerigk, 2008; Abramowicz-Gerigk & Burciu, 2012). The accessibility study carried out for a particular vessel allows the reduction of the number of examined parameters. In the simplest cases the required towing force and manoeuvring procedures are assumed in the range close to the maximum permissible weather conditions for the port operation.

The current situation and prognosis of shipping market development is the reason of widely performed accessibility studies in many ports, with the assumed smaller safety margins than those used before.

East Asia is the area of the fastest development in the global container shipping services. Since 2012 the main Far-East container shipping lines: AE10 (Maersk), Loop 3 (G6), FAL1 (CMA CGM) have introduced in their services the biggest ships in the world and they have the further plans to increase their ULCS (Ultra Large Container Ship) fleets in near future.

There are several reasons for shipping companies to operate ultra large container ships. Operational costs for modern ultra-large eco-ships, characterized with 50% reduction of CO2 emissions per unit of transported cargo (TEU), are now 25% to 35% less than the ships built before 2010.

Widening reconstruction works of Panama Canal allow the vessels up to 12,000 TEU to use this waterway. The new Panamax vessel—maximum vessel to pass the Panama Canal, has the main particulars almost equal to the largest ships in the world: 385.7 m length, 54.9 m beam and 15.2 m draft.

For the planned Post Malacca-Max vessels, with the main particulars: 400 m length, 60 m beam and 21 m draft only two accessible ports Singapore and Rotterdam are now available.

Harbour efficiency and safety is defined by its nautical accessibility, capacity and economic viability. The increase in size of container ships will cause marginalization or even elimination of the ports which are unable to handle the largest ships over 8,000 TEU. Service of ultra large vessels requires infrastructure changes in the ports.

Due to the changes in the fleet structure, and elimination of the smaller feeder containerships, many of the competitive ports have already adopted their infrastructure to fulfil the requirements of ultra-large container ships services. The others are still in front of these challenges planning a navigational safety analysis which allow determining the possible solutions of the accessibility problems.

1.2 *Accessibility studies*

The knowledge and the possibility of prediction of the manoeuvrings performance of large vessels in shallow and confined waters are the basis to perform the navigational safety analysis.

The important aspects in the accessibility studies of ships larger than the design vessel for the particular port are depth, length, width and curvature

of approach channels and port internal channels, depth, length and width of docks and berthing areas, diameters of turning basins. The other aspects are the possibilities and cost of dredging and making changes in the port lay-out. The stakeholders involved in decision making process are port authorities and ship-owners.

In cases of already operated vessels moved to the new shipping routes, the first opinion about port accessibility is given by the experienced ship master of a particular vessel. In case of a new vessel different methods should be applied. In all cases the opinion of local maritime pilots based on their experience and real time simulation trials performed by pilots is very important.

2 METHODS

2.1 *Preliminary expert assessment of ship accessibility*

The usual preliminary assessment of ship accessibility starts during the meeting of the port authority, shipowner and ship operator representatives, experienced ship masters, experienced local pilots and naval architects, specialists in ship hydrodynamics, maritime engineers and port engineers.

The method based on a desk study comparing the control forces of the ship with the forces required to compensate for disturbing forces or to perform a given trajectory is used.

The example of this kind of analysis is presented in Figure 1, where the control forces are compared

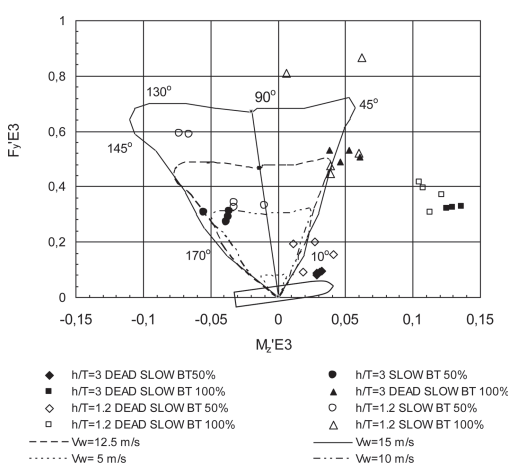


Figure 1. Control forces—non-dimensional lateral force F_y' and yawing moment M_z' compared with the envelope of disturbing wind forces for ship crabbing during berthing, distance from the berth equal to 0.75 ship beam, v_w—wind speed.

with the envelope of disturbing wind forces during ship berthing.

The presented crabbing manoeuvre can be examined for the different combinations of main engines (Dead Slow, Slow) and bow thrusters (50% or 100% of maximum available power) settings at shallow water (water depth to ship draft ratio h/T = 1.2) and deep water conditions (h/T = 3) and at different distances from the berth. In Figure 1 the assumed distance to the berth is equal to 0.75 ship beam.

Prediction of ship performance in real conditions allows estimating the influence of the propeller jets on the seabed (Gucma & Jankowski, 2007; PIANC, 2012).

For propeller driven ships, there are limits of applied main propulsion power usually assumed as 25% of full power in dependence on the type of seabed protection (Abramowicz-Gerigk. & Burciu, 2011).

The empirical methods, rules and best practice can be used to predict safe ship manoeuvring areas during the sequence of ship manoeuvres in port (Abramowicz-Gerigk & Burciu, 2013).

The local bylaws and national rules are different in different ports and countries. For example the diameter of turning basin according to Polish rules should be not less than 1.6 to 2.5 ship length, in dependence on type of the vessel and new design or conversion of the port layout case.

USACE U.S. Army Corps of Engineers rules are less restrictive. For the 180° turn the diameter of turning basin should be not less than 1.2 times overall ship length. If the assumed wind speed during manoeuvres is greater than 12.9 m/s and current is greater than 0.8 m/s safety analysis based on computer simulation of turning manoeuvres is required.

The requirements of PIANC (World Association for Waterborne Transport Infrastructure) are formulated with respect to ship steering-propulsion equipment. The diameter of turning area should be not less than 1.5 overall ship length when main propulsion and bow thrusters can be used. In other cases the diameter should be not less than 1.6 ship length.

In many ports the restrictive rules cannot be obeyed if the large vessels are going to be operated. In these cases the exemptions given by maritime administration are based on the detailed navigational analyses mainly using simulation studies.

The estimation of vessel draft includes the ship squat defined as the overall decrease in the static under keel clearance due to ship motion in shallow water. Ship squat of ultra large container vessels can be predicted using the empirical methods recommended by PIANC (Briggs, 2011).

The squat values calculated using different methods for the ship velocities in the range of

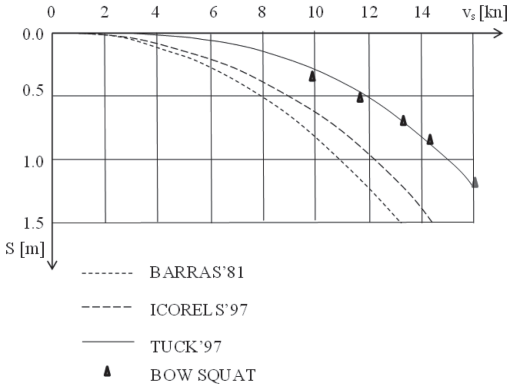


Figure 2. Maximum ship squat of ULCS with the main particulars: 400 m length, 50 m beam and 17 m draft block coefficient c_B = 0.837, with the static under keel clearance UKC = 2 m, calculated by different methods (Barras'81, Icorels'97, TUCK'97) and bow squat calculated on the basis of the physical model tests results (www.baw.de, 2005).

6–10 knots (3–5 m/s), usually assumed in approach and port areas, can be even three times greater than the real values (Briggs M.J. 2011, www.baw.de, 2005).

The comparison of squat assessment calculated using the selected empirical methods for ULCS with main particulars: 400 m length, 50 m beam, 17 m draft and block coefficient c_B = 0.837, with the static under keel clearance UKC = 2 m (www.baw.de, 2005) is presented in Figure 2.

The strategic dimensioning lay-out and operational entrance windows depended on weather, tide or current can be optimized by fast-time simulation, physical model tests and real time simulations.

2.2 *Fast time simulation*

Fast Time Simulation (FTS) technique uses algorithms simulating the decision-making logic of the master or pilot. By using this technique, it is possible to carry out simulations by off-line fast-time mode, which enables simulations for a number of scenarios The number of the examined cases can be about a few hundred runs (Gong et al., 2006).

Similar to the Real Time Simulation (RTS) technique the manoeuvring indices: rudder angle, engine revolutions, drift indices, proximity to fixed points and towing force can be analysed in dependence on environmental conditions.

The statistically evaluated data from independent runs can be used to determine the probability of accident. The dimensions of the area should meet the safe area at the confidence level related to the value of probability of the accident (Alfredini et al., 2011).

The accepted confidence level for the safe navigation should be not less than 95% or not less than the level related to the acceptable risk level. FTS method is a very useful tool however not all practical cases, including instant variable settings of propulsion and manoeuvring devices or special escort towing techniques can be studied using FTS (Gong et al., 2006; Abramowicz-Gerigk & Burciu, 2012).

FTS allows for the synthetic analysis but in most cases it is combined with RTS technique to compare the results with experts—pilots and ship masters opinions.

2.3 *Open water physical model tests*

The physical model tests are usually performed in towing tank to develop simulation model of ship motion (Eloot et al., 2010) or accessibility and siltation study (Willems et al., 2013).

The analyses based on the open water physical model tests can be compared to the RTS techniques. They are less time consuming as the model time is equal:

$$t_m = \frac{t}{\sqrt{\lambda}} \tag{1}$$

where t_m = time in model scale; 1:λ = geometrical scale of the physical model; and t = time in real scale.

Physical model tests are more expensive than the computer simulation (Burciu & Grabski, 2011), the large geometrical scale of man manned models allows testing real procedures, however it is difficult or even not possible to model the shallow water effect and environmental forces. Wind, current and wave parameters can be measured on-line during the experiment.

The example results of physical model tests carried out in the Research and Training Centre of the Foundation for Safety of Navigation and Environment Protection are presented in Figures 3 and 4.

The ship model and escort tug boat models are in the same geometrical scale 1:24.

The models used in the experiments are equipped with instruments simulating ship's systems and the basic navigational aids. motion parameters of the model are measured by a precise GPS RTK system.

The big advantage of open water model tests is a possibility to observe manoeuvres performed by experienced ship masters and local pilots. The influence of human factor is more close to reality in this case than during simulation studies performed using the full mission simulator.

The main dimensions of the example containership and her physical model are presented in Table 1.



Figure 3. Physical model tests carried out in the training facilities of Research and Training Centre of Foundation for Safety of Navigation and Environment Protection, photo. P. Michalowski (Abramowicz-Gerigk et al., 2012).

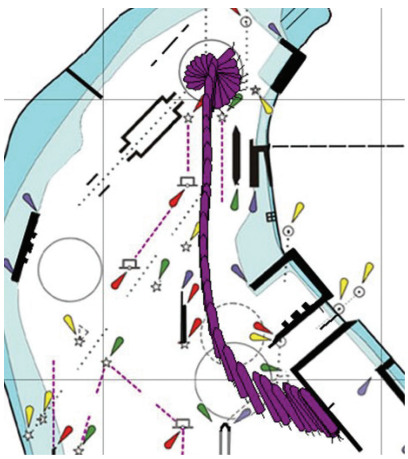


Figure 4. Ship manoeuvring area obtained using physical model tests: unberthing, towing ahead to the turning basin and turning carried out in the training facilities of Research and Training Centre of Foundation for Safety of Navigation and Environment Protection (Abramowicz-Gerigk et al., 2012).

Table 1. Main dimensions of the ship and physical model used in tests.

Parameter	Symbol	Ship	Model
Length	L [m]	372.00	15.50
Beam	B [m]	43.00	1.79
Draft	T [m]	14.50	0.60
Model scale	λ [–]	–	1:24

There are only a few facilities in the world where the open water tests, using large scale models can be carried out they are mainly used for training purposes. Therefore the basic tool used for navigational safety analysis is the real time simulation, integrating close to real conditions and experts knowledge.

2.4 *Real time simulation*

The process of manoeuvring safety analysis based on real time simulation studies starts with modelling of the examined vessel, harbour and environment. In most cases the commercial full mission simulators are used to carry out the real time simulations in collaboration with local pilots and ship masters.

The wide range of about 50 variables for the running ship models can be recorded along with the parameters to be assessed during the analysis.

The most important in the accessibility studies of large containerships is the determination of safe manoeuvring procedures, distances to the fixed points of port infrastructure, contact energy, minimum towing force and boundary hydro-meteorological conditions. The boundary values for dangerous situations can be also defined (Abramowicz-Gerigk & Burciu, 2012).

The repetitious simulations of the particular manoeuvre performed by the ship masters and pilots are the reason of the learning effect. It could be observed for the trials performed in the same weather conditions (Gong et al., 2006). Very often the second trial carried out by the same pilot even in strong wind conditions is more successful than the first trial in calm weather (Abramowicz-Gerigk et al., 2012).

3 REAL TIME SIMULATION AND EXPERT METHOD

Pilotage is an essential part of every Port Safety Management System. The essential part of navigational safety analysis based on RTS method is the contribution of local pilots. Their skills decide of the proper performance of manoeuvres and they can express their opinion about their difficulty and safety.

Their opinion before and after the trials can be different, but the observed results of several projects done with collaboration with the experienced pilots from three major Polish ports show well prediction of manoeuvres feasibility.

Human factor is the main factor in safety analyses performed in maritime transportation (Burciu, 2011; Gerigk, 2004; Gerigk, 2005; Gerigk, 2006; Gerigk, 2008; Gerigk 2012). Different combinations of the attitudes to the risk, safety assessment and performance of the manoeuvres have been observed. For example in the group of 10 pilots only one assumed a particular manoeuvre as not practical and decided not to try to perform it. The other wanted to try manoeuvres even if they assumed they are very difficult and unsafe.

The results of the navigational safety analysis performed in collaboration with 10 pilots, who performed 65 RTS accessibility trials of large container vessel, show the relationship between the pilot opinion and the results of the RTS analysis.

The trials were performed on full mission ship handling simulator SimFlex Navigator 4.0 at Gdynia Maritime University.

The assessment of safety and difficulty of particular manoeuvres was evaluated using semi quantitative approach. The proposed measures are presented in Table 2.

The pilots employed in the project were asked to fill questionnaires, evaluating the manoeuvres they had performed.

They assessed difficulty and safety of manoeuvres according to the scale presented in Table 2, taking into account weather conditions, towing force (tug boats currently available in the harbour and greater—up to 75 Tons), bow thrusters and stern thruster forces available for the tested vessels.

The calm weather conditions, 10 m/s, 15 m/s and 20 m/s wind speeds were simulated during the trials and taken into account in the questionnaires. The maximum available thruster forces and towing forces of bow and aft tug boats up to 75 Tons were allowed to use.

The example performances of the turning manoeuvres in the turning basin with diameter equal 1.3 ship length, using RTS are presented in Figure 5.

Lateral distances measured from the central point of the turning basin to the left side and right side berths, determined for the manoeuvring area occupied by the turning ship using RTS, during 20 trials (No.—number of a trial), wind sped 0 m/s, 10 m/s and 15 m/s are presented in Figure 6.

The trials performed at wind speed 15 m/s are marked with circles. It can be noticed that the ship manoeuvring area was not always tighter in calmer weather.

However as it is presented in Figures 7 and 8 the probability of safe performance of the manoeuvres and manoeuvres difficulty in pilots questionnaires were always assessed with respect to the wind speed.

All the manoeuvres carried out at the wind speed equal to 15 m/s—the boundary weather conditions for the port, were assessed as difficult (one

Table 2. Difficulty (D) and probability of safe manoeuvre performance (P).

%	Difficulty	Safety
100	Very easy to perform	Very safe
99–70	Easy to perform	Safe
69–30	Standard	Standard
29–10	Difficult	Unsafe
10–0	Not practical	Not acceptable

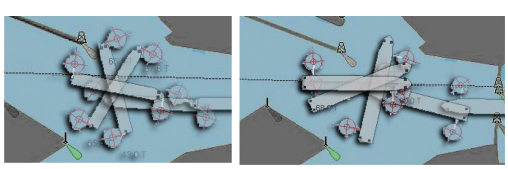


Figure 5. Ship manoeuvring area in the turning basin obtained using RTS (Abramowicz-Gerigk et al., 2012).

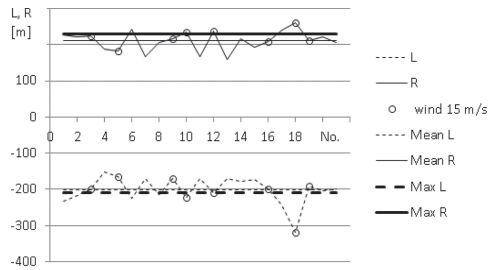


Figure 6. Lateral distances measured from the central point of turning basin to the Left side (L) and Right side (R) berths, determined for the manoeuvring area occupied by the turning ship using RTS. Mean L, Mean R—mean distances of the 20 trials, Max L, Max R—maximum safe distances.

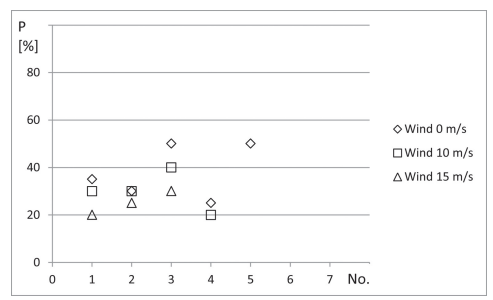


Figure 7. Probability of safe ship performance of the turning manoeuvre in the turning basin at wind speed 0 m/s, 10 m/s and 15 m/s (No.—number of a pilot performing the manoeuvre).

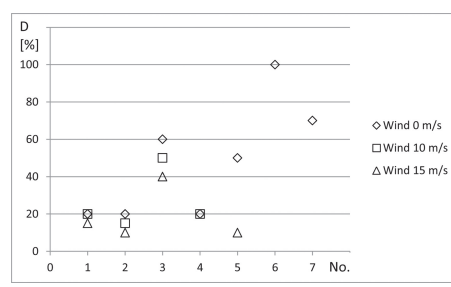


Figure 8. Difficulty of performance of the turning manoeuvre in the turning basin at wind speed 0 m/s, 10 m/s and 15 m/s (No.—number of a pilot performing the manoeuvre).

pilot placed the manoeuvre in the standard difficulty zone) and unsafe.

4 CONCLUSIONS

There are the following conclusions coming from the study presented in the paper: fast time simulation should be followed by real time simulation or open water trials on physical man manned models to include human factor in navigational safety analysis. Real time simulation is the most powerful tool as it allows examining all influencing factors at reasonable cost. It is also practical to use full mission simulator for the assessment of emergency manoeuvres.

The local pilots must be involved in navigational safety analysis as experts, because even if the mean result of the trials shows that the manoeuvre is feasible and safe with respect to its geometrical boundaries it can be assessed by the experts as feasible but unsafe and additional risk prevention measures should be undertaken.

REFERENCES

Abramowicz-Gerigk T. 2008. The risk analysis of harbour operations. in S. Martorell, C. Guedes Soares & Julie Barnet (eds.) *Safety Reliability and Risk Analysis: Theory, Methods and Applications. Proceedings of the ESREL 2008 and 17th SRA-Europe Conference*, Valencia, Vol. 4: 33343–3350, London: Balkema.

Abramowicz-Gerigk T. & Burciu Z. 2011. Comprehensive analysis of ship performance during self-berthing. *Advances in Engineering Research,* Chapter 13, Volume 3: 423–440, Hauppauge NY: Nova Science Publishers inc.

Abramowicz-Gerigk T., Burciu Z. 2012. Analysis of trends in navigational safety assessment an empirical and Bayes risk-based approach. 19*th International Conference on Hydrodynamics in Ship Design 4th International Symposium on Ship Manoeuvring*: 7–12, September, Ilawa, Poland.

Abramowicz-Gerigk T., Burciu Z. 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. in C. Guedes Soares, & F. Lopez Pena (eds.) *Developments in Maritime Transportation and Exploitation of Sea Resources. Proc. 15th Int. Congress of the International Maritime Association of the Mediterranean (IMAM'2013)*, A Coruna, Vol. 2: 699–704, London: Balkema.

Abramowicz-Gerigk T., Burciu Z., Lizakowski P., Pacholski M. 2012. Navigational Analysis. Phase III. Technical Report No. KES-2012-T3. Gdynia Maritime University.

Alfredini P., Gerent J.P., Arasaki E. 2011. Analogical Manoeuvring Simulator with Remote Pilot Control for Port Design and Operation Improvement. *International Journal on Marine Navigation and Safety of Sea Transportation* Vol. 5 No. 3: 315–322.

Briggs M.J. 2011. Sensitivity of PIANC ship squat formulas in unrestricted channels. *On Course PIANC E-Magazine* No. 142, January 2011: 13–24.

Burciu Z. & Grabski Fr. 2011. The experimental and theoretical study on the reliability of the life rafts. *Reliability Engineering and System Safety* 96: 1456–146.

Eloot K., Verwilligen J., Vantorre M. 2010. Synergy between theory and practice for ultra large container ships. *PIANC MMX Congress*: 1:13, Liverpool UK.

Gerigk M. 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. *Polish Maritime Research*, No. 1 (39), Vol. 11, 8–13.

Gerigk M. 2005. Challenges of modern assessment of safety of ships in critical conditions. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean IMAM 2005*, Volume 2, Lisboa, Portugal, 26–30 September 2005, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 1529–1536.

Gerigk M. 2006. A method for assessing hazards, risks and safety of damaged ships at sea. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006)*, Volume 3, Estoril, Portugal, 18–22 September 2006, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 2783–2790.

Gerigk M. 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference, ESREL 2008 and 17th SRA-Europe, Volume 4, Valencia, Spain, 22–25 September 2008*, Published by CRC Press, Taylor & Francis Group, Balkema, Boca Raton/London/New York/Leiden, 3303–3310.

Gerigk M. 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. in *Sustainable Maritime Transportation and Exploitation of Sea Resources. Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM)*, Volume 2: 715–719, London: Balkema.

Gong I-Y., Yang C-S., Kim Y-G., Lee C-M., Yang Y-H., Kim S-Y., Kim S-A. 2006. Maritime traffic safety assessment for Busan new port by using ship-handling simulator system. *Proceedings of International Conference MARSIM'2006*.

Gucma S. & Jankowski S. 2007. Depth Optimization of Designed New Ferry Berth. *7th International Symposium on Marine Navigation and Safety of Sea Transportation* Trans-Nav'2007. Gdynia 2007.

PIANC. 2012. Guidelines for berthing structures related to thrusters. *PIANC*, Brussels, Belgium.

Willems M., Van Dingenen B. & Verwaest T. 2013. Port of Zeebrugge: large physical model to study accessibility and siltation, in: Troch, P. et al. (Ed.). *Book of proceedings of the 4th international conference on the application of physical modelling to port and coastal protection—Coastlab12*: 1–8, Ghent, Belgium, September, 2012.

www.baw.de. 2005. Federal Waterways Engineering and Research Institute, 09.05.2005.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Causal modeling in industrial Reliability and Maintenance Management

Y. Pang & G. Lodewijks
Section Transport Engineering and Logistics, Delft University of Technology, The Netherlands

ABSTRACT: To ensure the healthy performance of complex industrial system and production process, Reliability and Maintenance Management (R&MM) requires accurate assessment of the degradation at both system level and component level, as well as the discovery of the interdependency among individual system components. This paper presents a novel intelligent R&MM system based on Bayesian belief network. The R&MM system models the causal relationship and assesses the reliability of complex industry systems in a generic way to optimize maintenance decision-making when degradation occurs. The study of two application cases proves that the developed generic R&MM system can be applied in various industrial areas.

1 INTRODUCTION

In industrial practice, a complex system is composed of a number of assembled components or subsystems. The reliability of the system relies on the combined reliability of the components. The malfunction of one of the components may lead to expensive process downtime if it causes a total shutdown of the system. Since an industrial system and relative production process cannot be designed to be 100% reliable and the reliability of system components decreases with aging and when degradation occurs, proper maintenance strategies and decision-making are required to maintain the reliability of the various components and the overall system. Therefore, reliability and maintenance management (R&MM) plays an important role to ensure the proper functioning and to achieve optimized performance of industrial systems.

To ensure the reliability of industry systems, preventive maintenance strategies are traditionally applied by means of Condition Monitoring (CM). CM is the continuous or periodic measurement and interpretation of the data and information to indicate the technical healthy condition of individual components to determine the needs for maintenance (Leaney & Sharpe 1999). CM deals with the acquisition of data and information from both human operators and sensor systems and further with taking corrective or preventive maintenance actions on the components that are to fail (Niu et al. 2010). It means that traditional CM aims to R&MM at either a parameter level or an individual components level (Leung & Romagnoli 2002). Due to the interdependency among the parameters and the components within complex industry systems, advance R&MM development, which is able to integrate the CM of individual components and subsystems, are desired to achieve:

- the overview of the operation condition at a system level instead of only taking monitored individual parameters and components into account;
- the exploration of the interrelationship among parameter and components instead of only taking separated monitoring outputs into account;
- the discovery of cause-effect relationship to provide optimal R&MM strategies and activities by means of data and information integration;
- the optimization of reliability assessment and maintenance decision-making for both the overall system and its components.

This paper presents the development and the application of a novel intelligent R&MM system by means of causal modeling. Such a R&MM system models the causal relationship of complex industrial systems in an generic way and assesses the reliability on a system level. Bayesian method is applied to model and integrate the data and information derived from individual parameters and components within complex systems. The intuitive modeling principle of Bayesian Belief Network (BBN), the mechanism of Bayesian inference and the intelligent reasoning ability enable the system to achieve the advanced R&MM. In the R&MM system, a generic Bayesian causal model and its reasoning framework are developed, which can deal with the R&MM for various complex industrial environments. Especially, the causal model takes the integration and reasoning on four R&MM levels, namely, the parameter level, the component level, the function level and the system level. The original concept of the integrated

R&MM system has been introduced and tested by the maintenance decision-making for large-scale material transport systems (Pang 2006). As the extended development of previous application, two case studies showed the opportunities to apply the developed generic R&MM system in wider industrial areas.

In this paper, Section 2 introduces the principles of Bayesian method and the inference of BBN. Section 3 describes the structure of the Bayesian causal modeling in the R&MM system and the approaches of reliability assessment and maintenance decision-making. In Section 4, both the main functions and the implementation of the generic R&MM system are provided to show the wide application scopes. Finally, Section 6 gives some conclusions.

2 BAYESIAN BELIEF NETWORK

Nowadays, with respect to reliability and maintenance decision-making, the management of complex industrial systems tends to complicated reliability analysis and optimized maintenance performance. The challenges of advanced industrial R&MM include the modeling of the overall systems, the representation of the reliability of both the system and its components, and the quantification of the uncertainty of system behaviors. In addition, the transition of system reliability, the integration of both quantitative and qualitative information at different levels, and the representation of the status of system events as well as the interdependency among events are also the issues to be taken into account for R&MM. Over the last decades, causal modeling approaches have been used to overcome the challenges of R&MM (Weber et al. 2012). Bayesian inference, as a proven sound causal modeling method, has been widely applied in various industrial areas, with respect to reliability assessment (Freitas, et al. 2010, Langseth & Portinale 2007), maintenance (Iung et al. 2005) and risk analysis (Trucco et al. 2008). However, there is still the lack of the applications of integrated intelligent system which takes the most issues of R&MM into account. Especially for complex industrial systems, these issues need to be considered simultaneously to achieve advanced R&MM.

2.1 *Bayesian method*

Bayesian method is a formalism for reasoning under uncertainty and causality (Pearl 2000). The foundation of Bayesian method is the Bayes theorem to use the prior knowledge $P(B)$, the probability that an event B occurs, to calculate the posterior probability $P(B|A)$ when the causal event A of B occurs:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} \tag{1}$$

where $P(A|B)$ is the conditional probability that A occurs with given event B, and $P(A)$ is the marginal probability that event A occurs.

Bayesian method can be applied to discover the cause-effect relationship between events, or in other words, to discover the occurrence of one event when other events occur. Considering multiple events in complicated industry systems, the Bayes theorem can be expressed as

$$P(e_i \mid H) = \frac{P(H \mid e_i) \cdot P(e_i)}{\sum_i P(H \mid e_i) \cdot P(e_i)} \tag{2}$$

which uses the prior knowledge $P(e_i)$ of a set of events e_i ($i = 1, 2, \ldots, n$) to discover the posterior knowledge $P(e_i|H)$ of the set of events with given hypothesis H.

Bayesian method has the advantages of handling both certain and ambiguous information and knowledge, representing both discrete and continuous events, and reasoning with partial or limited information. Most importantly Bayes theorem is used to confirm the belief that one event is approaching the truth based on the causal events that have been observed. Such advantages of Bayesian method enable the causal modeling and information integration by means of BBN.

2.2 *Inference of Bayesian Belief Network*

A BBN is an acyclic directed graph that represents a factorization of the joint probability over a set of events or random variables. The graphical structure of the network is the qualitative part of a BBN and embodies a set of nodes representing the random variables and a set or arrows representing direct dependencies between connected variables. Absence of an arrow between variables indicates that these variables are conditionally independent. The parents of a variable are the variables connected with an arrow with its direction going into this variable. The joint probability is the quantitative part of a BBN and embodies the conditional probability defined with each variable. This probability characterizes the influence of the valuated parents on the probabilistic values of the variable itself. A probability is the prior probability when a variable has no parents. The uncertainties in the parent nodes, represented by marginal probability, produce uncertainties in the child nodes that are based on conditional probabilities and physical cause-and-effect relationship. The directed

graphs of BBN provides a representation of the set of variables that are related to each other in providing knowledge about the state of the system (Pearl 2000).

Based on the principle of Bayes theorem, a BBN provides its inference mechanism in two directions: forward Bayesian inference and backward Bayesian inference (Kilner 2007). With respect to the events happened in industrial systems, forward inference is the inference from causes to effects, which gives the prediction of the occurrence of effect event(s). In forward inference, Bayesian method discovers the probability of a hypothesis (the effect) with known information of observed events (the causes). For instance, the probability of a poor braking operation of a material conveying system, with the key performance indication of long braking time, can be derived from known information of worn brake pads and degraded braking hydraulic system. Backward inference is the inference from effects to possible causes, which provides the diagnosis or explanation of the occurrence of cause event(s). In backward inference, Bayesian method concludes the conditional probability of observed events (the causes) with occurred hypothesis (the effect). For instance, the main cause between the observed worn brake pads and degraded braking hydraulic system can be identified, when a longer braking time is being known (Pang 2006).

3 CASUAL MODELING

3.1 *Modeling principle*

By applying the principle of Bayesian inference and the graphical intuitive structure of BBN, an generic R&MM system has been developed to integrate the data and information derived from industrial systems. Further, the R&MM system represents the interrelationship within the systems. In applications the a generic BBN model consists of four layers for inference and intelligent reasoning (Fig. 1).

Parameter layer monitors the parameters required for R&MM. It checks whether the values of individual parameters fall into the range of expectation. If not, it may indicate the degradation or potential failure of relative components. Then the uncertainty of the occurrence failure will be assessed by component layer. Based on the set points and pattern recognition algorithms of the parameter layer, the evaluation of the normality of the operational condition related to each parameters can be derived.

Component layer assesses the degradation and technical healthy condition of individual components based on the causal events monitored and

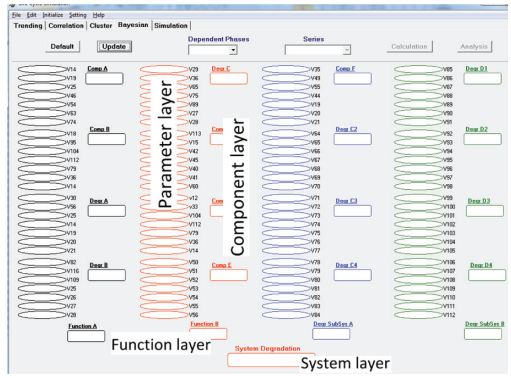


Figure 1. Structure of Bayesian causal modelling.

evaluated in the parameter layer. By obtaining the prior knowledge of the occurrence of individual causal events at the parameter level, the posterior probability derived from Bayesian inference provides the assessment of the effects of the monitored parameters. Then the technical healthy condition and the reliability of relative components can be represented.

Function layer integrates the assessment of the healthy conditions of individual components. By means of the integration, the overall performance of the system can be assessed with respect to specified system functions. The posterior probability derived in the function layer indicates whether the system is able to function in a proper and expected way when any abnormality or degradation is observed at component level.

System layer provides an overall reliability assessment at a system level by integrating all the assessments of system components and specified functions.

3.2 *Reliability assessment*

Based on the forward cause-effect inference of BBN, the R&MM system implements the reliability analysis and degradation assessment from a parameter level to an individual component level. Further, the reliability assessment arrives to a function and/or subsystem level until an overall system level by mean of information integration and causal analysis.

3.3 *Maintenance decision-making*

System layer has two functions. The first function is to assess the reliability of the entire system based on the forward inference from the monitoring of parameters to the assessment of individual components, and further to the evaluation of system

functions. If the assessment of the entire system shows undesired situation, maintenance decision-making will be needed. In this case, the second function of the system layer is to fulfill the backward inference of the BBN model to trace the main cause(s) of low system reliability with respect to degraded components, predictable system malfunctioning or system downtime. By doing so, the developed R&MM system enables advanced predictive maintenance to replace traditional preventive maintenance.

4 IMPLEMENTATION AND CASE STUDY

In the generic structure of the BBN model as shown in Figure 1, the currently developed intelligent R&MM system allows intuitive causal modeling to build up a large-scale BBN containing 120 parameters. For the application of the R&MM system with respect to various industrial systems and processes, in total the reliability of 16 individual components and 4 main system functions can be assessed based on the causal relationship from parameters to components and further to system functions. The reliability assessment at a system level can be provided by the R&MM system in term of the indication of system degradation.

4.1 *Main functions*

The R&MM system has following main functions (Fig. 2):

Modeling functions include trending analysis for monitored parameters, correlation and cluster analysis for causal relationship, Bayesian inference mechanism and simulation based analysis.

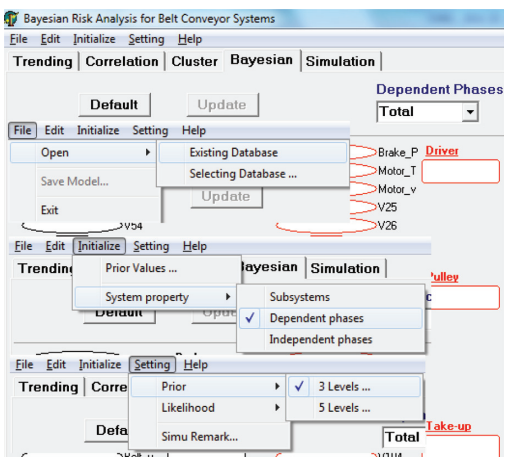


Figure 2. Main functions of the R&MM system.

Data acquisition functions enable the system to deal with both online R&MM and offline analysis by means of either selecting dynamic monitoring outputs or choosing existing historical database, respectively.

Initialization functions allow the system to initialize the configurations and properties of the R&MM system to match the requirements of different industry systems so that the generic causal model can be applied in various industry fields.

Setting functions allow the domain specialists of the industry systems to set and change the prior knowledge and the likelihood of events which are required for Bayesian inference and the intelligent reasoning of the R&MM system.

Model update functions provide users the possibility to change, update and reconfigure the BBN model intuitively. The original generic BBN model can be adjusted based on the specific requirements of the R&MM for a certain industrial system or process. After the update, the new model can be saved and utilized for future application.

Analysis functions can be mainly considered to be the backward Bayesian inference process. When the system reliability is assessed as lower than a threshold, in other words, when system degradation happens, analysis functions generate the analytic results based on Bayesian reasoning to indicate current healthy condition and reliability assessment at system level, function level and component level. The most important is that, based on the backward Bayesian inference, the analysis functions indicate the main cause(s) of low system reliability or system degradation and further provide optimized maintenance decisions.

As a generic modeling approach, the developed R&MM system needs to satisfy the requirements in different industrial areas. As well, the reliability assessment and relative maintenance decision-making need to be interpretable and accurate sufficiently. The ability and success of the developed R&MM system can be proved by the study of two application cases.

4.2 *Case I: R&MM for material conveying system*

In material conveying system, such as a belt conveyor system to transport large volume dry bulk material over a distance of kilometers in mining industry, dry bulk material terminal and power plants, diverse equipment and system components involve into the transportation process. Due to the large-scale of the system, the system components and information sources during CM are highly distributed which hinder the realization of accurate reliability assessment and optimal integrated maintenance decision-making.

The developed intelligent R&MM system has been applied on such a large-scale belt conveying system. Figure 3 shows the Bayesian model updated from the original generic model shown in Figure 1. This application integrate the data and information from the parameters that relate to the degradation of four system components (brake, take-up, belt and motor drive). It also integrates the assessment of the reliability and the technical healthy condition based on three main system operational functions (start, stop and loading situation). By means of the integration and uncertainty inference of the BBN model, the reliability of the overall system in term of system degradation can be gained for further maintenance decision-making.

The analytic output of the R&MM system is shown in Figure 4. Combined with the reliability assessment derived by the forward inference of BBN shown in Figure 3, the maintenance-decision results derived by the backward inference of BBN indicate the high degradation of the conveyor brake, which reduces the reliability of the entire system with a potential worse stop procedure. Further, after analyzing the interrelationship between the brake and the monitoring results regarding causally related parameters, optimized maintenance decision-making can be obtained to maintain the reliability of the overall belt conveyor system.

4.3 *Case II: R&MM for chemical production*

The second case study shows the implementation of the R&MM system for a polymerization chemical production process.

Figure 5 describes the overall polymerization production process and the basic components of the chemical system. The main aim of the R&MM system is to ensure the high quality of final polymerization products. Therefore, the overall system assessment, as the system degradation in the original system model, is represented by the key performance indication of product quality.

Figure 6 presents the basic structure of the BBN model updated and applied for the chemical production process. The results of forward Bayesian inference indicate the potential decrease of the quality of the production when any abnormalities are monitoring within the production process.

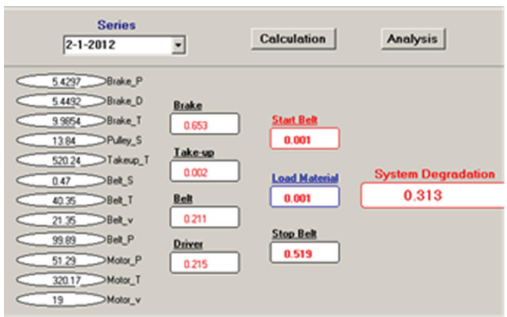


Figure 3. Bayesian causal model for belt conveying system.

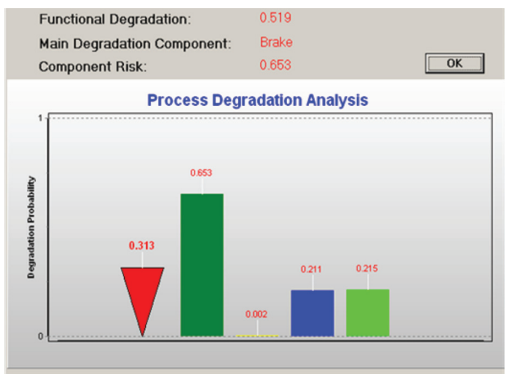


Figure 4. Analysis for system reliability.

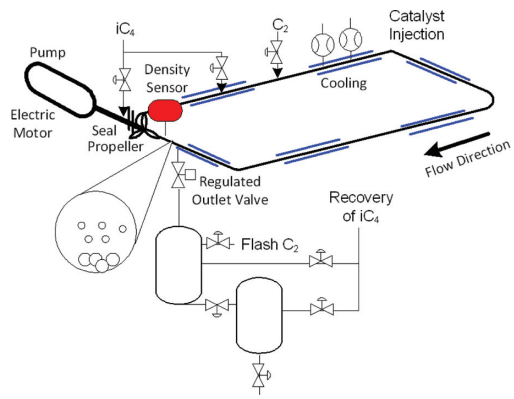


Figure 5. The process description of chemical production.

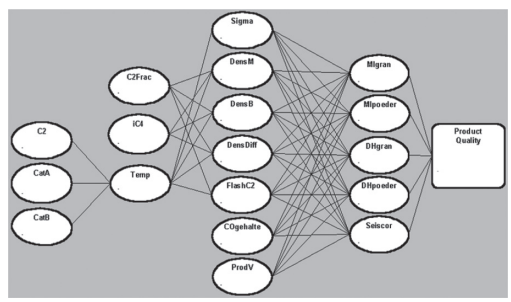


Figure 6. Model structure for polymerization process.

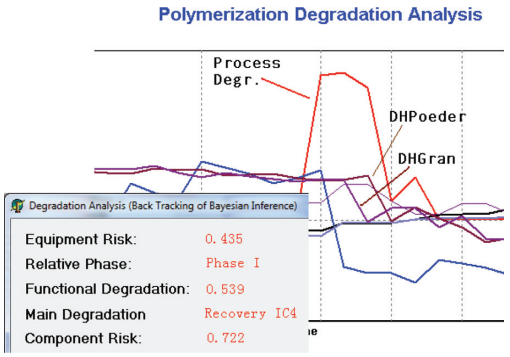


Figure 7. Results of Bayesian inference and analysis.

On the other hand, when poor product quality is observed after each production life cycle, the backward Bayesian inference provides the causal reasoning to discover the main causes to improve the performance of the chemical production.

In Figure 7, the intelligent reasoning outputs of the R&MM system are demonstrated, including the assessment of system degradation and the healthy condition regarding the individual components and functions within the production process. In addition, the main causes of system degradation and the optimized operational decision are provided by the analytic functions of the BBN model so that the performance of the production process with respect to the quality of final chemical products can be improved.

The study of both cases above has shown that BBN causal modeling and the developed R&MM system are able to provide accurate reliability assessment and maintenance optimization for industrial systems and production processes. In fact, past experiments and industrial applications have validated that the generic R&MM methodology can be applied in various industry areas.

5 CONCLUSIONS

Advanced industrial R&MM requires intelligent integrated reasoning towards accurate reliability assessment and optimal maintenance decision-making. By means of Bayesian inference and the causal modeling of Bayesian belief network, this paper presents the development and the implementation of a generic R&MM system. Such a system aims to provide the reliability assessment on both a system level and an individual component and function level. As a generic model and intelligent application, two case studies showed the opportunities to widen the applications of the developed R&MM system to various industrial areas. In fact, besides the case studies presented in this paper, the generic BBN model and the developed intelligent system have been successfully applied in diverse R&MM fields including electronic production line, steel manufacturing system, gasification process, and so on.

REFERENCES

Freitas, M.A., et al., 2010. Reliability assessment using degradation models: Bayesian and classical approaches. *Operational research* 30(1): 195–219.

Iung, B. et al., 2005. Integration of maintenance strategies into prognosis process to decision making aid on system operation. *Annals of the CIRP* 54(1): 5–8.

Kilner, J.M. et al., 2007. The mirror-neuron system: a Bayesian perspective. Neuro-Report 18(6): 619–623.

Langseth, H. & Portinale, L., 2007. Bayesian network in reliabiity. *Reliability engineering & system safety* 92(1): 92–108.

Leaney, V.C. & Sharpe, D.J., 1999. Condition monitoring techniques for optimization of wind farm performance. *Condition monitoring and diagnostic engineering management* 2: 5–13.

Leung, D. & Romagnoli, J., 2002. An integration mechanism for multivariate knowledge-based fault diagnosis. *Process Control* 12: 15–26.

Niu, G. et al., 2010. Development of an optimized condition-based maintenance system by data fusion and reliability-centered maintenance. *Reliability Engineering and System Safety* 95: 786–796.

Pang, Y. & Lodewijks, G., 2006. A Bayesian belief network approach to belt conveyor system monitoring. *BulkEurope 2006: international conference on storing, handling and transporting bulk*. Oct. 16–17, Barcelona, Spain.

Pearl, J., 2000. Causality: models, reasoning and inference. *Cambridge University press*, Boston.

Trucco, P. et al., 2008. A Bayesian belief network modelling of organizational factors and risk analysis: a case study in maritime. *Reliability engineering and system safety* 93(6): 945–856.

Weber, P. et al., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering applications of artificial intelligence* 25: 671–682.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The application of risk and reliability techniques to acquire knowledge in the development of expert system for fault diagnosis

E.M.P. Hidalgo & G.F.M. de Souza
University of São Paulo, Brazil

ABSTRACT: The process of knowledge acquisition is a major step in developing an expert system and is considered as one of the most difficult stages. This difficulty is due to the lack of an efficient methodology, reliable and standard for extraction and organization of knowledge from various sources. One of the great difficulties in the development and construction of an expert system is attributed to the extraction of expert knowledge. The contribution of this paper is to present a methodology to assist the knowledge engineer and expert in acquiring knowledge of a logical and orderly manner to develop the expert systems. The paper aims to propose a methodology to integrate the techniques of risk and reliability analysis in the acquisition of knowledge for the development of expert systems. The process of knowledge acquisition is proposed in two stages. The first step is to acquire knowledge of system operation through the study of engineering documents and operational description of the equipment. The second step is the process of knowledge acquisition for fault diagnosis applying HAZOP, FMEA and FTA techniques.

1 INTRODUCTION

Expert systems are a branch of applied artificial intelligence, and were developed by the artificial intelligence community in the mid-1960s. The basic idea behind expert systems is simply that expertise, which is the vast body of task-specific knowledge, is transferred from a human to a computer. (GRAHAM-JONES and MELLOR, 1995). This knowledge (heuristic nature) is the stored in the computer and users call upon the computer for specific advice as needed. The computer can make inferences and arrive at a specific conclusion. The expert systems powerful and flexible means for obtaining solutions to a variety of problems that often cannot be dealt with by other, more traditional and orthodox methods (ASHARAFI et al., 1995).

An expert system structure is made up of the following components (O'KEEFE and PREECE, 1996): a) the knowledge acquisition can be defined as the process of understanding and organizing the skilled knowledge through extraction, structuring, organization and representation of the same. It will be encoded and stored in a knowledge base for later redemption of an expert system; b) the knowledge base contains the expert's knowledge in the form of facts and rules. Rules are conditional statements that give the action that occurs of a specific condition is satisfied, and they are generally based on the problem-solving expertise developed by human experts; c) the inference engine is a computer program which simulates the user's deductive thinking. It applies a reasoning strategy, and generates solutions based on the rules in the knowledge base and the data collected by the expert system and d) the user interface links the expert system with the user and makes possible the data input about the special subject under discussion.

This paper will be focused on the knowledge acquisition for the development of an expert system. The process of knowledge acquisition is a major step in developing an expert system and is considered as one of the most difficult stages, Asharafi et al. (1995) and Maher et al. (1984). This difficulty is due to the lack of an efficient, reliable and standard methodology for extraction and organization of knowledge from various sources.

The potential sources of knowledge used in the knowledge acquisition process can be documented or not. Sources documented are: books, charts, diagrams, manuals, among others. The undocumented sources reside in the minds of people who work in the field of application of the system (experts who have the knowledge that must store on the expert system).

One of the great difficulties in the development and construction of an expert system is attributed to the extraction of expert knowledge. An initial problem is the communication between the expert and the knowledge engineer. The engineer can perform a series of interviews without have good grasp of the subject matter.

Thus, the expert to be understood must use trivial terms, but these are not terms that express their natural way of working, so there is a considerable loss of information in its transmission (SONG, 2008). Ideally, both the knowledge engineer and the expert, learn a little about each other's work so that the conversation more naturally. However, until that happens, a lot of time is consumed. For this reason, the quality, accuracy and completeness of acquired knowledge has a great effect on the quality of the expert system (SONG, 2008; O'KEEFE and PREECE, 1996).

In the area of knowledge acquisition efforts have been made to systematize and automate this process. The existing techniques used for the extraction of knowledge can be classified into manual and semi-automatic techniques.

Manual techniques are the traditional and conventional ways in which the knowledge engineer centralizes the incorporation of the same to build the program, gathered based on direct interaction with the domain expert. For this technique interviews experts with are carried out. Two types of interviews are used: unstructured and structured. Unstructured interviews are free and provide a good relationship between the knowledge engineer and the expert, but are not recommended beyond the early stages of identifying the knowledge and ambiance of the engineer with the domain. Structured interviews are more formal and questions are prepared with care and tend to take the conversation to the acquisition of specific knowledge about the domain. One problem encountered in this type of structured interview is that it can produce results influenced by the interviewer, so it must be planned and reviewed before being applied. The semi-automatic techniques consist in the use computational tools that provide a structured interface that help the experts and knowledge engineers to encode the knowledge base within a predetermined architecture.

Li and Liu (2010) had performed a comprehensive review of intelligence fault diagnosis. They pointed out that there are some problems in the existing intelligent fault diagnosis expert system theory, such as the difficulty in acquiring and managing knowledge extraction of expert, low online usage of fault diagnosis, high error rate, poor efficiency of inference process, and so on. This article proposes a structured method to improve efficiencies in the extraction of expert knowledge, allowing that interaction between the specialist and knowledge engineer be more didactics.

The goal of this paper is to present a methodology to assist the knowledge engineer and expert in acquiring knowledge in a logical and orderly manner to develop the expert system. The method integrates risk and reliability analysis techniques aiming at the acquisition of knowledge for the development of expert system.

This paper is organized in five sections. The first one presents the introduction and objective. In section 2 is presented the proposed method for knowledge acquisition. Section 3 presents the comparison between the methods presented by different authors cited in the bibliography and the proposed method. The application of method is carried out in the speed governing system of a Francis turbine, as shown in the section 4. Finally, section 5 presents the conclusions and recommendations for future work.

2 METHOD

According to O'Keefe and Preece (1996), the process of knowledge acquisition is the most difficult challenge for the development of an expert system. The quality of knowledge acquired supports on the quality of the analysis results obtained of expert system.

The process of knowledge acquisition proposed is divided in two steps. The first step is the knowledge acquisition of system operation through study and operational description of the equipment. The second is the process of knowledge acquisition for fault diagnosis.

2.1 *Study and operational system description*

This first step is characterized by a sequence of activities aimed to carry out an operating description of the equipment to be analyzed. To accomplish with the goals it is important to follow the steps specified in Figure 1.

As shown in Figure 1 it can be observed that the study and operational system description starts by defining the system to be analyzed, and then is carry out the survey of main subsystems and components. To carry out operational description

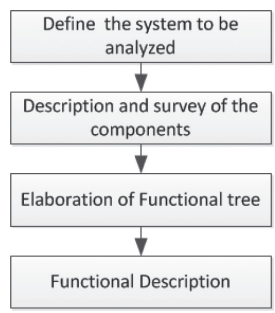


Figure 1. Procedure of study and functional description of the system.

is necessary to survey the technical characteristics of the components through the study of plans, catalogs, manufacturer manuals, etc. This step may present some difficulties in the industry since this information may not be available. Its correct execution influences the success of the analysis; in addition, allow the identification of the components and their functions performed in the system within a specific operational context. The authors propose the use of functional tree to support that analysis.

The functional tree allows the definition of the functional links between the equipment subsystems. To develop the functional tree it is necessary to clearly define the functions performed by the system components' aiming at attending a given system operational performance (CASAL, 2008).

The functional tree can be applied to various types of systems. The detail of the analysis depends on the amount of components and the level of functions to be analyzed. Functional analysis is represented by a graph called functional tree having a hierarchical structure, formed by branches as shown in Figure 2. The system breakdown structure used in the functional tree is the top-down division of a system into subsystems and components (KRISHNASAMY et al., 2005).

Finally, the functional description goal is to establish the interconnection between the components that compose the system and further to identify the functions performed by each of the identified components in the different functional levels of the tree. The development of this tool it is important since it allows understanding the complex functional relationships of the system components (RAUSAND and ARNOLJOT, 2004).

2.2 *Knowledge acquisition for fault diagnosis*

As for knowledge acquisition to support fault diagnosis the method proposes the use of reliability and risk analysis tools, such as HAZOP, FTA and FMEA. In Figure 3 is presented the sequence of use of those tools.

As suggested by Figure 3, the first step is the application of HAZOP technique. The HAZOP is

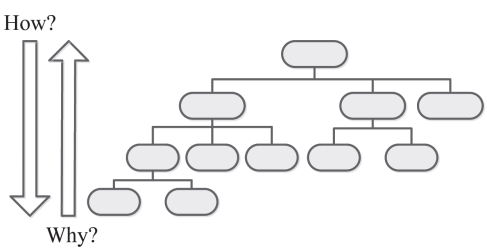


Figure 2. Functional tree.

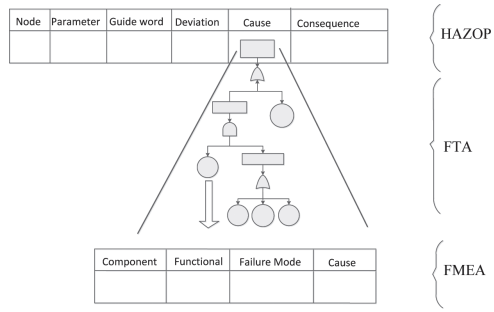


Figure 3. Application of risk and reliability techniques for knowledge acquisition for fault diagnosis.

Table 1. Guide word to analysis (ERICSON, 2005).

Parameter	Guide word	Deviation
Flow	No	No flow
	Low	Low flow
	High	High flow
	Reverse	Reverse flow
Pressure	Low	Low pressure
	High	High pressure
Temperature	Low	Low temperature
	High	High temperature
Level	Low	Low level
	High	High level
Viscosity	Low	Low viscosity
	High	High viscosity
Vibration	Low	Low vibration
	High	High vibration

used to identify deviations of operation parameters in the system and to identify its consequences. The procedure for performing this technique for fault diagnosis can be synthesized in the following steps (CUI et al., 2010; BRITISH STANDARD, 2001):

- Choose the node (are the points of the process) where deviations should be analyzed;
- Identify which operating parameters can be measured at each node to be analyzed: temperature, flow, vibration, pressure, among others;
- Application of "word-guides", determining the possible deviations that are occurring at that node. For each shift, investigate the possible causes of teasing him. To search for possible causes the Fault Tree method is applied.

Table 1 provides a list of parameters and guides words, along with the types commonly used in HAZOP analysis.

To carry out HAZOP a table composed of five columns is used, as shown in Table 2. The node

Table 2. Spreadsheet used in HAZOP analysis.

System					
Component					
Node location	Parameter	Guide word	Deviation	Causes	Consequences

location (points in the process are located through the flowcharts of the plant, which are examined in cases where deviations occur), the parameter (which are the physical process variables), the guide word (are applied to the process parameters that remain within the standards established by the intention of operation), deviation (intentions are operating clearances which are evidenced by the systematic application of the words study guides), causes (are the reasons why deviations occur, this step will be taken of fault trees) and consequence (the consequences are the outcome of a deviation from the intended operating on a given node-of-study).

Once identified the deviation the Fault Tree technique is used to search for causes that led to the occurrence of that deviation. The deviation is recognized as the top event for the tree construction. The reason for applying the Fault Tree is the capacity of dealing with simultaneous failures, which usually happens in electro-mechanical systems. The development of the Fault Tree enables the identification of the basic events which lead to the occurrence of the top event or deviation.

Once the Fault Tree for each identified deviation is elaborated, the qualitative evaluation of combinations of basic events that cause the occurrence of the top event can be executed. In other words, the cut set of tree that cause the top event are identified. To identify the minimum cut is necessary to apply the main rules of Boolean algebra.

The minimal cut of a Fault Tree is the set of basic events that cause the occurrence of the top, in other words, the deviation of a given operating condition. Thus a cut is the combination of basic events that modify the operating condition of the system. A cut is defined as the minimum cut when it is constituted by the smallest possible number of basic events whose occurrence is necessary and sufficient to cause the occurrence of the top event cannot be reduced without losing its cutting condition (O'CONNOR, 1985).

Once identified these basic events that lead to the occurrence of the deviation of the operating condition the Failure Modes and Effects Analysis is applied, because the basic events listed in the FTA

Table 3. Margin settings for A4 size paper and letter.

Failure mode and effects analysis			
Component	Functional	Failure mode	Cause

are the failure modes of the system components. The analysis will help to identify the causes of failures and propose recommendations for maintenance to repair the machine.

For the application of Failure Modes and Effects Analysis was used the Table 3 that consists of four columns: component (identifying each component belonging to the system), function (summary description and precise task that must carry out by the component), potential failure mode (description of how the loss of function is observed by operating staff) and cause of failure (simple and concise description of the causes that generate the occurrence of the failure mode) (BRITISH STANDARD, 2007).

Finally, the most appropriate maintenance policies to each component can be selected through the application of decision diagrams for selection of maintenance practices proposed by the RCM philosophy.

3 COMPARATIVE ANALYSIS BETWEEN THE METHODS LISTED IN THE REFERENCES AND THE PROPOSED METHOD

A literature review was executed to search for articles that present methods based on reliability and risk analysis techniques to support the development of fault diagnosis expert systems. Those articles, published from 1995 to 2014, are used to define the main contributions of the present methodology.

Batanov et al. (1993) presented an approach to the design and development of knowledge-based systems in general and their application in the field of maintenance management. The case study was a

rotary screw type air compressor. The knowledge-acquisition process has been organized and realized using a decision tree diagram and functional tree. The knowledge base contains 154 rules for the fault diagnosis and 54 rules for the maintenance model selection.

Wang et al. (2012) carried out a fault diagnosis expert system based on neural network and fault tree to study control box faults of a certain digital control system. Duan and Zhou (2012) presented a method for diagnosing faults using fault tree analysis and Bayesian networks to optimize system diagnosis in oil pressure warning instructions system. Zhou et al. (2009) presented a fault diagnosis expert system for the EAST cryoplant based on fault tree analysis. The EAST cryoplant consists of a 2 kW/4 K helium refrigerator and a helium distribution system. Zhi-Ling et al. (2012) carried out an Expert System of Fault Diagnosis for Gear Box in Wind Turbine based on fault tree.

Leone (1996) presented one of the main aspects of SERO, a knowledge representation structure, which has been developed to encode the different kinds of knowledge used in a HAZOP study. Venkatasubramanian et al. (2000) presented an intelligent system which allows identifying and suggesting hazard mitigation measures in a chemical process facility based on Process Hazards Analysis (PHA) and HAZOP analysis. Chan (2005) presented the development process of an expert decision support system for monitoring, control and diagnosis of a petroleum production and separation plant. The system can monitor operations at the plant based on input data, detect abnormalities in the data and suggest diagnostic actions to the operator. Rahman et al. (2009) developed ExpHAZOP+ which is the fault propagation algorithm, an aspect of the inference engine, which defines the propagation of deviations to all downstream equipment. The dynamic knowledge-base of ExpHAZOP+ allows a user to update knowledge while performing the HAZOP analysis.

The main innovations and contributions of the proposed method are:

– After doing the literature review it can be concluded that the articles only applied one of the risk or reliability analysis technique. It can be observed also that the FMEA analysis was not applied in the knowledge acquisition for expert systems. The contribution of this paper is to integrate the HAZOP, FMEA and FTA techniques to develop the proposed method for knowledge acquisition in expert systems
– The proposed method is different from others presented in the literature by the fact that it integrates and apply the reliability and risk analysis techniques for acquiring knowledge in the elaboration of the expert system.

The proposed method is suitable for acquiring knowledge for the development of an expert system applied in the diagnosis of deviations in the process including operational failures in order to search for the components which fail can cause these deviations. It is emphasized the importance of following the proposed flow chart that shows the sequence of activities that allows to make detailed and reliable analysis, because they are used and organized in a logical order, so that the method is applied correctly.

– The method proposed in knowledge acquisition step is divided into two phases. In the first phase techniques of functional tree and functional description are applied as a starting point for knowledge acquisition. The functional tree technique allows to create a functional structure of the system, which maps the relationships between the various components within a system. The functional description is used to establish the interconnection between components that comprise the system. Additionally it identifies the functions performed by each of the components in the different functional levels of the tree. The second phase applies risk and reliability techniques. The integration and application of these techniques will help the knowledge engineer and the expert to represent knowledge in an organized way based on logical rules. The HAZOP analysis is used to select the nodes where the analysis will be held, covering all possible deviations in the operating system. In order to identify the causes of deviations, FTA is applied, enabling modeling the occurrence of simultaneous events, which usually happens in electro-mechanical systems. Given the FTA, it is possible to identify those basic events which led to the occurrence of the deviation. The Failure Modes and Effects Analysis is applied to identify the causes of the occurrence of the basic events identified in the Fault Tree. Moreover, FMEA will assist in the proposition of recommendations for preventive or predictive maintenance.

4 METHOD APPLICATION

The system to be analyzed is the speed governing system of Francis turbine (schematically presented in Fig. 4) installed in a hydroelectric power plant localized in São Paulo state in Brazil. The hydroelectric power plant has a generation capacity of 120 MW.

The first step is to obtain knowledge of system operation through the study and description of the

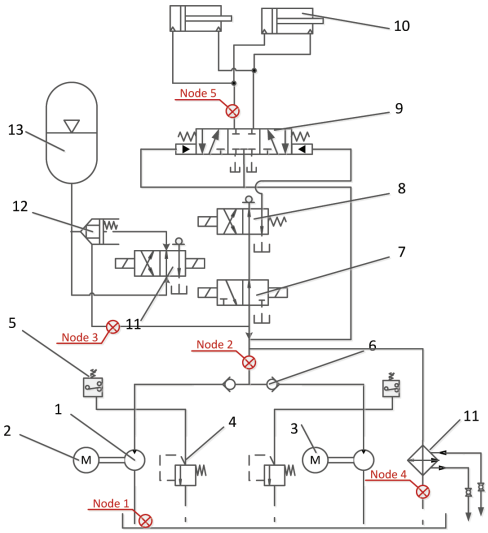


Figure 4. Speed governing system of Francis turbine. Legend: 1) Pump 2) Motor A.C. 3) Motor D.C. 4) Relief Valve 5) Pressostat 6) Check Valve 7) Proport Ional Valve 8) Emergency Valve 9) Distribution Valve 10) Cylinders Hydraulics 11) Insulation Valve 12) Command Valve 13) Accumulator 11) heat exchanger.

operating equipment. The second is the process of knowledge acquisition for fault diagnosis.

4.1 *Study and operational system description*

The speed governing system has the primary function of increasing or decreasing the power generated by the turbine when speed or frequency deviate from a reference value. According to the system demand, the speed governing system acts on the position of the blades of the distributor controlling the distributor opening and therefore the flow that reaches the rotor, generating only the required power for consumption. Figure 4 shows the speed governing system components of the Francis turbine.

The speed governor is an electro-mechanical device that detects any variation of speed in the turbine shaft and the correct it according to a reference value. In the case of Francis turbines a hydraulic actuator is used to move the ring distributor and consequently, to adjust the water flow. The distributor is a ring of adjustable blades involving the turbine rotor. To change the rotation speed of the turbine it is necessary to modify the volume of water flowing through the rotor.

Once defined the system to be studied, the functional tree of the speed governing system is presented in Figure 5. The functional tree is developed

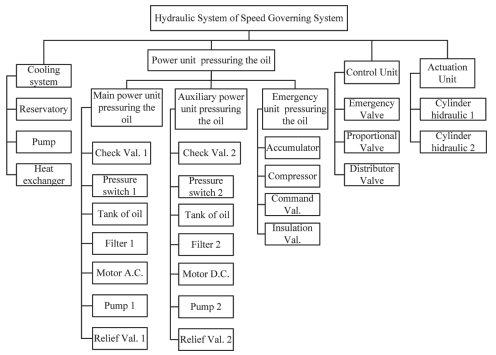


Figure 5. Functional tree of speed governing system.

based on information presented in the flow sheet presented in Figure 4 and in the plant operational guide.

The equipment is divided into main subsystems: Cooling system, oil power pressuring unit, control unit and actuation unit. Those subsystems are divided in components, each one performing a specific function linked with the subsystem main function. A failure in a component at the bottom of the tree affects all subsystems above it, causing a possible degradation in the system, represented by any change in regulation capacity or even environmental degradation.

4.2 *Knowledge acquisition for fault diagnosis*

The main purpose of a Hazard and Operability Study is to investigate thoroughly and methodically each thread of a process (focusing on specific aspects of the project—node—one at a time), in order to discover all possible deviations from normal conditions operation, identifying the causes responsible for such deviations and their consequences.

It was consulted manuals, articles, book and maintenance personnel of the plant, who regularly participate in the maintenance of equipment and possess the necessary experience about the system operation.

As a result of this systematic process four points or reference nodes were identified and considered relevant, shown in Figure 4, and the parameters and deviations associated with the guide words are described in Table 4. For each deviation identified, in each node, the causes for the events were investigated using the technique of tree failures that allows us to identify faults in simultaneously. Through the FMEA technique allowed us to identify the medium to detect these causes and present the possible maintenance policies.

In the Figure 6 the application of HAZOP and FTA analysis to node 2 can be observed as a

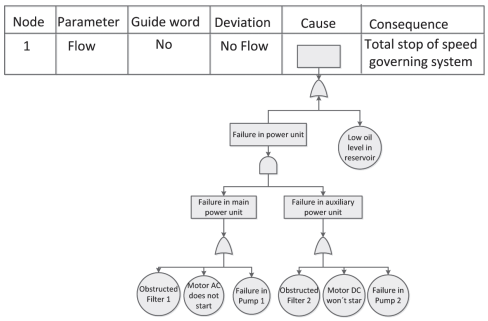


Figure 6. Application of HAZOP and FTA to node 1.

deviation when it does not have flow. As can be noted in the column of causes two causes are basic source of speed governing system stop: failure in power unit and low oil level in the reservoir. For the event failure in power unit to happen is necessary the simultaneous failure of main and auxiliary power unit. As a result of this deviation the speed is governing system inoperable causing the turbine emergency stop. The system failure can bring economic and material consequences and consecutively affecting the generation of electric power. The same way was used to prepare for each node identified in Table 4 their respective HAZOP, FTA and FMEA analysis.

Once identified the basic events analyzed for the occurrence of deviation (as an example no flow), it can observe that the basic events correspond to the failure mode of a component for that reason the FMEA technique is applied in order to identify the causes of failure that lead to the occurrence failure mode and consecutively select maintenance policies. As an example, the failure modes and effects analysis for the Electric Motor A.C. considering the failure "Motor A.C. won't start" is shown in Table 5. Those systems are submitted, according to manufacturer's recommendation, to a detailed maintenance policy based on predictive or preventive techniques.

To select an appropriate maintenance policy for the identified failure mode the maintenance team has to apply a decision process, which allows selecting the most recommended maintenance practices for each component, in accordance with the characteristics of their failure modes.

To apply the decision diagram proposed by RCM philosophy (MOUBRAY, 2000) it is necessary to carry out the classification of failures of components, as a function of the consequences of their failure on the operational performance. On the point of view of decision making in maintenance, failures can be functional or potential. Functional failures are non-fulfillment of desired component functions. The potential failure is represented by the presence of physical evidences that a process of deterioration of a component is going on, which will culminate in a functional failure.

The application of maintenance decision diagram for hydraulic systems components is shown in Table 6 taking as an example of application the analysis of the Electric Motor A.C.

According to Jingyi (2006) about 50% of the problems encountered in hydraulic systems are related to the hydraulic fluid. In this way, maintaining, controlling or eliminating the failure modes of the hydraulic fluid, can prevent a greater number of undesirable effects on the system.

The authors recommend carrying out periodical oil analysis. The tests can be performed to determine the viscosity, particle contamination and the presence of water in the fluid. The results of those tests will allow the maintenance team to identify the quality and state of the hydraulic fluid. The presence of metallic particles in the fluid can be used as indicators of bearing material degradation allowing maintenance actions planning before the bearing failure.

In case of electric motor failure can be associated to both mechanical and electrical faults. The main mechanical failures are: bearing failures and rotor and stator winding failure. Their maintenance can be based on scheduled replacement or inspection. The thermography analysis can be applied to monitor the wear of the insulation. Also for the electric motor, the shaft vibration analysis pattern can be used as an indication of potential bearing failure. Regarding the electrical devices preventive inspection, the use of thermography inspection technique is recommended aiming at checking the component temperature at periodical scan.

The pump failure can be associated with wear that can cause unbalancing and consequently mains shaft vibration. The use of accelerometers as vibration transducers allows the use of condition-based monitoring of the pump. Also, ultrasound analysis can be applied for detection of cavitation at the pump.

The use of thermography inspection technique is recommended aiming at checking the component temperature to identify internal leaks in valves and in hydraulic actuators. The seal wear can be associated particle contamination of hydraulic oil causing internal or external leaks in the valves and actuators.

The failure of the check and relief valve can be associated to both wear and fatigue degradation of spring. The use of preventive maintenance inspection and replacement can reduce the failure frequency of occurrence.

In case of accumulator failure can be associated to failed valve access oil or air, bladder rupture,

Table 4. Reference node, parameter, words guide and deviations from HAZOP analysis.

Node	Parameter	Guide word	Deviation	Consequences
1	Level	No/low	No level	SGS total stop
			Low level	High oil temperature
				Possible stop of SGS
2	Flow	No/low	No flow	Total stop of SGS
			Low flow	Total stop or possible of SGS
				Low or erratic pressure in the system
	Pressure	Low/high	Low pressure	SGS possible stop
				Actuator unstable speed
			High pressure	SGS possible stop
				Actuator unstable speed
				High oil temperature
3	Flow	No/low	No flow	SGS total stop
				Emergency unit pressuring the oil stop.
			Low flow	Total stop or possible of SGS
				Low or erratic pressure in the system
	Pressure	Low/high	Low pressure	SGS possible stop
				Actuator unstable speed
			High pressure	SGS possible stop
				Actuator unstable speed
				High oil temperature
4	Temperature	Low/high	Low temperature	Increased resistance to outflow (increase in friction losses)
				Low oil viscosity
			High temperature	Loss of lubricity
				Increase of internal leaks (pump, valves and actuator)
5	Flow	No/low	No flow	SGS Total stop
			Low flow	Total stop or possible of SGS
	Pressure	Low/high	Low pressure	SGS possible stop
			High pressure	Actuator unstable speed
				SGS possible stop
				Actuator unstable speed
				High oil temperature

(SGS = Speed Governing System)

Table 5. Failure mode and effects analysis: example electric motor.

Component	Functional	Failure mode	Failure causes
Electric motor A.C.	Transforma electrical energy in mechanical energy to drive the pump	Motor A.C. does not start	Failure in motor terminal or broken connections
			Overload
			Low voltage to allow motor start
			Loss of insulation of the coils
			Bearings damage causing excessive friction

presence of cracks in the structure and seal wear. Their maintenance can be based on scheduled replacement or inspection. As inspection can be carry out ultrasound analysis for detection presence of cracks.

Other very important elements in the hydraulic system are the filters. The state of the filters is shown by the pressure difference observed between the input and output, which indicates possible obstruction of the component. The filters must be changed before the blockage or rupture of the filter element. The temporal evolution of this pressure differential is indicative of the occurrence of deposits on the filter and can be used as a parameter for applying the practice of predictive maintenance.

Table 6. Maintenance policies for the electric motor.

	System				Speed governing system						
	Component				Electric motor AC						
					H1	H2	H3				
					S1	S2	S3				
	Consequence evaluation				O1	O2	O3	Default action			
Failures mode	H	S	E	O	N1	N2	N3	H4	H5	S4	Proposed task
Motor won't start	N	S	S	S	X	X					Preventive maintenance task 1. Check all electrical connections 2. Bearing Lubrication 3. Motor cleaning Predictive maintenance task 1. Vibration analysis 2. Thermography analysis 3. Electrical test (Insulation Resistance)

5 CONCLUSIONS

The implementation of this research has provided method to integrate reliability, risk and expert system concepts for diagnosing of operating conditions and to proposed maintenance policies in mechanical systems.

The proposed method proved to be feasible for knowledge acquisition for the development of expert system. It is important to follow the proposed flow chart, showing the sequence of activities that allow you to make detailed and reliable analysis of the system, because they are used in a logical order and organized, so that the method is applied correctly.

The process of knowledge acquisition is a major step in developing an expert system and is considered as one of the most difficult and important stages. The proposed steps for the acquisition of knowledge allows the knowledge engineer and experts to acquire the knowledge in an organized and clean manner, ensuring the quality of this acquisition.

The method developed in this paper presents the use of Functional tree and Functional Description techniques as a starting point for the knowledge acquisition. Functional tree enables to create a functional structure that maps the relationships between the various components within the system. Functional description enables to establish the interconnection between the components of the system. Moreover, identifies each component function, supporting the implementation of FMEA.

The HAZOP analysis is used to select the nodes where the analysis will be held, covering all possible deviations in the operating system by associating guide words to each of these nodes. These guide words are applied to the variables of the process and then the deviations of the processes corresponding to these variables are obtained. In order to identify the causes of deviations, FTA is applied, enabling modeling the occurrence of simultaneous events, which usually happens in mechanical systems. Given the FTA, it is possible to identify those basic events which led to the occurrence of the deviation. The Analysis of Failure Modes and Effects is applied to identify the causes of the occurrence of the basic events identified in the Fault Tree. Moreover, FMEA will assist in the proposition of recommendations for preventive or predictive maintenance, in order to minimize the possibility of the occurrence of operational deviations considered critical to the system under analysis.

As future work the fault diagnosis expert systems of Francis turbine speed governing will be developed. The expert system will be divided into four steps. In this article, the knowledge acquisition modulus is presented. Once acquired the knowledge, it will be presented in form of rules IF/THEN to build the knowledge base. Also, it will be developed the inference engine and user interface. The expert system will be developed using two programming language: Clips (C Language Integrated Production System) and Java.

REFERENCES

Ashrafi, N. Kuilboer, J.P. e Wagner, J.M., 1995. Expert systems reliability: A life cycle approach. Information & Management-28. pp 405–414.

Batanov, D. et al., 1993. EXPERT-MM: a knowledge-based system for maintenance management. Artificial intelligence in engineering—8. pp. 283–291. 1993.

British Standard. 2001. BS IEC 61882:2001 Hazard and operability studies (Hazop studies)—Application guide.

British Standard. 2007. BS IEC 61025:2007 Fault tree analysis (FTA).

Casal, J. 2008. Evaluation of the effects and consequence of major accidents in industrial plants. Amsterdam; Elsevier.

Chan, C., 2005. An expert decision support system for monitoring and diagnosis of petroleum production and separation processes. Expert system with applications—29. pp 131–143.

Cui, L.; Zhao, J. e Zhang, R., 2010. The integration of HAZOP expert system and piping and instrumentation diagrams. Process Safety and Environmental Protection—88. pp 327–334.

Duan, R. and Zhou, D. 2012. A new fault diagnosis Method based on fault tree and Bayesian networks. Energy Procedia—17, pp 1376–1382.

Ericson, C.A., 2005. Hazard Analysis Techniques for System Safety. New Jersey: John Wiley & Sons.

Graham-Jones and Mellor, B.G., 1995. Expert and knowledge-based systems in failure analysis. Engineering Failure Analysis—2, pp. 137–149.

Jingyi, Z. et al. 2006. The development and prospect of hydraulic reliability engineering.

Krishnasamy, L.; Kan, F. I., e Haddara, M. 2005. Development of a Risk-Based Maintenance (RBM) for a power generating plant. Jornal of Loss Prevention in the process industries - 18, pp 69:81.

Li, Z.H., Liu, M.K., 2010. Review of intelligence fault diagnosis in power system. Electric Engineering - 8, pp. 21–24.

Leone, H., 1996. A Knowledge-Based system for HAZOP Studies. The knowledge Representation structure. European Symposium on Computer Aided Process Engineering—6. pp 363–374. 1996.

Maher, M. et al., 1984. Tools and techniques for Knowledge Based expert system for engineering design. Adv. Eng. Sofware—6. pp 178–188.

Moubray, J., 2000. Reliability Centered Maintenance. 2° ed. New York: Industrial Press, 445p.

O'Connor, P.D.T., 1985. Practical Reliability Engineering. 2nd Edition. New York: Wiley&Sons, 500 pp.

O'Keefe, R.M. and Preece, A.D., 1996. The development validation and implementation of knowledge based systems. European journal of operational research—92, pp 458–473.

Rahman, S. et al. 2009. ExpHazop: Knowledge-based expert system to conduct automated HAZOP. Journal of Loss Prevention in the Process Industries—22. pp 373–380.

Rausand, M. e Arnoljot, H., 2004. System Reliability Theory, Models, Statistical, Methods and Applications. 2° ed. New Jersey: John Wiley & Sons, 668p.

Song, G. et al., 2008. HYDES; A Wed-based hydro turbine fault diagnosis system. Expert System with Application—34. pp. 764–772.

US MIL-STD-1629A. 1977. Procedures for Performing a Failure Mode, Effects and Criticality Analysis.

Venkatasumramanian, V.; Zhao, J. e Viswanathan, S., 2000. Intelligent systems for HAZOP analysis of complex process plants. Computers and Chemical Engineering—24. pp 2291–2302.

Wang, Y. et al., 2012. Research on Fault diagnosis Expert system based on the neural network and the fault tree technology. Procedia Engineering—3. pp. 1206–1210.

Zhi-Ling, Y. et al., 2012. Expert System of Fault Diagnosis for Gear Box in Wind Turbine. Systems Engineering Procedia—4. pp 189–195.

Zhou, Q. et al., 2009 A monitoring and diagnosis expert system for carbon dioxide capture. Expert system with applications—36. pp 1621–1631.

Failure identification and degradation processes

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Life and reliability evaluation of tuner by Constant-Stress Accelerated Degradation Testing method

Fuqiang Sun & Xiaoyang Li
Science and Technology on Reliability and Environmental Engineering Laboratory, Beihang University, Beijing, P.R. China

Tongmin Jiang
School of Reliability and Systems Engineering, Beihang University, Beijing, P.R. China

ABSTRACT: The tuner is a kind of microwave electronical assembly with long-life and highly-reliable characteristics. In order to evaluate the life and reliability of tuner, the Constant-Stress Accelerated Degradation Testing (CSADT) is applied by varying temperature. The principal component analysis method is utilized to analyse the tuner degradation data of multiple performance parameters. Then, the drift Brownian motion is used in describing the degradation process of the principal component. After fitting the model by maximum likelihood estimation, the life and reliability of the tuner under operational temperature is obtained.

1 INTRODUCTION

The tuner is a kind of microwave electronical assembly, which is used to simulative process the useful signal received. It is the key part which affects the reliability of the system and has long-life and highly-reliable characteristics. For this kind of long-life and highly-reliable products, it is not an easy task to assess the lifetime and reliability by using the traditional life-testing procedures which record only time to failure data.

The Accelerated Degradation Testing (ADT) technology is the effective way to solve this problem. The ADT is not need to observe the occurrence of failure and just need to monitor the changes of specified products performance parameters. Recently, ADT has been successfully applied in many kinds of products, such as direct methanol fuel cells (Bae Suk-Joo et al. 2010), aerospace electrical connector (Chen Wenhua et al. 2011), light bars (Wang Fu-Kwun & Chu Tao-Peng 2012), satellite assemblies (Li Xiao-yang & Jiang Tong-min 2007), and so on. However, most of previous researches have been focusing on the ADT method based on single performance parameter. In practice, a product may have multiple performance parameters, but the related research is still little presently (Wang Peng & Coit David W 2004, Yang Kai & Yang Guangbin 1997, S. Lu et al. 2001). These works assume either independence of the performance parameters, or dependent with a multivariate normal distribution, which may be unrealistic in practice.

A life and reliability evaluation method of tuner by Constant-Stress Accelerated Degradation Testing (CSADT) based on multiple performance parameters is proposed in this paper. Firstly, in order to evaluate the lifetime and reliability of the tuner rapidly, the CSADT is applied by varying temperature, and the power gain and noise figure are measured. Then, the Principal Component Analysis (PCA) method is introduced to simultaneously analyse the accelerated degradation data of multiple performance parameters. Finally, the drift Brownian motion model is used in describing the degradation process of the principal component. After fitting the model by maximum likelihood estimation, the life and reliability of tuner can be obtained.

2 THE CSADT OF TUNER

The failure mechanism analysis shows that temperature is the major factor that causes tuner output degradation. So, in order to evaluate the lifetime and reliability of the tuner rapidly, a temperature CSADT with 4 stress levels has been conducted, and the power gain and noise figure of tuner are measured by a computerized measuring system. The sample size of each accelerated stress level is 3 and the parameters of testing are shown in Table 1. Where, S_1, S_2, S_3, and S_4 are indicated the accelerated stress level, and the operational stress level is $S_0 = 25°C$.

During the testing, every tuner has four performance parameters need to be measured,

Table 1. Testing parameters of tuners' CSADT.

Stress level	Temperature/°C	Censoring/hours
S_1	55	494
S_2	70	348
S_3	80	310
S_4	85	228

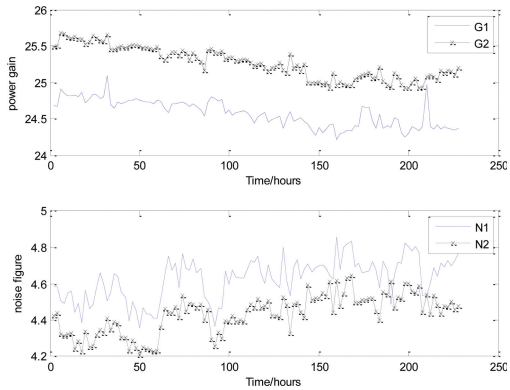


Figure 1. The degradation data of a tuner obtained by CSADT.

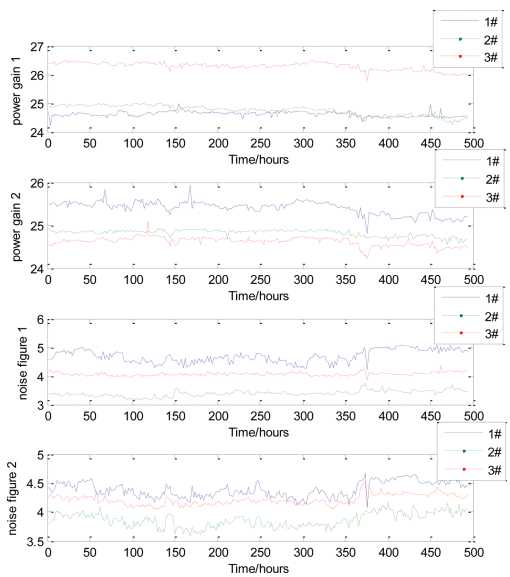


Figure 2. The testing data of all tuners on S_1.

including: the power gain of channel 1 and channel 2, the noise figure of channel 1 and channel 2. The tuner performance parameters degradation data obtained by CSADT are shown in Figure 1–Figure 5.

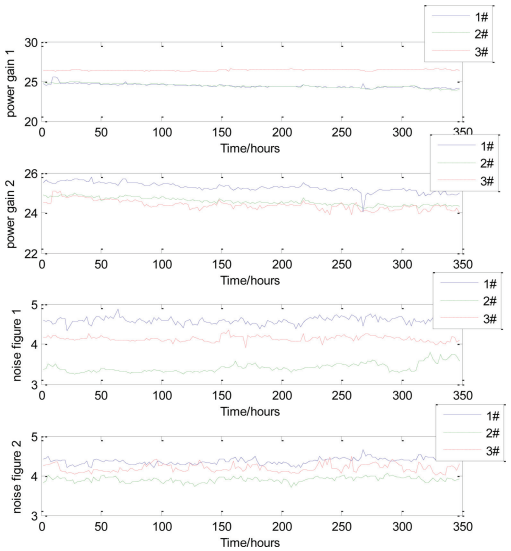


Figure 3. The testing data of all tuners on S_2.

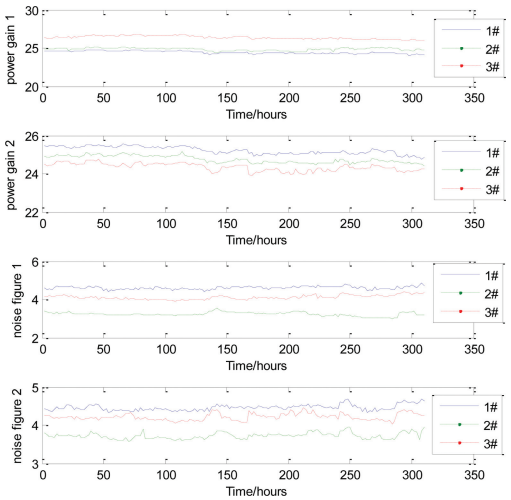


Figure 4. The testing data of all tuners on S_3.

3 EVALUATION METHOD OF MULTIPLE PARAMETERS CSADT

3.1 *Life and reliability evaluation procedure*

The PCA and the drift Brownian motion is utilized to analyse the tuner multiple performance parameters degradation data obtained by CSADT. The research program is show in Figure 6.

In order to reduce the dimension of the tuner's performance parameters, PCA is performed on the testing data firstly. Since the obtained princi-

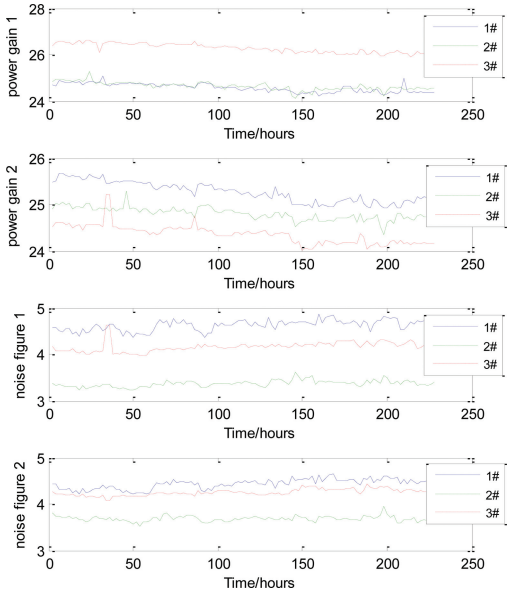


Figure 5. The testing data of all tuners on S_4.

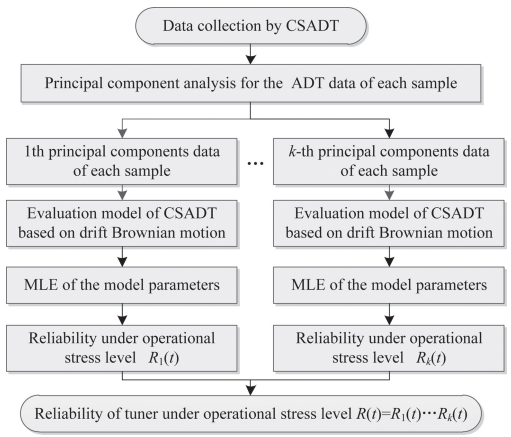


Figure 6. Life and reliability evaluation procedure of tuner.

pal components are independent to each other, the below analysis process is similar with the reliability series model. Then, the drift Brownian motion is adopted to evaluate the accelerated degradation data of the principal components. The parameters of the model are obtained through regression analysis and maximum likelihood estimating.

3.2 *Principal component analysis of ADT data*

Principal Component Analysis (PCA) is a kind of multivariate statistical analysis method, which is able to transform multiple variables into a few principal components through dimension reduction techniques.

Suppose that the number of the product performance parameters is p, and the total number of the parameters monitored in ADT is M. The matrix of the parameters observation is noted as:

$$\boldsymbol{X} = \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_M \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & & \vdots \\ x_{M1} & x_{M2} & \cdots & x_{Mp} \end{bmatrix} \tag{1}$$

where, each column of $\boldsymbol{X}$ corresponds to a product performance parameter, and each line corresponds to the observed values of the parameters at one monitoring. Then, the covariance matrix and correlation coefficient matrix of the sample are

$$\boldsymbol{S} = \frac{1}{M-1}\sum_{i=1}^{M}\left(\boldsymbol{x}_i - \bar{\boldsymbol{x}}\right)'\left(x_i - \bar{\boldsymbol{x}}\right) = (s_{ij})_{p\times p}$$
$$\hat{\boldsymbol{R}} = (r_{ij})_{p\times p}, \quad r_{ij} = \frac{s_{ij}}{\sqrt{s_{ii}}\sqrt{s_{jj}}} \tag{2}$$

where, $\bar{\boldsymbol{x}} = \frac{1}{M}\sum_{i=1}^{M}\boldsymbol{x}_i$ is the sample mean.

Then, the PCA can be performed by solving the eigenvalues and related eigenvectors of $\hat{\boldsymbol{R}}$. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p \geq 0$ be the eigenvalues of $\hat{\boldsymbol{R}}$, and $\mathbf{a}_1$, $\mathbf{a}_2$, …, $\mathbf{a}_p$ be the related orthogonal identity eigenvectors. The principal components are

$$\boldsymbol{y}_i = \boldsymbol{X}\boldsymbol{a}_i, \quad i = 1,2,\ldots,p \tag{3}$$

The accumulative contribution rate can reflect how much information that the principal components have extracted from the initial variable. It is usually to choose the k ($k < p$) principal components to make the accumulative contribution reach a required threshold (such as 85%).

3.3 *Accelerated model*

Accelerated model quantifies the manner in which the "life" changes with different stress levels. On the basis of the failure mechanism analysis, the key sensitive stress of tuner is temperature. Therefore, the Arrhenius model is adopted to describe the relationship between the degradation rate and the temperature.

$$L = A\cdot\exp(-E_a/kT) \tag{4}$$

where, T is the absolute temperature; k is the Boltzmann constant, 8.6171×10^{-5} eV/°C;

E_a is the activation energy with unit eV; A is a constant.

3.4 *Reliability modeling*

The drift Brownian motion (Wiener process) is commonly used stochastic processes degradation model for the degradation process.

In this research, the tuner performance degradation process $Y(t)$ can be described by the following drift Brownian motion model:

$$Y(t) = Y_0 + \sigma B(t) + \mu \cdot (t - t_0) \tag{5}$$

where, $Y(t)$ is the tuner performance parameter, and $B(t)$ is a standard Brownian motion on [0, ∞), $B(t)$~$N(0, t)$. Y_0 is the initial degradation level at time zero, and μ is the drift. σ is the dispersion and describes unit-to-unit variability due to operating and environmental conditions.

In the equation (5), the drift coefficient μ is the concerned degradation rate of the product. It characterizes the function relation between the environmental stress and the performance variables. Therefore, the relation of the drift coefficient and the temperature is the accelerated model, noted as $d(T)$, where T is the temperature. Then,

$$d(T) = A \cdot \exp(-E_a / kT) \tag{6}$$

Bhattacharyya & Fries (1982) pointed out that the product's failure time is the first passage time of the drift Brownian motion to a critical value (threshold), and it follows inverse Gaussian distribution. The corresponding reliability function is

$$R(t) = \Phi\left[\frac{a - y_0 - d(T)t}{\sigma\sqrt{t}}\right] - \exp\left(\frac{2d(T)(a - y_0)}{\sigma^2}\right) \Phi\left[-\frac{a - y_0 + d(T)t}{\sigma\sqrt{t}}\right] \tag{7}$$

where, a is the threshold, Φ is the standard normal cumulative distribution function.

For a drift Brownian motion, the differences of two consecutive performance measurements are independently, normally distributed with mean and variance proportional to the time lag between two measurements. Utilizing this property, Doksum & Normand (1995) discussed the maximum likelihood estimation of the parameters in degradation mean function and variance. Therefore, the solution to model parameter estimation is obtained by maximizing the marginal likelihood function, which in turn is obtained by integrating out the random coefficient from the joint conditional probability of individual observations (Rong Pan & Taeho Crispin 2011).

4 DATA ANALYSIS OF THE TUNER CSADT

The proposed evaluation method is used to analyse the tuner CSADT data. At the start, PCA is performed on the performance degradation data of each tuner. And the accumulative contribution rates of first principal component of all tuners are larger than 85%. Therefore, only the first principal component of each product is adopted. The first principal components of all tuners are shown in Figure 7.

Then, the drift Brownian motion is utilized to establish the reliability model for the first principal component data. The parameter estimation results

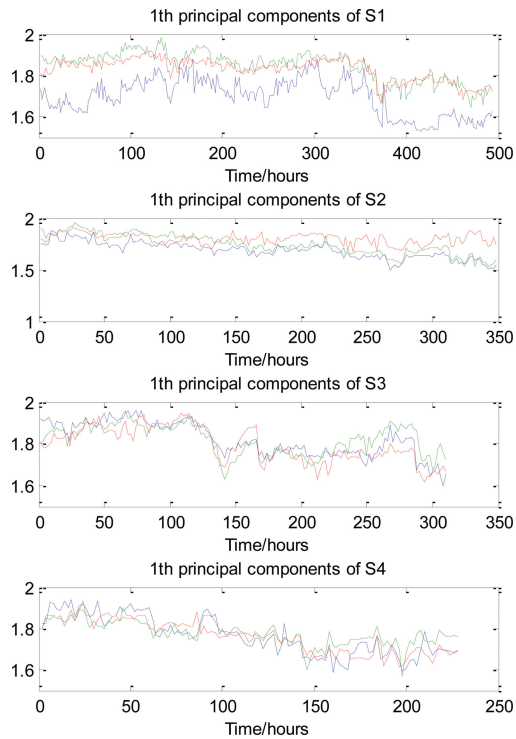


Figure 7. The first principal components of all tuners.

Table 2. Parameter estimation results.

Parameters	A	E_a	σ
Estimates	2404.0368	0.4503	0.0156

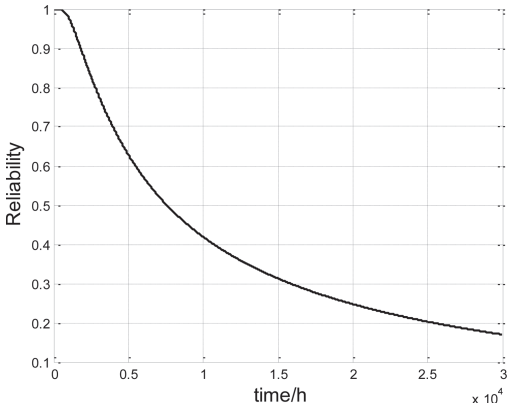


Figure 8. The reliability curve of tuner under 25°C.

are obtained through MLE, as shown in Table 2. If the failure criterion is 50% of the performance parameter initial value, the reliability curve of tuner under operational stress level (S_0 = 25°C) is shown in Figure 8.

5 CONCLUSION

Life and reliability evaluation of high reliability and long life products is hotspot and difficulty in the field of reliability research. This paper introduced a statistical analysis approach for a multiple performance parameters CSADT based on principal component analysis and drift Brownian motion. And, the life and reliability of tuner is evaluated using the proposed method. The proposed method can evaluate product life and reliability in the case of zero-failure data, which has certain reference significance to the long-life and highly-reliable products.

ACKNOWLEDGEMENT

This work was supported by the Fundamental Research Funds for the Central Universities of China.

REFERENCES

Bae Suk-Joo, Kim Seong-Joon, Park Jong, 2010. In Lifetime prediction through accelerated degradation testing of membrane electrode assemblies in direct methanol fuel cells. International Journal of Hydrogen Energy, 35(7): 9166–9176.

Bhattacharyya GK, Fries A, 1982. Fatigue failure models—Birnbaum–Saunders vs. inverse Gaussian. IEEE Transactions on Reliability, 31, 439–441.

Chen Wenhua, Liu Juan, Gao Liang, 2011. Accelerated degradation reliability modeling and test data statistical analysis of aerospace electrical connector. Chinese Journal of Mechanical Engineering (English Edition), 24(6):957–962.

Doksum KA, Normand ST, 1995. Gaussian models for degradation processes—Part I: Methods for the analysis of biomarker data. Lifetime Data Analysis, 1, 131–144.

Li Xiao-yang, Jiang Tong-min, 2007. Constant-stress accelerated degradation Testing of Satellite assemblies. Hangkong Xuebao/Acta Aeronautica et Astronautica Sinica, 28, 100–103.

Lu S., H. Lu, W.J. Kolarik, 2001. Multivariate performance reliability prediction in real-time. Reliability Engineering and System Safety, 72(1): 39–45.

Rong Pan, Taeho Crispin, 2011. A Hierarchical Modeling Approach to Accelerated Degradation Testing Data Analysis: A Case Study. Quality and Reliability Engineering International, 27(2):229–237.

Wang Fu-Kwun, Chu Tao-Peng, 2012. Lifetime predictions of LED-based light bars by accelerated degradation test. Microelectronics Reliability, 52(7): 1332–1336.

Wang Peng, Coit David W, 2004. Reliability prediction based on degradation modeling for systems with multiple degradation measures. Annual Reliability and Maintainability Symposium, 302–307.

Yang Kai, Yang Guangbin, 1997. Performance degradation analysis using principal component method. Annual Reliability and Maintainability Symposium, 136–141.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Estimation of lifetimes of components that operate under ageing-attributable wearing conditions

H. Tomaszek & M. Zieja
Air Force Institute of Technology, Warsaw, Poland

M. Ważny
Military University of Technology, Warsaw, Poland

ABSTRACT: The paper presents a probabilistic method to assess lifetimes of devices/components that operate under conditions typical of ageing processes. It has been assumed that the random rate of the component's wear is of the form taken by the failure rate function for the Weibull distribution, or approximately follows the linear pattern. From the point of view of mathematics, it has been based on the difference equation that, after some rearrangements, results in a partial differential equation of the Fokker-Planck type. From the particular solution to this equation one gets density function of the wear-and-tear in the form of normal distribution. Having found the density function of the wear-and-tear, one can formulate a relationship for reliability for the assumed permissible value of the wear-and-tear. With the normal distribution normalized and the required level of reliability reached, one can then compute the lifetime of a device or component under consideration.

1 INTRODUCTION

The paper presents a probabilistic method to assess lifetimes of components and (sub)assemblies that operate under conditions typical of ageing processes (induced by corrosion and/or other phenomena) within aircraft devices. Health of at least some of aircraft devices can be assessed by means of diagnostic parameters. The assessment in question needs that known are boundary values of parameters, for which the device or component is acknowledged to be serviceable (fit for use).

The diagnostic parameters can be used to describe the general condition of both the device under analysis and particular components thereof. An aircraft sight system with one of its primary functions being generation of sight information in the form of a sight marker is a pretty good example of such a device. The data found determines both the sighting angle and the angle of allowance, which reflects position of the point at which the warfare agent launched from the aircraft meets (hits) the target. Such being the case, it is necessary to determine the zero position of the optical line of sight to make the sighting system operate correctly and the aiming process proceed properly. Due to ageing processes the zero position of the line of sight given consideration gets out of the adjustment. Therefore, to improve the aiming accuracy, there is a chance and possibility to adjust the zero position of the line of sight. Such a chance appears in the course of the periodic maintenance. Corrections that allow for destructive factors are fed to the sighting system. Then, the line of sight is given its nominal parameters. What is of importance through this process is determination of time points, at which the system should be subjected to adjustment. With the system used as an example, one has to determine the system's life, i.e. to find the time up to the moment the current position of the line of sight reaches the permissible boundary value (Ważny 2008).

2 ASSUMPTIONS

The following assumptions have been made in the proposed life-assessment model (Tomaszek et al. 2011):

– the device's/system's health is determined with one diagnostic parameter „z" in the form of deviation from the initial (zero) value:

$$z = |X - X^{nom}| \tag{1}$$

where: X = current value of the diagnostic parameter, X^{nom} = nominal value of the diagnostic parameter;

– value of the diagnostic parameter's deviation keeps changing throughout the system's

operational phase (i.e. operations and maintenance, or operational use and down time);
- the 'z' parameter is non-decreasing;
- if random changes follow the linear pattern, the rate of changes in the diagnostic parameter can be described with the following relationship:

$$\frac{dz}{dt} = c \tag{2}$$

where: c = a random variable which describes the system's/component's susceptibility to changes that depend on their features and operating conditions; t = the calendar-based time;
- in the case the increment in the diagnostic parameter is non-linear it is assumed that the intensity of deviation increments takes the following form:

$$\lambda(t) = \frac{\alpha}{\theta} t^{\alpha-1} \tag{3}$$

where: α and θ = constants in the Weibull distribution.

3 HOW TO FIND THE DENSITY FUNCTION WITH ACCOUNT TAKEN OF THE RELATIONSHIP (2)

With stochastic approach applied, the dynamics of changes in value of the deviation „z" is described with the following difference equation (Casciati & Roberts 1996):

$$U_{z,t+\Delta t} = (1 - P)\, U_{z,t} + P U_{z-\Delta z,t} \tag{4}$$

where: $U_{z,t}$ = probability that at time instance t the diagnostic parameter will take value z; P = probability that in the course of time interval Δt the deviation will increase by value Δz; Δz—*i*ncrement in deviation.

For the case $P = 1$, equation (4) written down in functional notation takes the following form:

$$U(z,\ t + \Delta t) = U(z - \Delta z, t) \tag{5}$$

Equation (5) illustrates the following point: probability that at time instance t value of the deviation was $z - \Delta z$ and has increased in the course of time interval Δt by value Δz. Equation (5) is now to be rearranged in the partial differential equation. Therefore, the following approximations are assumed (Żurek et al. 2012):

$$U(z,t + \Delta t) = U(z,t) + \frac{\partial U(z,t)}{\partial t}\Delta t \tag{6}$$

$$U(z - \Delta z,t) = U(z,t) - \frac{\partial U(z,t)}{\partial z}\Delta z + \frac{1}{2}\frac{\partial^2 U(z,t)}{\partial z^2}(\Delta z) \tag{7}$$

With equations (6) and (7) applied, equation (5) takes the following form:

$$\frac{\partial U(z,t)}{\partial t} = -b\frac{\partial U(z,t)}{\partial z} + \frac{1}{2}a\frac{\partial^2 U(z,t)}{\partial z^2} \tag{8}$$

where:
$b = E[c]$ = a mean increment in value of the diagnostic parameter's deviation per time unit;
$a = E[c^2]$ = a mean square of increment in the diagnostic parameter's deviation per time unit.

Now, a particular solution to equation (8) is looked for, such that at $t \to 0$ is convergent to the so-called Dirac delta function, i.e. $u(z,\ t) \to 0$ for $z \neq 0$ and $u(0,\ t) \to +\infty$, in such a way, however, that the function integral u equals „1" for all and every $t>0$. Equation (8) takes the following form for the above defined condition (Risken 1984):

$$u(z,t) = \frac{1}{\sqrt{2\pi A(t)}} e^{-\frac{(z-B(t))^2}{2A(t)}} \tag{9}$$

where:

$$B(t) = \int_0^t b\,dt = bt = \overline{c}t, \tag{10}$$

$$A(t) = \int_0^t a\,dt = at = \overline{c}^2 \tag{11}$$

The density function of the increase in the diagnostic parameter's deviation can be used to assess reliability of the device's/system's assembly/component.

4 HOW TO FIND THE DENSITY FUNCTION WITH ACCOUNT TAKEN OF THE RELATIONSHIP (3)

With stochastic approach applied, the dynamics of changes in value of the diagnostic parameter, including the deviation, will be described with the difference equation. Let $U_{z,t}$ denotes probability that at time instance t the diagnostic parameter's deviation takes value 'z'.

A difference equation takes the following form for the assumed conditions and relationship (3):

$$U_{z,t+\Delta t} = \left(1 - \frac{\alpha}{\theta} t^{\alpha-1}\Delta t\right) U_{z,t} + \frac{\alpha}{\theta} t^{\alpha-1}\Delta t\, U_{z-\Delta z,t} \tag{12}$$

where: Δz—increment in the diagnostic parameter's deviation in time interval Δt.

Equation (12) written down in functional notation takes the following form:

$$u(z,t+\Delta t)=\left(1-\frac{\alpha}{\theta}t^{\alpha-1}\Delta t\right)u(z,t)+\frac{\alpha}{\theta}t^{\alpha-1}\Delta t\,u(z-\Delta z,t) \quad (13)$$

where:
$u(z,\ t)$ = density function of the diagnostic parameter's deviation;
$(1-\alpha/\theta(t^{\alpha-1}\Delta t))$ = probability that in time interval Δt there will be no increment in the diagnostic parameter's deviation;
$\alpha/\theta(t^{\alpha-1}\Delta t)$ = probability that in time interval Δt the increment in the diagnostic parameter's deviation will be Δz.

Rearrangement of equation (13) in a partial differential equation results in the following approximation:

$$u(z,t+\Delta t)=u(z,t)+\frac{\partial u(z,t)}{\partial t}\Delta t \quad (14)$$

$$u(z-\Delta z,t)=u(z,t)-\frac{\partial u(z,t)}{\partial z}\Delta z+\frac{1}{2}\frac{\partial^2 u(z,t)}{\partial z^2}(\Delta z)^2. \quad (15)$$

Having substituted relationships (14) and (15) in equation (13) and with some rearrangements done, the following is arrived at:

$$\frac{\partial u(z,t)}{\partial z}=-\frac{\alpha}{\theta}t^{\alpha-1}\Delta z\frac{\partial u(z,t)}{\partial z}+\frac{1}{2}\frac{\alpha}{\theta}t^{\alpha-1}(\Delta z)^2\frac{\partial^2 u(z,t)}{\partial z^2}. \quad (16)$$

Consideration is given to the increment in the diagnostic parameter's deviation per time unit (when $\Delta t=1$), hence

$$\frac{\Delta z}{\Delta t}=c,\Rightarrow \Delta z=c\Delta t,\ \underset{\Delta t=1}{\Rightarrow}\ \overline{c} \quad (17)$$

where $\overline{c}$ denotes increment in the diagnostic parameter's deviation per one time unit.

With account taken of what has been deduced above, equation (16) takes the form:

$$\frac{\partial u(z,t)}{\partial z}=-\underbrace{\frac{\alpha\overline{c}}{\theta}t^{\alpha-1}}_{\gamma(t)}\frac{\partial u(z,t)}{\partial z}+\frac{1}{2}\underbrace{\frac{\alpha\overline{c}^2}{\theta}t^{\alpha-1}}_{\beta(t)}\frac{\partial^2 u(z,t)}{\partial z^2} \quad (18)$$

As one can see, the forms of coefficients in equation (18) depend on values of parameters α. For $\alpha=1$ the coefficients take the forms:

$$\gamma(t)=\frac{\overline{c}}{\theta};\ \beta=\frac{\overline{c}^2}{\theta} \quad (19)$$

For $\theta=1$, the case in question resolves itself into the description of linear wear of stochastic form. Solution to equation (18) (for conditions described in p. 3) takes the following form:

$$u(z,t)=\frac{1}{\sqrt{2\pi A(t)}}e^{-\frac{(z-B(t))^2}{2A(t)}} \quad (20)$$

where:
$B(t)$ = an average value of the diagnostic parameter's deviation for the operating time t,

$$B(t)=\int_0^t\gamma(t)dt \quad (21)$$

$A(t)$ = a variance of the diagnostic parameter's deviation for the operating time t,

$$A(t)=\int_0^t\beta(t)dt \quad (22)$$

With integrals (21) and (22) calculated, the following expressions are arrived at:

$$B(t)=\int_0^t\frac{\alpha\overline{c}}{\theta}t^{\alpha-1}dt=\frac{\alpha\overline{c}}{\theta}\int_0^t t^{\alpha-1}dt=\frac{\alpha\overline{c}}{\theta}\frac{1}{\alpha}t^{\alpha}\Big|_0^t=\frac{\overline{c}}{\theta}t^{\alpha}-0=\frac{\overline{c}}{\theta}t^{\alpha} \quad (23)$$

$$A(t)=\int_0^t\frac{\alpha\overline{c}^2}{\theta}t^{\alpha-1}=\frac{\alpha\overline{c}^2}{\theta}\frac{1}{\alpha}t^{\alpha}\Big|_0^t=\frac{\overline{c}^2}{\theta}t^{\alpha} \quad (24)$$

5 DETERMINATION OF RELIABILITY AND LIFETIME OF THE DEVICE'S COMPONENT

With the density function found, one can write down the relationship for reliability and life with respect to time of the diagnostic parameter's deviation increasing up to the boundary value. The formula takes the form:

$$R(t)\cong\int_{-\infty}^{z_d}u(z,t)dz\cong\int_0^{z_d}u(z,t)dz \quad (25)$$

where: $u(z,t)$ = density function determined with equation (9) or equation (20); z_d = a permissible value of the diagnostic parameter's deviation with respect to safety; t = the calendar-based time of operating the device/system.

Figure 1 schematically shows how the density function proceeds and how reliability and life are determined.

If the relationship

$$\omega(t) = \frac{B(t)}{\sqrt{A(t)}} \tag{26}$$

exceeds the value of 3.5 in a short time, then the lower limit of the integral in equation (25) can be assumed $-\infty$ (Pham 2006).

The random variable z is standardized:

$$l_t = \frac{z - B(t)}{\sqrt{A(t)}} \tag{27}$$

After standardization equation (25) takes the form

$$R(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{z_d - B(t)}{\sqrt{A(t)}}} e^{-\frac{l_t^2}{2}} dl \tag{28}$$

Assuming that the required value of reliability is $R(t)=R^*$, the value of the upper limit of the integral, such that the integral (28) equals R*, is to be found in the Standard Normal Distribution Table. Let w be this value. Hence,

$$w = \frac{z_d - B(t)}{\sqrt{A(t)}} \tag{29}$$

Having solved equation (29) with respect to t one receives such value of t^*, for which the level of reliability, for $t \le t^*$, is $R(t) \ge R^*$. Therefore, t^* can be assumed either the component's life or time of the deviation's increasing up to the value that does not exceed the level assumed the permissible value.

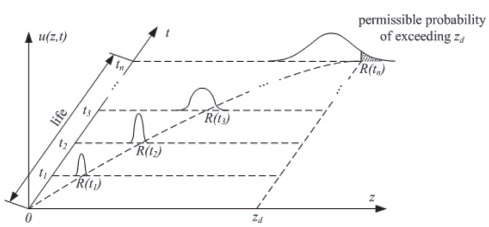


Figure 1. Schematically shown density function.

Two models have been given consideration. One linear, of stochastic nature, and the other one non-linear. The relationship (29) takes, therefore, two forms:

– for a linear model:

$$w = \frac{z_d - \bar{c}t}{\sqrt{\bar{c}^2 t}} = \frac{z_d - bt}{\sqrt{at}} \tag{30}$$

– for a non-linear model:

$$w = \frac{z_d - \frac{\bar{c}}{\theta} t^\alpha}{\sqrt{\frac{\bar{c}^2}{\theta} t^\alpha}} = \frac{z_d - \bar{b} t^\alpha}{\sqrt{\bar{a}} t^\alpha} \tag{31}$$

Now, t is found from the relationship (30).

$w\sqrt{at} = z_d - bt,$
$w^2\, at = (z_d - bt)^2,$
$w^2\, at = z_d^2 - 2z_d\, bt + b^2\, t^2,$
$b^2t^2 - 2z_d\, bt + z_d^2 - w^2\, at = 0,$
$b^2t^2 - (2z_d\, \mathrm{b} + w^2 a)t + z_d^2 = 0.$

Hence,

$$t_{1,2} = \frac{-\left(-\left(2bz_d + w^2 a\right)\right) \pm \sqrt{\left(2bz_g + w^2 a\right)^2 - 4b^2 z_d^2}}{2b^2},$$

$$t^* = \frac{\left(2bz_d + w^2 a\right) \pm \sqrt{\left(2bz_g + w^2 a\right)^2 - 4b^2 z_d^2}}{2b^2} \tag{32}$$

From relationship (31) t is found. We assume $\theta = 1$ and find $t^\alpha = s$. Hence,

$$w = \frac{z_d - bs}{\sqrt{as}} \tag{33}$$

Equation (33) is in its notation exactly the same as equation (30); after rearrangement the following is, therefore, arrived at:

$$s^* = \frac{\left(2bz_d + w^2 a\right) \pm \sqrt{\left(2bz_g + w^2 a\right)^2 - 4b^2 z_d^2}}{2b^2} \tag{34}$$

Hence,

$$t^* = \frac{\log s}{\alpha} \tag{35}$$

To make use of the above written relationships, one should find values of (assess) constants in these equations. Therefore, it is assumed that data on values

of deviation of the diagnostic parameter come from monitoring the device under examination throughout its operational phase (Kececioglu 2002):

$$[(z_0, t_0), (z_1, t_1), (z_2, t_2), \ldots, (z_n, t_n)]. \quad (36)$$

The best method to find values of b and a is one that uses the likelihood function. The form of it in the general case can be presented as the following relationship (37) (Dhillon 1999):

$$L = \prod_{k=0}^{n=1} g(t_k, z_k, \theta_1, \theta_2, \ldots, \theta_m) \quad (37)$$

where: $g(t_k, z_k, \theta_1, \theta_2, \ldots, \theta_m)$ = the density function of the total probability of the variable z; $(\theta_1, \theta_2, \ldots, \theta_m)$ = parameters of the density function; z_k = the measured values of the wear-and-tear parameter z with suitably at time instances $(t_1, t_2, \ldots, t_k)$. Finding estimates $\theta_1^*, \theta_2^*, \ldots, \theta_m^*$ of unknown parameters $(\theta_1, \theta_2, \ldots, \theta_m)$ with the maximum likelihood method resolves itself in solving equations of the following form (Tomaszek et al. 2008):

$$\frac{\partial \ln L}{\partial \theta_j} = 0 \quad (38)$$

where: $j = 1,2, \ldots, m$; m = the number of parameters that best describe the engineered object in question.

Such being the case, estimation of b^* and a^* of unknown parameters b and a with the maximum likelihood method resolves itself into solving a system of equations:

$$\begin{cases} \dfrac{\partial \ln L}{\partial b} = 0 \\ \dfrac{\partial \ln L}{\partial a} = 0 \end{cases} \quad (39)$$

Solving the system of equations (39) one finds b^* and a^*:

$$b^* = \frac{z_n}{t_n} \quad (40)$$

$$a^* = \frac{1}{n} \sum_{k=0}^{n-1} \frac{\left[(z_{k+1} - z_k) - b^*(t_{k+1} - t_k)\right]^2}{(t_{k+1} - t_k)} \quad (41)$$

6 A NUMERICAL EXAMPLE

One of the components of a sighting system is a surveillance-and-sighting head, by means of which the aiming information is displayed. Its health is determined with diagnostic parameters that describe coordinates of the sighting marker's position. Having analyzed results of checks of some specific population of sighting heads it has been found that as the operating time elapses, due to destructive factors affecting the system, values of these parameters suffer changes. A sample course of changes in value of one of the diagnostic parameters recorded in the course of the operational process has been presented in Figure 2. From the plot one can deduce that in this case a linear model of changes in diagnostic parameters is used (Ważny 2008 & 2009).

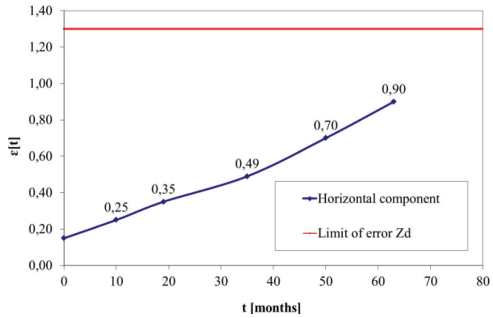


Figure 2. Changes in value of the diagnostic parameter throughout the sighting head's operation.

Therefore, having got data that describe values of diagnostic parameter's deviation in the following form:

$$[(z_0, t_0), (z_1, t_1), (z_2, t_2), \ldots, (z_n, t_n)]$$

and on the basis of equations (40) and (41), values of coefficients of the density function could be found:

$$b_\varepsilon^* = 0{,}034 \qquad a_\varepsilon^* = 0{,}001 \quad (42)$$

Assuming the level of maintaining the zero state, value of the parameter $\gamma^* = 2{,}35$ could be found from the Standard Normal Distribution Table. The z_d parameter could be found in the system's technical documentation (Maintenance Manual), where values of permissible deviations of diagnostic parameters are given.

Thus, values of parameters $b_\varepsilon^*, a_\varepsilon^*, \gamma^*, z_d$ have been substituted in equation (32); time, after which values of deviations of the diagnostic parameters reach and exceed the boundary state has been calculated. For the case under analysis this time is:

$$t_\varepsilon = 17 \text{ [months]} \quad (43)$$

Results gained (43) can be used in maintenance procedures, depending on the maintenance

strategy accepted. On the basis of the above-presented methodology, one can find subsequent time intervals (periods of time), when the device's/system's diagnostic parameter(s) should be checked and adjustments made to bring values of measured quantities to the zero (nominal) position.

7 FINAL REMARKS

To recapitulate, one can state that the above-presented method seems to be correct and right, and allows of analyses of the device's/system's health with reference to the nature of changes in values of diagnostic parameters. The presented numerical example has made verification of the formulated model possible and emphasizes application-oriented qualities of the developed method. The method may prove suitable for further works on improving both the operational/maintenance processes and the way of using the aircraft with its on-board systems, all this owing to the capability of determining time the device/system remains serviceable (fit for use).

Furthermore, owing to its versatility, the method can be successfully used to determine residual life of any engineered object, the health of which is determined on the basis of analyses of values of diagnostic parameters.

REFERENCES

Casciati, F. & Roberts, B. 1996. *Mathematical Models for Structural Reliability Analysis*. Boca Raton/New York/London/Tokyo: CRC Press.

DeLurgio, S.A. 1998. *Forecasting principles and applications*. University of Missouri-Kansas City: Irwin/McGraw-Hill.

Dhillon, B.S. 1999. *Design Reliability. Fundamentals and Applications*. Ottawa: Boca Raton/New York/London/Washington: CRC Press.

Kececioglu, D.B. 2002. *Reliability Engineering Handbook*. Lancaster: DEStech Publications.

Pham, H. 2006. *Handbook of Engineering Statistics*. London: Springer-Verlag.

Risken H. 1984. The Fokker-Planck Equation. Methods of Solution and Applications. Berlin/Heidenberg/New York/Tokio: Springer Verlag.

Tomaszek H. & Wróblewski M. 2001. *The essentials of estimating operational effectiveness of air weapons systems*. Warsaw: Publishing House „Bellona".

Tomaszek, H. & Jasztal, M. & Zieja, M. 2011. A simplified method to assess fatigue life of selected structural components of an aircraft for a variable load spectrum. *Maintenance and Reliability* 4: 29–34.

Tomaszek, H. & Żurek, J. & Jasztal, M. 2008. *How to predict failures hazardous to aircraft flight safety*. Warsaw: Scientific Publishing Office of Institute for Sustainable Technologies—National Research Institute.

Tomaszek, H. & Żurek, J. & Zieja, M. 2012. The reliability estimation of structural components with some selected failure model. *Proc. 11th International Probabilistic Safety Assessment and Management Conference PSAM 11 & The Annual European Safety and Reliability Conference ESREL 2012, Helsinki, 25–29 June 2012.*

Ważny, M. 2008. The method of determining the time concerning the operation of a chosen navigation and aiming device in the operation system. *Maintenance and Reliability* 2.

Ważny, M. (2009). The method for assessing residual durability of selected of devices in avionics system. *Maintenance and Reliability* 3.

Zio, E. 2009. *Computational Methods For Reliability and Risk Analysis*. Singapore: World Scientific Publishing.

Żurek, J. & Tomaszek, H. & Zieja, M. 2012. A model to assess lives of selected structural components of an aircraft using time distribution of exceeding a boundary condition—an outline. *Advances in Safety, Reliability and Risk Management*. London: CRC/Balkema.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A Physics-of-Failure-based approach for failure behavior modeling: With a focus on failure collaborations

Z. Zeng, R. Kang & Y. Chen
School of Reliability and Systems Engineering, Beihang University, Beijing, China

ABSTRACT: Traditional Physics-of-Failure (PoF) methods assume independence among failure mechanisms. In this paper, a failure behavior modeling approach is proposed to allow for considering interdependence in PoF modeling. The interdependence is characterized by modeling failure mechanisms and relations among them. Three basic relations among failure mechanisms, i.e., competition, superposition and coupling are discussed in the first place. Models for the three relations are also established. Based on the developed relation models, the failure behavior modeling approach is presented. Finally, a case study of a spool valve is conducted to show that the proposed method can provide a more accurate description of failure behaviors than traditional PoF methods.

1 INTRODUCTION

Failure behaviors of a system refer to the observable changes of system states which take place during the system's failure process. Characterization of failure behaviors plays a central role in reliability engineering (Zeng et al. 2013). Traditionally, failure behaviors of a system are characterized by recording time-to-failure of the system and fitting a probability distribution to them (Meeker & Escobar 1998). However, fitting TTF distributions requires collecting large amount of failure data, which severely limits the applicability of TTF-based characterization of system failure behaviors. To cope with this problem, more and more researchers are trying to use Physics-of-Failure (PoF) as a new way to characterize system failure behaviors.

PoF models establish relationships among failure inducing factors, their corresponding failure times and failure phenomena by understanding physical processes leading to the failure (failure mechanisms). The concept of PoF was formally established in 1962 in the first of a series of symposia (which now becomes the International Reliability Physics Symposium, IRPS) organized by the Rome Air Development Center (RADC) of the US Air Force (Chatterjee et al. 2012). From then on, researches have been conducted to develop PoF models for various failure mechanisms and products. Till today, most of the commonly encountered failure mechanisms have been well understood and modeled. For example, McPherson (2010) and Liu et al. (2011) discuss commonly encountered failure mechanisms for electronic products and interconnects and summarize PoF models. For discussions on mechanical failure mechanisms and corresponding PoF models, readers can refer to Tinga (2013) and Collins et al. (2009).

The well-established PoF models lay down a solid foundation of PoF-based system failure behavior modeling. Generally, there are three PoF-based system failure behavior modeling approaches. Pecht & Dasgupta (1995) propose a TTF-oriented method to characterize a system's failure behavior based on components' PoF models. They assume that the shortest TTF among all failure mechanism will determine the TTF of the whole system (failure competition) and thus, by calculating TTF of each failure mechanism, TTF of the system can be decided.

The second PoF-based failure behavior modeling method is the Failure-Rate-oriented (FR-oriented) method. The method uses failure rates as a measure of system failure behaviors. A typical example of the method is the RAMP method developed by IBM cooperation (Srinivasan et al. 2003). Under the assumptions of constant failure rate and failure competition, the method firstly calculates the Mean Time To Failure (MTTF) of each component from corresponding PoF models. Then, failure rates of the system are established by summing up all components' failure rates.

Apart from the aforementioned two methods, another PoF-based failure behavior modeling method tries to model the variation of systems' performance measures over time and uses the performance measures as an indicator of failure behaviors. For example, Savage & Son (2011) proposes a framework to obtain the variations of systems' performance measures over time from

PoF-based degradation models. Cao et al. (2014) uses PoF-based degradation model of electronic devices to determine the performance degradation in circuit levels.

The three PoF-based failure behavior modeling methods have been applied widely in both academia and industries. However, they share a defect, i.e., all of them are grounded on the assumption of failure competition. The assumption suggests that all the failure mechanisms evolve independently from each other and the mechanism with the shortest TTF will determine the TTF of the system. However, in actual cases, failure mechanisms often interact with each other and thus exhibit some collaboration behaviors (by collaboration we mean the mechanisms "work together" to cause failures). For example, it is widely observed that collaborations exist among failure mechanisms to accelerate the failure processes, e.g., the interaction between fatigue and corrosion (Dong et al. 2012), fatigue and creep (Zhu et al. 2012), erosion and corrosion (Malka et al. 2007), etc. The assumption of failure competition ignores these collaboration effects and thus will lead to inaccurate results when predicting failure behaviors.

In fact, some progress has been achieved in modeling the collaboration effects among failure mechanisms, e.g. Burgazzi (2009) used coefficient of variances to model the interdependence among failure mechanisms. Peng et al. (2010) developed a model for interdependency among a generic degradation process and a shock process. Keedy & Feng (2013) proposed a similar model and applied it to analysis a stent with dependent competing failure processes. However, all these researches provide methods to model the collaboration effects in a statistical way. Few methods have provided the physical insights of failure collaborations. In this paper, we will present a physics-based method to analysis and model the failure collaborations.

2 A TWO-TIER STRUCTURE FOR MODELING FAILURE COLLABORATIONS

Since the principle of failure competition obtains the TTF of the system as the shortest TTF among all the failure mechanism models, it does not take the interaction among the failure mechanisms into account. The interaction, referred to as failure collaboration in this paper, has a hierarchical structure of two tiers, as shown in Figure 1. In the component-tier, failure collaboration refers to the interactions among failure mechanisms. When a component is subjected to multiple failure mechanisms, the mechanisms might exert influences on each other, as shown in Figure 1. For example,

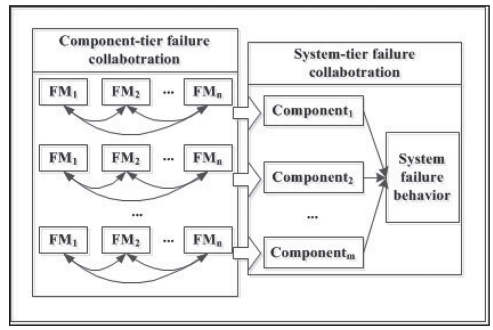


Figure 1. The two-tier structure of failure collaboration. FM: Failure Mechanism.

it is observed from experiment data that the two mechanisms, erosion and corrosion are mutually enhanced, resulting in a more significant degradation effect (Malka et al. 2007). Also, failure collaboration exists in test specimens exposed to high temperature and heavy load, where the two failure mechanism of fatigue and creep interact with each other and severely reduce the TTF of the test specimens (Zhu et al. 2012). In microelectronic devices, similar but more sophisticated phenomena can also be observed between the two mechanisms Hot Carrier Injection (HCI) and Negative Bias Temperature Instability (NBTI) (Kufluoglu 2007). The interactions among the failure mechanisms are regarded as component-tier failure collaboration.

Even for components subjected to only one failure mechanism, which means there is no failure collaboration in the component-tier, we still have to consider the effect of the system-tier failure collaboration. In the system-tier, failure collaboration refers to the joint effects of the components on the failure behavior of the system, as shown in Figure 1. According to Figure 1, the failure behavior of components is determined from their corresponding failure mechanisms. Failure behaviors of the system are in turn decided by the failure behaviors of the components. In the process, different components might contribute to the same failure behavior of the system and thus result in the system-tier failure collaboration.

In order to accurately model the system's failure behavior, both the component-tier and system-tier failure collaboration should be addressed properly. However, in this paper, we mainly focus on the modeling of component-tier failure collaboration (the treatment of system-tier collaborations will be addressed in a separated paper) and model the component-tier failure collaboration from two perspectives, i.e., failure mechanisms and interactions among them.

3 COMPONENT-TIER FAILURE BEHAVIOR MODEL DEVELOPMENT

3.1 *Performance parameter and failure behavior model*

In this section, a PoF-based component failure behavior modeling approach will be presented to characterize failure behaviors under the influences of component-tier failure collaborations. Failures are the event or state that a system no longer fulfills its intended function. In most cases, a system's function can be represented by several performance parameters. A failure state is reached when the performance parameter exceeded its associated failure threshold.

Definition 1. Suppose a given function of a system (or a component) will not be fulfilled if and only if the following inequality holds,

$p \geq p_{th}$.

Then parameter p is defined as a performance parameter of the system, while p_{th} is defined as the associated failure threshold.

Example 1. A beam is designed with a function of withstanding a given load. Thus, its performance parameter is the stress σ calculated from the load, and associated failure threshold is the strength of the beam $[\sigma]$. When $\sigma \geq [\sigma]$, failures of the beam will take place.

Example 2. A spool valve is designed with a function of controlling the flow of hydraulic oils. The enlargement of the spool's clearance due to wear will lead to oil leakage and thus affects the desired function. Therefore, a performance parameter of the spool is its clearance x, and its corresponding failure threshold x_{th} will be determined from its functional requirements, so that when $x \geq x_{th}$, failures of the spool will take place.

Thus, failure behaviors can be characterized by developing a model for the performance parameter and its variation over time, as shown in equation (1). In equation (1), $\mathbf{x}$ denotes a vector of failure inducing factors. By substituting p_{th} into equation (1), TTF of the system (or component) can be determined, as shown in equation (2).

$$p = f_{be}(\mathbf{x};t). \tag{1}$$

$$\mathrm{TTF} = \arg_t \left(f_{be}(\mathbf{x};t) = p_{th} \right). \tag{2}$$

3.2 *Models for mechanism interaction relations*

Performance parameters in equation (1) can be obtained from PoF models. However, as shown in Figure 1, failure collaboration effects exist in component tier and should be accounted for in the development of component failure behavior model. The collaboration effects can be modeled as a combination of three basic interaction relations among failure mechanisms, i.e., competition, superposition and coupling.

3.2.1 *Models for mechanism competition*

Competition is an interaction relation among two or more failure mechanisms where each mechanism contribute to a specific performance parameter and the presence of one mechanism has little or no influence on the others, as shown in Figure 2(a). Thus, the interactions among failure mechanisms can be modeled by the weakest-link model, where the failure mechanism first evolves to failure will determine the failure behavior of the component. If the failure mechanism models takes the form of equation (1) (which means, the performance parameters will vary over time), the weakest-link model can be expressed as equation (3).

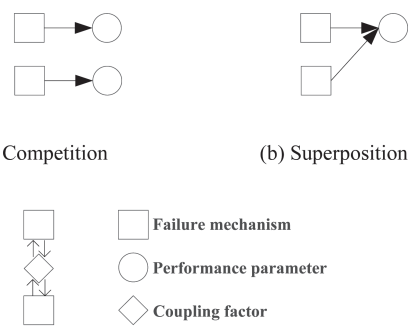
$$TF = \min_{i=1}^{n} TF_n. \tag{3}$$

Example 3. An example of mechanism competition is the failure of composite plies (Whiteside et al. 2012). There are three failure mechanisms for the composite ply and each of them results in a specific failure mode. The mechanisms include fiber tensile (f_{ft}), matrix failure (f_{mat}) and fiber kinking/splitting ($f_{kink/split}$) and models describing them are presented in Eq. (4) to (6).

1. Fiber tensile

$$f_{ft} = \left(\frac{\sigma_1}{\sigma_L^+} \right)^2 \geq 1, \tag{4}$$

where σ_1 is the main stress and σ_L^+ is the tensile strength in the longitudinal direction parallel to the fibers.



(a) Competition (b) Superposition

(c) Coupling

Figure 2. Illustrations of the three basic interaction relations.

2. Matrix failure

$$f_{mat} = \left(\frac{\tau_{23}^{\phi_0}}{\tau_T - \mu_T \sigma_n^{\phi_0}} + \frac{\tau_{12}^{\phi_0}}{\tau_L - \mu_L \sigma_n^{\phi_0}} + \frac{\sigma_{n+}^{\phi_0}}{\sigma_T^+} \right) \geq 1, \tag{5}$$

where $\tau_{23}^{\phi_0}, \tau_{12}^{\phi_0}, \sigma_n^{\phi_0}$ is the components of stresses in the specific directions, $\tau_T, \tau_L, \sigma_T^+$ are the corresponding strengths and μ_L, μ_T are coefficient of frictions in the specific directions.

3. Fiber kinking/splitting

$$f_{kink} = f_{split} = \left(\frac{\tau_{23}^{m_0}}{\tau_T - \mu_T \sigma_2^{m_0}} \right)^2 + \left(\frac{\tau_{12}^{m_0}}{\tau_T - \mu_T \sigma_2^{m_0}} \right)^2 + \left(\frac{\sigma_{2+}^{m_0}}{\sigma_T^+} \right). \tag{6}$$

The meaning of each parameter is consistent with those in equation (4) and (5). In an actual composite ply, the three mechanisms are independent from each other and the weakest link model can be used to model the interactions among them, as shown in equation (7).

$$f_{PB} = \max\left(f_{ft}, f_{max}, f_{kink}, f_{split} \right) \geq 1. \tag{7}$$

3.2.2 *Models for mechanism superposition*

Superposition is an interaction relation among two or more failure mechanisms where all the mechanisms contribute to one performance parameter, as shown in Figure 2(b). Superposition of failure mechanisms can be modeled by summing up all the variation rates individually determined by each failure mechanism, as shown in equation (8),

$$\frac{dp}{dt} = \sum_{i=1}^{n} \frac{dp_i}{dt}, \tag{8}$$

where dp/dt is the variation rate resulting from all mechanisms and $dp_i/dt, i = 1,2,\ldots,n$ are the variation rates resulting from each individual failure mechanism. From the performance variation rate determined from equation (8), the failure behavior model in equation (1) can be obtained easily given the initial conditions.

Example 4. An example of mechanism superposition is the relation between two failure mechanism models contributing to Time-Dependent Dielectric Breakdown (TDDB) (McPherson 2010). TDDB can be modeled by two mechanism models, the E-model (equation (9)) and the 1/E-model (equation (10)).

$$TF = A_0 \exp\{-\gamma E_{ox}\} \exp\left\{ \frac{Q}{K_B T} \right\}. \tag{9}$$

$$TF = \tau_0(T) \exp\left\{ \frac{G(T)}{E_{ox}} \right\}. \tag{10}$$

Since the two mechanisms exist simultaneously, the velocity summation principle is employed to model the time to failure of TDDB, as shown in Eq (11),

$$k = k_E + k_{1/E}, \tag{11}$$

where k, k_E, $k_{1/E}$ are the rate constant of the whole process, the E-model and the 1/E-model, respectively. If the rate of each model is a constant, equation (11) leads to

$$TF = \frac{TF_E \cdot TF_{1/E}}{TF_E + TF_{1/E}}. \tag{12}$$

3.2.3 *Models for mechanism coupling*

Coupling is an interaction relation among two or more failure mechanisms where the presence of one mechanism will exert influence on the other mechanisms, as shown in Figure 2(c). In order to accurately model failure behaviors under coupled failure mechanisms, one has to start with an investigation of the way in which the mechanisms are coupled. Often the couplings are caused by the change of driving conditions of one mechanism due to the affections from other mechanisms. For example, the wear of materials will deteriorate their strengths and in turn affect the fatigue life under cyclic loads. The coupling effect can be modeled by introducing the concept of coupling factor.

Definition 2. Coupling factors are parameters in one of the coupled failure mechanisms which are influenced by the other failure mechanisms.

Equation (13) shows how to use coupling factors to model the coupling effects of two failure mechanisms. In equation (13), p denotes the performance parameter, $f_{FM_1}(\cdot), f_{FM_2}(\cdot)$ are the two PoF models, respectively, x_{couple} is the coupling factor and $\mathbf{x}_{rest}, \mathbf{x}_2$ are other parameters in the PoF models.

From an analysis of the coupling process, we can identify the coupling factors, i.e., the x_{couple} in equation (13). Then, coupling relations are modeled by the $g(\cdot)$ in equation (13). To determine the form of $g(\cdot)$, a deeper analysis should be conducted into the coupling mechanisms. Finally, equation (13) is solved to obtain the performance parameter p. Sometimes the $\mathbf{x}_2$ in $g(\cdot)$ might be a function of p, making equation (13) hard to be solved. Thus,

approximations are often needed when trying to solve equation (13).

$$\begin{cases} p = f_{FM_1}\left(\mathbf{x}_{rest}, x_{couple}; t\right), \\ x_{couple} = g\left(f_{FM_2}\left(\mathbf{x}_2; t\right)\right). \end{cases} \tag{13}$$

Example 5. An example of modeling coupled failure mechanisms is the failure behavior model for components subjected to the coupling of fatigue and creep (Collins et al. 2009). For components subjected to only low-cycle fatigue, a Coffin-Manson model will approximate the failure behaviors quite well (Equation (14)). In equation (14), N_f is the TTF in cycles, $\Delta\gamma_p$ is the plastic strain range and both m and C are constants associated with material properties.

$$\left[N_f\right]^m \Delta\gamma_p = C. \tag{14}$$

The coupling effects of creep and fatigue result that frequency of applied loads also influences the failure behavior. Thus, a coupling factor k is introduced in equation (14) to model the coupling effect, as shown in equation (15). In equation (15), υ is the frequency of applied loads and k is the coupling factor. The coupling factor k is determined from the coupling mechanism of creep and fatigue. Since it is much too complicated to be modeled, the value of k in equation (15) is often determined via experiments (Collins et al. 2009).

$$\left[N_f \upsilon^{k-1}\right]^m \Delta\gamma_p = C. \tag{15}$$

In actual cases, interaction relations among failure mechanisms might be a combination of the three basic relations discussed above. The failure behavior models can be built by the same combination of the three relation models. An example will be given in Sect. 4 to illustrate how to use combinations of basic relations to model failure mechanisms.

4 CASE STUDIES

4.1 *Failure mechanisms and PoF models*

A spool valve in an aviation hydraulic actuator is chosen as a case study to demonstrate the proposed PoF-based component failure behavior modeling approach. As discussed in Example 1, the performance parameter of the spool is its clearance. According to the result of failure mode, mechanism, effect analysis (Liao, 2013), the spool is subjected to two failure mechanisms, i.e., adhesive wear and abrasive wear.

Adhesive wear can be modeled by Archard model (Archard 1953), as shown in equation (16). In equation (16),

x_{adh} is wear depth cause by adhesive wear,

K_{adh} is a constant associated with surface conditions and lubrication,

W_a is the normal load in the wear surfaces and

H_m is the hardness of the wear surface.

$$\frac{dx_{adh}}{dt} = K_{adh}\frac{W_a}{H_m} = k_1. \tag{16}$$

Abrasive wear can be modeled by equation (17). In equation (17), K_{abr} is a constant associated with the wear properties of the wear surfaces while other parameters in equation (17) share the same meaning as those in equation (16).

$$\frac{dx_{abr}}{dt} = K_{abr}\frac{W_a}{H_m} = k_2. \tag{17}$$

The constants k_1 and k_2 are often estimated from wear experiments. Both equation (16) and (17) suggest that the wear depth is a linear function of time. Thus, if we do not take into the collaboration effects into account, the PoF models will suggest constant rate wear process.

4.2 *Failure collaboration effects*

However, collaboration effects exist between the two failure mechanisms, as shown in Figure 3. Both the wear depth from adhesive wear and abrasive wear contribute to the total wear depth x_{total}. Thus, superposition relation exists between the two mechanisms.

Besides, the K_{adh} in Archard model is influenced by the surface roughness σ_S. The result of the two wear mechanism will in turn change the surface roughness. Thus, the two failure mechanisms are coupling together.

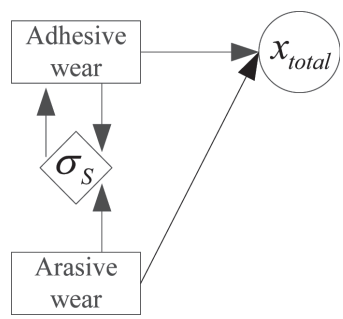


Figure 3. Failure collaborations of the two mechanisms.

4.3 *Failure behavior model development*

In order to develop failure behavior model for the spool, the model for mechanism superposition and coupling should be combined. From superposition model (equation (8)), we have

$$\frac{dx_{total}}{dt} = \frac{dx_{adh}}{dt} + \frac{dx_{abr}}{dt} = k_1 + k_2. \tag{18}$$

In equation (18), k_1,k_2 denote the wear velocity decided from adhesive and abrasive wear, respectively. Traditionally, the coupling effects between the two failure mechanisms are omitted in the development of failure mechanism model. Thus, a linear model shown in equation (18) is used as the traditional PoF model for components subjected to wear mechanisms.

In this case study, we use the proposed method to model the coupling of the two failure mechanisms. Since K_{adh} is a function of σ_S and σ_S is a function of x_{total}, it is assumed that

$$k_1 = g\left(x_{total}\right). \tag{19}$$

By using its first order Tylor expansion as an approximation of equation (19) and assuming that $g(0) = 0$, we have,

$$k_1 = -k'_1 x_{total}. \tag{20}$$

Substitute equation (20) into equation (18) and solve for x_{total}, we have,

$$x(t) = \frac{k_2 - \exp\left\{-k'_1 t + \ln k_2\right\}}{k'_1} \tag{21}$$

Equation (21) is the failure behavior model after considering the collaboration effects.

4.4 *Experimental results and discussions*

In order to compare the built failure behavior model built from the proposed method with that from traditional method, a wear test is conducted. Wear depths are monitored at equal intervals, as shown in Figure 4 (The wear depth data are scaled for confidential reasons). Failure behavior model in equation (21) and a linear model (traditional method) are both fitted to experimental data. The results are also shown in Figure 4.

It can be seen from Figure 4 that the failure behavior model from the proposed method provides a better fit to experimental data than the linear one from traditional method. This conclusion can be justified from the Mean Square Error (MSE) of both models. The MSE of proposed model is 0.5298, which is far less than the 5.7981 of the traditional model.

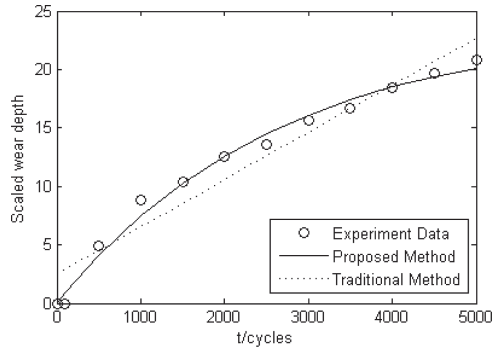


Figure 4. Experimental results and model fitting.

The result can be explained by the trends of experimental data. From Figure 4, we can see that the wear rate of the spool is decreasing over time, which suggests that the spool is in running-wear period. In this period, the interaction between the two wear mechanisms tends to slow down the wear process. However, the traditional method ignores this interaction effects and thus leads to inaccurate results. Since the proposed method has taken the interaction between the two failure mechanisms into account, it outperforms the traditional model in this case study.

5 CONCLUSIONS

In this paper, three basic interaction relations among failure mechanisms are discussed and the models for these relations are developed. A PoF-based component-tier failure behavior modeling approach is then proposed. Based on the developed interaction relation models, the proposed method provides a tool to model the interdependencies among failure mechanisms in a physical way.

ACKNOWLEDGEMENT

The work in this paper is supported by the Innovation Foundation of Beihang University (BUAA) for PhD Graduates.

The authors would also like to express special appreciations to Mr. Liao Xun for his help in the analysis of wear mechanisms and the design and implementation of wear tests.

REFERENCES

Archard, J.F. 1953. Contact and rubbing of flat surfaces. *Journal of Applied Physics* 24(8): 981–988.

Burgazzi, L. 2009. Evaluation of the dependencies related to passive system failure. *Nuclear Engineering and Design* 239(12): 3048–3053.

Cao, Y., et al. 2014. Cross-Layer modeling and simulation of circuit reliability. *IEEE Transactions On Computer-Aided Design of Integrated Circuits and Systems* 33(1): 8–23.

Chatterjee, K., et al. 2012. Fifty years of physics of failure.

Collins, J.A., et al. 2009. *Mechanical design of machine elements and machines*, Wiley.

Dong, W., et al. 2012. Fatigue reliability analysis of the jacket support structure for offshore wind turbine considering the effect of corrosion and inspection. *Reliability Engineering and System Safety* 106: 11–27.

Keedy, E.& Feng, Q. 2013. Reliability analysis and customized preventive maintenance policies for stents with stochastic dependent competing risk processes. *IEEE Transactions On Reliability* 62(4): 887–897.

Kufluoglu, H. 2007. Mosfet degradation due to negative bias temperature. West Lafeyette, US, Purdue University. Ph.D. Dissertation.

Liao, X., et al. 2013, Research on the wear life analysis of aero-hydraulic spool valve based on a dynamic wear model. WCEAM2013, Hong Kong.

Liu, J., et al. 2011. *Reliability of microtechnology, interconnects, devices and systems*, Springer:

Malka, R., et al. 2007. Erosion-corrosion and synergistic effects in disturbed liquid-particle flow. *Wear* 262(7): 791–799.

McPherson, J.W. 2010. *Reliability physics and engineering: time-to-failure modeling*, Springer: New York.

Meeker, W.Q. & Escobar, L.A. 1998. *Statistical methods for reliability data*, Wiley: New York.

Pecht, M. & Dasgupta, A. 1995. Physics-of-failure: An approach to reliable product development. *In Proc. Integrated Reliability Workshop.*, Lake Tahoe, US, 1995, IEEE.

Peng, H., et al. 2010. Reliability and maintenance modeling for systems subject to multiple dependent competing failure processes. *Iie Transactions* 43(1): 12–22.

Savage, G.J. & Kap Son, Y. 2011. The set-theory method for systems reliability of structures with degrading components. *Reliability Engineering & System Safety* 96(1): 108–116.

Srinivasan, J., et al. 2003. Ramp: A model for reliability aware microprocessor design, IBM Corporation, US.

Tinga, T., Ed. 2013. Principles of loads and failure: Applications in maintenance, reliability and design. London, Springer.

Whiteside, M.B., et al. 2012. Stochastic failure modelling of unidirectional composite ply failure. *Reliability Engineering and System Safety* 108(0): 1–9.

Zeng, Z., et al. 2013. Failure behavior modeling: Towards a better characterization of product failures. *Chemical Engineering* 33: 571–576.

Zhu, S., et al. 2012. A generalized energy-based fatigue-creep damage parameter for life prediction of turbine disk alloys. *Engineering Fracture Mechanics*.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Fault diagnosis method for circuit board based on BP neural networks

Y. Peng & J. Shi
School of Reliability and System Engineering (Science and Technology on Reliability and Environmental Engineering Laboratory), Beihang University, Beijing, China

ABSTRACT: This paper presents a new fault diagnosis method for circuit boards based on BP neural networks. First, a description of traditional fault diagnosis methods is given and the shortcomings are demonstrated. To improve the accuracy of fault diagnosis, a new method based on BP neural networks is proposed, which takes the temperature data of chips as well as voltage data as the basis of diagnosis. Finally, an example is provided, which shows that the proposed method performs better in fault diagnosis of the circuit board.

1 INTRODUCTION

In modern times, electronic equipment has become more and more complex, which usually leads to a higher failure rate of the system. Once a crucial fault happens, the function of the equipment may be heavily affected. To guarantee the efficiency of maintenance, the system capability of accurate fault identification is of great significance (Shi et al. 2012).

In recent years, some intelligent fault diagnosis methods, such as fault trees, expert systems and fuzzy comprehensive evaluation, are commonly used in electric devices (Yu et al. 2012). Besides, with its strong ability of parallel information processing and adaptive learning, ANN (Artificial Neural Network) has also become an ideal tool for fault diagnosis. Among the ANNs, BP neural network, which is a typical feedforward neural network owning strong capabilities to execute function approximation, classification and non-linear mapping, has been widely used in fault diagnosis of circuits (Li et al. 2011).

However, there are some shortcomings in the traditional method of circuit fault diagnosis with BP neural network. Firstly, because of the limit of test points, not all the failure modes can cause obvious voltage changes of the specific points monitored by the voltage acquisition system, which lowers the system fault identification rate. Next, when a fault happens in the feedback circuit, change in voltage data is sometimes too slow for neural networks to diagnose the fault correctly. Moreover, BP neural network may make specific mistake in fault diagnosis due to the data characteristics in practical application. Last but not the least, there are always some failure types causing the same voltage change that the network cannot distinguish.

To solve the problems above, we propose a multi-BP neural network, which takes both voltage and chip temperature data of a circuit as diagnosis information. In this paper, the principle of BP neural network is given. Then the new fault diagnosis method based on BP neural network is proposed. Finally, the new method is applied to an experiment, which shows its efficiency in fault identification.

2 PRINCIPLE OF BP NEURAL NETWORK

2.1 *Structure and algorithm*

As is shown in Figure 1, BP neural network is a multi-layer feedforward network with error back-propagation learning, which consists of an input layer, an output layer and several hidden layers. Each layer includes a set of neurons interconnected by weight (Han et al. 2009).

A Common BP ANN has two basic steps of execution. The first step is forward computation, which means the output value is calculated layer

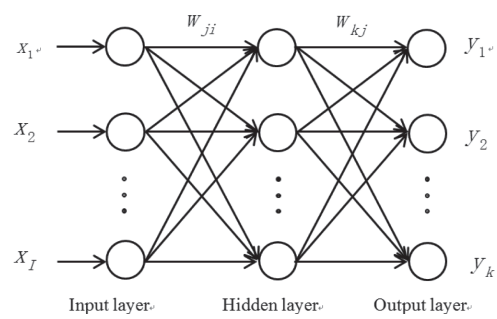


Figure 1. Three layer BP neural network.

by layer due to the weights and biases. The second step is backward computation, at which step the weights and biases are updated by reducing the error between the output value and the expected one. The process of training a network is the repetition of forward and backward computations (Dong & Watanabe 2008).

Taking a three-layer BP network model for example, the BP algorithm is described as follows. Appoint the input vector $X = \{x_1, x_2, x_3, \ldots, x_I\}$, the output vector $Y = \{y_1, y_2, y_3, \ldots, y_K\}$, and the hidden layer neuron number J.

For the input layer nodes i, its output is equal to $x_i (i = 1, 2, 3, \ldots, I)$. So the input and the output of the hidden layer nodes j are as follows:

$$s_j = \sum_{i=1}^{I} w_{ji} \cdot x_i - \theta_j \tag{1}$$

$$o_j = f(s_j) \tag{2}$$

where $j = 1, 2, \ldots, J$; s_j stands for the input of the hidden layer nodes j; o_j stands for the output of the hidden layer nodes j; w_{ji} stands for connection weight from the hidden layer to the input layer; θ_j stands for the threshold.

The input and output of the output layer nodes k are as follows:

$$h_k = \sum_{k=1}^{K} w_{kj} \cdot o_j - \theta_k \tag{3}$$

$$y_k = f(o_k) \tag{4}$$

where $k = 1, 2, \ldots, K$; h_k stands for the input of the output layer nodes k; y_k stands for the output of the output layer nodes k; w_{kj} stands for connection weight from the output layer to the hidden layer; θ_k stands for the threshold (Sun & An 2009).

2.2 *Application in fault diagnosis*

In the traditional fault diagnosis of circuits based on BP neural network, voltage data of key points which can be obviously affected by faults is usually taken as input information of the network. Generally, the output of the net is the codes of failure modes. After the data samples obtained from the simulation or fault injection experiments, training and testing can be carried out (Ma et al. 2013).

3 FAULT DIAGNOSIS METHOD

3.1 *Structure*

Considering the problems of traditional diagnosis method based on BP neural network put forward in INRODUCTION, this paper propose a new method of fault identification.

According to the experiment results, the occurrence of faults in circuits usually causes obvious temperature variation of the main chips. Though the variation speed is lower than that of voltage, it can be used for supplementary information to make results more accurate in fault diagnosis.

In this arithmetic, two BP neural networks are established, named net α and net β.

The input information of net α is the key voltage data of the circuit. Sometimes, for a better effect of classification the data ought to be processed in advance such as filtered or uniformized when necessary. As usual, the output of net α is the codes of failure modes, which indicate where the faults locate. Generally a code usually represents several failure modes, for the reason that there are always some failure types causing the same voltage change.

The temperature data of main chips can be obtained from temperature sensors. In spite of the influence of environment, the difference value of temperature between chips remains stable in rated working condition. Thus the difference between the temperature and the average value of chips in the circuits can be taken as a feature of working state. So the input of node i of net β is described as follows:

$$x_i = temp_i - \frac{\sum_{q=1}^{I} temp_q}{I} \tag{5}$$

where *temp* stands for the temperature value of the chip.

If the variation ranges differ greatly, the temperature values can be classified into groups according to the variation. At this time, the input data of net β is the difference between the temperature and the average of the group. Same with net α, the output of net β is the codes of fault modes.

Data samples obtained from the simulation or fault injection experiments ought to be divided into training and testing data set. After separate training and testing, make record of all the wrong identification results of net α. Then the final diagnosis result can be gained from the integration of net α and net β outputs, the arithmetic of which is proposed in the Section 3.2.

3.2 *Arithmetic of output integration*

Appoint the failure mode set represented by net α output codes is S_1, the set represented by net β output codes is S_2, and the set of the final diagnosis result is S. When a set is empty, it

means the circuit works normally with no faults happening.

As usual, the shortcomings that neural networks may present in fault diagnosis are described as follows:

– There are several failure types causing the same voltage change that the network cannot distinguish.
– The failure mode set C in fact is identified as set D.
– The normal working state is identified as failure mode set E by mistake.
– Failure mode set F cannot be identified when happening.

All the C, D, E, F sets can be recorded in the testing process. Appoint the C, D, E, F sets of net α are C_1, D_1, E_1, F_1 and those of net β are C_2, D_2, E_2, F_2. Then arithmetic of output integration is proposed as follows based on the logic:

– When S_1 is empty, if $S_2 = S_1$ or $S_2 \subseteq E_2$, then $S = S_1$, meaning that the circuit works normally. If $S_2 \subseteq F_1$, then $S = S_2$.
– When $S_1 \subseteq D_1$, if $S_2 = S_1$, then $S = S_1 = S_2$. If $S_2 \subseteq C_1$, then $S = C_1$.
– When $S_1 \subseteq E_1$, if $S_2 = S_1$, then $S = S_1 = S_2$. If S_2 is empty, then $S = S_2$.

Table 1. Output integration rule.

$S_1 = \phi$	$S_2 = \phi$	$S = \phi$
	$S_2 \subseteq E_2$	$S = \phi$
	$S_2 \subseteq F_1$	$S = S_2$
$S_1 \subseteq D_1$	$S_2 = S_1$	$S = S_1 = S_2$
	$S_2 \subseteq C_1$	$S = C_1$
$S_1 \subseteq E_1$	$S_2 = S_1$	$S = S_1 = S_2$
	$S_2 = \phi$	$S = S_2$
$S_1 \neq \phi$	$S_2 \neq \phi$	$S = S_1 \cap S_2$
$S_1 \not\subset (D_1 \cup E_1)$	$S_2 \not\subset (D_2 \cup E_2)$	

– When S_1, S_2 is not empty, $S_1 \not\subset (D_1 \cup E_1)$, and $S_2 \not\subset (D_2 \cup E_2)$, then $S = S_1 \cap S_2$.

As is shown is Table 1, the description above can be summarized.

4 APPLICATION

4.1 *Transformer circuit*

The fault diagnosis method is applied to a transformer circuit which is designed to alternate current of 28 V to 12 V, 5 V, and 0.9 V. Shown in Figure 2, the circuit consists of three main parts, the 12 V transforming and voltage-stabilizing circuits, the 5 V transforming and voltage-stabilizing circuits, and the 0.9 V transforming and voltage-stabilizing circuits, each of which also contains a temperature sensor circuit.

4.2 *Neural network establishing*

As is shown in Table 2, there are 9 main failure modes in this circuit. Due to the influence on the voltage, the faults are classified into 4 groups, in each of which net α cannot distinguish a failure mode from another. For convenience, these groups are coded from 001 to 100, which is the output of net α. In the same way, the modes are also grouped according to the influence on temperature in experiments.

Then construct net α. The data of three output voltage is taken as the input. For net β, the input is the difference value between the chip temperature and the average. The nodes of each network input layer, hidden layer and output layer are set as 3, 5 and 3. Overall system error is E = 0.001.

With the data acquisition system, 300 sets of samples are obtained. Then execute the training and testing. Record the results as Table 3.

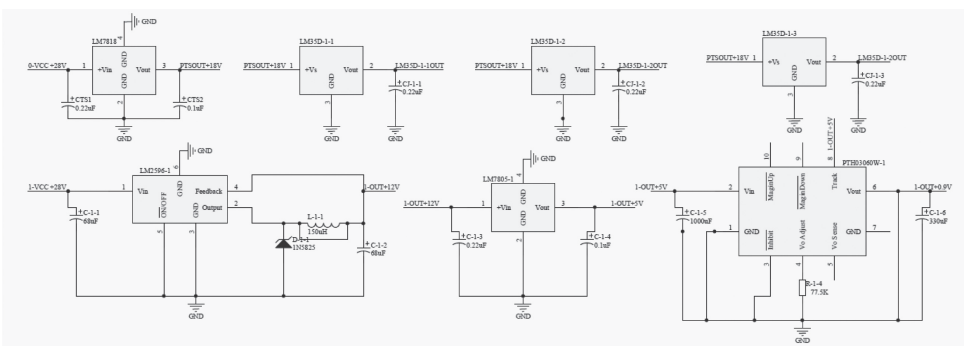


Figure 2. Transformer circuit.

Table 2. Failure modes.

	Failure mode	Group of net α	Group of net β
F1	Break of Pin1 of LM2596	001	001
F2	Break of Pin2 of LM2596	001	001
F3	Break of L-1-1	001	010
F4	Break of Pin1 of LM7805	010	010
F5	Break of Pin3 of LM7805	010	011
F6	Break of C-1-3	011	100
F7	Break of C-1-11	011	101
F8	Break of Pin2 of PTH003060W	011	110
F9	Break of Pin3 of PTH003060W	100	110

Table 3. Testing results.

	C	*D*	*E*	*F*
net α	F9	F5	F9	F6, F7, F8
net β	–	–	F3	F7

Table 4. Results of net α.

Failure	Output 1	Output 2	Output 3	T/F
F1	0.1025	0.0458	0.9267	T
F2	0.1029	0.1853	0.8739	T
F3	0.0754	0.2531	0.9062	T
F4	0.2076	0.8365	0.1431	T
F5	0.1622	0.9038	0.1437	T
F6	0.3015	0.3592	0.4066	F
F7	0.3927	0.3135	0.2740	F
F8	0.1952	0.3648	0.2193	F
F9	0.2450	0.7467	0.1921	F

Table 5. Results of net β.

Failure	Output 1	Output 2	Output 3
F1	0.1652	0.2644	0.8739
F2	0.2261	0.1732	0.7994
F3	0.1054	0.9376	0.2268
F4	0.0943	0.8792	0.2655
F5	0.1375	0.9121	0.8747
F6	0.8649	0.2032	0.1295
F7	0.1053	0.2476	0.2341
F8	0.8264	0.8753	0.1429
F9	0.9023	0.8937	0.1362

Carry out the experiments separately and make record of the neural network outputs when a fault happens, shown as Table 4 and Table 5. Then make a judgment of the correctness of net α results.

Table 6. Final diagnosis results.

	Results of net α	Results of new method
F1	F1, F2, F3	F1, F2
F2	F1, F2, F3	F1, F2
F3	F1, F2, F3	F3
F4	F4, F5	F4
F5	F4, F5	F5
F6	–	F6
F7	–	–
F8	–	F8, F9
F9	F5	F8, F9

After the calculation of output integration, we can get the final fault diagnosis results and make a comparison with the traditional diagnosis results, shown as Table 6.

From the comparison of the fault diagnosis results, it can be seen that the new method increases the fault identification rate from 44.4% to 88.9%, and makes the diagnosis result more accurate.

5 CONCLUSIONS

Based on BP neural network, a new method of fault diagnosis of circuits is proposed. According to the results of experiments, the problems which traditional diagnosis methods are faced with are solved with this method. With the increase of fault identification rate, this method enhances the efficiency of circuit fault diagnosis.

ACKNOWLEDGMENT

This research is supported in part by Major State Basic Research Development Program (61316705), Foundation Scientific Research Program (A2120110004), and Advanced Research Program (51319040301).

REFERENCES

Dong Y. & Watanabe T., 2008. Network on chip architecture for BP neural network. 2008 *International Conference on Communications, Circuits and Systems Proceedings*, ICCCAS 2008, 964–968.

Han X., Zheng Z., Tian N., Hou Y. 2009. Voltage Stability assessment based on BP Neural Network. 2009 *Asia-Pacific Power and Energy Engineering Conference*, APPEEC 2009—Proceedings.

Ma D., Liang Y., Zhao X., Guan R., Shi X., 2012. A method for searching and evaluating diagnosable sequence fault sets of a dependency matrix. *Proceedings of IEEE 2012 Prognostics and System Health Management Conference*, PHM-2012.

Shi J., Lin X., Lv K., 2012. A method for searching and evaluating diagnosable sequence fault sets of a dependency matrix. *Proceedings of IEEE 2012 Prognostics and System Health Management Conference*, PHM-2012.

Sun Y. & An Y., 2009. Research of fault diagnosis system for picking and cold-rolling electric device based on BP neural network. *ICTM 2009–2009 International Conference on Test and Measurement*, 161–164.

Xiang L., Yang Z., Shujuan W., Guofu Z., 2011. A method for analog circuits fault diagnosis by neural network and virtual instruments. *2011 3rd International Workshop on Intelligent Systems and Applications, ISA 2011—Proceedings.*

Yu J., Niu X., Han Y., Yu S. 2012. The fault diagnosis of transformer based on BP neural network. *Proceeding of 2012 International Conference on Information Management, Innovation Management and Industrial Engineering*, 487–489.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Physics of Failures (POF) version B for MTBF prediction

Y. Bot & J.B. Bernstein
BQR Reliability Engineering Ltd., Israel

ABSTRACT: In this article we will presents a method for predicting the failure rate, MTBF, and thus the reliability of an electronic system by summing the failure rates of each known failure mechanism, as specified in the JEDEC standard JEP-122G. We use a competing acceleration factor methodology by combining the physics of failure for each mechanism with their effects as observed by High/Low temperature and High/Low voltage stresses. Our new method assumes that lifetime of each of its failure mechanisms follows constant rate distribution and each mechanism is independently accelerated by the stress factors, which include also frequency, current, and other factors that can be entered into a reliability model. The overall failure rate also follows an exponential distribution and is described in the standard FIT (Failure unIT or Failure in Time). The method combines mathematical models for the known failure mechanism and solves them simultaneously at a multiplicity of accelerated life tests to find a consistent set of weighting factors for each mechanism. The result of solving the system of equations is a more accurate and a unique combination for each system model by proportional summation of each of the contributing failure mechanisms. This method is applied to board design using our established parameters based on the chip technology and to chip manufacturers by matching HTOL Data with the foundry's reliability models.

1 THE CHALLENGE

Modern chips are composed of tens or hundreds of millions and even billions of transistors. Hence, chip level reliability prediction methods are mostly statistical allowing a constant-rate assumption to be applied. Chip level reliability prediction tools, today, model the failure probability of the chips at the end of life, when the known wear-out mechanisms are expected to dominate. However, modern reliability tools do not predict the random, post burn-in, constant failure rate that would be seen in the field. All the current physics of failure solutions try to determine an average effect that can be represented by a single relation that gives an average value for the Mean Time Between Failures (MTBF), however this single relation can never reflect the true physics of multiple mechanisms.

Chip and packaged system reliability is measured by a FIT. The FIT is a rate, defined as the number of expected device failures per billion part hours. A FIT is assigned for each component multiplied by the number of devices in a system for an approximation of the expected system reliability, MTBF. The semiconductor industry provides an expected FIT for every product that is sold based on operation within the specified conditions of voltage, frequency, heat dissipation and etc. Hence, a system reliability model is a prediction of the expected for an entire system as the sum of the FIT rates for every component.

A FIT is defined in terms of an acceleration factor, A_F, as:

$$\mathrm{FIT} = \frac{\#\mathrm{failures}}{\#\mathrm{tested} \cdot \mathrm{hours} \cdot \mathrm{AF}} \cdot 10^9 \tag{1}$$

where #failures and #tested are the number of actual failures that occurred as a fraction of the total number of units subjected to an accelerated test. The acceleration factor, A_F, must be supplied by the manufacturer since only they know the failure mechanisms that are being accelerated in the High Temperature Operating Life (HTOL) and it is generally based on a company proprietary variant of the MIL-HDBK-217 approach for accelerated life testing. The true task of reliability modeling, therefore, is to choose an appropriate value for A_F based on the physics of the dominant failure mechanisms that would occur in the field for the device.

The acceleration of a single failure mechanism is a highly non-linear function of temperature and/or voltage. The temperature Acceleration Factor (AF_T) and voltage Acceleration Factor (AF_V) can be calculated separately and is the subject of most studies of reliability physics. The total acceleration factor of the different stress combinations will be the product of the acceleration factors of temperature and voltage,

$$AF = \lambda(T_2,V_2)/\lambda(T_1,V_1) = [\![AF]\!]_t * [\![AF]\!]_v = \exp[E_a/k(1/T_1 - 1/T_2)]\exp(\gamma_1(V_2 - V_1)) \tag{2}$$

This acceleration factor model is widely used as the industry standard for device qualification. However, it only approximates a single dielectric breakdown type of failure mechanism and does not correctly predict the acceleration of other mechanisms. The challenge to accurate reliability prediction is to incorporate multiple mechanisms into the calculation of MTBF.

1.1 *Multiple mechanism solution*

Our unique system makes the assumption of multiple failure mechanisms whereby each will be accelerated differently depending on the physics that is responsible for each mechanism. If an HTOL test is performed at an arbitrary voltage and temperature for acceleration based only on a single failure mechanism, then only that mechanism will be accelerated. In that instance, which is generally true for most devices, the reported FIT (especially one based on zero failures) will be meaningless with respect to other failure mechanisms. Thus, In order to make an accurate approximation to a true field failure rate, electronic devices should be considered to have several failure modes degrading simultaneously. Each mechanism 'competes' with the others to cause an eventual failure. When more than one mechanism exists in a system, then the relative acceleration of each one must be defined and averaged at the applied condition. Every potential failure mechanism should be identified and its unique AF should then be calculated for each mechanism at a given temperature and voltage so the FIT rate can be approximated for each mechanism separately. Then the final FIT will be the sum of the failure rates per mechanism, as is described by:

$$FIT_{total} = FIT_1 + FIT_2 + \ldots + FIT_i \quad (3)$$

whereby each mechanism leads to an expected failure unit per mechanism, FIT_i. Unfortunately again, individual failure mechanisms are not uniformly accelerated by a standard HTOL test, and the manufacturer is forced to model a single acceleration factor that cannot be combined with the known physics of failure models.

In order to address this fundamental limitation of qualifying the reliability with only a single mechanism model, we developed a special multiple-mechanism qualification approach that allows companies to tailor specifications to a variety of customer's needs.

Chip manufacturers can use our software to design a custom Multiple HTOL *(M-HTOL)* test that matches their results with the foundry's reliability models or with JEDEC models to make accurate MTBF calculations based on specific customer's environments including voltage, temperature and speed. The board manufacturers can use the data from our models based on multiple failure mechanisms to calculate the system MTBF based on the device technology.

1.2 *Benefits*

This approach fits the highly developed and sophisticated models of the foundry based on years of knowledge and testing of the physical failure mechanisms. These mechanisms are known inherently to lead to degradation and ultimately to a chip failure. Our approach puts this knowledge in the hands of the chip designers allowing for qualification at any expected operating conditions. This way, the same product may accommodate additional potential markets by selling the same design for higher reliability applications with broader operating margins or higher performance applications where long life is not as critical.

The traditional single-model HTOL gives an unrealistically low value for the expected FIT and customers invariably find that their application shows a much higher reported failure rate than what was provided by the supplier using the traditional approach. Our M-HTOL matrix methodology will give a more accurate prediction for the expected field failure rate that is based on actual test data and on the reliability models provided by the foundry to the chip designer. This way, the designer has a much more dependable picture for device reliability and the customer will be satisfied that his design will match their customer's expectations for performance life.

1.3 *Features the matrix method*

As part of processing the results, experimental results are collected into a database. Determine acceleration factors for the various failure mechanisms, a matrix is constructed based on the JEDEC standard and experimental results. The matrix is a forecasting tool that allows the supplier to determine the dominance of each failure mechanism and its relative contribution to the chance occurrence of a system failure. By solving a system of equations whose information can be obtained from the matrix, one can assess and even predict the acceleration time for the multiple causes of a component failure and thus can calculate the duration of the warranty and the exact lifetime of the component.

The basic method for solving the system of equations is based on the suggestion of a Sum-of-failure-rate method as described in JEDEC Standard JEP122G. It is clear that the manufacturers of

electronic components recognize the importance of combining failure mechanisms in a sum-of-failure-rates method. Also, the formula for each mechanism is well studied and published.

Hence, the standard system reliability FIT can be modeled using traditional MIL-handbook-217 type of algorithms and adapted to known system reliability tools, however, instead of treating each component as individuals, we propose treating each complex component as a series system of sub-components, each with its own reliability matrix.

1.4 *Workflow*

The workflow for solving MTBF using our Sum-Of-Failure-Rate Matrix is shown:

A failure mechanism matrix can be solved at any given set of conditions, i.e. voltage, temperature and frequency, as a percentage at each stressed operating condition, there is a unique proportion of each mechanism for a given set of stressed conditions that will result in the given time to fail.

In order to find a relative failure rate for each mechanism, we take the accelerated life test at various voltages and temperatures and extrapolate to an end-of-life time at each temperature and voltage condition. For each condition, a consistent failure criterion must be chosen and the times to reach that condition yield "Mean Time To Fail" (MTTF) for the given conditions of voltage and temperature. Since the formula for percentage degradation is given as $y = \ldots$ Thus, solving each formula for the time to fail gives the results for the extrapolated failure rate. The Acceleration Factors (AF) are the ratio of the longest time to fail divided by the extrapolated time to fail for the other conditions. Also, an absolute FIT value

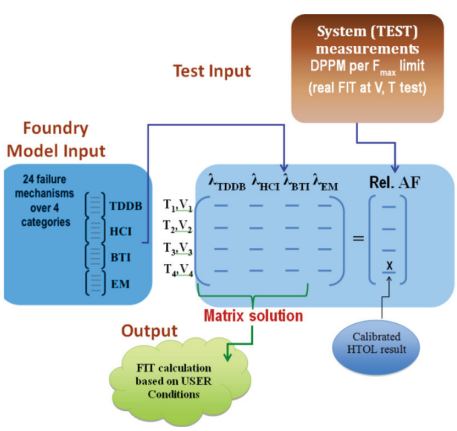
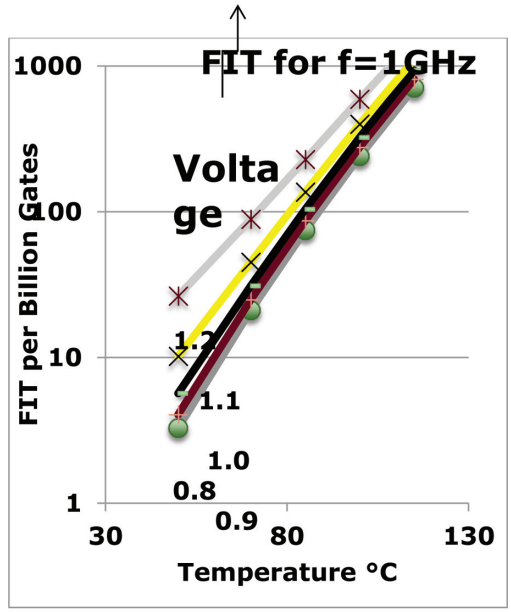
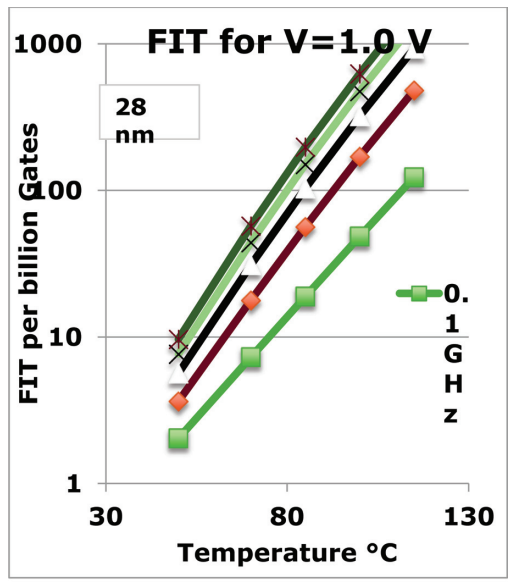


Figure 1. Workflow.



a) Voltage



b) Frequency

Figure 2. Extrapolated failure rate (FIT) versus temperature for different a) Voltage and b) Frequency.

is determined in the next row based on the Mean time to fail. This allows calibration of the final results in operation. The solution of this matrix gives us a relative importance for each mechanism and allows for failure rate prediction at any given voltage, frequency and temperature as seen below.

2 SUMMARY

We present here for the first time a simple and accurate way to combine the physics of failure equations for reliability prediction from accelerated life testing. We show that a matrix approach allows the reliability physics equations to be fit proportionally to the results of monitored accelerated life testing in order to extrapolate failure rate one would expect given actual operating parameters. This methodology can be extended to include radiation effects, frequency and even packaging and solder joint effects to give a complete system reliability evaluation framework.

This approach fits the highly developed and sophisticated models of the foundry based on years of knowledge and testing of the physical failure mechanisms. These mechanisms are known inherently to lead to degradation and ultimately to a chip failure. Our approach puts this knowledge in the hands of the chip designers allowing for qualification at any expected operating conditions. This way, the same product may accommodate additional potential markets by selling the same design for higher reliability applications with broader operating margins or higher performance applications where long life is not as critical.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An adaptive fault detection threshold hardware circuit design to reduce False Alarms

Y. Cui, J. Shi, L. Chen, K. Liu & W. An
School of Reliability and System Engineering, Beihang University, Beijing, China

ABSTRACT: Built-In Tests (BITs), responsible for detecting and isolating faults, are widely used in mechanical and electronic products to improve reliability and testability. However, the False Alarm (FA) phenomenon greatly reduces the BIT accuracy and credibility, which becomes one of the most troublesome problem in BIT applications. Compared with the single-threshold fault detection method, an adaptive and automatically adjustable threshold for determining the current state would better to reduce false alarms. In this paper, an adaptive fault detection threshold hardware circuit is designed and tested. The concept of the adaptive fault detection threshold strategy is introduced at the beginning. The outlines and details of circuit design implementations are also discussed, including the function requirements, input/output specifications, and implementation tools. Finally, a hardware BIT circuit board monitoring a typical fault mode is made out, and a performance analysis of the hardware design is carried out.

1 INTRODUCTION

Built-In Tests (BITs) are widely used in mechanical and electronic systems to find whether system faults occur (Malcolm 1982, Jager 1984), aiming at reducing the time of fault detection, raising system availability and reliability (Steininger 2000). However, the false alarms phenomenon is always a troublesome problem in BIT applications: a BIT can make a noise when a fault does not occur, resulting in extra detachments and inspections (Anderson & Laskey 1988, Westervelt 2004, Khan et al. 2014). The operators may lose heart towards the unreliable indications, or feel disturbed and annoyed towards the nuisance alarms (Adnan et al. 2011).

One of the major causes of false alarms is the operating condition factors or environment changes (Allen 2003, Byington 2010). A BIT using a single fixed threshold is more apt to be entangled with false alarms (Qi et al. 2008). For an open fault, the basic detection and judgment rules are: when the monitoring voltage is higher or equal to the fixed threshold, the BIT will remain silent. When the monitoring voltage declines and cross below the fixed threshold, the BIT will give an alarm.

However, the operating condition of a product is uncertain and unsteady. A voltage deviation is common for a product in the normal operating stage, but the voltage at some time points may be lower than the threshold and causes the BIT actions (Westervelt 2002). In this case, there is actually no faults, and a fixed BIT threshold would not be so satisfactory. Some researchers proposed the concept of adaptive threshold to reduce false alarms (Balaban & Simpson 1983, Simpson & Agre 1983). However, only the concept of adaptive threshold are discussed in these papers. It remains to be seen how to determine the value of the threshold, as well as the adaptive BIT can solve what kinds of problems. At the same time, the current researches focused much less on the hardware implementations of the adaptive threshold BITs than the BIT design concept.

The major contribution of this paper is to propose a designing method of an adaptive threshold BIT that can accommodate to operation condition changes, which is seldom considered in pervious works. The adaptive BIT aims at identifying real hard faults from environmental changes, and thus reduce false alarm rate. To achieve this, the hardware designing approach of capturing signal changing speed is presented to distinguish an environmental change from a hard fault. The BIT can automatically adjust its threshold following the direction of the signals under test.

The remainder of this paper mainly focuses on the fault detection model of the electronic products containing instant faults (i.e. hard faults), and take the environmental changes and external stresses into consideration. The fault and false alarm model is introduced and a type of BIT circuit adopting an adaptive threshold is developed. The hardware implementations are discussed in this paper according to the designing requirements, and a printed circuit board is also made for test and verification.

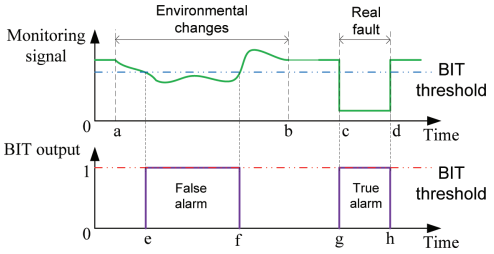


Figure 1. False alarm profile.

2 FALSE ALARM PROFILE

This part we mainly consider the faults and false alarm phenomenon of electronic product experiencing environmental changes or sustaining external stresses. For electronic products, the typical hard faults like open faults or short faults are all instant faults, i.e. hard faults (Fenton et al. 2001, Weglarz & Saluja 2004). The fault occurs suddenly, and the duration of fault development can be regarded as zero.

The operating environment of the electronic product may have an effect on the output signal monitored by a BIT. For one thing, the parameter drifts caused by temperature or humidity changes are very common for electronic products. For another, some external stresses (e.g. vibration) can indirectly reflected on the monitoring signal. These variations of the monitoring signal do not necessarily mean a fault occurs, yet the BIT would not recognize it and declares a fault. Compared with a hard fault, the effect of the environmental changes or the external stress is relatively slow.

A false alarm profile records the monitoring signal and false alarm conditions during a period of time. Figure 1 gives an example of a BIT using a single fixed threshold for fault detection. In Figure 1(a), the operating environment begin to change before at t = a, leading down the voltage of the monitoring signal. At t = e when the voltage begin to be lower than the threshold, the BIT misunderstands this and false alarm happens. With the revocation of the environmental changes, the voltage climes up and the BIT stops alarming at t = f. At t = c, a hard fault (e.g. open fault) really happened, and the BIT gives a correct indication. The false alarm coverage rate is dependent on the false alarm profile.

3 SYSTEM-LEVEL DESIGN

3.1 *Designing principles*

From Figure 1, we can see that the BIT using a single fixed threshold is not a good choice when the operating condition of the electronic product is not very optimistic. To solve the problem, we proposed the approaches of adopting adaptive detection threshold.

The designing principles are as follows. If an environmental change or external stress is identified, the BIT threshold will change following the direction of the original monitoring signal. This means when the monitoring signal climbs up, the BIT threshold will also rise; when the monitoring signal goes down, the BIT threshold will correspondingly decline. The reaction volume of the BIT threshold follows a direct proportion relationship. In our research, the direct ratio is set to be 0.5. However, when a hard fault (open or short) is identified, the threshold will remain the same, and the BIT should detect the fault.

3.2 *System structure*

The system structure of the BIT circuit is shown in Figure 2. The names and functions of the modules are listed below.

- Signal Variation Detection Module (SVDM), which detects the changing speed of the monitoring signal.
- Comparison Module (CM), which compares the changing speed. If the speed is lower than the predetermined value, then an environmental change or external stress is identified and CM outputs "1". On the contrary, if the speed is higher than the predetermined value, then a hard fault is identified and CM outputs "0".
- Gating Module (GM), which controls signals to pass through. When CM outputs "1", the SVDM output will be selected and pass through. Otherwise, the SVDM output is blocked.
- Threshold Difference Construction Module (TDCM), which makes compensations for the monitoring signal variations. In other words, TDCM is responsible for generating a reaction volume of the BIT threshold following a direct proportion relationship.

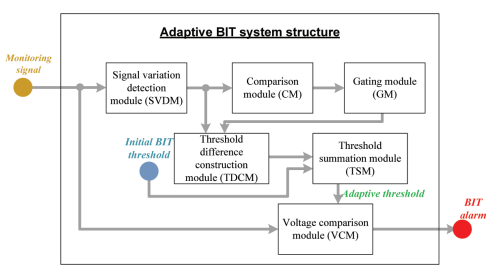


Figure 2. System structure of adaptive BIT circuit design.

– Threshold Summation Module (TSM), which adds the threshold difference on the original threshold to construct new adaptive threshold.
– Voltage Comparison Module (VCM), which executes the BIT voltage comparison function to give an alarm that indicates a fault.

4 HARDWARE IMPLEMENTATIONS

4.1 *Signal Variation Detection Module (SVDM)*

In order to capture the speed change of the monitoring signal, we use the differentiation circuit carried out with the aid of LM324 op amps. A capacitor is used at the input connection. A typical integration circuit using an op amp is placed as the feedback loop of the main op amp. For this application, a positive differentiation of the monitoring signal can be obtained. A low pass filter composed of a capacitor and a resistance is attached at the end of this module to avoid undesired peaks. The schematic diagram of Signal Variation Detection Module (SVDM) is shown in Figure 3.

4.2 *Comparison Module (CM)*

We compare the output of SVDM with a preset determination value. If the absolute value of the former is below the latter, then the comparison module outputs a digital high level "1"; otherwise a digital low level "0". The function of the module is achieved by using two voltage comparators in a LM339 chip. The first one is responsible for restricting the upper bound, and the second is responsible for restricting the lower bound. With the pull-up resistors linked to a +5V voltage, the outputs of the LM339 chip can either be about 5V or 0V, which can be recognized as the digital high level "1" or the digital low level "0". The schematic diagram of Comparison Module (CM) is shown in Figure 4.

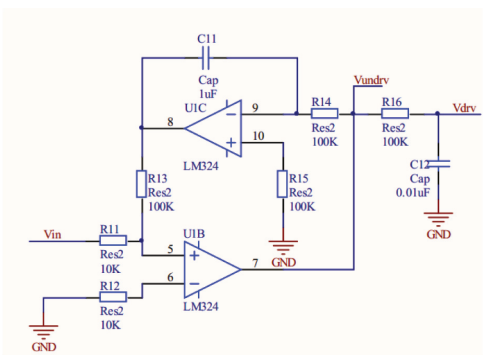


Figure 3. Schematic diagram of Signal Variation Detection Module (SVDM).

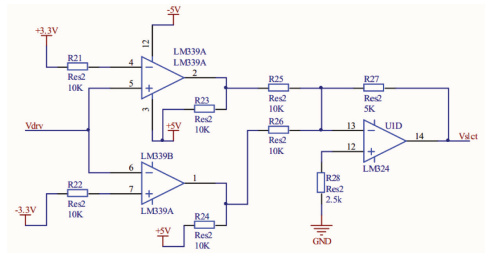


Figure 4. Schematic diagram of Comparison Module (CM).

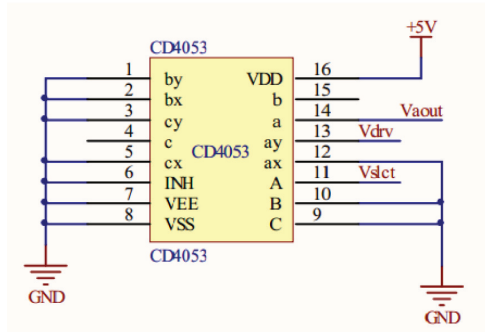


Figure 5. Schematic diagram of Gating Module (GM).

4.3 *Gating Module (GM)*

In this BIT circuit, we use a CD4053 Triple 2-channel analog multiplexer to serve as the gating module. The analog multiplexers in the chip are digitally controlled analog switches. CD4053 has three separate digital inputs A, B and C. We only use switch a and ax, ay for convenience. The analog ground and the digital ground are all set to be 0V. The connections of the chip are determined according to the truth table. The schematic diagram of Gating Module (GM) is shown in Figure 5. Together with CM, the theoretical comparison and gating model is illustrated in Figure 6.

4.4 *Threshold Difference Construction Module (TDCM)*

This module is responsible for constructing a threshold difference that follows the variation direction/volume of the monitoring signal. This is actually the complementary function to differentiation, and can be carried out by an integration circuit with the aid of an op amp. The current in the feedback loop charges the capacitor, which provides a negative integration value of the input signal. It is noted that a switch is added in parallel with the capacitor.

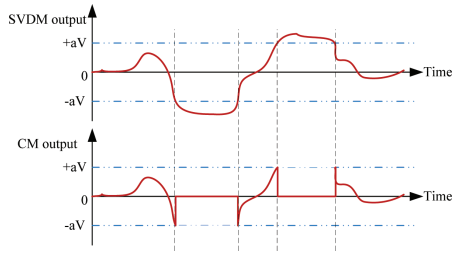


Figure 6. Theoretical comparison model.

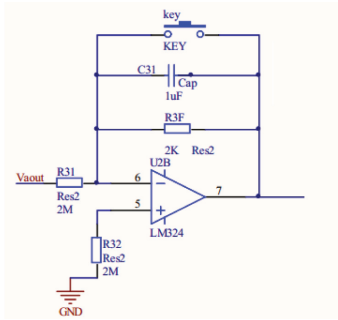


Figure 7. Schematic diagram of Threshold Difference Construction Module (TDCM).

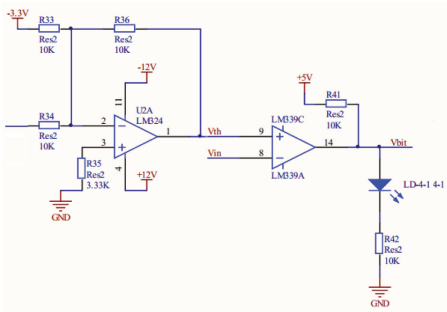


Figure 8. Schematic diagram of Threshold Difference Construction Module (TDCM) and Voltage Comparison Module (VCM).

Before the BIT works, it is required to press the switch button and discharges the capacitor to make sure that the integral initial value is 0. The schematic diagram of Threshold Difference Construction Module (TDCM) is shown in Figure 7.

4.5 *Threshold Summation Module (TSM) & Voltage Comparison Module (VCM)*

The adaptive threshold of the current BIT circuit is gained by the summation of a preset fixed threshold and the threshold difference generated by TDCM. The function is achieved by a simple oppositional op amp summation circuit. The new threshold is then brought to the BIT Voltage Comparison Module (VCM). The original monitoring signal is compared against the adaptive threshold, as an accomplishment of the BIT fault detection process. The schematic diagram of Threshold Difference Construction Module (TDCM) and Voltage Comparison Module (VCM) is shown in Figure 8.

5 EXPERIMENTAL RESULTS

In order to verify the effectiveness of the circuit design, we draw the circuit diagrams in Altium Designer software and make out the physical PCB hardware circuit, as is shown in Figure 9. The circuit has two input choices. The first one is CON1 Input, which is directly linked to the real monitoring signal. The second choice is a simulative fault injection part, in which a 5KΩ variable resistance serves as the external stress controlling unit, and a detachable connection pin serves as the hard fault injector. Critical test signals of the circuit are collected and recorded by the data acquisition computer.

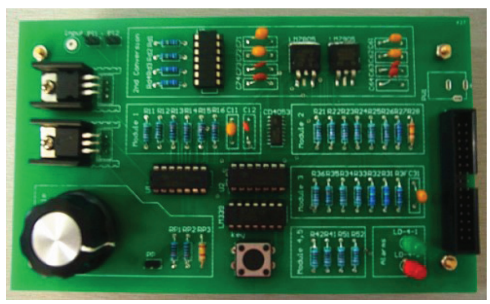


Figure 9. Physical circuit board.

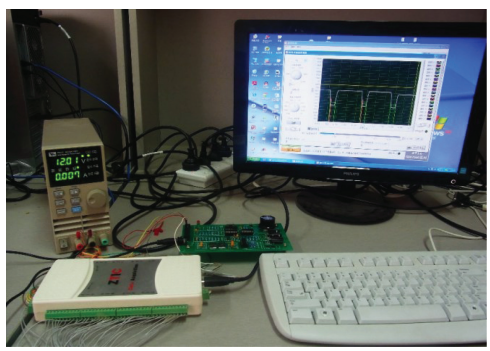
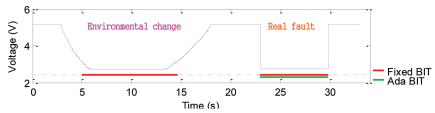
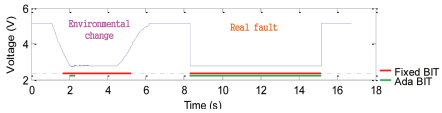
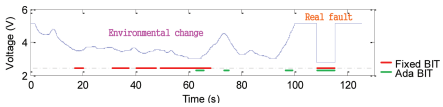


Figure 10. Data acquisition experiment environment.

Table 1. BIT performances under different false alarm profiles.

No.	False alarm profile	FACR of Ada BIT	FACR of fixed BIT	Reduction rate
1		0.00%	56.03%	100%
2		5.01%	33.20%	84.93%
3		47.70%	88.77%	49.64%

The traditional BIT using a single and fixed threshold is also installed for performance comparisons.

Several experiments are conducted with the BIT PCB and the results are analyzed. The data acquisition experiment environment is shown in Figure 10. The fixed BIT threshold is determined to be 3.3V, and an open fault is to be injected in the circuit. Table 1 lists several false alarm profiles, and the False Alarm Coverage Rates (FACR) of the BIT using the adaptive threshold and that using the single threshold are also given in Table 1, respectively.

It can be seen from Table 1 that the average false alarm coverage rates of BITs using the adaptive threshold are obviously lower than BITs using the single threshold. When the environmental changes are mild, the false alarm phenomenon can be fully eliminated, as is the case in Profile 1. When the environmental changes are relatively rapid and dramatic, the adaptive BIT has some false alarms, yet the FACR is much less than traditional fixed BIT, as is the case in Profile 2 and 3. The false alarm coverage rate for the former is about 1/6 and 1/2 of the latter in Profile 2, Profile 3, respectively. The results reveal that the adaptive threshold BIT really has an advantage over the fixed BIT concerning the false alarm phenomenon.

6 CONCLUSIONS

This paper introduces a designing concept of adaptive detection threshold for a Built-In Test (BIT).

The background knowledge and working principles are discussed. The circuit design implementations are also presented in this paper. A hardware BIT circuit board monitoring a typical fault mode is manufactured. Finally, the experimental analysis show that the BIT using adaptive detection threshold has a much lower false alarm coverage rate than the tradition BIT adopting a single fixed threshold. A major contribution is that the concept of adaptive BIT threshold is implemented in a hardware design corresponding to the fault model. Although a hardware design is feasible, the adaptive threshold concept can sufficiently be realized by a software BIT design, which will not add additional weight on the whole product to reduce weight and raise robustness.

ACKNOWLEDGEMENT

The authors express sincere appreciation to the editor and reviewers for their efforts to improve this paper. The work is under the sponsorship of Science and Technology on Reliability and Environmental Engineering Laboratory, Beihang University. This work is also supported by fund projects 61316705, 51319040301 and Z132014B002.

REFERENCES

Adnan N.A., Izadi I., Chen T., 2011. On expected detection delays for alarm systems with deadbands and delay-timers, Journal of Process Control, vol. 21, pp. 1318–1331.

Allen D., 2003. Probabilities associated with a built-in-test system, focus on false alarms. In AUTOTESTCON 2003. IEEE Systems Readiness Technology Conference. Proceedings IEEE, pp. 643–645.

Anderson J.M., Laskey J.M., 1988. The enemy is FA, CND, and RTOK [avionics testing], in AUTOTESTCON '88. IEEE International Automatic Testing Conference, Futuretest. Symposium Proceedings, pp. 185–189.

Balaban H.S., Simpson W.R., 1983. Testability/Fault Isolation by Adaptive Strategy. Proceedings Annual R&M Symposium, pp. 344–350.

Byington C.S., Watson M.J., Amin S., Begin M., 2008. False alarm mitigation of vibration diagnostic systems. In Aerospace Conference, 2008 IEEE, pp. 1–11.

Fenton W.G., McGinnity T.M., Maguire L., 2001. Fault diagnosis of electronic systems using intelligent techniques: A review. IEEE Transactions on Systems Man, and Cybernetics—Part c: Applications and Reviews, vol. 31, pp. 269–281.

Jager R., 1984. A Systematic Approach to Designing for Testability. Proceedings Annual R & M Symposium.

Khan S., Phillips P., Hockley C., Jennions I., 2014. No Fault Found events in maintenance engineering Part 2: Root causes, technical developments and future research, Reliability Engineering & System Safety, pp. 196–208.

Malcolm J.G. 1982. BIT False Alarm: An Important Factor in Operational Readiness. Proceeding Annual R & M Symposium, pp. 206–212.

Qi H., Ganesan S., Pecht M., 2008. No-fault-found and intermit-tent failures in electronic products, Microelectronics Reliability, vol. 48, pp. 663–674.

Simpson W.R., Agre J.R. 1983. Adaptive Fault Isolation with Learning. AUTOTESTCON, pp. 331–335.

Steininger A., 2000. Testing and built-in self-test—A survey, Journal of Systems Architecture, vol. 46, pp. 721–747.

Weglarz E.F., Saluja K.K., Mak T.M., 2004. Testing of hard faults in simultaneous multi-threaded processors. In On-Line Testing Symposium, 2004. Proceedings. 10th IEEE International, pp. 95–100.

Westervelt K., 2002. F/A-18D (RC) built-in-test false alarms. In Aerospace Conference Proceedings, Vol. 6, pp. 2961–2970.

Westervelt K., 2004. Root cause analysis of bit false alarms. In Aerospace Conference, 2004. Proceedings IEEE, pp. 3782–3790.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

MUSTADEPT: A tool for the analysis of industrial equipment degradation

M. Compare & L. Legnani
Aramis Srl, Milan, Italy

E. Zio
Politecnico di Milano, Milan, Italy
Ecole Centrale Paris and Supelec, Paris, France
Aramis Srl, Milan, Italy

ABSTRACT: This paper illustrates the main features of the MUlti-STAte DEgradation Process analysis Tool (MUSTADEPT), a new software tool which allows quantitatively describing the evolution of the degradation process of an industrial equipment, modeled as a discrete-state transport process. Two different, complementary approaches are offered. One is based on statistics, specifically the Maximum Likelihood Estimation (MLE) technique to estimate the parameters of the degradation process model and the Fisher Information Matrix for evaluating the uncertainty associated to the estimates. The other approach relies on information elicited from experts and describes and propagates the associated uncertainty within the DSTE framework. In both cases, the probabilities that the component occupies the different degradation states over time are estimated with the associated uncertainties.

1 INTRODUCTION

The degradation mechanisms affecting industrial systems, structures and components (SSCs) can be modeled as discrete-state transport processes (e.g., Baraldi et al., 2013 a and b; Moghaddas & Zuo, 2011). The stochastic transitions between the states obey known models (e.g., Weibull distribution, exponential distribution, etc.), whose parameters (e.g., the scale and shape factors for the Weibull distribution, the failure rate for the exponential distribution, etc.) need to be estimated. Degradation models are used in support to maintenance decision making, for example to optimize the inspection period in a preventive maintenance approach or to estimate the remaining useful life of a SSC in a predictive maintenance approach (Zio & Compare, 2013).

In this context, MUSTADEPT has been developed to characterize and describe the evolution of the degradation processes affecting industrial SSCs, modeled as discrete-state transport processes. In particular, the following assumptions are made:

- There are 4 degradation states, which are identified by the maintenance operators on the basis of the associated symptoms;
- Transitions can occur from one degradation state to the next degraded state, only;
- The stochastic transition models are supposed to be known, for example on the basis of mathematical/physical considerations.
- At least one out of the following two sources of information is available:
  1. A dataset containing, for every SSC, the degradation state in which it has been found at inspection and the corresponding inspection time. This means that the available data must be interpreted as left censored test data (i.e., interval censored data, with the initial time set to 0, Zio, 2007).
  2. A number of experts with different skills and competences, who can provide the intervals in which they suppose the true values of the uncertain parameters are contained.

In these conditions, MUSTADEPT allows exploiting the available information to evaluate the probabilities that the SSC will occupy the different degradation states over time.

Two different, complementary approaches are offered:

1. 'Statistical', which exploits the available dataset containing left censored data to estimate the parameters of the stochastic transitions between the degradation states, and the associated uncertainties.
2. 'DSTE'. This approach allows integrating field data and expert knowledge for estimating the parameters of the stochastic laws of degradation, and propagating the associated uncertainty. The methodology used in MUSTADEPT is based on the DSTE (Baraldi et al., 2013 a; Baraldi et al., 2012; Dempster, 1967; Helton et al., 2004).

The rest of the paper is organized as follows. Sections 2 illustrates an example of industrial case study where the application of MUSTA-DEPT is shown to bring an added value. Section 3 focuses on the statistical approach: some theoretical bases are given, the main features of the approach described, and the results provided are discussed. Section 4, illustrates the features of the DSTE-based approach, and its outputs. The theoretical background of this latter approach has been already presented by the authors (Baraldi et al., 2013 a and b), and, thus, is not reported in this work. Section 5 concludes the paper.

2 CASE STUDY

The illustrative case study concerns the crack growth degradation mechanism of a mechanical component subject to cyclic load, which is typically modeled as a four-state degradation process (Fig. 1, Grall et al., 2007):

- Good state: crack incubation; it is the short initial phase of the phenomenon, which is connected with plastic strains locally occurring in the most stressed parts of the mechanical component subject to cyclic loads. At this stage, coalescence of dislocations and vacancies, as well as ruptures due to local stresses lead to the formation of sub-micro-cracks in the slip bands at the boundaries of blocks, grains and twins.
- Light State: crack initiation; it is characterized by the growth and coalescence of the sub-micro-cracks, which transform into micro-cracks; these start increasing under the cyclic loads, and form macro-cracks, which are typically detectable by measurement instrumentation.
- Medium State: crack rapid-propagation; the crack grows under cyclic loads, up to a critical threshold.
- Heavy State: the failure state; the crack length is above the acceptable threshold.

The presence of four steps requires characterizing the statistical behavior of three stochastic processes:

- Degradation from Good state to Light degradation state;
- Degradation from Light state to Medium degradation state;
- Degradation from Medium state to Heavy degradation state;

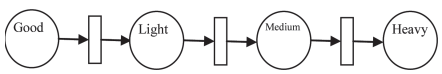


Figure 1. Scheme of the degradation mechanism.

For brevity, the degradation states will be indicated by S_k, $k = 1, \ldots, 4$, whereas the transition times from state S_k to state S_{k+1} by T_k, $k = 1, 2, 3$.

A further assumption is that the transition from any degradation state towards its next more degraded state obeys a Weibull or Log-normal distribution. In this respect, the Weibull distribution is often considered to describe the evolution of ageing processes (e.g., Moghaddas & Zuo, 2011) and in particular of fatigue processes (Baraldi et al., 2013). The Cumulative Distribution Function (CDF) of the transition time T_k, $k = 1, 2, 3$, reads:

$$F_{T_k}(t \mid \alpha_k, \beta_k) = 1 - e^{-\left(\frac{t}{\beta_k}\right)^{\alpha_k}} \quad (1)$$

where α_k and β_k are the shape and scale factors, respectively.

Also the Log-normal distribution is often considered to model the stochastic behavior of the transitions of the fatigue degradation process (e.g., Ray et al., 1998). The CDF of Log-normally distributed transition times T_k, $k = 1, 2, 3$ is:

$$F_{T_k}(t \mid \mu_k, \sigma_k) = \Phi\left(\frac{ln(t) - \mu_k}{\sigma_k}\right) \quad (2)$$

where μ_k and σ_k are the mean and the standard deviation, respectively, of the standard normal distribution, whose CDF Φ is defined as:

$$\Phi(t) = \left(\frac{1}{\sqrt{2\pi}}\right)\int_{-\infty}^{t} e^{-z^2/2dz} \quad (3)$$

3 STATISTICAL APPROACH

3.1 *Main concept*

The statistical approach analyzes the degradation mechanisms affecting industrial SSCs by exploiting the information contained in a database of outcomes of maintenance inspections. In details, the available dataset consists of $N \geq 1$ records containing:

- The ID;
- The inspection time;
- The degradation state of the component;
- The time at which the observation started, to give due account to the left censored data;
- In some cases, a number n of SSCs may be installed on the same system (i.e., the SSCs have the same ID). For example, every turbine (system) has a given number of nozzles (SSC), affected by the crack growth degradation process; then, a record in the dataset may also refer to a system with n SSCs: in this case, the record

contains the numbers n_k of SSCs found in state S_k, $k = 1, \ldots, 4$, where $n = \sum_{k=1}^{4} n_k$.

The procedure implemented in MUSTADEPT to exploit the maintenance inspection records uses the MLE technique to estimate the stochastic transition parameters, and a bootstrap-based technique to estimate the Fisher Information Matrix, which allows evaluating the uncertainty in the MLE values.

3.2 *Theoretical issues*

The parameter estimation problem tackled by MUSTADEPT consists in inferring the values $(\theta_{k1}, \theta_{k2})$ of the transition time T_k from state S_k to state S_{k+1}, for $k = 1, 2, 3$. The model parameters are arranged in the vector $\theta = (\theta_{11}, \theta_{12}, \theta_{21}, \theta_{22}, \theta_{31}, \theta_{32})$. In particular, we have $\theta_{k1} = \alpha_k$, and $\theta_{k2} = \beta_k$ in the Weibull case, whereas $\theta_{k1} = \mu_k$, and $\theta_{k2} = \sigma_k$ in the Log-normal case.

To find the MLE of θ, we need determining the analytical expression of the Likelihood function $L(T; \theta)$, where T is the vector containing the three stochastic transition times T_k, $k = 1, 2, 3$, we are interested in.

To this aim, we first compute the probabilities P_k^i of finding the component in state S_k at inspection time t_i, $k = 1, \ldots, 4$ (number of states), $i = 1, \ldots, N$ (number of records in the dataset). Namely, P_1^i is the probability of finding the component in state S_1 at inspection time t_i, which reads:

$$P_1^i = R_{T_1}(t_i; \theta_{11}, \theta_{12}) \tag{4}$$

where $R_{T_1}(t; \theta_{11}, \theta_{12})$ is the Complementary Cumulative Distribution Function (CCDF) of the transition time T_1 from state Good to state Light.

The probability P_2^i is given by:

$$P_2^i = \int_0^{t_i} f_{T_1}(\tau; \theta_{11}, \theta_{12}) R_{T_2}(t_i - \tau; \theta_{21}, \theta_{22}) d\tau \tag{5}$$

where $f_{T_1}(t; \theta_{11}, \theta_{12})$ is the probability distribution function (pdf) of T_1, whereas $R_{T_2}(t; \theta_{21}, \theta_{22})$ is the CCDF of the transition time T_2 from state Light to state Medium.

The probability P_3^i reads:

$$P_3^i = \int_0^{t_i} f_{T_1}(\tau_1; \theta_{11}, \theta_{12}) \int_{\tau_1}^{t_i} f_{T_2}(\tau_2 - \tau_1; \theta_{21}, \theta_{22}) R_{T_3}(t_i - \tau_2; \theta_{31}, \theta_{32}) d\tau_2 d\tau_1 \tag{6}$$

where $f_{T_2}(t; \theta_{21}, \theta_{22})$ represents the pdf of T_2, whereas $R_{T_3}(t; \theta_{31}, \theta_{32})$ is the CCDF of the transition time T_3 from state Medium to state Heavy.

Finally, the probability P_4^i of finding the component in state Heavy at inspection at time t_i is computed as:

$$P_4^i = 1 - P_1^i - P_2^i - P_3^i \tag{7}$$

The Likelihood function is a multinomial distribution, which reads:

$$L(T; \theta) = \prod_{i=1}^{N} \frac{n!}{n_1^i! n_2^i! n_3^i! (1 - n_1^i - n_2^i - n_3^i)!} \cdot P_1^{i\,n_1^i} P_2^{i\,n_2^i} P_3^{i\,n_3^i} (1 - P_1^i - P_2^i - P_3^i)^{n - n_1^i - n_2^i - n_3^i} \tag{8}$$

where

- n_k^i represents the number of SSCs in state k at time t_i, $k = 1, 2, 3$
- n is the total number of SSCs for every system.

MUSTADEPT utilizes optimization algorithms available in Matlab to find the maximum of the Log-likelihood function log $(L(T; \theta))$, as detailed in Section 3.3.3.

To estimate the uncertainty in the ML estimate, MUSTADEPT exploits the asymptotic properties of the ML estimator (Papoulis & Pillai, 2002). That is, if $\hat{\theta} = (\hat{\theta}_1, \ldots, \hat{\theta}_M)$ is a unique solution to the maximization problem of $L(T; \theta)$, then:

i. $E(\hat{\theta}) \to \theta$
ii. $\hat{\sigma}_{\hat{\theta}} = (\hat{\sigma}_{\hat{\theta}_1}, \ldots, \hat{\sigma}_{\hat{\theta}_M}) \to (\hat{\sigma}_{\hat{\theta}_1}, \ldots, \hat{\sigma}_{\hat{\theta}_M})_{CR}$ where $(\hat{\sigma}_{\hat{\theta}_1}, \ldots, \hat{\sigma}_{\hat{\theta}_M})_{CR}$ is the Cramer-Rao lower bound (Papoulis & Pillai, 2002) of the standard deviations of any unbiased estimator of θ. That is, any choice of an unbiased estimator of θ brings a variability in $\hat{\theta}_m$ necessarily larger than $\hat{\sigma}_{\hat{\theta}_{m\,CR}}$, $\forall m = 1, \ldots, M$.
iii. $\hat{\theta}$ is asymptotically normal.

Approximated values of the variances $\hat{\sigma}_{\hat{\theta}} = (\hat{\sigma}_{\hat{\theta}_1}, \ldots, \hat{\sigma}_{\hat{\theta}_M})$ of the parameters $\hat{\theta}_m$ of $\hat{\theta}$, are provided by the main diagonal of the estimated covariance matrix. This is defined the inverse $F(\theta)^{-1}$ of the expected Fisher information matrix $F(\theta)$, whose generic (r, j) entry, for any (r, j) and $j = 1, \ldots, M$ is:

$$F_{rj} = E\left[\frac{\partial log L(T; \theta)}{\partial \vartheta_r} \cdot \frac{\partial log L(T; \theta)}{\partial \vartheta_j} \right] \tag{9}$$

Under mild regularity conditions, the covariance matrix we are interested in is equal to:

$$\begin{pmatrix} -E\left[\frac{\partial^2 log L(T;\theta)}{\partial \vartheta_1^2}\right] & \cdots & -E\left[\frac{\partial^2 log L(T;\theta)}{\partial \vartheta_1 \partial \vartheta_M}\right] \\ \vdots & \ddots & \vdots \\ -E\left[\frac{\partial^2 log L(T;\theta)}{\partial \vartheta_M \partial \vartheta_1}\right] & \cdots & -E\left[\frac{\partial^2 log L(T;\theta)}{\partial \vartheta_M^2}\right] \end{pmatrix}^{-1} \tag{10}$$

In particular, these second derivatives can be interpreted as measures of how quickly the pdfs change when we change the parameters in the closeness of the MLE estimation. The expectations of the square of these values give us a more robust version of the measure. In turn, if Fisher information is large, then the distributions change quickly when we move far from the MLE value of the parameters. This entails that we should be able to properly estimate $\hat{\theta}$ based on the data. On the other hand, if Fisher information is small, this means that the distributions corresponding to $\theta = \hat{\theta}$ are 'very similar' to those with parameter values not so close to $\hat{\theta}$ and, thus, more difficult to distinguish: then, our estimation would be worse.

To estimate $F(\theta)$, MUSTADEPT resorts to a bootstrap-based approach proposed in (Spall 2009), which is useful when analytical methods for computing $F(\theta)$ are infeasible.

The essence of the method is to produce a large number of Simultaneous Perturbation (SP) estimates of the hessian matrix (i.e., the matrix of the second derivatives) of $logL(T; \theta)$, and, then, average the negative of these estimates to obtain an approximation to $F(\theta)$.

In details, the algorithm consists of the following steps:

Step 0. (Initialization). Set the number S of pseudo-data vectors that will be generated, and inizialize $s = 1$.

Step 1. (Generating pseudo-data). Based on the ML Estimate $\hat{\theta}$, generate the s-th pseudo-dataset Z_{pseudo} (s) of N records. That is, to produce the SP hessian estimates, we implement the following procedure to generate a dataset similar to the original:

1. Set $i = 1$.
2. Consider the inspection time of the i-th record in the available dataset.
3. Simulate the histories of the n SSCs in the i-th record, assuming that the parameters of the stochastic process take their ML estimates θ.
4. Store the outcomes.
5. $i = i+1$.
6. Repeat steps 2–4 until $i > N$.

Step 2. (Hessian estimation): With the s-th pseudo-data vector in Step 1, compute the Γ Hessian estimates H_γ, $\gamma = 1, \ldots, \Gamma$.

To do this, we first build the perturbation vector $h = (h_1, \ldots, h_M)$, whose elements are uniformly distributed mean-zero random variables with bounds satisfying the condition $E[|1/h_m|] < \infty$, $m = 1, \ldots, M$.

Then, we use the finite difference method (Quarteroni, 2013) for estimating the second derivates. In particular, the r-th element on the diagonal of H_γ is:

$$\frac{\partial^2 logL(\theta|Z_{pseudo})}{\partial \vartheta_r^{\,2}} \cong \frac{logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r+h_r}\middle|Z_{pseudo}\right) - 2logL(\theta|Z_{pseudo}) + logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r+h_r}\middle|Z_{pseudo}\right)}{h_r^2} \tag{11}$$

whereas the (r, j) elements, $r, j = 1, \ldots, M$ and $r \neq j$, outside the diagonal, are:

$$\frac{\partial^2 logL(\theta|Z_{pseudo})}{\partial \vartheta_r \partial \vartheta_j} \cong \frac{logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r+h_r,\vartheta_j=\widehat{\vartheta}_j+h_j}\middle|Z_{pseudo}\right) + logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r-h_r,\vartheta_j=\widehat{\vartheta}_j-h_j}\middle|Z_{pseudo}\right)}{4h_rh_j} - \frac{logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r+h_r,\vartheta_j=\widehat{\vartheta}_j-h_j}\middle|Z_{pseudo}\right) + logL\left(\theta_{\vartheta_r=\widehat{\vartheta}_r-h_r,\vartheta_j=\widehat{\vartheta}_j+h_j}\middle|Z_{pseudo}\right)}{4h_rh_j} \tag{12}$$

where $\theta_{\vartheta_r=\vartheta_r^*,\vartheta_j=\vartheta_j^*}$ represents vector $\hat{\theta}$, with its r-th and j-th elements taking values ϑ_r^* and ϑ_j^*, respectively.

Finally, the sample mean $H^{(s)} = H^{(s)}(\theta|Z_{pseudo})$ of the Γ estimates is computed.

Step 3. (Averaging Hessian estimates). Repeat Steps 1 and 2 until $s = S$. Then, the negative of the average of the S Hessian estimates $H(s)$ produced in Step 2 give the estimate of $F(\theta)$.

The approach is computationally efficient because it requires a low number of Log-likelihood values to produce each estimate.

3.3 *Input setting*

In order to perform the statistical analysis MUSTADEPT requires the user to specify four different pieces of information concerning: the data set, the stochastic model representing the transition from a state to another, the MLE algorithms and the level of confidence for the visualization of the results.

3.3.1 *Dataset*

The dataset is stored in a text file; then, to start the analysis, the user just specifies the name and the path of this file.

3.3.2 *Stochastic model*

The user is required to select between Weibull and Log-normal, the probability distribution used

to model the transitions among the degradation states.

3.3.3 *Algorithm in support to MLE*

The software asks the user to select and set the algorithm to find the maximum of the Log-Likelihood Function (i.e., the ML estimates of the parameters of the probability distributions). In particular, the user can:

- Select the preferred Matlab optimization algorithm among two alternatives: constrained and unconstrained algorithms. In the former case, MUSTADEPT calls the 'fmincon' Matlab function, whereas in the latter case the 'fminsearch' algorithm.
- Suggest the starting point for the search of the maximum of the Log-likelihood function. In this respect, notice that the closer is the starting point to the MLE point, the smaller is the computational time.
- Define the number of optimization runs and the number of iterations in each run. In this respect, notice that setting the number of optimization runs larger than 1 allows cross-validating the result of the search.
- Choose the number of parallel jobs, to optimally exploit the computing capabilities of the CPU when running MUSTADEPT.

3.3.4 *Level of confidence*

The user needs to specify the level of confidence conf ∈ [1, 100[for the visualization of the results (Zio, 2007).

3.4 *Results*

MUSTADEPT provides in output the probability with which the SCC occupies the different degradation states over time, and the uncertainty associated to this evaluation. In particular, such uncertainty encodes both aleatory (i.e., inherent to the SSC stochastic behaviors) and epistemic (i.e., due to the lack of precise knowledge of the model parameters and the Monte Carlo estimation) contributions.

Two different outputs are provided, which are discussed in the following Sub-Sections:

Specific solutions, referred to specific time instants.

Overall solutions, representing the probabilities that the analyzed SSC resides in the different states over the considered time horizon.

3.4.1 *Specific solutions*

The specific solutions are computed for all the time instants of the discretized time horizon, and give the CDFs of the probabilities of finding the SSC in the 4 degradation states (i.e., a plot for each degradation state).

For example, Figure 1 shows the results relevant to state S_1 at time instant $t = 14$ Units of Time (UoT). The interpretations of the Figure may be: the probability of the SSC being in state S_1 at $t = 14$ cannot be smaller than 0.25; it is smaller than 0.3 with probability 0.5; certainly, it is smaller than 0.4. Another example is reported in Figure 2. The probability that the SSC is in the fourth state at time $t = 14$ UoT is smaller or equal to 0.1 with probability almost 1. Similar plots are produced for S_2 and S_3.

The information contained in the plots of the specific solutions is also summarized by MUSTADEPT, on the basis of the confidence level entered by the user: specifically, MUSTADEPT estimates the values of the 0.5(100-*conf*)th and the [100–0.5(1-*conf*)]th percentiles of the CDF of the specific solutions.

With reference again to $t = 14$ UoT (Figs. 2–3), considering $conf = 90$, MUSTADEPT estimates the 5th and 95th percentiles of the CDFs relevant to t.

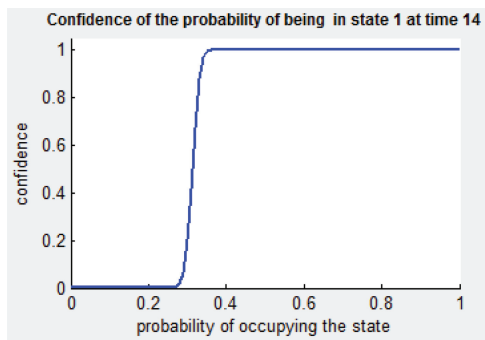


Figure 2. Specific solution, referred to state S1 and t = 14 UoT (statistical approach).

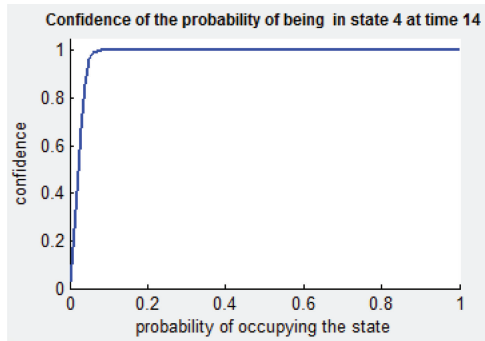


Figure 3. Specific solution, referred to state S4 and t = 14 UoT (statistical approach).

This information is also summarized in the following statements:

- the probability of being in state 1 is between 0.28% and 0.34%;
- the probability of being in state 2 is between 0.34% and 0.39%;
- the probability of being in state 3 is between 0.26% and 0.33%;
- the probability of being in state 4 is almost 0% (between 0% and 0.04%).

3.4.2 *Overall solutions*

The overall solutions lump together the specific solutions to provide a representation of the evolution of the probability of having the SSCs in the different states over time. In particular, for every time instant the overall solutions give the percentiles computed as explained above. For clarity, Figure 4 shows the link between the specific and the overall solutions. In general, the higher the confidence required by the user, the wider the bands in Figures 5–8.

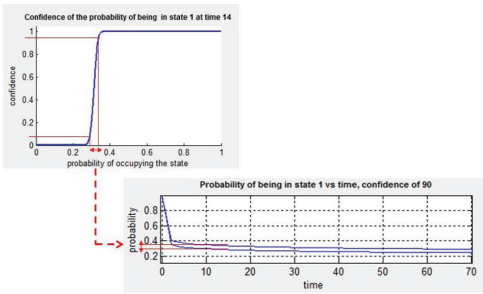
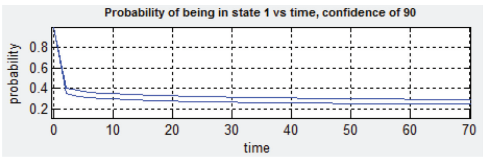
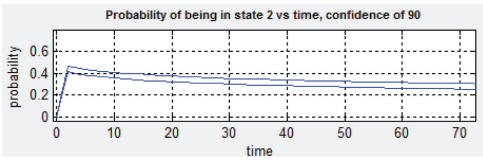


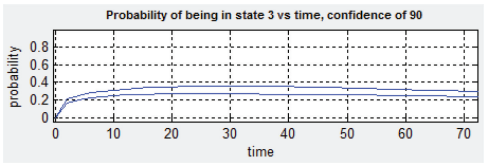
Figure 4. Example of passage from specific to overall solution.



Figures 5. Overall solution referred to state S_1 (statistical approach).



Figures 6. Overall solution referred to state S_2 (statistical approach).



Figures 7. Overall solution referred to state S_3 (statistical approach).

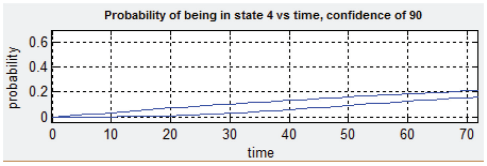


Figure 8. Overall solution referred to state S_4 (statistical approach).

The comparison of the probability values of the SSC being in the four degradation states over time provides the analyst with a useful information to make decisions. For example, from Figures 5–8 it emerges that:

- At the beginning of the simulation all the items are healthy, being the probability of finding the SSC in state 1 at time 0 equal to 1.
- In successive time instants, the SSC starts to leave state 1 and pass into state S_2.
- As the time goes on, all the probability that SSC undergoes a transition from state S_2 to state S_3 increases.
- Finally, as the time evolves, the SSC reaches the failure state.

4 DSTE APPROACH

4.1 *Main concept*

The DSTE procedure implemented in MUSTADEPT allows investigating the same degradation model analyzed by the statistical approach, within the framework of DSTE. This allows exploiting the rough and imprecise estimations of the model parameters retrievable from experts. A detailed description of such procedure is provided in (Baraldi et al., 2013, Helton et al., 2004, Baraldi et al., 2012) whereas its theoretical bases are given in (Dempster 1967, Shafer 1976, Baudrit et al., 2006).

4.2 *Input data*

To carry out the analysis based on the DSTE approach, MUSTADEPT requires three different

input types concerning: the stochastic model for the representation of the transition between different states, the Monte Carlo-DSTE algorithm, and the level of confidence for the visualization of the results.

4.2.1 *Stochastic model*

Similarly to the statistical approach, the user can select the probability distributions governing the transitions among two alternatives: the Weibull distribution or the Log-normal distribution.

Once the model is selected, the software requires information about the 6 model parameters $\theta(\theta_{11}, \theta_{12}, \theta_{21}, \theta_{22}, \theta_{31}, \theta_{32})$. In details, for every parameter, the user enters the information elicited from the experts, who have estimated the bounds of the intervals they believe to contain the true values of the parameters. In this respect, notice that the output of the statistical approach may be considered as given by a 'virtual' expert, and thus accounted for in the DSTE analysis.

Figure 9 shows the MUSTADEPT graphical user interface to enter the bounds of the intervals provided by the experts and the other parameters.

4.2.2 *Monte Carlo-DSTE algorithm*

The software allows the user to customize the Monte Carlo-DSTE method implemented in MUSTADEPT for the representation and propagation of the uncertainty associated to the imprecise information provided by the experts. In particular, the user has to set two parameters: the length of the time steps partitioning the time horizon of interest and the number of Monte Carlo simulations. These variables determine the level of precision of the final results and the computational efforts required to carry out the analysis: the larger the desired precision, the more expensive the computational cost. A good compromise solution between reasonable computational efforts and precision needs to be found by the user, depending on the application and the intended use of its results.

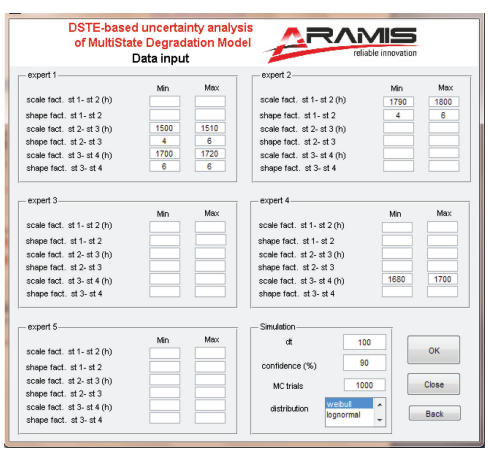


Figure 9. User interface to enter the algorithm settings.

4.2.3 *Level of confidence*

The user has to specify the level of confidence for the visualization of the results.

4.3 *Results*

The results provided by the DSTE approach are similar to those in output from the statistical approach; also in this case the results are divided into:

- Specific solutions, referred to given time instants;
- Overall solutions, representing the probabilities of the SSC being in the different states over the considered time.

In general, the considerations reported for the statistical approach in sub-Section 3.3 hold also in this case. However, attention must be paid to the fact that the statistical approach considers probability distributions, whereas the DSTE approach refers to Plausibility and Belief functions, and Pignistic probability, as discussed in the following Sections.

4.3.1 *Specific solutions*

For each time instant, the specific solutions of the DSTE approach give the bounds of the probabilities of finding the SSC in the 4 degradation states, and the associated uncertainties, described in terms of Belief and Plausibility functions. These encompass both epistemic and aleatory uncertainties and, roughly speaking, can be regarded as the lower and upper bounds, respectively, of all the possible CDFs encoded by the imprecise estimations provided by the experts on the model parameters.

Therefore, for every degradation state S_k, the output distributions provided by MUSTADEPT as specific solutions at time t, bracket the unknown probability of occupying S_k at time t corresponding to the true value of θ. Generally speaking, the closer the Plausibility and Belief functions, the smaller the uncertainty in the solution, which however, heavily depends on the width of the intervals provided by the experts.

For example, Figure 10 shows the specific results at time instant t = 14 UoT. A possible interpretation is that the probability of the SSC being in state 1 at the considered time instant is smaller than 0.3 (on abscissa) with a probability value between 0 and 0.7 (on ordinate).

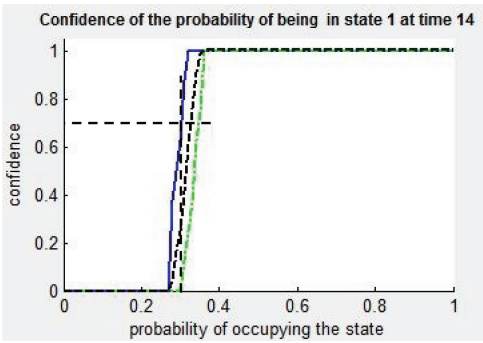


Figure 10. Specific solution, referred to state 1 and 14 UoT (DSTE approach). Continuous blu line = Plausibility; Dashed black line = Pignistic; Dashed-Dotted green line = Belief.

Finally, the specific solutions also give for every degradation state the Pignistic distribution associated to the uncertainty setting defined by the user. Roughly speaking, this distribution allows 'translating' the representation of the uncertainty from the DSTE framework to the probability theory framework, with the minimum commitment of information (Smets & Kennes, 2008).

4.3.2 *Overall solutions*

The overall solutions represent the evolution of the probability of having the SSCs in the different states over time. In the DSTE approach, such solutions are computed similarly to what explained in sub-section 3.3.2, but with reference to Belief, Plausibility and Pignistic functions. Namely, given the level of confidence conf set by the user, MUSTADEPT computes for every time bin partitioning the time horizon, the following values:

a. the 0.5(100-*conf*)th percentile on the Plausibility function and the [100–0.5(1-*conf*)]th on the Belief function (Fig. 9) of the corresponding specific solutions. For example, if the user sets *conf* = 90, then MUSTADEPT takes the 5th percentile of the Plausibility measure and the 95th percentile of the Belief curve.
b. The 0.5(100-*conf*)th and the [100-0.5(1-*conf*)]th percentile of the Pignistic distribution function, of the corresponding specific solutions.

These values are the upper and the lower bounds of the probability of occupying the degradation states provided by the overall solutions.

The user can select from the alternatives a) and b) above the preferred method to obtain the overall solutions from the specific ones. Generally speaking, method a) yields a wider range of probability values (i.e., a wider band), which gives due account to the uncertainty deriving from the propagation of the imprecision in the input collected information.

In addition, the larger the confidence required by the user, the wider the band of the results.

5 CONCLUSION

In this paper, a new software tool has been presented, which allows to exploit the information available in terms of statistical data and expert judgments to build and simulate a multistate degradation model. A typical industrial case study has been shown. The sound theoretical bases which the tool is based on have been summarized, the information required to the user detailed, and the output results described.

Additional research work will be dedicated on developing computational methods that can easily guide the user in making maintenance decisions on the basis of the four-states degradation model.

REFERENCES

Baraldi, P., Compare, M., Zio, E. 2013a. Maintenance policy performance assessment in presence of imprecision based on Dempster-Shafer Theory of evidence. *Information Sciences* 245: 112–113.

Baraldi, P., Compare M, Despujols, A., Lair, W., Zio, E. 2013b. A practical analysis of the degradation of a nuclear component with field data. *Proceedings of European Safety and Reliability Conference 2013, ESREL 2013*.

Baraldi, P., Compare, M., Zio, E. 2012. Dempster-shafer theory of evidence to handle maintenance models tainted with imprecision. *Proceedings of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012.*

Baudrit, C., Dubois, D., Guyonnet D. 2006. Joint Propagation and Exploitation of Probabilistic and Possibilistic Information in Risk Assessment. *IEEE Transactions on Fuzzy Systems.* 14 (5)*:* 593–608.

Dempster A.P. 1967. Upper and lower probabilities induced by a multi-valued mapping. *Annals of Mathematical Statistics* 38: 325–339.

Grall, A., Blain, C., Barros, A., Lefebvre, Y., Billy, F. 2007. Modeling of Stress Corrorsion Cracking with Periodic Inspection. *Proceeding of the 32nd ESReDA Seminar*. Alghero. Italy.

Helton J.C., Johnson J.D., Oberkampf W.L. 2004. An exploration of alternative approaches to the representation of uncertainty in model predictions. *Reliability Engineering and System Safety* 85: 39–71.

Moghaddass, R. and Zuo, M.J. 2011. A parameter estimation method for a multi-state deteriorating system with incomplete information. *Proceedings of the Seventh International Conference on Mathematical Methods in Reliability: Theory, Methods, and Applications (MMR 2011)*: pp. 34–42.

Papoulis A., Pillai U. 4th Edition. 2002. *Probability, Random Variables, and Stochastic Processes.* Mc Graw-Hill.

Quarteroni, A. 2nd Edition. 2013. *Numerical Models for Differential Problems.* Springer-Verlag.

Ray A., Tangirala S., Phoha S. 1998. Stochastic modeling of fatigue crack propagation. *Applied Mathematical Modelling* 22: 197–204.

Shafer, G. (1976). *A Mathematical Theory of Evidence.* Princeton University Press.

Smets, P., Kennes, R. 2008. The Transferable Belief Model. *Studies in Fuzziness and Soft Computin,* 219: 693–736.

Spall, J.C. 2009. Monte Carlo Computation of the Fisher Information Matrix in Nonstandard Settings. *Journal of Computational and Graphical Statistics* 14 (4): 889–909.

Yager R.R. 2011. On the fusion of imprecise uncertainty measures using belief structures. *Information Sciences* 181: 3199–3209.

Zio, E. 2007. *An Introduction to the Basics of Reliability and Risk Analysis. Series in Quality, Reliability and Engineering Statistics. Vol. 13*. Singapore: World Scientific.

Zio, E., Compare, M. 2013. Evaluating maintenance policies by quantitative modeling and analysis. *Reliability Engineering and System Safety* 109: 53–65.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Provision of the reliable video surveillance services in heterogeneous networks

P. Lubkowski & D. Łaskowski
Military University of Technology, Warsaw, Poland

E. Pawlak
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: Process of ensuring the security of citizens requires access to the information from sensors located in different points of monitoring and data acquisition systems. The IP video surveillance networks are nowadays the main part of such a systems. Transmission of data from multiple video sensors may lead to the degradation of video quality and even to lack of transmission abilities especially in heterogeneous networks. The paper presents a study of selected QoS supporting mechanisms and components elaborated for video monitoring service that were implemented in the prepared testbed which consists of QoS-aware application, QoS Streaming Server and Resource Broker modules. Suitable testing scenarios were selected in order to present an effect of functioning of these components in the QoS-supporting video monitoring network.

1 INTRODUCTION

Video surveillance systems for many years are used to enhance the safety of citizens and the protected objects. With video surveillance we meet both in public and national utility facilities, in places publicly available and in the areas with limited access. Monitoring systems are a combination of video recording (sensors), transmitting, storing and reproducing devices in one integral unit. They enable the observation of people or objects in real time as well as the event recording for later analysis.

The possibility of cooperation between video surveillance and security forces (police, municipal police and private companies) provides a rapid intervention and the precise identification of the perpetrators of the offense or offenses. Another application is to identify, in near real-time, persons performing essential roles in numerous and various systems of transportation for people and goods.

As it can be seen the detection and identification of persons and events is one of the main advantages offered in today's surveillance systems. A characteristic feature of the video monitoring systems is also their performance on an ongoing basis. A relatively brief interruption of the surveillance system may determine the overall effectiveness of the solution. Requirements for video surveillance systems are defined in the area of functional and quality constraints. Quality assurance at the network level (QoS—Quality of Service) is extremely important because it allows prediction of the size of the available bandwidth and the level of losses at the application layer. However, this information will only allow a fair distribution of bandwidth between the cameras and does not reflect the user's requirements on service severability. Thus in the case of video surveillance systems it is important to consider also the quality at the application layer. The QoS at the application layer is defined in ITU-T Recommendation G.1010 and includes parameters related to the establishing, disconnecting and call-blocking of connection (ITU-T G.1010 Recommendation 2001). Within this group of parameters, service accessibility and service retainability are particularly relevant. They determine the possibility of obtaining on demand services in the specified range and under certain conditions, and to continue it for the required period. Provision of QoS with respect to network layer and the application layer for such systems is a great challenge and requires an appropriate QoS platform with traffic control mechanisms to handle video traffic transferred through such systems.

Many QoS-enabled architectures and protocols have been proposed to solve the problem of end-to-end quality of real-time video services (Engel T. 2003, Callejo-Rodriguez MA 2008, Awduche D. 2001). However the mentioned solutions are not well suited to the large variation of maximum available data rate of video monitoring systems. In our proposal we decided to use our own cross-layer

mechanism discussed in (Lubkowski P. et al 2006, Lubkowski P. et al 2013). It uses a Cross-Layer Data Base (CLDB) and Cross-Layer Signaling (CLS) to share information's between LINK and APP layers.

In this paper, the QoS platform is presented which is composed of QoS Streaming Server and Resource Broker modules and QoS-aware Client module. They are part of modified End-to-end RatE Adaptation (EREA (Lubkowski P., Laskowski D., 2013)) application with ability to negotiate of traffic contract parameters for preserving service accessibility and retainability.

2 THE CONCEPT OF QoS PLATFORM

The QoS platform should be based on the layer independent from the techniques as well as network mechanisms applied in the administrative domains of video monitoring network. It should also deliver unified interfaces to individual network devices and applications. In order to fulfill these requirements, the QoS platform consist of QoS Streaming Server and Resource Broker modules and QoS-aware Client module with signaling and link capacity estimation functionalities, as it was already mentioned. Such platform is shown in Figure 1.

The QoS-aware application is based on cross-layer signaling between layers and implements a series of procedures that result in the adaptation of video bit rate to the available throughput of the transmission channel. It is also equipped with the dedicated signaling module that is able to acquire QoS requests to QoS Streaming Server (Qo3S). Each Qo3S is responsible for informing the Resource Broker (RB) about the QoS requirements coming from applications. The RB manages and estimates its known resources and decides about resources allocation for video stream transferred from IP camera in access device.

All the mechanisms located in adequate QoS-supporting components and responsible for QoS

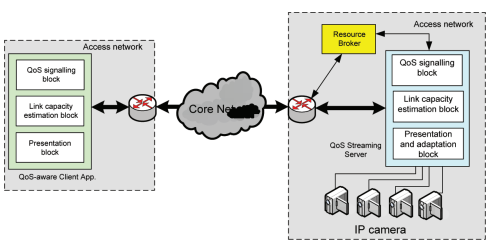


Figure 1. Functional diagram of QoS platform.

support were elaborated within the framework of the ongoing project. The QoS-aware client application was initially described and verified in (Lubkowski P., Laskowski D., 2013) and (Lubkowski P., Laskowski D., 2014). This paper is focused on the practical verification of these mechanisms implemented in prepared testbed configuration. Next section describes the functionalities of Qo3S and RB. The testbed structure and the testing plan are also presented.

3 QoS SUPPORTING IMPLEMENTATIONS

In this paragraph, the focus is set on functional description of QoS supporting implementations developed for provisioning of reliable video surveillance service. These include, as already mentioned, the QoS-aware client application and the QoS Streaming Server with the functionality of Resource Broker modules. The modules, named respectively "user" and "admin", were implemented in the form of executable programs written in C++ and configured to operate under Windows. Running the application requires the installation of additional C/C++ libraries included in the "libjpeg-turbo-1.2.0-vc" application. This application accelerates the video encoding and decoding as well as floating point operations, so it is possible to use the full power of x86 computing.

Qo3S and RB module ("admin") retrieves images from surveillance cameras and provides it on demand to the Client application ("user"). Streaming server (Qo3S) cooperates simultaneously with eight cameras of monitoring system. For each video stream Qo3S performs the procedure of video rate adaptation according to the throughput estimated by RB. Throughput estimation and video rate adaptation procedures have been described in detail in (Lubkowski P., Laskowski D., 2013). Additionally, RB executes also resource reservation for the selected video stream according to the QoS requirements coming from "user" application. The RB manages and estimates its known resources and decides about resources allocation for each selected video stream. Functional characteristics of "admin" application are given in Table 1 while the application window is shown in Figure 2.

The "user" application provides a possibility of communication with "admin" module and reception of video sequences from cameras supported by the server Qo3S. As it was already mentioned the customer of "user" application has the ability to manually select the best image quality and the priority of video stream in each of maintained class of services.

Table 1. Functional characteristics of "admin" application.

Functionality	Description
Number of supported surveillance cameras	More than 1, max. 8
Measurement of bandwidth	Yes
Transmission protocol	TCP/IP
Video rate adaptation according to the variable bandwidth	Yes
Visualization of link occupancy	Yes
Support for Diff Serv class of service Code Points	Yes
The ability to prioritize video stream	Yes, for each of supported cameras

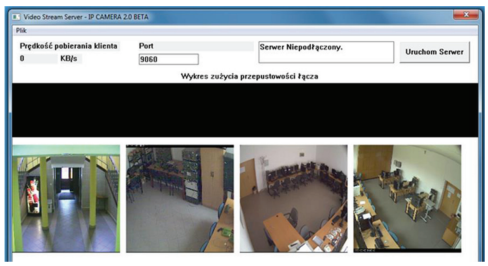


Figure 2. The "admin" application window.

4 QoS RISK ASSESSMENT

The provision of end-to-end QoS while maintaining the required level of service accessibility and retainability is an important issue as far as heterogeneous video surveillance networks are taken into account. It should be noted, that in order to provide the video surveillance services with required QoS some threats and consequences have to be taken into account. This so called risk analysis is a part of validation process of proposed QoS solution.

The heterogeneous video surveillance networks are often characterized by such properties as topology changes, mobility of users and service providers, common use of wireless links and limited processing and power capacity of network nodes. In turn the video transmission requires sufficient bandwidth and small delays but tolerates partial packet losses. Taking this into account the following threats can be identified: lack of bandwidth, large packet delivery delay (round trip time), large jitter, considerable percentage of packet loss and high level of packet duplication. The mentioned threats can lead to

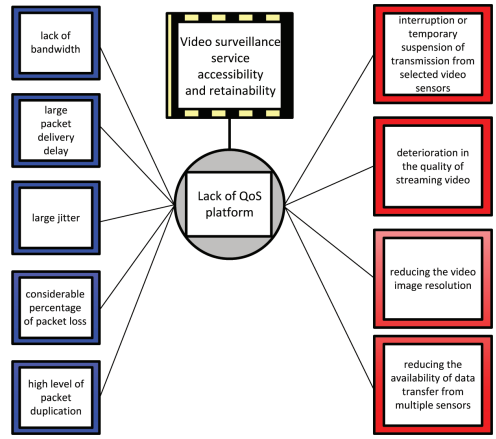


Figure 3. The Bow-tie risk assessment for proposed QoS platform.

the following consequences: the interruption or temporary suspension of transmission from selected video sensors, deterioration in the quality of streaming video, reducing the video image resolution and reducing the availability of data transfer from multiple sensors (Fig. 3). The proposed QoS platform ensures the minimization of the presented risks and reduces identified consequences in the provision of video surveillance services.

5 VALIDATION AND VERIFICATION OF QoS PLATFORM

All components of the QoS platform were implemented in the demonstration network established in the MUT (Military University of Technology) laboratory within the INSIGMA project. The main goal of the project is the development and implementation of a complex information system for comprehensive detection and identification of risks and the monitoring and identification of moving objects. The demonstration network consists of three access domains, which are connected by a backbone network. Two domains are a source of information from video monitoring and one of them represents a monitoring centre. The domains are connected over backbone network where tunnels of predefined bandwidth are established. Only under this condition we can use our mechanism for available bandwidth evaluation. The overall architecture of demonstration network is presented in Figure 4.

The set of tests and scenarios were proposed for verification and validation of the developed QoS supporting implementations. For this paper only

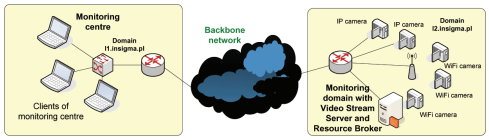


Figure 4. The overall architecture of demonstration network.

Table 2. Practical experiment scenarios.

#	Experiment	Description
1	Functional tests	Evaluation of QoS supporting mechanism in terms of bandwidth changes
2	Qualitative tests	Evaluation of image quality in case of class of service change Assessment of image quality with PSNR (Peak Signal-to-Noise Ratio)

Table 3. The characteristics of cameras (Axis).

The camera model	Resolution of video stream
Axis M1031-W	640×480
Axis Q1755	1280×720
Axis 207MW	640×480
Axis 207MW	640×480
Axis 215 PTZ	702×576

some of them were selected and discussed. The tests were divided onto following groups:

1) Functional tests.
2) Qualitative tests.

The goal of the functional tests was to verify the QoS-support implementations. The goal of qualitative tests was to validate the implementations and its usefulness in surveillance network.

Detailed description of each group of tests is given in Table 2.

The image was derived from IP Axis cameras whose main characteristics are given in Table 3. The server performs additional video compression using bilinear interpolation based on the designated bandwidth. Throughput restriction is performed by the client application. It reduces the bandwidth of the client interface to the value declared in the application window. The measurement results are related to quality indicators defined in the following recommendations (ITU-T G.1010 Recommendation, 2001), (ITU-T P.800 Recommendation, 1996).

The first experiment selected for discussion in this paper is based on a video streams transmitted to client application with different quality and priority. It represents the behaviour of QoS supporting mechanism caused by changes of throughput given in the transmission channel. The "admin" application handled five video cameras. Five video streams were sent to the "user", of which the last three are assigned the highest class of service and different priorities (high, medium and lowest). During the experiment a reduction of the available bandwidth was carried out from the maximum value (approximately 10 Mbps) to 100 kbps.

Figure 5 show a picture of the main application window once all cameras are plugged. With respect to the supported cameras (marked with colour squares) information concerning percentage occupancy of the available bandwidth is presented. The figures show also the colour indicator which represents actual link occupancy by each of the handled cameras. Cameras marked with red, magenta and dark blue are serviced with highest class of service. The others (green, blue) are not supported with developed QoS mechanisms. In the first part of the experiment, all cameras share the bandwidth according to the approved resolution of video stream (Table 3). The overall bandwidth occupancy is equal to 4.08% of available link capacity.

Next, the available bandwidth was restricted. As a result the quality of the video streams of the first two cameras was also restricted (reduction of available bandwidth) while the throughput for other cameras were maintained according to the values declared for the supported class of service (Fig. 6).

We can also observe only three color bars presented in the link occupancy indicator due to the fact that with respect to the other two streams (without QoS support) a significant reduction of the resources was made.

Further reduction of the available bandwidth should lead to a situation in which the STR server

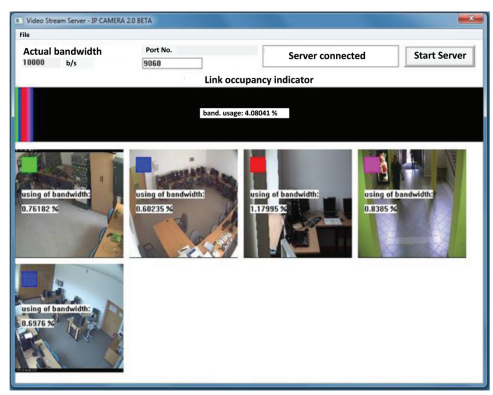


Figure 5. The "admin" application window during the experiment.

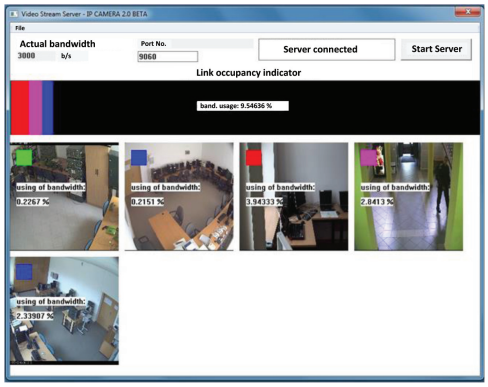


Figure 6. The effect of available bandwidth reduction—only throughput for cameras supporting QoS mechanisms is maintained (red, magenta, dark blue squares).

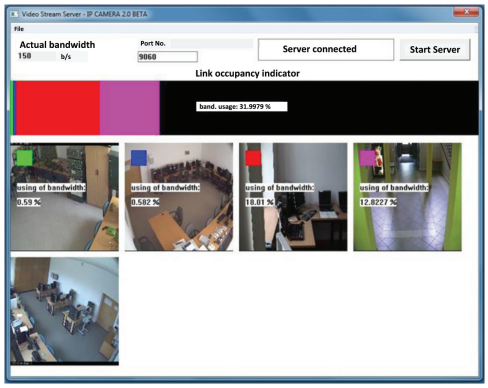


Figure 7. Suspension of video from the camera with the lowest priority due to lack of resources.

will stop streaming of a video data from the camera with the lowest priority. This is due to the fact that the server task is to maintain the guaranteed quality of video transmission according to given class of service and priority. The lack of resources results in termination of data transmission from the camera, which is assigned the lowest permissions.

We can observe this in Figure 7 which show that the streaming of video data from the fifth camera (marked previously with dark blue square) was stopped. The link occupancy indicator show red and magenta bars which occupy more than 30% of available link capacity. Also first two streams are still serviced according to the fact that remaining resources can be used for video data transmission from cameras without any QoS requirements.

The results obtained confirm the effective functioning of the proposed QoS mechanisms in the presence of changes in the available bandwidth.

Further part of the paper presents the results of qualitative tests. The results showing the impact of the applied-class services on achieved video stream quality are discussed first. During the tests the video from the camera Axis 207MW operating at a resolution of 640×480 was used. Figure 8 presents the video shown by the client application serviced in highest (DSCP = EF) and lowest class of service (DSCP = BE), respectively. It can be seen that in the case of highest quality there is no significant degradation of image quality. A deterioration of the image is invisible; we can observe a high focus and good contrast. However, for BE class of services, visible artifacts can be observed with respect to the previous image (the fields marked with a red border).

Qualitative tests of QoS platform incorporate also the assessment of image quality with PSNR. This parameter is used to determine the level of similarity between the reference image and the compressed one, and is expressed in decibels (dB). In practice, the smaller value of coefficient-t means lower similarity. For the measurements of PSNR, a MSU Video Quality Measurement Tool 3.0 application was used (MSU). Figure 9 show the value of PSNR when video serviced with EF and AF class

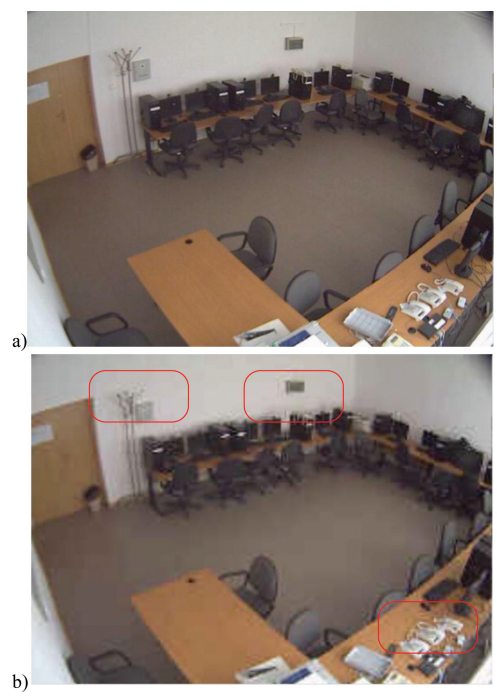
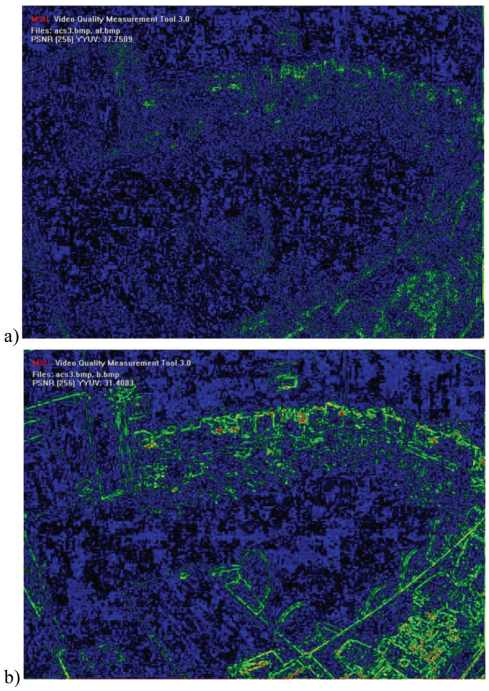


Figure 8. Image quality shown in client application window (a—EF class of services selected for video stream, b—BE class of services selected for video stream).



a)

b)

Figure 9. Result of the comparison of the images with MSU application (a—PSNR = 37.75, b—PSNR = 31.408).

of services is compared. Increasingly bright colors can be noticed in image quality, which means a greater difference of images. An even greater lack of fit can be seen when comparing video quality of video streams serviced in EF and BE class of services, respectively. However, the value of PSNR is still high, indicating a high probability of correct identification of the information contained within the image.

6 CONCLUSIONS

Testing results presented here confirm that the elaborated QoS mechanisms work correctly in conditions of changing the throughput of the transmission channel. From these results we can see that video monitoring can be ensured using proposed QoS platform.

The results obtained show also that the provision of video stream classification preserves the continuity of service without significant deterioration of image quality. This enables the support of end-to-end QoS in terms of service accessibility and retainability. The proposed QoS platform supports the INSIGMA monitoring network in maintaining the transmission of video stream with a specified level of quality.

ACKNOWLEDGEMENT

The work has been supported by the European Regional Development Fund within INSIGMA project no. POIG.01.01.02,00,062/09.

REFERENCES

Awduche D. & Berger L. & Gan D.T. Li, Srinivasan V. & Swallow G. 2001. RSVP-TE: Extensions to RSVP for LSP Tunnels, RFC3209.

Axis, available at: http://www.axis.com/pl/products/video/ camera/index.htm.

Callejo-Rodriguez M.A. et al. 2008. EuQoS: end-to-end QoS over heterogeneous networks, in: *Proceedings of the K-INGN 2008*, Geneva, May.

Engel T. et al. 2003. AQUILA: Adaptive Resource Control for QoS Using an IP-Based Layered Architecture, *IEEE Communications Magazine*, vol. 41: 46–53, January.

ITU-T P.800 Recommendation, 1996, Methods for subjective determination of transmission quality.

ITU-T G.1010 Recommendation. 2001. End-User Multimedia QoS Categories Series G: Transmission Systems and Media, Digital Systems and Networks Quality of Service and Performance-Study.

Lubkowski P. & Bednarczyk M. & Maslanka K. & Amanowicz M. 2013. QoS-Aware end-to-end Connectivity Provision in a Heterogeneous Military Environment, *Military Communications and Information Systems Conference*, Saint Malo, France.

Lubkowski P. & Krygier J. & Amanowicz M. 2006. Provision of QoS for multimedia services in IEEE 802.11 *Wireless network, Information System Technology Panel Symposium on "Dynamic Communications Management" IST-062*, Budapest.

Lubkowski P. & Laskowski D. 2013. The end-to-end rate adaptation application for real-time video monitoring, *Advances in Intelligent Systems and Computing*, vol. 224: 295–305, Switzerland: Springer International Publishing AG.

Lubkowski P. & Laskowski D. 2014. Test of the multimedia services implementation in information and communication networks, *Advances in Intelligent Systems and Computing* (accepted for publication), Switzerland: Springer International Publishing AG.

MSU, MSU Video Quality Measurement Tool 3.0, available at: http://compression.ru/video/quality_measure/video_measurement_tool_en.html.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Identification of degradation processes of seabed protection in ports

T. Abramowicz-Gerigk
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: Monitoring and maintenance of seabed protection is vital for the safe operation of vessels in shallow waters. The growing number of self-manoeuvring high powered vessels is the reason of the growth of the protected seabed areas of in ports. The variety of bottom protection systems is related to the variety of the degradation processes to be controlled. Traditionally the identification of degradation processes is based on empirical methods and periodical inspections. It is followed by maintenance works. The cost of maintenance is related to the state of degradation. The method of the permanent identification of degradation is proposed in the paper. The monitoring method based on the measurement of the ship propeller jets velocities is presented in the paper.

1 INTRODUCTION

Degradation processes of seabed in the areas exposed to the direct action of ship propellers and thrusters or strong sea currents have a significant influence on the port operational costs. The maintenance costs are dependent on the type of soil, type of seabed protection and proper schedule of the maintenance works.

In modern ports due to economic reasons port manoeuvres of large vessels are commonly performed in the conditions very closed to the limiting values related to ship dimensions, under keel clearance, used power of thrusters and main propulsion, weather conditions and towing assistance.

This is mainly caused by the introduction of Ultra Large, high powered Container Ships (ULCS) over 8,000 TEU (Twenty feet Equal Unit), of 300–400 m length, equipped with 2000–3500 kW thrusters and 60–80 MW propulsion systems (Hermans & Degens, 2011). They can perform manoeuvres in very tight areas and strong weather conditions, up to port operational limits, using their thrusters and propellers to increase efficiency of manoeuvres assisted by tug boats.

The large power of vessel main engines is the reason of high propeller jets velocities. To protect the seabed from scouring and seabed protections from damage the maximum used power of main propellers is reduced to 40%–25% of maximum power.

In the cases the port operations intensity is on nearly equal level, the identification of seabed degradation can be assessed on the basis of prediction methods developed on the basis of real observations, physical model tests and CFD (Computational Fluid Dynamics) calculations (Kraskowski, 2009). If the port operations are carried out near the limiting values of operational characteristics for seabed or seabed protections more often inspections are included in the maintenance plan and they are carried out after each crossing of the limits.

2 DEGRADATION PROCESS OF SEABED PROTECTION

2.1 *Types of seabed protection*

To allow more powered manoeuvres in the areas exposed to strong influence of propeller jets the dredging works are followed by seabed protection works.

In ports with bigger water depth to draft ratios assumed for the design (maximum for the port) vessel the three layered granular filter of rip rap, a block mat on geotextile or a stone asphalt mat with riprap can be applied (Gijt & Broeken, 2005).

In ports with smaller depths where the soft bottom (similar to sand) effect is required the mattress of geotextile bags filled with sand on geotextile sheet are used. The reason is the required under keel clearance. It should be 0.45 m for sand and 0.6 for rocks and stone riprap.

When the berth is in operation it is possible to apply seabed protection that allows increasing size of ships manoeuvring in this area. In the available limited space the expensive and fragile 0.15–0.25 m thick stone asphalt mat can be used.

For example riprap bottom protection made of the 10–60 kg quarries limestone is necessary for a current 1.5–2.5 m/s, for the greater velocities 1.8–3.3 m/s the required weight is 60–300 kg.

Several layers built up a good filter structure depending of soil filter characteristics.

The flirter layer is usually the sand–tight geotextile. For the highly turbulent propeller jets over 3.5 m/s the required weight of block is 1–3 t. The alternative protection is asphalt mattress, quarry stone pattern grouted with asphalt bitumen or colloidal concrete.

2.2 *Prediction of degradation process of seabed protection*

This phenomenon depends on the type of protection, frequency and capacity of loading. Design and operation of seabed protection including the frequency of inspections of its technical condition undergoes the rules of civil engineering codes. Up to this rules the inspection should be carried out once a year.

The technical state between inspections is not known. It can be predicted using models of system degradation. If the seabed protection systems undergo the gradual degradation the limiting state of a system is assumed as the state when the preventive maintenance is required.

Time to the maintenance is a random variable. To avoid the discrete time and states of the system the model based on gamma process can be used (Zhou et al., 2009). Degradation process of a system

$$(\tilde{X}_t)_{t\geq 0}$$

is a gamma process, which can be described using system degradation characteristics, for every s:

$$0 \leq s < t, \tilde{X}_t - \tilde{X}_s$$

it has gamma distribution with parameters

$$\alpha(t-s), \beta$$

$$f_{\alpha\cdot(t-s),\beta}(x) = \frac{1}{\Gamma(\alpha\cdot(t-s))}\cdot\frac{1}{\beta^{\alpha(t-s)}}\cdot x^{\alpha(t-s)-1}\exp\left(-\frac{x}{\beta}\right)I_{\{x\geq 0\}} \quad (1)$$

where: $\alpha\cdot\beta$ = mean index of process degradation rate, $\alpha\cdot\beta^2$ = variance.

The characteristics of this monotonically increasing process are related to irreversible degradation processes of concrete structures, dykes, hydro-technical constructions during one service cycle. The inspection dates and the limit state of the system are the decision variables.

If the gradual degradation of the seabed protection system cannot be assumed different methods based on prediction of the propeller and thruster jet velocities are applied in the models degradation processes.

They are used to predict the maximum design loads and distribution of the loads in time and space domains to determine reliability or safety functions of seabed protection (Abramowicz-Gerigk & Burciu 2013; Roubos, 2006, Verheij, 1983; Verheij et al., 2010; Wilson et al., 2006; Zhou, 2009.). The methods of jet velocities assessment are based on different empirical formulae for open water propellers modified to real conditions (Hamill et al., 1999; PIANC, 2012; Gucma & Jankowski 2007; Whitehouse, 1998.) or numerical methods (Lam et al., 2006; Muscari et al., 2011.).

The effect of water depth to draft ratio and influence of rudder angle examined on big physical model with geometrical scale 1:16 was presented in (Abramowicz-Gerigk, 2010; Abramowicz-Gerigk, 2011). The mean axial velocities v of propeller jet behind the rudder in deep water (water depth to ship draft ratio h/T = 3) and shallow water (h/T = 1.2) conditions related to v_o—jet velocity in deep water with rudder angle 0 are presented in Table 1.

The observed velocities in shallow water are 20% higher than in deep water. The effect of 35° helm to port is propeller jet deflection to the port side and smaller area of higher velocities observed within the asymmetrical measuring plane.

In 2011 Ryan and Hamill (Ryan & Hamill, 2011) presented the findings from the experiment of a ship berthing alongside a quay wall and the effect of rudder angle on the magnitude of the scouring.

Van den Brink and Nielsen (van den Brink, 2014; Nielsen, 2005) performed physical model research in order to investigate the diffusion or spreading of velocity field due to bow thrusters of vessels moored near a vertical quay. More complex investigations on ship accessibility and port presented Willems (Willems et al., 2012).

In maritime transportation the results of model experiments are used in all aspects to o bserve the physical phenomena and predict the performance of real object (Burciu & Grabski, Gerigk 2005, Gerigk 2012; Kee et al., 2006). The modern trend is the development of complex methods including operational limits and human factor (Abramowicz-Gerigk & Burciu, 2011; Gerigk, 2004; Gerigk, 2008; Gerigk, 2012) to determine system safety.

Table 1. Mean axial velocities of propeller jet behind the rudder for Half Ahead.

h/T	Rudder angle [°]	v/v_o [m/s]
3	0	1.000
	35	0.970
1.2	0	1.251
	35	1.119

In 2013 the full scale measurements of scour holes formed due to bow thrusters and main propellers action in front of the quay wall were performed in Port of Rotterdam. After each departure the bathymetry near the quay was measured using a multi-beam echo sounder.

Along the full scale measurements in Port of Rotterdam Van den Brink (van den Brink, 2014) presented CFD study of bow thruster induced score holes formation at the quay wall in number of departures domain. However the results of prediction were very sensitive to the type of the seabed soil (sand and clay layers) and did not give the satisfactory results.

CFD methods can be used to determine the characteristics of the flow around berthing or unberthing vessel: stream lines, flow velocity and pressure fields (Kraskowski, 2009). Flow field generated by bow thruster during ship unberthing is presented in Figure 1.

This method of prediction can be used for the flat layer of unmovable protection material, like geotextile mattresses. A good conformity of CFD calculation with real performance of seabed protection was observed in Port of Gdynia in ferry terminal (Abramowicz-Gerigk & Burciu, 2011).

The presented methods are used in ports to predict the degradation processes however due to the operation of large vessels in divergent operational conditions and relatively cheap monitoring methods the inspections using a multi-beam echo sounder in many ports are carried out in month periods.

2.3 *Monitoring of loads determining the degradation process*

Data collection allows following the behaviour of the structure over time and determination of its remaining lifetime. The monitoring is essential to give well found information if the design loads are exceeded.

The best method of monitoring is a multi-beam echo sounding (Hermans & Degens, 2011). The program of inspections includes periodical, usually every month inspection and additional inspections after hazardous operations. The multi-beam echo sounders can map the seafloor by a fan of narrow acoustic beams, providing 100% coverage of the bottom. The three dimensional seabed maps are enough detailed to observe score holes or local damages of seabed protection.

Comparing the measurements with the results of CFD flow field calculations (Abramowicz-Gerigk & Burciu, 2011; Kraskowski, 2010) the velocities near the seabed can be predicted. Every crossing of limits can be noted and immediate inspection and repair works can be ordered. The example of CFD prediction of streamlines in the aft and fore parts of the car-passenger ferry during unberthing is presented in Figure 2.

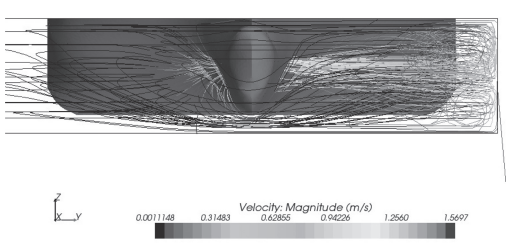


Figure 1. Bow thruster influence on the quay wall and seabed, CFD calculations.

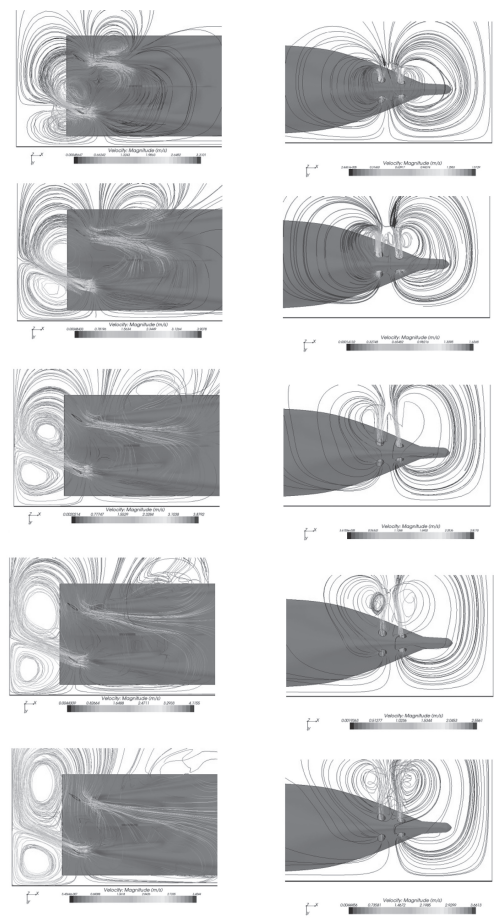


Figure 2. CFD streamlines prediction in the aft and fore parts of the car-passenger ferry during unberthing. Distance from the berth is equal to 0.1 ship breadth, water depth to draft ratio h/T = 1.2 (Abramowicz-Gerigk & Burciu, 2011).

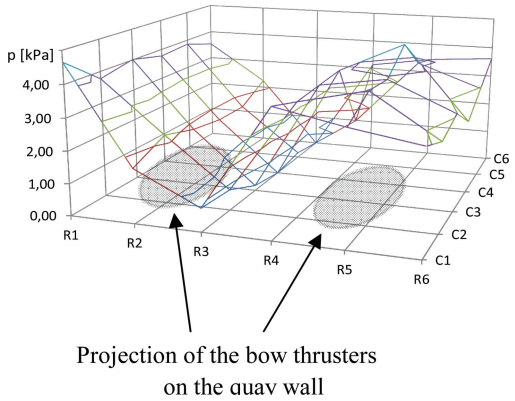


Figure 3. Pressure distribution measured on the quay wall during unberthing of m/f Stena Baltica, generated by bow thrusters. Positions of pressure meters CiRj: j = 1, ..., 6, i = 1, ..., 6 (Abramowicz-Gerigk, 2014).

The experimental solution for monitoring loads on the quay wall, introduced by Gdynia Maritime University in Port of Gdynia was a system for measurements of propeller or thruster jet induced pressure field. The system was installed in ferry terminal at berth Helskie II.

The pressure distribution measured on the quay wall is presented in Figure 3.

3 INFLUENCE OF LOADS MONITORING ON MAINTENANCE COSTS OF SEABED PROTECTION

The costs of inspections and repairs of seabed protection in berthing areas depend on berth construction and type of seabed protection.

Examples of expenses bear for the inspections and repair of mattress of geotextile bags filled with sand and pinned together, placed along the steel Larsen type tight wall are presented in Table 2 (Abramowicz-Gerigk, 2014).

This type of seabed protection is used in Port of Gdynia. The protected areas cover the zone along the whole length of the berth but have different width. In the area of propeller influence the protected area is about ship's beam.

The cost of hydrographical survey due to the technological development of echo sounding survey systems is still getting cheaper. Since last 10 years the cost dropped down about six times.

Comparing the costs of inspections giving 3D analysis of seabed protection with the costs of a system for monitoring loads from propeller jets, based on pressure meters it can be assumed that the pay of time of this system is 5 years. The calculations are based on the prototype system designed for research purposes. The main part of the cost is due to the expensive pressure meters.

Table 2. Examples of a unit price for expenses bear for the inspections and repair.

No	Type of costs	Cost
1	Soundings officially approved by the state marine hydrographical services in 50 m wide zone along the berth	11.00 EUR/1000 m^2
2	Inspections of protected seabed with siltation and damage measurements with divers attest	0.25 EUR/m^2
3	Inspections of protected seabed with siltation and damage measurements with divers attest, graphical cataloguing and digital recordings	0.35 EUR/m^2
4	Replacement of a damaged element of seabed protection	350 EUR/apiece

Loads monitoring has another economic aspect. The seabed protection in the form of mattress, made of single elements, pinned and tight together with ropes, should be repaired immediately after the damage of a few elements because the next excess of loads can result in extensive damage. The cost of not detected repair can include replacement of several dozen elements and delays in berth operation.

4 CONCLUSIONS

To limit scour of the seabed several pro-active measures can be undertaken. The higher water depths, limits of used power of propulsion units, seabed protection and frequent monitoring are the most popular solutions.

The latest investigations with respect to the prediction methods of score holes formation still need more research.

It can be observed that the differences between modelled and real soil—grain, cohesion, layers formation have the significant influence on the accuracy of prediction (van den Brink, 2014). The more departures the larger is the deviation between measured and calculated scour depth, therefore the complex methods including all influencing parameters should be introduced (Abramowicz-Gerigk & Burciu, 2013; Gerigk 2006).

The monitoring of loads induced by propeller jets on the seabed near the quay wall is especially important in shallow water, defined in the non-dimensional sense, with respect to the ship draft.

The loads monitoring system presented in the paper operated on line allows for the detection of all emergency situations, when ship master uses the power of propellers and thrusters over the permissible limits. This is the most important factor in the prediction of the condition of seabed protection made as geotextile sand filled bags mattresses. It can save maintenance costs related to the replacement of wide area of damaged elements and are the most important for a modern port as allows avoiding the delay in the berth operation.

REFERENCES

Abramowicz-Gerigk T. 2010. Distribution of flow velocity generated by propellers of twin propeller vessel. *Scientific Journals Maritime University of Szczecin, No. 20/92:* 5–13.

Abramowicz-Gerigk T. 2014. Wpływ monitorowania obciążeń umocnień dna i nabrzeża w rejonie cumowania statków na koszty eksploatacji basenów portowych. *Logistyka* 2/14.

Abramowicz-Gerigk T. & Burciu Z. 2011. Comprehensive analysis of ship performance during self-berthing. *Advances in Engineering Research,* Chapter 13, Volume 3: 423–440, Hauppauge NY: Nova Science Publishers inc.

Abramowicz-Gerigk T., Burciu Z. 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. in C. Guedes Soares, & F. Lopez Pena (eds.) *Developments in Maritime Transportation and Exploitation of Sea Resources. Proc. 15th Int. Congress of the International Maritime Association of the Mediterranean (IMAM'2013)*, A Coruna, Vol. 2: 699–704, London: Balkema.

Burciu Z. & Grabski Fr. 2011. The experimental and theoretical study on the reliability of the life rafts. *Reliability Engineering and System Safety* 96: 1456–146.

de Gijt J.G. & Broeken M.L. 2005. Handbook of Quay Walls. Center for civil Engineering Research and Codes, Balkema: Gouda, The Netherlands.

Gerigk M. 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. Polish Maritime Research, No. 1 (39), Vol. 11, 8–13.

Gerigk M. 2005. Challenges of modern assessment of safety of ships in critical conditions. Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean IMAM 2005, Volume 2, Lisboa, Portugal, 26–30 September 2005, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 1529–1536.

Gerigk M. 2006. A method for assessing hazards, risks and safety of damaged ships at sea. Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006), Volume 3, Estoril, Portugal, 18–22 September 2006, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 2783–2790.

Gerigk M. 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference, ESREL 2008 and 17th SRA-Europe, Volume 4, Valencia, Spain, 22–25 September 2008, Published by CRC Press, Taylor & Francis Group, Balkema, Boca Raton/London/New York/Leiden, 3303–3310.

Gerigk M. 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. in Sustainable Maritime Transportation and Exploitation of Sea Resources. Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM), Volume 2: 715–719, London: Balkema.

Gucma S. & Jankowski S. 2007. Depth Optimization of Designed New Ferry Berth. 7th International Symposium on Marine Navigation and Safety of Sea Transportation Trans-Nav'2007. Gdynia 2007.

Hamill G., Johnston H. & Stewart D. 1999. Propeller wash scour near quay walls. J. Waterway, Port, Coastal, Ocean Eng., 170–175.

Hermans M.A. & Degens S. 2011. Impacts of evolving shipping and vessels characteristics on berth maintenance dredging. 38th Annual Texas A&M Dredging Conference, www.westerndredging.org/index.php/information/proceedings-presentations/category/42-8th-aannualtexas-aam-dredging-conference.

Kee C., Hamill G., Lam W. & Wilson P. 2006. Investigation of the Velocity Distributions within a Ship's Propeller Wash. *Proc. of the Sixteenth Int. Offshore and Polar Engineering Conference: 451–456, San Francisco, California, USA, 2006.*

Kraskowski M. 2009. CFD calculations of interactions during harbour manoeuvres of vessel Kolobrzeg. Research project N N509 293635 sponsored by Polish Ministry of Science and Higher Education: "Safety of berthing of ships in the Motorway of the Sea transportation system", Gdynia Maritime Univesity. Technical report CTO S.A. N0 RH-2009/T-027.

Lam W., Robinson D.J. Hamill G.A. & Raghunathan S., Kee C. 2006. Simulations of a Ship's Propeller Wash. *Proc. of the Sixteenth (2006) Int. Offshore and Polar Engineering Conference, San Francisco, California, USA.* Copyright © 2006 by The International Society of Offshore and Polar Engineers, 1380–1388.

Muscari R., Felli M. & Mascio A. 2011. Analysis of the flow past a fully appended hull with propellers by computational and xperimental fluid dynamics. *Journal of Fluids Engineering,* vol. 133, Issue 6.

Nielsen B. 2005. Bowthruster-Induced Damage-a physical model study on bowthruster-induced flow—*MSc Thesis*. Delft University of Technology.

PIANC. 2012. Guidelines for berthing structures related to thrusters. *Report of working group 48 of PIANC*, Brussels: Belgium.

Ryan, D. & Hamill, G. 2011. Estimating propeller scour at quays alongside a berthing ship. *Proceedings of the ICE -Maritime Engineering*, 164(2): 59–70.

Roubos A.A., 2006. Dealing with uncertainties in the design of bottom protection near quay walls. *M. Sc. thesis in hydraulic structures*. Faculty of Civil Engineering and Geosciences. TU Delft, Delft, Netherlands. www.citg.tudelft.nl/.../doc/paperRoubos.pdf. 2006.

van den Brink A.J.W. 2014. Modelling Scour Depth at Quay Walls due to Thrusters.—*MSc Thesis*. Delft University of Technology.

Verheij, H.J. 1983. The stability of bottom and banks subjected to the velocities in the propeller jet behind ships. *Proceedings 8th Int. Harbour Congress*.

Verheij H., Sas M., Hermans M. & Schmidt, E. (2010) Guidance on the Design of Berthing Structures Related to the Flow Velocities in Ship Thrusters. Scour and Erosion: 914–923. *International Conference on Scour and Erosion* (ICSE-5) 2010.

Whitehouse R. 1998. Scour at marine structures: a manual for practical applications. Thomas Telford Publications: London: 1998.

Willems M., Van Dingenen B. & Verwaest T. 2012. Port of Zeebrugge: large physical model to study accessibility and siltation, in: Troch, P. et al. (Ed.). *Book of proceedings of the 4th international conference on the application of physical modelling to port and coastal protection*—Coastlab12: 1–8, Ghent, Belgium, September, 2012.

Wilson P.R., Hamill G.A. Johnston H.T. & Kee C. 2006. Influence of a Horizontal Boundary on a Marine Propeller Wash. Proc. of the Sixteenth (2006) *International Offshore and Polar Engineering Conference, San Francisco*, California, USA, 2006 Copyright © 2006 by The International Society of Offshore and Polar Engineers.

Zhou, Y., Ma, L., Mathew, J., Sun, Y. & Wolff, R. 2009. Asset life prediction using multiple degradation indicators and failure events: a continuous state space model approach: *Operation and Reliability* No. 4.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The use of Self-Organizing Maps for diagnosing faults in motor bearings

S. Al-Dahidi
Energy Department, Politecnico di Milano, Milan, Italy

ABSTRACT: In this paper, the use of Self-Organizing Maps (SOM) for fault diagnostics is proposed. The method is tested with an artificial case study representing three start-up faulty behaviors of equipment and then, applied for diagnosing faults in motor bearings: the data have been collected from Case Western Reserve University Bearing Data Center with three failure modes. The method has been tested and compared to the K-Nearest Neighbor (KNN) method. The obtained results show that the SOM algorithm is a powerful visualization tool able to recognize the fault classes with a low misclassification rate. Furthermore, the quality of the SOM has been assessed using two measures: average quantization error and topographic error and their sensitivity with respect to the map size is investigated.

1 INTRODUCTION

In industries such as nuclear, oil and gas, and chemical, equipment may have different types of faults, for example, motor bearings may degrade due to cracking, valves may leak or sensors may provide wrong readings (Gonçalves et al. 2011, Huang 2012, McDonnell et al. 2014).

In modern society, motor systems are used in industrial applications in a wide range of operating areas. Thus, the reliability of motor systems is of paramount importance in several industrial applications (Isermann & Balle 1997, Kowalski & Orlowska-Kowalska 2003, Önel et al. 2006, Huang 2012). Various studies show that more than 40% of all machine failures occur because of bearing failures (Schoen et al. 1995, Ng et al. 2014). Therefore, a prompt diagnosis of these faults can greatly increase equipment reliability and safety and reduce corrective maintenance costs (Tamilselvan et al. 2013a).

For these reasons, several fault diagnosis techniques have been developed in the last few decades. Some examples of fault diagnosis techniques applied in diagnosing faults of motor bearings are: Artificial Neural Networks (ANNs) (Alguindigue et al. 1993, Li et al. 2000, Gao & Ovaska 2001, Yang et al. 2002, Samanta & Al-Balushi 2003), Support Vector Machines (SVMs) (Abbasion et al. 2007, Sugumaran et al. 2007, Yu et al. 2007), Deep Belief Networks (DBNs) (Tamilselvan & Wang 2013b), Fuzzy Logic (FL) (Klir & Yuan 1995, Gao et al. 2001, Wang & Hu 2006, Zio & Gola 2006b, Wang & Chen 2007), Genetic Algorithms (GA) (Gao & Ovaska 2001), and Self-Organizing Maps (SOM) (Kalyan et al. 2010, Gonçalves et al. 2011). Recently, SOM have got much interest because of their performance in fault detection and diagnosis in numerous industrial systems (Gonçalves et al. 2011).

These methods can be broadly classified into supervised and unsupervised learning methods. The supervised learning methods learn the relationship between the input values and the desired target values, i.e. labels, by feeding the method with a set of inputs and the desired target outputs, whereas the unsupervised learning methods learn a hidden relationship in the input values without the target outputs (Baraldi et al. 2013, Tamilselvan et al. 2013a).

In this work, the SOM technique has been adopted for fault diagnosis purposes for both, supervised and unsupervised learning. The method has been applied firstly to an artificial case study representing three start-up faulty behaviors of equipment and then applied to a real case study concerning three failure modes of motor bearings (inner race, outer race and ball faults): the data have been collected from the Case Western Reserve University Bearing Data Center (CWRU). The method has been tested using 144 test patterns and the misclassification rate has been calculated and compared to the misclassification rate obtained by using the K-Nearest Neighbor (KNN) method for the same dataset.

The final results show that the SOM algorithm is a powerful visualization tool able to recognize the fault classes with a lower misclassification rate than those of other empirical classifiers such as KNN. Furthermore, the quality of the SOM has been assessed using two measures: average quantization error and topographic error and their sensitivity with respect to the map size is investigated.

The remaining of this paper is organized as follows; in Section 2, the problem is stated, in Section 3, the Self-Organizing Maps (SOM) are briefly introduced, Section 4 presents the application of SOM to the artificial case study, whereas Section 5 presents the application of SOM to motor bearings datasets. In Section 6, a sensitivity analysis of the SOM quality measures for different map sizes is introduced. Finally, some conclusions are reported.

2 PROBLEM STATEMENT

In this work we assume that we have available the vibration measurements of a motor corresponding to different types of bearing faults. These vibration values have been used to extract several features which are used to train a fault diagnostic model whose objective is the classification of the fault type. Each fault is assumed to be represented by a cluster, *C* (Baraldi et al. 2013). In the following sections, we discuss the use of Self-Organizing Maps (SOM) for diagnosing the motor bearing faults.

3 THE SELF-ORGANIZING MAPS (SOM)

Self-Organizing Maps (SOMs) or Kohonen maps are types of Artificial Neural Networks (ANNs) that are trained using supervised/unsupervised learning to produce a low-dimensional discretized representation (typically 2-dimensional) of an arbitrary dimension of input space of the training samples (Zhong et al. 2005).

Figure 1 shows the basic SOM in which the continuous *n*-dimensional input $\vec{x} = [x_1, ..., x_n]$ is mapped into a discrete output of ℓ neurons (map units) organized in 2-dimensional lattice matrix with a height *h* and a width *w*, $\ell = h \times w$.

The number of neurons may vary from a few dozen up to several thousand depending upon the application. Each neuron *j* is represented by an *n*-dimensional weight vector $\vec{w}_j = [w_{j1}, ..., w_{jn}]$ and is connected to its adjacent neurons by a neighborhood relation, which dictates the topology or structure of the map. Furthermore, it is fully connected to all inputs (Vesanto et al. 2000, Zhong et al. 2005).

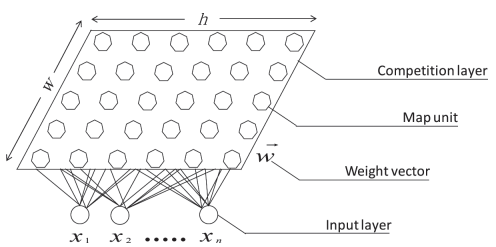


Figure 1. Basic SOM structure.

For each input vector, the best matching weight vector is selected and its topological neighbours on the map are updated. The final results are that the neighbouring neurons have similar weight vectors (Zhong et al. 2005). In more detail, the internal process of SOM can be divided into the following steps (Zhong et al. 2005, Zio & Popescu 2006a, Gonçalves et al. 2011):

1. Initialization: in which random values are chosen for the initial weight vector $\vec{w}_j(0)$ of each neuron *j*, $j = 1, \ldots, \ell$ in the output layer, and
2. Training the map: that is based on three principles repeated for *NI* iterations (Kohonen 1997, Araujo & Barreto 2002):
   - Competition: in which a competition between all the ℓ neurons for each input vector *x* is done, with the winning neuron being called the Best Matching Unit (BMU) for which the Euclidean distance $\|\vec{x} - \vec{w}_j\|$ is minimized. The BMU index for the corresponding input vector *x* is denoted by $i(x)$.
   - Cooperation: in this process, the neighbors of the BMU of the corresponding input sample *x* are selected. This is done according to the topological neighborhood function $h_{j,i}(x)$. A typical choice of this function is the Gaussian function $h_{j,i}(x) = exp(-d^2_{j,i}/2\sigma^2)$, where $d_{j,i}$ is a lateral distance between the winning neuron *i* and neuron *j*, and σ is the neighborhood radius. The neighborhood shrinks gradually with time, i.e. number of iterations, according to a time constant τ_1.
   - Adaption: in which the weights of the BMU neighbors are updated according to the formula $w_j(t+1) = w_j(t) + \alpha(t) \times h_{j,i(x)}(t)[\vec{x} - \vec{w}_j(t)]$, where $\alpha(t)$ is the learning rate. The learning rate decreases gradually with time, i.e. number of iterations, according to a time constant τ_2.

     Since the SOM algorithm is based on Euclidian distances; the scale of the input features is very important in determining the map, so the features in the dataset are usually normalized. For example, each feature to have a unit variance (Vesanto et al. 2000).
3. Visualization and analysis: in which the trained SOM map is shown as a regular lattice of cells, the properties of which show the associated values. For this purpose, several ways can be used such as (Vesanto et al. 2000, Ultsch 2003):
   - Unified distance matrix (U-matrix) that visualizes distances between neighboring map units using indexed colour coding and helps to recognize the clusters of the map:

high values of the U-matrix indicate a cluster boarder, whereas uniform areas of the low values indicate clusters themselves.

Labelling that is typically an empty grid that shows the edges of the map units and helps to categorize the units by giving them names, i.e. labels.

- Hit histogram that shows for a given dataset the distribution of their hits on the U-matrix.

Several indicators can be calculated to measure the quality of the trained SOM. In this work, the following indicators have been considered (Vesanto et al. 2000, Pölzlbauer 2004):

1. Average quantization error (q_e) between training vectors and their BMUs on the map: it is used to measure the data representation accuracy.
2. Topographic error measure (t_e) which is the percentage of data vectors for which the first and second BMUs are not adjacent units: it is used to measure the dataset topology representation accuracy.

In this work, training and testing of the SOM have been performed using the SOMVIS software package, an adds-on for the Matlab SOM toolbox (Vienna University of Technology). The learning has been done under the default settings: the learning algorithm is the batch algorithm with linear initialization (Vesanto et al. 2000).

4 ARTIFICIAL CASE STUDY

In this Section, the results of the application of SOM to an artificial case study are presented and the performance of the method is examined. The artificial case study is designed by simulating $N = 750$ transients representing the start-up behaviors (Baraldi et al. 2013, Al-Dahidi et al. 2014) of $C = 3$ faulty classes (250 transients for each class); exponential, parabolic, and linear. The length of each transient T is 101 time steps. All transients of the same class differ only for different values of the parameters governing the functional behavior e.g. the slope value in the linear behavior, whereas two transients of different classes are in a different functional behavior (Baraldi et al. 2012a, Baraldi et al. 2013).

Figure 2 shows the simulated 750 transients of the three faulty classes. Among these transients, 450 transients have been used to train the SOM, i.e. 150 transients for each class, whereas the remaining transients have been used to verify the performance of the method.

However, the total number of classes, C, and the target outputs i.e. labels are not expected to be known and hence, they will not be used to derive the fault classification but only to verify the performance of the method i.e. unsupervised learning (Zhong et al. 2005).

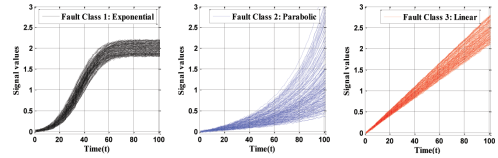


Figure 2. Simulated 750 transients of the three fault classes: exponential, parabolic, and linear.

The definition of the similarity between the transients is performed by considering the functional characteristics of the signal transients, e.g. slope, form, curvature.

In this regard, a statistical indicator feature extraction technique has been used to describe the functional characteristics of the i-th transient by considering its mean μ^i, standard deviation σ^i and skewness s^i, $i = 1, \ldots N$, according to the Equations 1, 2, and 3, respectively (Joentgen et al. 1999):

$$\mu^i = \frac{1}{T}\sum_{\ell=0}^{T-1} x_\ell^i \tag{1}$$

$$\sigma^i = \sqrt{\frac{1}{T}\sum_{\ell=0}^{T-1}\left(x_\ell^i - \mu^i\right)^2} \tag{2}$$

$$s^i = \frac{\frac{1}{T}\sum_{\ell=0}^{T-1}\left(x_\ell^i - \mu^i\right)^3}{\left(\sigma^i\right)^3} \tag{3}$$

In this way, each transient i is transformed into a vector of length 3 and hence, a matrix of size 750×3 is produced when considering the 750 transients. The matrix data has been normalized so that each feature has a unit variance and the SOM map has been trained using the Matlab SOM toolbox under the default settings. The topology of the map was fixed manually to contain 240 neurons, i.e. map size $(h \times w) = 20 \times 12$.

The results of the training phase are shown in Figure 3. The U-matrix (Fig. 3 (left)) shows the distances between the neighbouring map units and thus visualizes the cluster structure of the map. Each value is indicated with a colour, and the colour bar on the right shows what the colours represent: high values on the U-matrix mean large distances between the neighbouring map units, and thus indicate cluster borders, whereas uniform areas of the low values indicate clusters themselves (Vesanto et al. 2000).

From the visual assessment of the U-matrix, it is clear that there are three clusters ($C = 3$) denoted

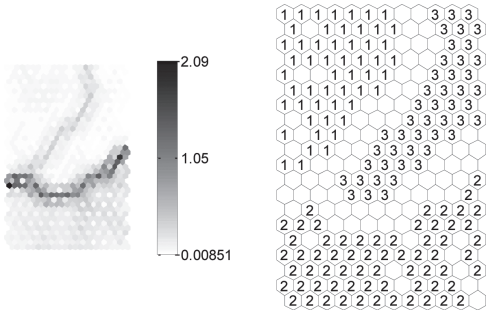


Figure 3. Unsupervised training phase (U-matrix (left) and labelling (right)).

by 1, 2, and 3 as shown in Figure 3 (right): the labelling plot that shows the label of each training transient added to the map to verify the performance of the method.

It is clear that each cluster contains only the transients which have the same functional behaviour represented by the three statistical indicators, μ^i, σ^i, and s^i. It is worth noticing that the distance between fault class 1, i.e. the exponential behaviour, and fault class 3, i.e. the linear behaviour, is small as indicated by the whiter map units compared to the distance between fault class 2 and fault class 3 (blacker map units).

Several measures have been developed to quantify the quality of the trained SOM maps, among these:

- The average quantization error (q_e), in which the average distances of the sample data to their correspondence BMUs is calculated. The actual average quantization error (q_e) of the trained SOM map is 0.06.
- The topological error measure (t_e), in which the respective first and second BMUs of all the data samples, are determined: If these are not adjacent on the map, then, this is considered an error. The total error is then normalized to a range from 0 to 1, where 0 means perfect topology preservation (Pölzlbauer, 2004). The actual topological error (t_e) of the trained SOM map is 0.05.

Finally, 300 test samples, i.e. 100 transients for each fault class, have been used to verify the performance of the trained SOM map: for each test sample, the BMU is located in the map, a counter in the map unit is increased each time it is the BMU and hence its size is increased, i.e. hit histogram (Vesanto et al. 2000). Figure 4 shows the hit histogram of the 300 testing data. It is worth noticing that each of the 100 test samples belonging to one fault class have been grouped inside its corresponding cluster. Hence, the actual misclassification rate is 0%.

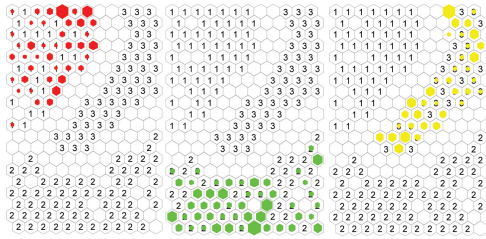


Figure 4. Hit histogram of 300 test samples.

5 MOTOR BEARING CASE STUDY

In this Section, the results of the application of the SOM algorithm to motor bearing datasets are presented and the performance of the method is examined. The bearing data have been collected from the Case Western Reserve University Bearing Data Center (CWRU). Three failure modes have been considered, $C = 3$: inner race, outer race, and ball faults that have been denoted in this work by 2, 3, and 4, respectively.

It is worth mentioning that the experiments were conducted using a 2 hp Reliance Electric motor, and acceleration data was measured at locations both near to and remote from the motor bearings. Faults ranging from 0.007 inches in diameter to 0.021 inches in diameter have been considered and 720 vibration data were recorded for four different operational conditions represented by motor loads from 0 to 3 horsepower (motor speeds of 1797 to 1720 RPM). More details can be found in (CWRU).

Then, five features extracted using Haar basis (Baraldi et al. 2012b) and Symlet6 basis (Chebil 2009) have been used: minimum & maximum Haar wavelet coefficients, Norm Node 5 Symlet6 wavelet, Norm Node 7 Symlet6 wavelet, and Norm Node 12 Symlet6 wavelet. 80% of the total collected data set has been used as the training set, i.e. 576 vectors, whereas the remaining data, i.e. 144 vectors, has been used as the testing set. In this way, the size of the training data is 576×5, whereas the size of the testing data is 144×5. Then, according to the differences in the ranges of the features values, the data has been normalized by applying the natural logarithm and the SOM map has been trained using the Matlab SOM toolbox under the default settings. The topology of the map was fixed manually to contain 375 neurons, i.e. map size $(h \times w) = 25 \times 15$.

The total number of classes, C, and the target outputs i.e. labels will not be used to derive the fault classification but only to verify the performance of the method, i.e. unsupervised learning (Zhong et al. 2005). The results of the training phase are shown

in Figure 5. Again, the U-matrix (Fig. 5 (left)) shows the distances between the neighbouring map units and thus visualizes the cluster structure of the map, whereas the labels plot (Fig. 5 (right)) shows the label of each training transient added to the map to verify the performance of the method (Vesanto et al. 2000). From the visual assessment of the U-matrix, it is clear that there are more than 10 clusters ($C > 10$). This means that each of the original fault classes has been split into three/four sub classes. This can be explained by the fact that the vibration data was recorded for different load levels, i.e. 0 to 3 horsepower (motor speeds of 1797 to 1720 RPM) (CWRU).

For this reason, each main cluster has been divided into several sub clusters each containing the same fault behavior but for different load levels, i.e. 0 to 3 horsepower. Another way to see the classification of the fault data is shown in Figure 6 in which the distance measure has been used to indicate the differences between the map units.

The actual average quantization error (q_e) and the topological error (t_e) of the trained map are calculated and equal to 0.09 and 0.02, respectively.

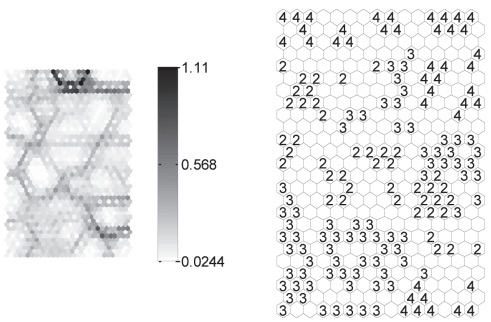


Figure 5. Unsupervised training phase (U-matrix (left) and labelling (right)).

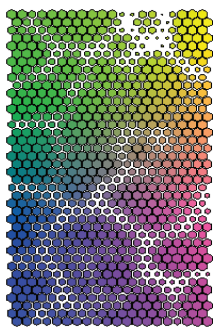


Figure 6. Unsupervised training phase using another visualization tool.

One has to remember that the class information has not been used to derive the fault classification and thus, the obtained results could be suboptimal. However, within the SOM toolbox, it is possible to train the network taking the class information into account, i.e. supervised learning (Vesanto et al. 2000), so the map has been trained, in addition to the 576 training patterns and the five features with the class information, i.e. the labels.

Figure 7 shows the results of the supervised 25×15 trained SOM. Again, from the visual assessment of the U-matrix, it is clear that there are more than 10 clusters, whereas the labelling plot shows the three main fault classes. For each main class, one can determine the sub clusters of each from the U-matrix.

It is worth mentioning that the class of each map unit shown in Figure 7 has been determined by taking the label of the maximum similarly added patterns to that map unit (Vesanto et al. 2000). In this way, the misclassification rate of the 576 patterns has been calculated to be 0.87% (5 out of 576 patterns are misclassified).

Figure 8 shows the hit histogram of the 144 testing data classified into their corresponding clusters. It is worth mentioning that two test patterns belonging to cluster 3 have been classified wrongly as belonging to cluster 4 as indicated in the Figure.

To verify the power of the SOM method compared to other classification methods: the K-Nearest Neighbour (KNN) method has been adopted to classify the same bearing dataset and the misclassification rate has been compared to the misclassification rate obtained by using the SOM method. Both methods, KNN and SOM, have been trained and tested with the same 576 and 144 patterns, respectively. It is worth mentioning that in the KNN method the number of neighbors has been fixed to 24 (i.e. square root of the number of patterns in the training set). Again, using the

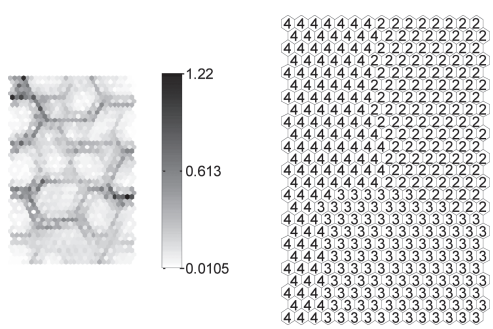


Figure 7. Supervised training phase (U-matrix (left) and labelling (right)).

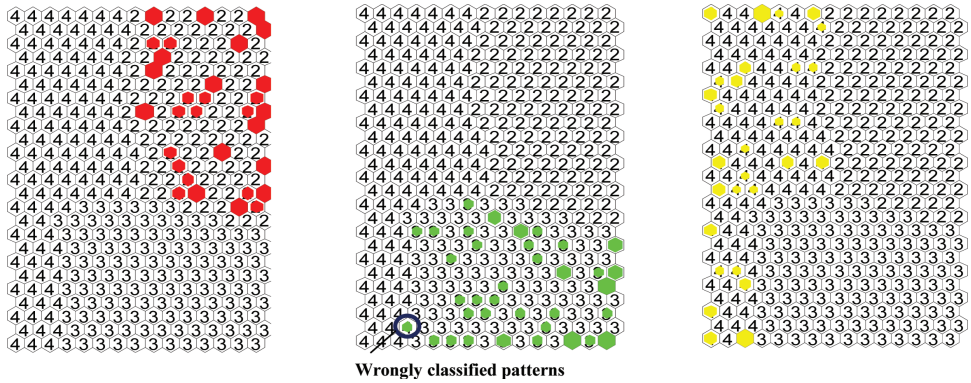


Figure 8. Hit histogram of 144 test samples.

Table 1. SOM quality measures with respect to the different map sizes of the two case studies.

Parameters	Artificial case study			Bearing case study		
Map sizes	5×3	10×6	20×12	10×5	20×10	40×20
q_e	0.34	0.12	0.05	0.34	0.13	0.05
t_e	0.01	0.03	0.06	0.017	0.018	0.019

KNN method, three fault classes have been identified, whereas the misclassification rate has been calculated that as 4.17% (i.e. 6 patterns have been classified wrongly). However, the misclassification rate obtained by using the supervised trained SOM has been calculated as 1.39% (i.e. 2 patterns have been classified wrongly). For more details of the KNN method, refer to (Moosavian et al. 2013).

6 SENSITIVITY ANALYSIS OF SOM QUALITY MEASURES FOR DIFFERENT MAP SIZES

In this Section, the sensitivity of the SOM quality measures with respect to the map size is discussed for the two case studies of Section 4 and 5. According to the size of the dataset in each case; three map sizes have been examined. Table 1 reports the three map sizes and the corresponding SOM quality measures, q_e and t_e, for each case study.

It is worth noticing that as the map units are increased, the average quantization error (q_e) decrease s since the data samples are distributed more sparsely on the map, whereas the values of the topographic error (t_e) increase because an unnecessary fold (train) occurs (Pölzlbauer 2004).

7 CONCLUSIONS

In this work, a diagnostic method based on Self-Organizing Maps (SOM) has been presented. The method has been tested on an artificial case study representing the behavior of equipment during start-up in the presence of different faults. The model has then been applied to a real industrial case study concerning motor bearing degradation data.

The method shows its ability in identifying correct fault classes and classifying the subsequent test data with a low misclassification rate compared to other fault diagnosis methods such as the K-Nearest Neighbour (KNN) method.

In addition, two quality indicators have been calculated for each trained map: the average quantization error, q_e and the topographic error measure, t_e. In addition, their sensitivity to the map size has been investigated. Their sensitivity to other SOM parameters could be an object of future research work.

ACKNOWLEDGEMENTS

This research has been carried out within the European Union Project INNovation through Human Factors in risk analysis and management

(INNHF, www.innhf.eu) funded by the 7th framework program FP7-PEOPLE-2011- Initial Training Network: Marie-Curie Action.

REFERENCES

Abbasion, S., Rafsanjani, A., Farshidianfar, A. & Irani, N. 2007. Rolling element bearings multi-fault classification based on the wavelet denoising and support vector machine. *Mechanical Systems and Signal Processing* 21(7): 2933–2945.

Al-Dahidi, S., Baraldi, P., Di Maio, F. & Zio, E. 2014. Quantification of Signal Reconstruction Uncertainty in Fault Detection Systems, accepted, *the Second European Conference of the Prognostics and Health Management Society 2014, Nantes, France, July 2014*.

Alguindigue, I.E., Loskiewicz-Buczak, A. & Uhrig, R.E. 1993. Monitoring and diagnosis of rolling element bearings using artificial neural networks. *Industrial Electronics, IEEE Transactions on* 40(2): 209–217.

Araujo, A.F. & Barreto, G. 2002. Context in temporal sequence processing: a self-organizing approach and its application to robotics. *IEEE Trans Neural Netw* 13(1): 45–57.

Baraldi, P., Di Maio, F. & Zio, E. 2012a. Unsupervised Clustering for Fault Diagnosis. *Proceedings of Prognostics and System Health Management Conference (PHM2012)*, Beijing, China, 23–25 May 2012: 1–10.

Baraldi, P., Zio, E., Di Maio, F., Pappaglione, L. & Seraoui, R. 2012b. A Wavelet-Based Approach for Condition Monitoring of a Gas Turbine During Start-Up Transients, *PSAM 11 & ESREL 2012 Conference, Joint Probabilistic Safety Assessment and Management Conference and European Safety and Reliability Conference, Helsinki, Finland, 25–29 June 2012*: 1–10.

Baraldi, P., Di Maio, F. & Zio, E. 2013. Unsupervised Clustering for Fault Diagnosis in Nuclear Power Plant Components. *International Journal of Computational Intelligence Systems* 6:4: 764–777.

Case Western Reserve University (CWRU), Bearing data centre. Reference Website accessed on December 2013: http://csegroups.case.edu/bearingdatacenter/pages/welcome-case-western-reserve-university-bearing-data-center-website.

Chebil, J. 2009. Wavelet Decomposition for the Detection of Faults in Rolling Bearing Elements, *Jordan Journal of Mechanical and Industrial Engineering* 3(4): 260–267.

Gao, X.Z. & Ovaska, S.J. 2001. Soft computing methods in motor fault diagnosis. *Applied Soft Computing* 1(1): 73–81.

Gonçalves, L.F., Bosa, J.L., Balen, T.R., Lubaszewski, M.S., Schneider, E.L. & Henriques, R.V. 2011. Fault detection, diagnosis and prediction in electrical valves using self-organizing maps. *Journal of Electronic Testing* 27(4): 551–564.

Gonçalves, L.F., Schneider, E.L., Henriques, R.V.B, Lubaszewski, M., Bosa, J.L. & Engel, P.M. 2010. Fault Prediction in Electrical Valves Using Temporal Kohonen Maps.

Huang, J. 2012. Bearing Fault Diagnosis Using Information Fusion and Intelligent Algorithms, Performance Evaluation of Bearings, Dr. Rakesh Sehgal (Ed.), ISBN: 978-953-51-0786-6, InTech, DOI: 10.5772/51079.

Isermann, R. & Balle, P. 1997. Trends in the application of model based fault detection and diagnosis of technical processes. *Control Engineering Practice* 5(5): 709–719.

Joentgen, A., Mikenina, L., Weber, R., Zimmermann, H.J. 1999. Dynamic Fuzzy Data Analysis based on Similarity between Functions. *Fuzzy Sets and Systems* 105 (1): 81–90.

Kalyan M. Bhavaraju, Kankar, P.K., Satish C. Sharma & Harsha, S.P. 2010. A Comparative Study on Bearings Faults Classification by Artificial Neural Networks and Self-Organizing Maps using Wavelets *International Journal of Engineering Science and Technology* 2(5): 1001–1008.

Klir, G. & Yuan B. 1995. Fuzzy Sets and Fuzzy Logic: Theory and Application. *Prentice Hall, Englewood Cliffs, NJ*.

Kohonen, T. 1997. Self-organizing maps. *Series in information sciences, Springer, Heidelberg* 30.

Kowalski, C.T. & Orlowska-Kowalska, T. 2003. Neural networks application for induction motor faults diagnosis. *Mathematics and Computers in Simulation* 63: 435–448.

Li, B., Chow, M.Y., Tipsuwan, Y. & Hung, J.C. 2000. Neural-network-based motor rolling bearing fault diagnosis. *Industrial Electronics, IEEE Transactions on 47*(5): 1060–1069.

McDonnell, D., Balfe, N., Al-Dahidi, S. & O'Donnell, G.E. 2014. A Model for Human-Centred Decision Support System Design in PHM, accepted, *the Second European Conference of the Prognostics and Health Management Society 2014, Nantes, France, July 2014*.

Moosavian, A., Ahmadi, H., Tabatabaeefar, A. & Khazaee, M. 2013. Comparison of Two Classifiers; K-Nearest Neighbor and Artificial Neural Network, for Fault Diagnosis on a Main Engine Journal-Bearing. *Shock and Vibration*, 20(2): 263–272, doi:10.3233/SAV-2012-00742.

Ng, S.S., Tse, P.W. & Tsui, K.L. 2014. A One-Versus-All Class Binarization Strategy for Bearing Diagnostics of Concurrent Defects. *Sensors 14*(1): 1295–1321.

Önel, I.Y., Dalci, K.B. & Senol, I. 2006. Detection of bearing defects in three-phase induction motors using Park's transform and radial basis function neural networks. Sadhana 31(3): 235–244.

Pölzlbauer, G. 2004. Survey and comparison of quality measures for self-organizing maps. *Fifth Workshop on Data Analysis*: 67–82.

Samanta, B. & Al-Balushi, K.R. 2003. Artificial Neural Networks based fault diagnostics of rolling element bearings using time domain features. *Mechanical Systems and Signal Processing* 17: 317–328.

Schoen, R.R., Habetler, T.G., Kamran, F. & Bartheld, R.G. 1995. Motor bearing damage detection using stator current monitoring. *IEEE Trans. Ind. Appl.* 31: 1274–1279.

Sugumaran, V., Muralidharan, V. & Ramachandran, K.I. 2007. Feature selection using decision tree and classification through proximal support vector machine for fault diagnostics of roller bearing. *Mechanical Systems and Signal Processing* 21(2): 930–942.

Tamilselvan, P., Wang, P. & Pecht, M. 2013a. A multi-attribute classification fusion system for insulated gate bipolar transistor diagnostics. *Microelectronics Reliability* 53(8): 1117–1129.

Tamilselvan, P. & Wang, P. 2013b. *Failure diagnosis using deep belief learning based health state classification. Reliability Engineering & System Safety* 115: 124–135.

Ultsch A. 2003. U-Matrix: A Tool to visualize Clusters in high dimensional Data, *Dept. of Computer Science University of Marburg, Research Report* 36.

Vesanto, J., Himberg, J., Alhoniemi, E. & Parhankangas, J. 2000. SOM toolbox for Matlab 5. *Helsinki, Finland: Helsinki University of Technology*.

Vienna University of Technology: Institute of Software Technology and Interactive Systems. Data Mining with SOMVIS. Reference Website accessed on December 2013: http://ifs.tuwien.ac.at/dm/somvis-matlab/index.html.

Wang, H.Q. & Chen, P. 2007. Fault Diagnosis of Centrifugal Pump Using Symptom Parameters in Frequency Domain. *Agricultural Engineering International: the CICR Ejournal* 9: 1–14.

Wang, J.P. & Hu, H.T. 2006. Vibration-based Fault Diagnosis of Pump Using Fuzzy Technique. *Measurement* 39: 176–185.

Yang, D.M., Stronach, A.F., MacConnell, P. & Penman, J. 2002. Third-order spectral techniques for the diagnosis of motor bearing condition using artificial neural networks. *Mechanical systems and signal processing* 16(2): 391–411.

Yu, Y., Dejie Y. & Junsheng C. 2007. A fault diagnosis approach for roller bearing based on IMF envelope spectrum and SVM. *Measurement* 40: 943–950.

Zhong, F., Shi, T. & He, T. 2005. Fault diagnosis of motor bearing using self-organizing maps. *Electrical Machines and Systems, ICEMS 2005, Proceedings of the Eighth International Conference on* 3: 2411–2414.

Zio, E. & Popescu, I.C. 2006a. Fault Diagnosis of Nuclear Components by Kohonen Self-Organizing Maps. *Proceedings of the Eighth International Conference on Probabilistic Safety Assessment & Management (PSAM)*.

Zio, E. & Gola, G. 2006b. Neuro-fuzzy Pattern Classification for Fault Diagnosis in Nuclear Components. *Annals of Nuclear Energy* 33(5): 415–426.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Selected safety aspects of polymer composites with natural fibres

A. Krzyżak & D. Vališ
University of Economy and Innovation, Lublin, Poland

ABSTRACT: The paper deals with selected aspects of safety features of polymer composites with natural fibres. These kinds of composites have been starting to be used quite widely in the technical industry like automotive and aerospace, etc. Our paper will present approaches for selection of those properties and features of polymer composites which are to be used for an event cause description. In this paper we will present selected mechanical properties and qualities which usually create the fundamental point of view in terms of decision about the applicability of polymer composites. The materials measures like strength, hardness and elasticity play vital role in terms of physical in-situ applicability. Such properties are firstly observed and assessed in terms of system and object safety parameters.

1 INTRODUCTION

Failure is a term widely used in technical practice especially concerning dependability theory. It is inevitable to realize that a failure is of key importance for operation and function of technical items. Theory and practice in particular shows that failures occur under different situations, various circumstances, ranging conditions, etc. For safety and reliability practitioners failure is a basic term in theory, and it is key and essential for observing stochastic relations of item behaviour. It is an event which is used in probability theories on a general level; the term probability event is used. In dependability theory it is necessary to realize the fact of failure as a stochastic term, to understand its meaning, and to understand other links. What we need to catch up here is the meaning and relation to safety. The requirements on polymer composites are to be failure safe or to prevent further failure propagations—once failures occur. For more details see e.g. Elsayed 1996, Meeker & Luis 1998, Stodola et al. 2013, Werbinska-Wojciechowska 2013, Werbińska 2007.

It is inevitable at some point failure (of equipment, a device, an item or a system) will occur. The reasons for this occurrence can vary. Usually the main factor is that the applied load exceeds the dimension/robustness of the product. The load can be purely mechanical (i.e. force, tension), purely electrical (i.e. power, electromagnetic field), purely chemical (such as the effect of chemical substances), general physical (i.e. warmth, radiation), a combination of these or of a totally different nature. Whenever the applied load exceeds the assumed dimension of the item, unwanted (usually irreversible) processes start, and sooner or later a failure occurs. The load can be one time load or it can be applied a number of times. Concerning the first instance, overload failure will occur and in the second case fatigue failure will occur. As time passes, the product could become weaker for any one of many reasons (unless a failure occurs immediately). Our concern is focused on polymer composites characteristics which—influenced by operational environment—may lead to failures without expecting them.

In describing failures there are many factors and characteristics to consider. One of which is the failure profile—for general principles see Figure 1. This profile depends on the failure causes; the failure manifestations (namely the ways and mechanisms of failure) and the failure consequence. These failure causes can be design failures, manufacturing failures, overstress failures, misuse failures or degradation failures. The failure manifestations may be random, gradual, sudden, common cause, primary, secondary, intrinsic or extrinsic. The consequences could be insignificant, marginal, minor, major, critical, catastrophic or also scaled differently. For more

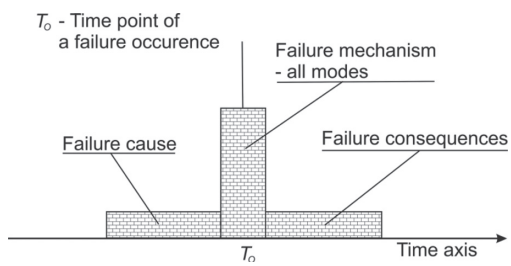


Figure 1. Failure profile—essential approach.

details see e.g. Blishke 2000, Modares et al. 1999, Woch & Leski 2014, Woch 2013.

While observing a technical item—the polymer composites in our case, the main concern is on the possible causes of failures and their development over time which might result from a failure occurrence. Theoretically dealing with failures, it is possible to describe their causes, nature of occurrence, process of development, and modelling of these failures is possible at the same time.

A range of importance and numerical values associated with the failures can be determined. However, the fundamental desire is to eliminate failure occurrence, reduce its frequency, limit the number of its occurrences over a specified time period or in relation to another observed dependent quantity (e.g., cycles, etc.). The ultimate intention is to be able to determine failure occurrence exactly, simply, the aim is to get a better profile of an observed item from the view of its dependability and related properties.

Furthermore, there is a necessity to be able to describe the possible classes of failures, their profiles, development, consequences, and other relations which might be important for dependability theory and especially for this paper itself.

Due to lack of knowledge in the area of composite materials our main concern is to determine principles for failure occurrence. We focus on assessment in the area of polymer composites with natural fibres where both failure causes and mechanisms will be investigated. As the composite materials are intended for using like safety measures e.g. covers, cases, shields, walls, etc. we try to investigate possible failures caused by hard impact onto the material structure. This impact is simulated in lab by concentrated mechanical load of defined features and characteristics. The composite covers are used in order to protect the surroundings of technical system both against failure propagation and impact from outside. Therefore the failure occurrence in the polymer composites with natural fibres will be our main concern from the safety aspects point of view.

1.1 *Current situation in terminology*

Due to the ISO/IEC representatives, industrial experts and national bodies there is a set of terminology related to the issue of failure. Failure according to the present version of the IEC 60050 (191) is defined as: "termination of the ability of an item to perform a required function". There are three things to note: (1) After failure the item has a fault; (2) Failure is an event, as distinguished from fault, which is a state; and (3) This concept as defined does not apply to items consisting of software only. Failure according to the newly upgraded version IEC 60050 (191) is defined as: "loss of ability to perform as required". It is noted that: (1) When the loss of ability is caused by a pre-existing condition, the failure occurs when a particular set of circumstances is encountered; (2) A failure of an item is an event, as distinct from a fault of an item, which is a state; and (3) Qualifiers may be used to classify failures according to the severity of consequences, such as catastrophic, critical, major, minor, marginal and insignificant, the definitions depending upon the field of application. We fully respect this concept regarding the polymer composites with natural fibres.

It results from these definitions and further analysis that the term "failure" will be in terms of polymer composites understood as an event which leads straight to either a partial or complete loss of ability of an item to fulfil a required function. There is currently in process the modification and updating of terminology related to this topic, and hence the existing view of the understanding of these concepts (failure and related facts) has been changing.

While working with the term failure, as well as with relating states, it is necessary to take the current terminology mismatch into account and to adapt possible decisions to it. The possibility of a realized change has to be accepted along with all the resulting consequences. Unfortunately, this change will violate the understanding of all existing terms/disciplines introduced so far that deal with failure and dependability.

Nevertheless our concept of understanding failures of polymer composites with natural fibres will be oriented on the identification of failure causes. The investigation shall open the area where safety aspects of failures of polymer composites with natural fibres will be clearer.

1.2 *Influence of the failure*

When considering a failure of polymer composites with natural fibres it is necessary to draw attention to some related events. As the term failure relates to the prevention of an item's ability in performing a required function it is clear that this inability of a system or a product to operate in a required way is a key term determining a failure.

Based on many studies and approaches a factual scale of individual functions description was formed for a system. On the basis of these assumptions it is also essential to distinguish the influence of a failure on a function performed by an item. A failure occurrence might affect the range of the function especially when main observed system serves as safety element. An outline of item functions is provided to make the understanding much easier, though it should be remembered that failure

occurrence is not strictly limited to the type of item function.

A required function specifies an item task. A correct, exact and unequivocal definition is a primary starting point for all dependability definitions as well as for a right failure definition. Operation conditions affect significantly both dependability and especially possible failure occurrence, hence the reason why they have to be determined very thoroughly. We concentrate on the main and support functions (Valis & Bartlett 2010) in terms of failure occurrence and function loss of polymer composites with natural fibres.

The required function and/or operation conditions might be time and operation environment dependent. In this case a mission profile has to be determined and all safety and dependability viewpoints have to be related to it. A representative mission profile and corresponding dependability targets have to be stated in the item's specification. The mission duration is often/usually considered as a parameter *t,* that is time. The dependability function—especially the reliability function is designated as R(t). R(t) is the probability that no failure at item level will occur in the interval (0;t⟩, often with the assumption R(0) = 1, meaning that at time $t = 0$ the item was in the state of operation. For clearer statement we will also work here with pdf $f(t)$. In order to avoid confusion a distinction between predicted and estimated (assessed) dependability should be made on the basis of a real evaluation during operation or tests. The predicted reliability—failure free interval or failure occurrence load point is calculated on the basis of the item's structure. The estimated reliability is specified on the basis of a statistical evaluation of reliability tests. Our experimental data and procedure for gaining them will be described further. The field data will be collected thank to the mechanical experiments with polymer composites with natural fibres while operating and environmental conditions will be changed. The change of environmental conditions is to serve the acceleration of system deterioration and technical life shortening. This will be possible thank to the climatic chamber used for experiments. We apply specific climate environment in the chamber for degradation and deterioration of the polymer composites with natural fibres. The climate will be represented by increased or decreased temperature with humidity influence in positive temperatures range.

1.3 *Failure occurrence cause*

According to the IEC 60050 (191) the circumstances occurring during design, manufacture or use which have resulted in a failure are the cause of a failure. To decide how to prevent a failure or its reoccurrence it is necessary to know the cause of a failure. This is the main concern of our assessment of polymer composites with natural fibres. Failure causes can be classified in relation to the life cycle of the system. The cause of a failure can be intrinsic, due to weaknesses in the item and/or wear out, or extrinsic, due to errors, misuse or mishandling during the design, production and especially the use itself. Extrinsic causes often lead to systematic failures which are deterministic and might be considered like defects (dynamic defects in software quality). Defects are present at $t = 0$, even if they cannot be discovered at $t = 0$. Failures always seem to appear in time, even if the time to failure is very short as it can be with systematic or early failures.

The main causes according to Valis & Bartlett 2010 can be further explained. However we will concentrate only on:

– design failure,
– weakness failure,
– manufacturing failure,
– ageing failure.

These causes are shown diagrammatically in Figure 2. Design failure occurs due to inadequate design. It is basically any failure directly related to the item design. It means that due to the item design a part of the whole degraded or got damaged and this resulted in a failure of the whole. Weakness failure occurs due to weakness (internal) inherent or induced in the system so that the system cannot stand the stress it encounters in its normal environment. Manufacturing failure is caused by nonconformity during manufacturing and processing. It is basically any failure caused by faulty processing, or inadequate manufacturing, or an error made while controlling the process during manufacturing, tests and repairs. An ageing failure is caused by the effects of usage and/or age.

In further steps principles of failure occurrence investigation in the area of polymer composites with natural fibres will be presented.

The investigation will cover laboratory mechanical tests which will be performed on composited materials after accelerated environmental influence.

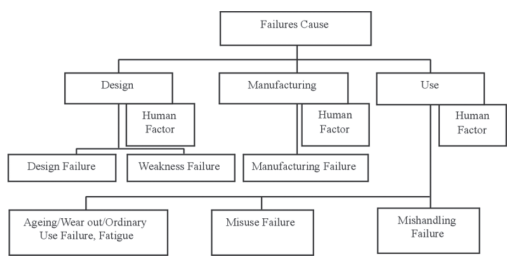


Figure 2. Typical failure causes.

At the moment of this paper submission several climatic tests on composite materials have been completed (see details in the proposed methodology bellow) and mechanical tests launched. Since this paper is describing a possible methodology for composite materials investigation the results describing composite materials properties in terms of safety features will be presented at the conference presentation.

1.4 *Context with risk assessment*

Since we are aware of co-relation of the obtained outcomes with risk area we propose following principles. We expect the risk here is again the combination of probability of undesired event occurrence and consequences measure of the composite material. We do not take into account the sometimes used discover/detection ability neither the countermeasures. Therefore for further calculation the probability of composite material fracture at certain level of load will be taken into account.

Our point of view on risk therefore looks following way:

$$\text{Risk} = \text{Probability} \times \text{Consequences} \tag{1}$$

We respect that the probability will be delivered in the numerical form. Therefore also the consequences will be described in the quantitative form in order to perform further description of the risk. For more details please refer e.g. to Vališ et al. 2011.

2 PROPOSAL OF ESSENTIAL STEPS IN METHODOLOGY FOR ASSESSMENT OF A POLYMER COMPOSITES FAILURE OCCURRENCE

2.1 *Properties of laminate*

Composite materials consist of at least two components constituting the reinforcement and the matrix. Laminates are specific group of composites with reinforcement layer. They are used for structural components such as a plate, which are loaded on the surface in points. The properties, characteristics, structure and texture of the laminates-composites was given and guaranteed during the manufacturing process. For more details see e.g. Błażejewski et al. 2010, Krzyżak 2013.

The active forces acting on the laminate are generally orthogonal to surface of the laminate. Plates are loaded with static and dynamic forces. Therefore there is a need for research on the flexural strength and impact resistance. Currently there are used significant quantities of composite reinforcements with plant origin such as for example, kenaf, jute, flax. The increase in the volume fraction of the strengthening increases flexural strength. In some cases, it is important the way how to prepare the production of composites, and increase the adhesion in combination two materials: fibre—resin. Yousif and others (Yousif et al. 2012) showed that reinforcement of epoxy with treated kenaf fibres increased the flexural strength of the composite by about 36%, while, untreated fibres introduced only 20% improvement. Often natural fibres of plant origin are used as reinforcement in a hybrid combination with, for example, glass fibre (Ramesh et al. 2013), carbon fiber (Noorunnisa Khanam et al. 2010) or others natural fibers (Jawaida et al. 2010). This increases the mechanical strength of the laminates, which is advantageous in view of the potential use of natural composites.

With respect to the laminates as a structural material, regardless of the type of reinforcement, there are known some behaviour characteristics during the mechanical loading of laminates. Composites with woven reinforcement demonstrate (Dauda et al. 2009) a linear relationship between stress and deformation. Whereas the reinforcement of laminates in the form braided reinforcement show a non-linear dependence is determined by an angle of orientation of the fibre bundles with respect to the axis of symmetry. The increase in flexural strength and modulus values affects the volume fraction of fibres in the composite volume, and the surface density of the strengthening.

The volume fraction of fibres in the composite greatly affects a method of producing composites. Composites produced by hand lay-up method have the most resin. Therefore, their strength is relatively small because of the small percentage of fibres. In addition, a significant share of the resin also contributes to their rapid destruction. The resin in a larger volume is fragile and easily undergoes cracking under stress. The lack of continuity of the resin matrix leads to the direct and uniformly distributed impact of the load on the reinforcing fibres of the composite, causing their premature failure. Hand lay-up method is fraught with a total lack of the possibility of eliminating the defects of the composite structure in the form of air bubbles, which significantly decrease the mechanical properties of composites. Other methods such as pressing, vacuum bagging method, and the infusion method with other more technologically and machine advanced—like winding methods or the autoclave. Such methods allow greater or lower extent to the elimination formation of defects in the structure. They also contribute to an increase in the volume fraction of the strengthening and greater repeatability in production. The principles in listed methods reduce the large measurement

errors that are typical for measurements by most physical and mechanical properties of all polymer composites. Measurement error may become large while it does not show any statistically significant changes in the properties despite considerable differences in the average value of the flexural strength (de Deus et al. 2005).

Natural fibres unfortunately have a high water absorption and susceptibility to deformation under the influence increased temperature. Composites reinforced natural fibres demonstrate significant decrease in the mechanical strength even at 75°C (Kaundal et al. 2012).

Laminates are subject to mechanical damages as a result of the creation of dynamic, cyclic loads. The sudden point impact of quite a considerable force over a large area of the laminate causes a surface and internal damages to the composite structure at the impact's place. Surface damage consists in break of the continuity of the matrix and its possible chipping. Cracks of resin at the impact point are in general a network of densely arranged features. In contrast, outside the place of impact cracks usually move more or less radially from the point of impact and direction collapses in places of occurring defects in the structure. Furthermore by local action of sudden forces there are also ruptures of brittle fibres, for example, glass fibres (Xu et al. 2012). As a result of impact is also created delamination between each inner reinforcement layers (Sevkat et al. 2009). At each successive dynamic load there has been increasing internal delamination, increasing damage of surface and brittle failure of the fibre, until complete destruction of the laminate which occurs at the moment of puncture (Evci & Gülgeç 2012). In the case of stroke during impact testing according to standards such as standard Charpy method, occur usually to fracture of laminate samples.

2.2 *Methodology*

Polymer composite materials which we investigated on failure occurrence are made on the basis of natural fibres, such as linen, cotton and jute. As the matrix material used epoxy resin R70 with hardener H71 often used for laminating contact while the texture is determined in advance. Jute fabric has a surface density in level 340 $g \cdot m^{-2}$, linen fabric 320 $g \cdot m^{-2}$ and cotton fabric 130 $g \cdot m^{-2}$. For each reinforcement three components types have been prepared. Laminates structures with two, four and six layers have been prepared.

The resin has a relatively low viscosity to improve its adhesion to the non-homogeneous natural fibres. The process of manufacture of polymer composites containing fibres of natural origin has been based on the method of contact lamination process in combination with pressing process.

High compression pressure during the press process guarantees achievement of repeatable product type. We want to prepare pieces of composites which fit dimensionally and will also fulfil the required quality. The air bubbles remaining in the structure of laminates during the manufacture of laminates, especially those with fibres of non-homogeneous geometry, are important factor that influence the quality and formation damage during their use. Each empty space is a defect, from which a crack may develop leading to lower mechanical properties and the bulk destruction of the composite. Each empty space is a defect, from which it can develop a crack leading to the total destruction of the composite.Therefore the proper manufacturing procedure helps to limit the number of these defects to a minimum. High compression pressure will push the resin voids and reduce their number, but their complete elimination by using natural fibres is not possible.

Polymer composites based on natural fibres were produced with an equal number of material layers 2, 4 and 6. A small number of layers allow keeping possibility of modelling the shape of the laminates easily in the application to cover curves into bows. For this reason it is very important appointment flexural strength of laminates, as well as the maximum angle of deflection and angle deflection from the destruction of the sample. Research will be carried out by using standard EN ISO 14125 Fibre-reinforced plastic composites—determination of flexural properties. Brittle fracture of the resin takes place during flexion and bending of the laminates based on glass fibres, carbon or jute fibres with small elongation (Sgriccia, Hawley & Misra 2008).

Brittle fractures of fibres in the lower layers of the laminate structure can be also observed as the results of further flexure and bending. This is the same principle to breaching the strength of the whole laminate. Breaking the continuity fibres is unacceptable from the point of view of the further exploitation of the laminate, as a construction material.

Natural fibres are characterized by high water absorption. It is therefore necessary check the flexural strength of laminates during their using in terms of exposure to the effects of water in the air with a relative humidity of 75%. Moreover, in the case of polymeric materials important factor in determining functional characteristics is temperature of they use. Simultaneous interaction of high humidity at variable air temperature from –25°C to +95°C during a month period of time, will allow the estimation of the probability of a failure in a simulated operational environment of use of the laminate.

Our tests of composite materials were set up to simulate accelerated life usage. The equipment used for the climatic testing is Vötsch chamber VC^3 7034. Therefore we organised two climatic tests so far. First one was performed on the three types of composites samples (for exact composition see above) at the temperature –25°C for a month. The second test has been performed at the temperature 95°C and relative humidity 75%. In both instances significant influence of the climatic condition on the mechanical properties of the materials are expected. Flexural test will go by using testing machine for static tests Zwick Z100. Speed of traverse will be constant at 5 mm/min. Flexural stresses σ_f can calculate based on formula:

$$\sigma_f = \frac{3FL}{2bh^2} \tag{2}$$

where: F—force [N], L—length of sample between the supports [mm], b—width [mm], h—thickness of sample [mm].

Deformation ε on the outside surface of the sample is given by:

$$\varepsilon = \frac{6sh}{L^2} \tag{3}$$

where s is band deflection [mm].

After the mechanical test we expect having set of results presenting initially level of mechanical stress corresponding to fracture of the composite material. Secondary we will create probability distribution, where the stress will be continuous variable representing fracture occurrence. This will be our initial information to the equation (1) for determining the risk level in case if mechanical impact into the composite shield occurs. Investigation the possible consequences in the equation (1) is not the goal of this paper. Both graphical and numerical results will be presented during the conference.

2.3 *Conclusions*

The "green" composites are very important new engineering materials. Natural laminates are a good possibility for laminates reinforcement with glass fibres. Laminates with glass fibres have higher mechanical properties, but natural composites are more friendly to ecology. Composites with natural fibres as for example jute, kenaf, flax or cotton, have an application in means of transport. The significant properties of laminates in their application are flexural and impact strength. This properties of samples will be measurement when the will be ageing one month by different value of air temperature and by constant value of relative humidity.

The safety aspect of these kind of materials are based on the area of their utilisation and application. In this instance we investigate and focus on their resistance against mechanical load—dynamic impact. Their strength, stability and flexibility are important in order to guarantee no-propagation of failure occurred. So the composites might be indirectly responsible for propagation of initial failures which may cause secondary failures or domino effects. However if the initial failure is severe the composites used as a shield for example are supposed to stop it. Our proposed methodology shall present approach how failure occurrence once emerging may influence the safety features of the whole system. It will extend the principles published e.g. in (Babiarz 2006, Babiarz 2014, Rak & Pietrucha 2008, Stodola & Mazal 2012, Studzinski & Pietrucha-Urbanik 2012).

ACKNOWLEDGEMENTS

This paper has been prepared with support of the project nr 4/2013-14 of the University of Economy and Innovation, Lublin, Poland.

REFERENCES

Babiarz B. 2014 (in prep.): *Heat supply system reliability management*. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Babiarz B. 2014 (in prep.): *Risk assessment in heat supply system*. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Babiarz, B. 2006: *An introduction to the assessment of reliability of the heat supply systems*. International Journal of Pressure Vessels and Piping 83(4): 230–235.

Błażejewski W., Gąsior P., Kaleta J., Krzyżak A. & Rybczyński R. 2010: *Koncepcja Konstrukcji nośnej lekkiego kompozytowego mostu pływającego do transportu kołowego.* Autobusy 11, 6:11.

Blishke, W.R. 2000. *Reliability: Modelling, Prediction, and Optimisation.* New York: John Willey.

Dauda B., Oyadiji S.O. & Potluri P. 2009: *Characterising Mechanical Properties of Braided and Woven Textile Composite Beams.* Appl Compos Mater 16: 15–31.

De Deus J.F., Monteiro S.N., d'Almeida J.R.M. 2005: *Effect of drying, molding pressure, and strain rate on the flexural mechanical behavior of piassava (Attalea funifera Mart) fiber–polyester composites.* Polymer Testing 24: 750–755.

Elsayed, A.E. 1996. *Reliability Engineering*. New York: Addison-Wesley.

Evci C., Gülgeç M. 2012: *An experimental investigation on the impact response of composite materials*. International Journal of Impact Engineering 43: 40–51.

Jawaida M., Abdul Khalil H.P.S., Abu Bakar A. 2010: *Mechanical performance of oil palm empty fruit bunches/jute fibres reinforced epoxy hybrid composites*. Materials Science and Engineering A 527: 7944–7949.

Kaundal R., Patnaik A., Satapathy A. 2012: Comparison of the Mechanical and Thermo-Mechanical Properties of Unfilled and SiC Filled Short Glass Polyester Composites. Silicon 4: 175–188.

Krzyżak A., Komsta J. 2013: Kompozyty wzmocnione włóknem długim. *Materiały Kompozytowe* 2: 18–21.

Meeker, W.Q. & Luis, A.E. 1998. *Statistical Methods for Reliability Data*. New York: John Willey.

Modares, M., Kaminskyi, M. & Kritsov, V. 1999. *Reliability Engineering and Risk Analysis. A Practical Guide*. New York: Marcel Dekker.

Noorunnisa Khanam P., Abdul Khalil H.P.S., Jawaid M., Ramachandra Reddy G., Surya Narayana C., Venkata Naidu S. 2010: *Sisal/Carbon Fibre Reinforced Hybrid Composites: Tensile, Flexural and Chemical Resistance Properties*. J Polym Environ 18: 727–733.

Rak J. & Pietrucha K. 2008: *Risk in drinking water quality control*. Przemysl chemiczny 87(5): 554–556.

Ramesh M., Palanikumar K., Hemachandra Reddy K. 2013: *Mechanical property evaluation of sisal–jute–glass fiber reinforced polyester composites.* Composites: Part B 48:1–9.

Sevkat E., Liaw B., Delale F., Raju B.B. 2009: *Drop-weight impact of plain-woven hybrid glass–graphite/toughened epoxy composites*. Composites: Part A 40: 1090–1110.

Sgriccia, N., Hawley, M.C. & Misra, M. 2008. Characterization of natural fiber surface and natural composites. *Composites Part A: Applied Science and Manufacturing*, 39(10): 1632–1637.

Stodola, P., Mazal, J. 2012: *The Trapezoid and S-curve for Real-time Servomotors Control*. In Proceedings of the 15th International Conference on Mechatronics—Mechatronika 2012. Prague: Czech Technical University in Prague, 165–168.

Stodola, P., Mazal, J., Mokrá, I. & Podhorec, M. 2013: *The Real-Time Control Algorithm and Control Curves for Servomotors*. International Journal of Circuits, Systems and Signal Processing. 7(2): 118–125.

Studzinski, A. & Pietrucha-Urbanik, K. 2012: *Risk Indicators of Water Network Operation*. Chemical Engineering Transactions 26: 189–194.

Valis, D. & Bartlett, L. 2010. The Failure Phenomenon: A Critique. *International Journal of Performability Engineering*, 6(2): 181–190.

Vališ, D., Mlynczak, M. & Nowakowski, T. 2011. How to manage risk? An approach based on standards. *Maintenance problems*, 1(80): 137–148.

Werbinska, S. 2007. *Interactions between logistic and operational system—an availability model. Risk, reliability and societal safety.* Eds. Terje Aven, Jan Erik Vinnem. Leiden: Taylor and Francis, 2045–2052.

Werbinska-Wojciechowska, S. 2013. *Time resource problem in logistics systems dependability modelling*. Eksploatacja i Niezawodnosc—Maintenance and Reliability 15(4): 427–433.

Woch, M. & Leski, A. 2014 (in prep.): *Risk analysis of the point on aging aircraft structure.* Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Woch, M. 2013. *Analysis of operating loads on an aircraft's vertical stabilizer on the basis of recorded data,* Chemical Engineering Transactions 33: 643–648.

Xu L.R., Krishnan A., Ning H., Vaidya U. 2012: *A seawater tank approach to evaluate the dynamic failure and durability of E-glass/vinyl ester marine composites.* Composites: Part B 43: 2480–2486.

Yousif B.F., Shalwan A., Chin C.W., Ming K.C. 2012: *Flexural properties of treated and untreated kenaf/epoxy composites*. Materials and Design 40: 378–385.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Application of selected diffusion processes on system state assessment

D. Vališ
University of Defence, Brno, Czech Republic

O. Pokora
Masaryk University, Brno, Czech Republic

ABSTRACT: The aim of the article is to apply selected diffusion processes in order to estimate system technical life. As we possess reasonably big set of field data the system residual technical life might be well estimated statistically. It includes the information about particles contained in oil which testify to oil condition as well as system condition. We focus on the particles which we consider to be interesting—both from the point of view towards the oil itself and also towards the system state and condition. This kind of information has good technical and analytical potential which has not been explored well yet. The way of modelling in this article is based on the specific characteristics of diffusion processes, namely the Wiener processes. Following the modelling results we could in fact set the principles of "CBM—Condition Based Maintenance", mission planning, life cycle costing, etc.

1 INTRODUCTION

Reliability, safety and availability of complex and time dynamic systems—like mechatronic, communication, space and smart systems—has attracted more and more attention in recent years—see, e.g. (Labeau 2000). The systems we would like to present work in various and mostly adverse operating conditions due to their applications. Therefore it is hardly possible to analyse the reliability of individual system using prior complex reliability tests, the historical pieces of information of other similar systems, or using expert judgement. Dependability characteristics are of our interest as we are concerned of a system reliability and availability level. However, the reliability and availability level of systems under our observation is the area of high interest for designers and engineers so that they could monitor condition and make decisions about maintenance. Based on the practical development in this area, it emerges that condition-based maintenance has become an attractive research area over the last decades—see, e.g. (Park 1993, Maillart & Pollock 2002, Yang 2003, Li & Pham 2005).

At present there is a tendency to change the format of technical maintenance. Preventive Maintenance (PM) at fixed intervals has been abandoned and condition based maintenance has been introduced instead. This trend might be followed only on condition that high-quality data on system condition is available. In technical literature, e.g. (Ghasemi et al. 2010a,b, Medjaher et al. 2012, Gebrael & Pan 2008, Ghasemi et al. 2010), there are different ways of using direct and indirect diagnostic data. There are introduced the possibilities of vibrodiagnostics, thermal radiation, and also tribo-diagnostics there. As for the vibro-diagnostics and the thermal radiation, they frequently appear in existing publications and scientific papers. Regarding the tribodiagnostic data, it has been assessed mainly empirically, restrictedly and by specialists.

Since specific types of technical equipment have been observed extensively, a big amount of data is available for the analysis. This special technical equipment is used in very harsh conditions. To have the observed technical equipment operating, it is important not only to have an adequate maintenance system, but also to operate under specific conditions, to plan and complete the mission.

1.1 *Motivation*

There were a few reasons for starting this research. The main reason was obviously to save costs during the phase of operation and maintenance of the observed technical equipment. It is rather clear that both the operation and the maintenance have the potential to save costs. The question is how the potential might be identified. The technical literature currently available shows us that the condition based maintenance is a right alternative. However, to introduce this type of maintenance, a certain amount of high-quality data as inputs should be available.

During the operation of the observed technical equipment in previous years, a lot of tribodiagnostic data were obtained. And the truth is that these data have not been used efficiently. The authors of this article identified the potential of these data and applied it in further analysis.

Another reason for assessing and searching for RUL (Residual Useful Life) was to find a lot more adequate model than the ones introduced earlier. Previous models are based on a regression analysis and fuzzy logic which has the potential to support regression models. What we are trying to do in the paper, is to present a new view on the same issue which is supposed to either support the conclusions or disprove them. Therefore we assume that First Hitting Time driven by Wiener process with drift is suitable tool for Residual Useful Life. Usage of Wiener process was motivation by generalisation of random walk suitable for this technical system.

2 OBJECTS OF DIAGNOSTICS AND OIL DIAGNOSTIC METHODS

The assumed objects of diagnostics are in our case engines from heavy tracked vehicles. These engines have not been designed and constructed to use an ON-LINE diagnostic system. However, there are other applications which might be used in practice, e.g. Gesellschaft et al. (2002), Czichos & Habig (2003), Quigley & Walls (2007), Revie et al. (2011) a,b, Rak & Pietrucha 2008, Cornak & Skolil (2009), Studzinski & Pietrucha (2012), Ghasemi & Hodkiewicz (2012). We still apply the OFF-LINE engine diagnostics system when sampling lubrication fluid at certain intervals, and use known and optimised special tribodiagnostic methods. We use the results and information from Atomic Emission Spectrometry (AES). Following this analysis we can obtain the information about the presence of specific individual elements and their amount. The amount is usually the weight of a respective element in one standardised unit of lubricant—e.g. milligrams of iron (ferrum) in one kilogram of oil [ppm]. However, we cannot identify the real origin of the respective elements because of fatigue, cutting or sliding. We also try to identify where these elements might come from. We will work with the idea to increase the potential for maintenance optimisation inputs and cost benefit analysis inputs (Stodola & Mazal 2012, Stodola et al. 2013). During the analysis we will focus on Fe particles, because we suppose that they originate from kinematic parts of a motor. We know the critical value of Fe particles amount.

3 OIL FIELD DATA, ASSESSMENT, MODELLING AND RESULTS

– As it has been mentioned before, the data are available in a big amount—it is a statistically important set. The data is collected at intervals and under conditions determined by a methodology. This includes:
– homogenous time intervals given by technical equipment mileage,
– oil temperature and right oil mixing,
– the same place of sample collection,
– the same way of performing the tribo analysis after the sampling.

Based on the data amount, the results are believed to be valuable and statistically reliable. We concentrate in this paper on Fe particles contents only. The example of the data form is in Table 1.

3.1 *Utilization of regression model*

A linear regression model is applied as a basic input characteristic. It helps to determine a linear course of Fe particles generation. The course is completed by dependability intervals for a mean (group) value and for an individual value. These courses are used for setting the point estimations of standard deviations of an individual and mean value for every instant of time—as stated in Table 1. These values are later used for Wiener process modelling. In the paragraph below there is an example of this procedure. In view of their random character, a random vector $\boldsymbol{X} = (\boldsymbol{X}_1, \ldots, \boldsymbol{X}_k)$ represents independent variables and a dependent variable is represented by a random variable Y. When describing and examining the dependence of Y on X, we use a regression analysis, and this dependence is expressed by the following regression function:

$$y = \varphi(x, \boldsymbol{\beta}) = E(Y \,|\mathbf{X} = \mathbf{x}), \tag{1}$$

Table 1. Input data of fe particles form engine oil—example.

Sample time [Mh]	Fe particles [ppm]	Standard deviation mean values	Standard deviation individual value
1/0.15	13.71158	0	4.753368
2/0.30	13.72016	0.001014	4.753368
3/0.45	13.73055	0.002029	4.753368
4/0.60	13.74004	0.003043	4.753369
5/0.75	13.74953	0.004058	4.753370
6/0.90	13.75902	0.005073	4.753371

where $\mathbf{x} = (x_1, \ldots, x_k)$ is a vector of numerical variables, y is a dependent variable, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$ is a vector of regression coefficients β_j.

For our data we will look for a regression function in a linear form and we will apply a linear regression model:

$$y = \sum_{j=1}^{m} \beta_j f_j(\mathbf{x}), \tag{2}$$

where $f_j(\mathbf{x})$ are well-known functions where $\beta_1, \ldots, \beta_m$ are not involved.

For the data we used the following regression functions:

- $m = 2$, $f_1(x) = 1$, $f_2(x) = x$, regression function: $y = \beta_1 + \beta_2 x$
- $m=2$, $f_1(x) = 1$, $f_2(x) = x$, regression function: $y = k + \beta_1 x$

The graphical outcomes from the regression analysis for an individual vehicle and a group of vehicles of the same type are presented below in Figure 1 and Figure 2. Numerical values have been also recorded and used later for the Wiener process.

3.2 *Utilisation of Wiener process*

We assume that the case we observe is a stochastic process with time dependence. Examples of applications might be found e.g. in Si et al. (2012), Linden (2000), Smith & Lánský (1994), Doksum & Hóyland (1992) or Sherif & Smith (1980), The generation of Fe particles is operation time dependant. Therefore the application of a diffusion process seems to be perfectly adequate. Due to normal distribution of random variable and its application capabilities, the Brownian motion might be used universally. The application of the Brownian motion can be found in many areas. Standard use is related to modelling with the use of differential

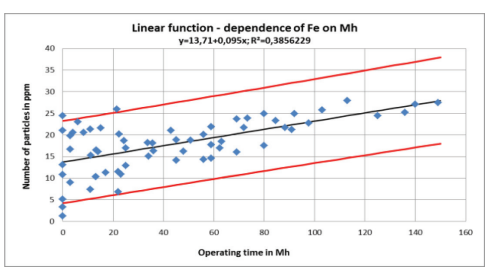


Figure 1. Dependence of Fe particles course on operating time in Mh: mean and 95% confidence interval for individual vehicle observation.

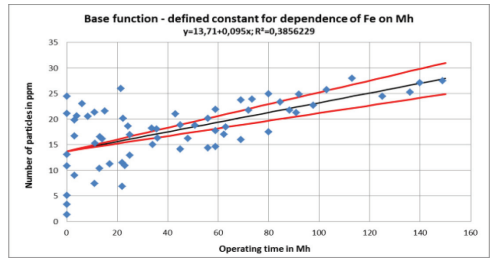


Figure 2. Dependence of Fe particles course on operating time in Mh: mean and its 95% confidence interval.

equations. We select one specific example of diffusion processes which is the Wiener process. Rules of the general Wiener process might be specified as follows. A real stochastic process $\{W(t)\ t \in \langle 0; +\infty)\}$ in a probability space (Ω, A, P) is called *the Brownian motion* or *the Wiener process*, if the following applies:

1. $W(0) = 0$,
2. $W(t) - W(s)$ has $N(0, t - s)$ distribution for $t > s \geq 0$,
3. For arbitrary $0 < t_1 < t_2 < \cdots < t_n$ increments $W(t_1), W(t_2) - W(t_1), W(t_3) - W(t_2), \ldots, W(t_n) - W(t_{n-1})$, $W(t)$ trajectories are mutually independent random variables and continuous almost everywhere.

Next, it applies that:

1. $E[W(t)] = 0$ for $t \geq 0$
2. Var $[W\text{^}2(t)] = t$ for $t \geq 0$

The Wiener process represents one possible form of diffusion processes. It is actually the integral of what in practical applications is called a white noise. The Wiener process with drift will be used in our application. The initial mean value (drift) is β_1 and standard deviations for each time increment have been previously calculated—see Table 1. For our model we apply Wiener process with drift given by stochastic differential equation.

$$dY(t) = \mu \cdot dt + \frac{\sigma \cdot dW(t)}{\sqrt{(t)}} \tag{3}$$

where dW(t) is increment of Wiener process and dt is increment of time, σ is a standard deviation (either of an individual or a mean value), μ is a mean value, t is an instant of time, process initial value $Y(0) = \beta_1$. Time increment for modelling was 0.15 Mh. When modelling—simulating, an example of the process course for individual course is shown in Figure 3, and for a mean value it is in Figure 4. The critical value of particles amount is 50.

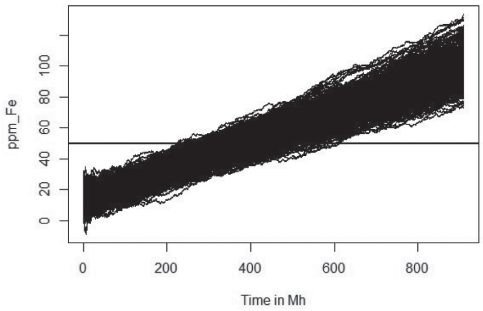


Figure 3. Course of Wiener process simulation for individual value.

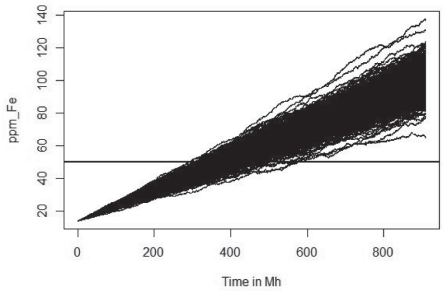


Figure 4. Course of Wiener process simulation for mean value.

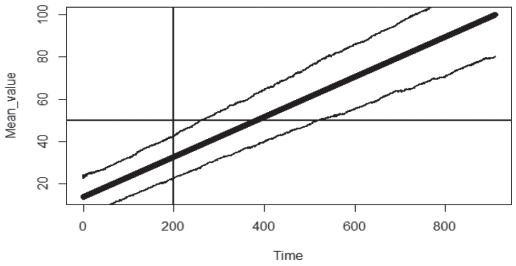


Figure 5. Confidence interval thresholds—95% for individual value.

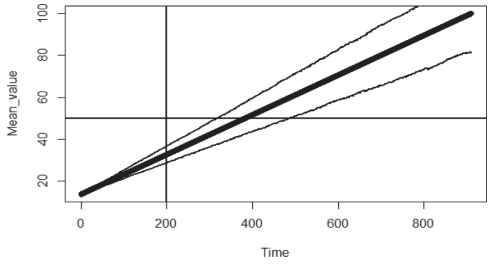


Figure 6. Confidence interval thresholds—95% for mean value.

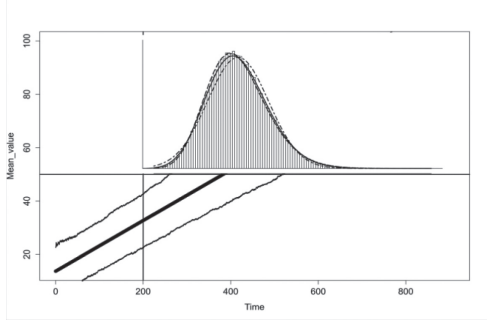


Figure 7. Course of FHT pdf for individual value.

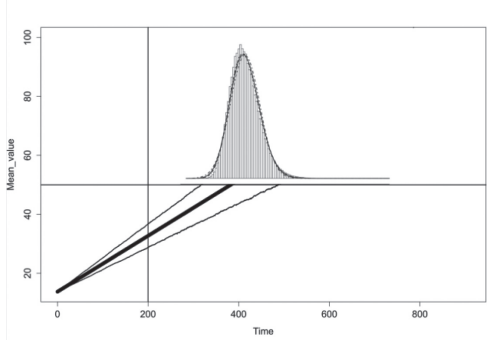


Figure 8. Course of FHT pdf for mean value.

We take into account 95% interval of trajectories which achieve a critical value 50. The vertical line 200 shows a determined interval of PM. These intervals are for the individual and mean value put in Figure 5 and Figure 6.

In order to determine the First Hitting Time (FHT) distribution of the individual and mean value, we set histograms and performed tests for a presumed type of distribution. The expected types of probability density distribution such as Gamma (full/firm line), LogNorm (dashed line—overcovered by IGD), Inverse Gaussian (IGD)—dotted line), Normal (dash and dotted line) or Weibull´s were not proved. The courses of these tested distributions are shown in Figure 7 and Figure 8. We expect then to obtain FHT distribution only in the form of empiric distribution function.

3.3 *Discussion*

The tested values reached for the individual value the following limits: minimum value = 134 Mh,

lower confidence interval 2.5% = 265 Mh, upper confidence interval 97.5% = 524 Mh, mean value = 382 Mh, median = 378 Mh, maximum = 887 Mh.

As to the mean value, the following limits were achieved: minimum value = 258 Mh, lower confidence interval 2.5% = 315 Mh, upper confidence interval 97.5% = 480 Mh, mean value = 385 Mh, Median = 381 Mh, Maximum = 746 Mh.

It follows from the results stated above that the mean value is more or less the same, but the lower threshold of confidence intervals are not. However, the lower confidence intervals are interesting for us in order to determine the possible beginning of PM interval. But if we used the mean value, it would be sufficiently far from the original/fixed PM interval. On the basis of the results we could work with a conservative version and set a new PM interval using the lowest value of lower threshold of confidence interval. This would be 265 Mh (individual value). If we were for a benevolent alternative, we could rely on the mean value and set the PM interval at 380 Mh (more or less the same for both the individual and for the mean value).

When planning a mission, we could work with versions that if common operating conditions were observed, a vehicle could be operated with one oil filling theoretically up to the upper confidence limit 97,5%. Considering conservative or benevolent versions, it would be 480 Mh, or 520 Mh.

4 CONCLUSION

In the article we have introduced possible approaches to modelling indirect diagnostic measures. We were looking for first hitting time distribution which represents a critical limit of Fe particles amount. The modelling is based on the diffusion Wiener process with drift. The observation and the analysis focused on the individual and mean value of Fe particles amount in oil.

The achieved results complement the set of approaches to the indirect observation of a technical condition. The approaches using purely a regression analysis and fuzzy logic, see e.g. Koucky & Valis (2011), Vališ et al. (2012), have been applied so far. Following the conclusions of modelling with the Wiener process, the results of previous approaches might be completed when searching for:

– optimum interval PM,
– recommended/allowed time for mission completion,
– optimizing dependencies of life cycle cost analyzing.

The approach introduced above opens the possibilities of analysing other important diagnostic indicators. It is important so that setting the time derived from the histogram and pdf course could be as accurate as possible and undistorted. Some inspirational examples for further development might be found e.g. in Babiarz 2006; Babiarz 2014a,b; Kierzkowski et al. 2012a,b; Kierzkowski 2010; Klimaszewski & Woch 2012, Kowalski et al. 2011, Nowakowski & Werbińska-Wojciechowska 2009, Wierbińska-Wojciechowska 2013, Wierbińska 2007, Woch 2013, Woch, M. 2014; Zajac et al. 2012.

In our further analysis we are going to develop this approach even more and complement it with other approaches like ARIMA or ARMA methods.

ACKNOWLEDGMENT

This paper has been prepared with the support of the Ministry of Defence of the Czech republic, Partial Project for Institutional Development, K-202, Department of Combat and Special Vehicles, University of Defence, Brno and of the project of Ministry of Defence of the Czech Republic—BOPROS nr. OFVTUV2013002.

REFERENCES

Babiarz, B. 2006. An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping* 83(4): 230–235.

Babiarz B. 2014 (in prep.) Heat supply system reliability management. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Babiarz B. 2014 (in prep.) Risk assessment in heat supply system. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Cornak S. & Skolil J. 2009. The Selected Aspects of Life Fluids Evaluation. In *Proc. International Conference on Military Technologies, ICMT 2009,* Brno: UO, pp. 39–45.

Czichos H. & Habig K-H. 2003. *Tribologie-Handbuch*; *Reibung und Verschleiß*, 2nd edition (in German). Weisbaden: Vieweg.

Doksum K.A. & Hóyland A. 1992. Models for Variable-Stress Accelerated Life Testing Experiments Based on Wiener Processes and the Inverse Gaussian Distribution. *Technometrics*. 1(34): 74–82.

Gebraeel N. & Pan J. 2008. Prognostic Degradation Models for Computing and Updating Residual Life Distributions in a Time-Varying Environment. *IEEE Transactions on Reliability* 57(4): 539–550.

Gesellschaft für Tribologie e.V. GfT Arbeitsblatt 7. 2002. Tribologie—Verschleiß, Reibung, Definitionen, Begriffe, Prüfung (GfT, Moers), (in German).

Ghasemi A. & Hodkiewicz M.R. 2012. Estimating Mean Residual Life for a Case Study of Rail Wagon Bearings. *IEEE Transactions on Reliability* 61(3): 719–730.

Ghasemi A., Yacout S. & Quali M.S. 2010a. "Evaluating the Reliability Function and the Mean Residual Life for Equipment With Unobservable States," *IEEE Transactions on Reliability* 59(1): 45–54.

Ghasemi A., Yacout S. & Quali M.S. 2010b. "Parameter Estimation Methods for Condition-Based Maintenance With Indirect Observations," *IEEE Transactions on Reliability* 59(2): 426–429.

Kierzkowski, A., Kowalski, M., Magott, J. & Nowakowski, T. 2012. Maintenance process optimization for low-cost airlines. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012. 8: 6645–6653.

Kierzkowski, A. & Zajac, M. 2012. Analysis of the reliability discrepancy in container transshipment. *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012* 1: 826–831.

Kierzkowski, A. 2010. Reliability models of transportation system of low cost airlines. *Reliability, Risk and Safety: Back to the Future*: 1325–1329.

Klimaszewski, S & Woch, M. 2012. Modified Hagg & Sankey method to estimate the ballistic behaviour of lightweight metal/composite/ceramic armour and a fuselage skin of an aircraft, *Journal of KONES* 19(2): 245–252.

Koucky M. & Valis D. 2011. "Suitable approach for non-traditional determination of system health and prognostics," *Zeszyty naukowe*, 1(159): 123–134.

Kowalski, M., Magott, J., Nowakowski, T., Werbinska-Wojciechowska, S. 2011. Analysis of transportation system with the use of Petri nets. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 13(1): 48–62.

Labeau P.E., Smidts C. & Swaminathan S. 2000. Dynamic reliability: Towards an integrated platform for probabilistic risk assessment, *Reliability Engineering and System Safety* 68(3): 219–254.

Li W. & Pham H. 2005. An inspection-maintenance model for systems with multiple competing processes, *IEEE Transactions on Reliability* 54(2): 318–327.

Linden M. 2000. Modelling Strike Duration Distribution: a Controlled Wiener Process Approach. *Applied Stochastic Models in Bussiness and Industry* 16: 35–45.

Maillart L.M. & Pollock S.M. 2002. Cost-optimal condition-monitoring for predictive maintenance of 2-phase systems, *IEEE Transactions on Reliability* 51(3): 322–330.

Medjaher K., Tobon-Mejia D.A. & Zerhouni N. 2012. Remaining Useful Life Estimation of Critical Components With Application to Bearing. *IEEE Transactions on Reliability*, 61(2): 292–302.

Nowakowski T., Werbińska-Wojciechowska S. 2009. On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing* 6(4): 364–378.

Park K.S. 1993. Condition-based predictive maintenance by multiple logistic function, *IEEE Transactions on Reliability* 42(4): 556–560.

Quigley J. & Walls L. 2007. Trading reliability targets within a supply chain using Shapley´s values. *Reliability Engineering and System Safety* 92(10): 1448–1457.

Rak J. & Pietrucha K. 2008. Risk in drinking water quality control. *Przemysl chemiczny* 87(5): 554–556.

Revie M., Bedford T. & Walls L. 2011. Supporting Reliability Decisions During Defence Procurement Using a Bayes Linear Methodology. *IEEE Transactions on Engineering Management* 58(4): 662–673.

Sherif Y.S. & Smith L.M. 1980. First-Passage Time Distribution of Brownian Motion as a Reliability Model. *IEEE Transaction on Reliability* 5(2): 425–426.

Si X.S., Wang W., Hu Ch-H., Zhou D-H. & Pecht M.G. 2012. Remaining Useful Life Estimation Based on a Nonlinear Diffusion Degradation Process. *IEEE Transactions on Reliability* 61(1): 50–67.

Smith Ch. E. & Lánský P. 1994. A reliability application of a mixture of inverse Gaussian distributions. *Applied Stochastic Models and Data Analysis* 10: 61–69.

Stodola, P., Mazal, J. 2012. The Trapezoid and S-curve for Real-time Servomotors Control. In *Proceedings of the 15th International Conference on Mechatronics—Mechatronika 2012*. Prague: Czech Technical University in Prague, 165–168.

Stodola, P., Mazal, J., Mokrá, I. & Podhorec, M. 2013. The Real-Time Control Algorithm and Control Curves for Servomotors. *International Journal of Circuits, Systems and Signal Processing*. 7(2): 118–125.

Studzinski, A. & Pietrucha-Urbanik, K. 2012. Risk Indicators of Water Network Operation. *Chemical Engineering Transactions* 26: 189–194.

Vališ D., Koucký M. & Žák L. 2012. On approaches for non-direct determination of system deterioration. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 14(1): 33–41.

Werbinska-Wojciechowska, S. 2013. Time resource problem in logistics systems dependability modelling. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 15(4): 427–433.

Werbinska, S. 2007. Interactions between logistic and operational system—an availability model. *Risk, reliability and societal safety. Eds. Terje Aven, Jan Erik Vinnem.* Leiden: Taylor and Francis, 2045–2052.

Woch, M. 2013. Analysis of operating loads on an aircraft's vertical stabilizer on the basis of recorded data, *Chemical Engineering Transactions* 33: 643–648.

Woch, M. 2014(in prep.) Risk analysis of the point on aging aircraft structure. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Yang, S.K. 2003 A condition based failure-prediction and processing-scheme for preventive maintenance, *IEEE Transactions on Reliability* 52(3): 373–383.

Zajac, M. & Kierzkowski, A. 2012. Uncertainty assessment in semi Markov methods for Weibull functions distributions. *Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011*: 1161–1166.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A modified Auto Associative Kernel Regression method for robust signal reconstruction in Nuclear Power Plant components

P. Baraldi, F. Di Maio & P. Turati
Energy Department, Politecnico di Milano, Milan, Italy

E. Zio
Energy Department, Politecnico di Milano, Milan, Italy
Aramis S.r.l., Milan, Italy
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy-Electricité de France, Ecole Centrale Paris-Supelec, France

ABSTRACT: The application of the Auto Associative Kernel Regression (AAKR) method to the reconstruction of correlated plant signals is not satisfactory from the point of view of the robustness, i.e. the capability of reconstructing abnormal signals to the values expected in normal conditions. To overtake this limitation, we propose to modify the traditional AAKR method by defining a novel measure of the similarity between the current measurement and the historical patterns. An application of the proposed modified AAKR method to the condition monitoring of a pressurizer of a Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP) shows benefits with respect to the traditional AAKR method, in terms of earlier detection of abnormal conditions and correct identification of the signals responsible for triggering the detection.

1 INTRODUCTION

The objective of condition monitoring is to assess the health state of industrial components and to identify possible incipient faults (Venkatasubramanian et al. 2003a, 2003b, 2003c, Hines et al. 2007). To this aim, a model is usually built to reconstruct the values of the monitored signals expected in normal conditions (Hameed et al. 2009). During operation, observed signal measurements are compared with the reconstructions provided by the model: abnormal conditions are detected when the reconstructions are remarkably different from the measurements.

Several empirical reconstruction modeling technique have been applied for condition monitoring of industrial components (Guglielmi et al. 1995, Nabeshima et al. 1998, Jack et al. 2002, Harkat et al. 2007, Chevalier et al. 2009, Baraldi et al. 2013a). These methods provide accurate reconstructions of the measured signals under normal operations, but they often tend to be not robust, i.e. in case of abnormal conditions the reconstructions of the signals are not properly estimating the values of the signals expected in normal conditions (Baraldi et al. 2012). In particular, it has been shown that the reconstruction provided by the Auto Associative Kernel Regression (AAKR) method (Baraldi et al. 2011a, Di Maio et al. 2013) of an anomalous transient characterized by a drift of one signal can be not satisfactory for two reasons: 1) the reconstruction of the signal affected by the drift tends to assume values in the middle between the drifted values and the expected values of the signal in normal conditions; 2) the reconstructions of other signals not affected by the drift tend, erroneously, to be different from the signal measurements. The consequence of 1) is a delay in the detection of abnormal conditions, whereas the consequence of 2) is that the condition monitoring system, although it correctly triggers an abnormal condition alarm, is not able to correctly identify the signal that triggers the alarm.

The objective of the present work is to propose a robust signal reconstruction method capable of early detecting abnormal conditions and providing accurate reconstructions of the values of the signals subject to the abnormal conditions.

The proposed method is based on the modification of the measure of similarity used by the AAKR method: instead of using the Euclidean distance, the proposed method introduces a penalty vector which reduces the contribution provided by those signals which are expected to be subject to the abnormal conditions. The rationale behind this modification is the attempt to privilege those abnormal conditions caused by the most frequently expected malfunctions and failures.

The performance of the proposed method has been tested on simulated data describing the behaviors of a pressurizer of a Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP) (Baraldi et al. 2010, Baraldi et al. 2013b). The remainder of the paper is organized as follows. In Section 2, the fault detection problem is introduced. In Section 3, the AAKR method is briefly recalled. Section 4 shows the limitation of the traditional AAKR approach to condition monitoring and states the objectives of the present work. In Section 5, the proposed modification of the traditional AAKR is described and discussed. In Section 6, the application of the proposed method to a case study concerning the monitoring of 6 signals in the pressurizer of a Nuclear Power Plant is presented. Finally, in Section 7 some conclusions are drawn.

2 FAULT DETECTION

The condition monitoring adopted in this work is based on an empirical model reproducing the plant behavior in normal conditions. The model receives in input the vector, $\boldsymbol{x}^{obs}(t)$, containing the actual observations of the J signals monitored at the present time, t, and produces in output the reconstructions, $\hat{\boldsymbol{x}}_{nc}(t)$, i.e. the values that the signals are expected to have in normal conditions (Baraldi et al. 2012) (Fig. 1). If the actual conditions at time t are abnormal instead, the residuals $\Delta\boldsymbol{x} = \boldsymbol{x}^{obs}(t) - \hat{\boldsymbol{x}}_{nc}(t)$, i.e. the variations between the observations and the reconstructions, are large and can be detected by observing the exceedance of a prefixed thresholds by at least one signal.

3 AUTO ASSOCIATIVE KERNEL REGRESSION (AAKR)

The basic idea behind AAKR is to reconstruct at time t the values of the signals expected in normal conditions, $\hat{\boldsymbol{x}}_{nc}(t)$, on the basis of a comparison of the currently observed signals measurements (also referred to as test pattern), $\boldsymbol{x}^{obs}(t) = [x^{obs}(t, 1), \ldots, x^{obs}(t, J)]$, and of a set of historical signals measurements collected during normal condition of operation. In practice, AAKR performs a mapping from the space of the measurements of the signals $\boldsymbol{x}^{obs}(t)$ to the space of the values of the signals expected in normal conditions, $\hat{\boldsymbol{x}}_{nc}(t)$:

$$\hat{\boldsymbol{x}}_{nc}(t) = \varphi\left(\boldsymbol{x}^{obs}(t) \mid \overset{=obs-nc}{X}\right) : \mathrm{R}^J \rightarrow \mathrm{R}^J \tag{1}$$

where $\overset{=obs-nc}{X}$ indicates a $N \times J$ matrix containing N historical observations of the J signals performed in normal conditions. Since the mapping is independent from the present time, t, at which the signals observations are performed, the present time t will be omitted from the notations. Thus, $x^{obs}(j)$, $j = 1, \ldots, J$, indicates the value of signal j at the present time. The reconstruction of the expected values of the signals in normal conditions, $\hat{\boldsymbol{x}}_{nc} = [\hat{\boldsymbol{x}}_{nc}(1), \ldots, \hat{\boldsymbol{x}}_{nc}(J)]$, is performed as a weighted sum of the available historical observations; for the generic j-th element of $\hat{\boldsymbol{x}}_{nc}$:

$$\hat{\boldsymbol{x}}_{nc}(j) = \frac{\sum_{k=1}^{N} w(k) \cdot x^{obs-nc}(k, j)}{\sum_{k=1}^{N} w(k)} \tag{2}$$

The weights, $w(k)$, measure the similarity between the test pattern, $\boldsymbol{x}^{obs}$, and the k-th historical observation vector, $\boldsymbol{x}^{obs-nc}(k)$. They are evaluated through a kernel, *Ker*, i.e. a scalar function which can be written as a dot product (Burges, 1998, Müller et al. 2001, Widodo et al. 2007).

Traditional AAKR adopts as *Ker* function the Gaussian Radial Basis Function (RBF) with bandwidth parameter h, i.e.:

$$w(k) = \frac{1}{\sqrt{2\pi h^2}} e^{-\frac{\|\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)\|^2}{2h^2}} \tag{3}$$

In fault detection applications, Euclidean and Mahalanobis distances are typically used to compute the distance in the Gaussian RBF (Baraldi et al. 2011b). In this work, in order to account for differences in the scale and variability of the different signals, a Mahalanobis distance is used, defined by the covariance matrix, S, such that:

$$\| \boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k) \|^2_{mahal} = \left(\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)\right) S^{-1} \left(\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)\right) \tag{4}$$

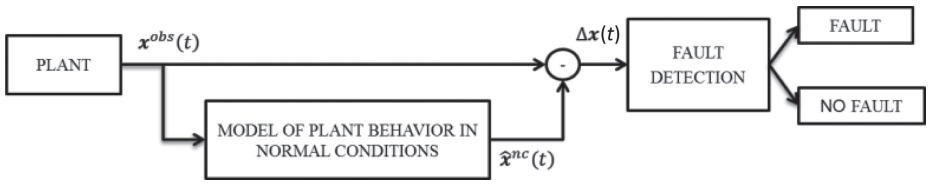


Figure 1. Scheme of condition monitoring for fault detection.

Assuming independence between the signals, S is given by:

$$S = \begin{bmatrix} \sigma_1^2 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_j^2 \end{bmatrix} \quad (5)$$

where σ_j^2 indicates the estimated variance of signal j in the historical observations.

4 LIMITATIONS IN THE USE OF AAKR FOR SIGNAL RECONSTRUCTION

The low robustness of the traditional AAKR method is well illustrated by the following case study concerning the monitoring of the pressurizer of a Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP) (Baraldi et al. 2010, Baraldi et al. 2013b). The dataset is composed of 37 simulated transients in normal conditions. Each transient is monitored for 100 time steps by 6 sensors measuring pressure, liquid temperature, steam temperature, spray flow, heaters power and liquid level. Table 1 reports the high degree of correlation between the signals.

Table 1. Degree of correlation between monitored signals. S1: pressure, S2: liquid temperature, S3: steam temperature, S4: spray flows, S5: heaters power, S6: liquid level.

	S1	S2	S3	S4	S5	S6
S1	1.00	–0.07	0.98	–0.46	–0.23	0.98
S2	–0.07	1.00	–0.08	0.01	0.18	–0.22
S3	0.98	–0.08	1.00	–0.46	–0.23	0.97
S4	–0.46	0.01	–0.46	1.00	–0.14	–0.45
S5	–0.23	0.18	–0.23	–0.14	1.00	–0.26
S6	0.98	–0.22	0.97	–0.45	–0.26	1.00

A traditional AAKR reconstruction model has been developed using the 37 transients. Then, an abnormal condition transient has been simulated by assuming sensor failures leading to a jump of the liquid temperature from time 10 to 20, a linear drift on the steam temperature signal from time 30 followed by a step at time 80 and an additive noise impacting the spray flow sensor from time 70 till the end of the observation period. Figure 2 shows the measured (dashed-light) and the real value (dotted-dark) of the 6 signals in the test transient, whereas Figure 3 shows the reconstructions of the signals provided by the AAKR method (dashed-light) and the signals expected in normal condition (dotted-dark). Notice that the reconstructions are not robust: 1) pressure, steam temperature and level reconstruction do not reflect the expected normal conditions after time step 30; 2) sprayers flow and heaters power reconstruction are far from the correct reconstruction during the time window 10–20.

A low robustness in the reconstruction leads to two practical problems: 1) delay in the detection of abnormal conditions; 2) identification of abnormal conditions on signals different from those which are actually affected by the abnormal behaviors.

5 MODIFIED AAKR

In order to enhance the AAKR robustness, we propose to modify the computation of the weights w performed by the traditional AAKR (Eq. 2). The basic ideas underling the proposed modification are (a) to identify the signals affected by abnormal behaviors and (b) to reduce their importance in the computation of the similarity between the test pattern and the historical observations.

With respect to (a), we assume that the probability of occurrence of a fault causing variations on a large number of signals is lower than that of

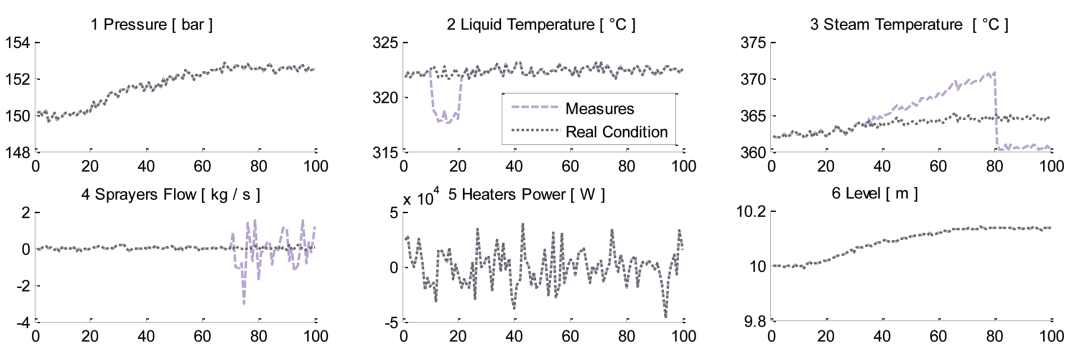


Figure 2. Measured abnormal value (light-dashed line) and corresponding normal condition value (dark-dotted line) of a test transient.

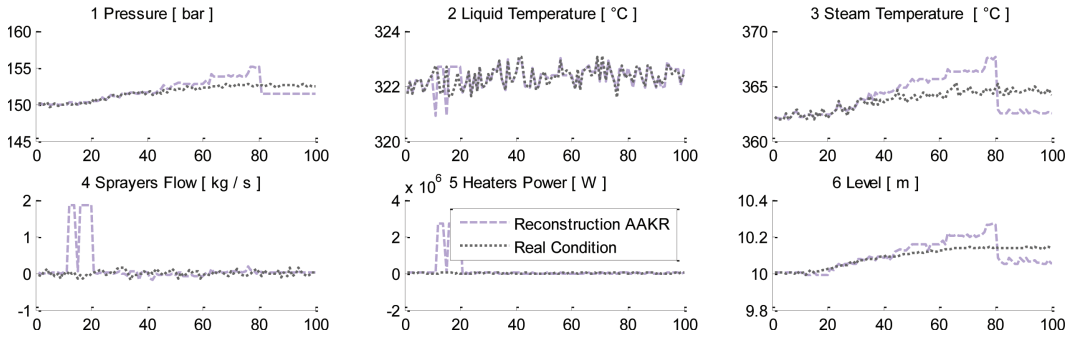


Figure 3. Reconstruction (light-dashed line) of the expected normal values (dark-dotted line) of a transient affected by abnormal conditions.

a fault causing variations on a small number of signals:

$$P(S_{fault\,1}) \leq P(S_{fault\,2}) \text{ if } |S_{fault\,2}| \leq |S_{fault\,1}| \quad (6)$$

where $S_{fault\,1}$ and $S_{fault\,2}$ indicate the sets of signals affected by variations due to the abnormal (faulty) conditions, and $|S_{fault\,1}|$ and $|S_{fault\,2}|$ their cardinality. If we consider, for example, the problem of sensor failures, it is reasonable to assume that the probability of having N_1 faulty sensors at the same time is lower than that of having a lower number of faulty sensors, $N_2 \leq N_1$, at the same time.

The proposed procedure computes the similarity measure between the observation, $\boldsymbol{x}^{obs}$, and the generic *k-th* historical observation, $\boldsymbol{x}^{obs-nc}(k)$, in two steps: (a) a pre-processing step consisting in the projection of $\boldsymbol{x}^{obs}$ and $\boldsymbol{x}^{obs-nc}(k)$ in a new space defined by a penalty vector, $\boldsymbol{p} = [p(1), \ldots, p(J)]$, with increasing entries, i.e. $p(1) \leq \ldots \leq p(J)$ and (b) the application of the Gaussian RBF kernel in the new space.

Step (a) is based on:

– computing the vector of the absolute values of the normalized differences between $\boldsymbol{x}^{obs}$ and $\boldsymbol{x}^{obs-nc}(k)$:

$$|x^{obs} - x^{obs-nc}(k)|_{\sigma} = \left(\left| \frac{x^{obs}(1) - x^{obs-nc}(k,1)}{\sigma_1} \right| \ldots \left| \frac{x^{obs}(J) - x^{obs-nc}(k,J)}{\sigma_J} \right| \right) \quad (7)$$

– defining a permutation matrix, P_{perm}, i.e. a matrix which, when multiplied to a vector, only modifies the order of the vector components; in our procedure, we define a matrix, P_{perm}, such that when it is applied to the vector $|\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)|_{\sigma}$, the components of the obtained vector are the same of that of $|\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)|_{\sigma}$, but they appear in a decreasing order, i.e. the first component is the one with the largest difference in $|\boldsymbol{x}^{obs} - \boldsymbol{x}^{obs-nc}(k)|_{\sigma}$;

– defining a diagonal matrix with decreasing entries on its diagonal:

$$D_p = \begin{bmatrix} \sqrt{p(1)} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{p(J)} \end{bmatrix} \quad (8)$$

where the vector $\boldsymbol{p} = [p(1), \ldots, p(J)] = tr(D_p)$ will be referred to as penalty vector;

– projecting $\boldsymbol{x}^{obs}$ and $\boldsymbol{x}^{obs-nc}(k)$ in a new space defined by the transformation:

$$\begin{aligned} &\psi : \mathbb{R}^J \rightarrow \mathbb{R}^J \\ &\psi(\boldsymbol{x}^{obs}) = D_{\boldsymbol{p}}\ P_{perm}\ \boldsymbol{x}^{obs} \\ &\psi(\boldsymbol{x}^{obs-nc}) = D_{\boldsymbol{p}}\ P_{perm}\ \boldsymbol{x}^{obs-nc} \end{aligned} \quad (9)$$

In step (b), we apply to $\psi(\boldsymbol{x}^{obs})$ and $\psi(\boldsymbol{x}^{obs-nc})$ the Gaussian kernel with Euclidean distance:

$$w(k) = \frac{1}{\sqrt{2\pi h^2}} e^{-\frac{\left\| \psi(\boldsymbol{x}^{obs}) - \psi(\boldsymbol{x}^{obs-nc}) \right\|^2}{2h^2}} \quad (10)$$

6 APPLICATION OF THE METHOD TO THE CASE STUDY

The data previously introduced in Section 4 are used to develop the modified AAKR reconstruction

Table 2. Alarm thresholds for traditional and modified AAKR.

AAKR	S1	S2	S3	S4	S5	S6
Traditional	0.37	0.10	0.32	0.23	5.74E+04	0.02
Modified	0.40	0.53	0.68	0.15	3.96E+04	0.02

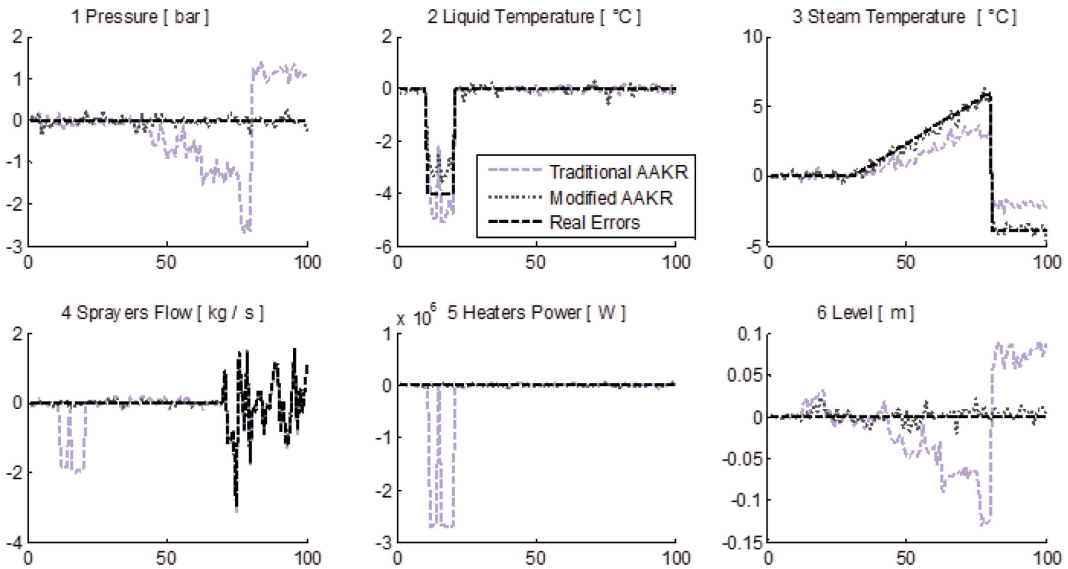


Figure 4. Residuals obtain by the traditional AAKR (light-dashed line) and by the modified AAKR (dark-dotted line); the synthetic error added to the signal is also reported (black-dashed line).

method. In particular, the 37 transients have been divided into 3 subsets:

- Training set $\overline{\overline{X}}_{train}^{obs-nc} \in \mathbb{R}^{2700\times 6}$, which is used as historical dataset to train the model;
- Validation set $\overline{\overline{X}}_{val}^{obs-nc} \in \mathbb{R}^{1000\times 6}$, which is used to set the optimal parameter values;
- Test set, $\overline{\overline{X}}_{test}^{obs-nc} \in \mathbb{R}^{400\times 6}$, which is used to test the performance of the method.

For both the traditional and modified AAKR methods, the optimal bandwidth parameter, h, has been identified by minimizing the Mean Square Error (MSE) of the reconstructions on the validation set, $\overline{\overline{X}}_{val}^{obs-nc}$:

$$MSE_h = \frac{\sum_{k=1}^{N_{val}} \sum_{s=1}^{J} (\hat{\boldsymbol{x}}_{val}(k,s) - \boldsymbol{x}_{val}^{obs-nc}(k,s))^2}{N_{val}} \quad (11)$$

The transients in the test set are used to set the alarm thresholds (see Table 2), which have been taken equal to 3 times the standard deviation of the obtained residuals. Notice that for signals 2 and 3 the traditional AAKR provides lower thresholds; on the contrary, the modified AAKR provides lower thresholds for signals 4 and 5. This is due to the fact that the traditional AAKR provides more accurate reconstructions of signals 2 and 3, whereas the modified AAKR of signals 4 and 5.

We have then tested the performance of the modified AAKR on the same abnormal condition transient introduced in Section 4. Figure 4 shows that the modified AAKR provides residuals that tend to reflect the simulated abnormal condition. For example, considering the time window 10–20, the modified AAKR identifies the wrong calibration of the liquid temperature sensor, whereas the traditional AAKR identifies, erroneously, an abnormal condition also on sprayer flow and heaters power sensors. Furthermore, the modified AAKR provides a more robust reconstruction of the steam temperature when the corresponding sensor is subject to a linear drift followed by a step change.

7 CONCLUSIONS

In this work, we have considered condition monitoring via Auto Associative Kernel Regression (AAKR) for fault detection in a pressurizer of a Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP). A modification of the traditional AAKR has been proposed to achieved a more robust reconstruction of the signal expected in normal condition. By projecting the data in a new signal space according to a penalty vector, the modification aims at reducing the contribution of the signals affected by malfunctioning to the evaluation of the similarity.

The application of the modified AAKR to the monitoring of 6 signals in a pressurizer of a Nuclear Power Plant has shown that it provides a more robust reconstructions of the signals than the traditional AAKR method.

REFERENCES

Baraldi P., Cammi A., Mangili F., Zio E., 2010, *"Local fusion of an ensemble of models for the reconstruction of faulty signals"*, IEEE Transactions on Nuclear Science, Vol. 57, No. 2 part 2, pp. 793–806.

Baraldi P., Canesi R., Zio E., Seraoui R., Chevalier R., 2011a, *"Genetic algorithm-based wrapper approach for grouping conditional monitoring signals of nuclear power plant system"*, Integrated computer-Aided engineering, vol. 18, pp. 221–234.

Baraldi P., Gola G., Zio E., Roverso D., Hoffman M., 2011b, *"A randomized model ensemble approach for reconstructing signals from faulty sensors"*, Expert systems with application, vol. 38, No. 8.

Baraldi P., Di Maio F., Pappaglione L., Zio E. and Seraoui R., 2012, *"Condition Monitoring of Power Plant Components During Operational Transients"*, Proceedings of the Institution of Mechanical Engineers, Part O, Journal of Risk and Reliability, 226(6) 568–583, 2012.

Baraldi P., Di Maio F., Genini D., Zio E., 2013a, "*A fuzzy similarity based method for signal reconstruction during plant transients*", Chemical Engineering Transactions, 33, pp. 889–894, 2013.

Baraldi P., Di Maio F., Zio E., 2013b, *"Unsupervised Clustering for Fault Diagnosis in Nuclear Power Plant Components"*, International Journal of Computational Intelligence Systems, Vol. 6, No. 4, pp. 764–777.

Burges C.J.C., 1998, *"A Tutorial on Support Vector Machines for Pattern Recognition",* Data Mining and Knowledge Discovery, vol. 2., pp. 121–167

Chevalier R., Provost D., and Seraoui R., 2009, *"Assessment of Statistical and Classification Models For Monitoring EDF's Assets"*, Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation.

Di Maio, F.; Baraldi, P.; Zio, E.; Seraoui, R., 2013, *"Fault Detection in Nuclear Power Plants Components by a Combination of Statistical Methods"*, IEEE Transaction on Reliability, 62(4), pp. 833–845, 2013.

Guglielmi G., Parisini T., Rossi G., 1995, *"Fault Diagnosis And Neural Networks: A Power Plant Application"*, Control Engineering Practice, vol. 3, No. 5, pp. 601–620.

Hameed, Z., Hong, Y.S., Cho, Y.M., Ahn, S.H., & Song, C.K., 2009. "*Condition monitoring and fault detection of wind turbines and related algorithms: A review"*, Renewable and Sustainable Energy Reviews, vol. 13, No. 1, pp. 1–39.

Harkat M.F., Djelel S., Doghmane N., Benouaret M., 2007, *"Sensor Fault Detection, Isolation and Reconstruction Using Nonlinear Principal Component Analysis"*, International Journal of Automation and Computing, vol. 4, No. 2, pp. 149–155.

Hines J.W., Garvey D., 2007, *"Process and Equipment Monitoring Methodologies Applied to Sensor Calibration Monitoring"*, Quality and Reliability Interantional, vol. 23, No. 1, pp. 123–135.

Jack L.B., Nandi A.K., 2002, "Fault detection using support vector machines and artificial neural networks, augmented by genetic algorithms", Mechanical Systems and Signal Processing, vol. 16, No. 2–3, pp. 373–390.

Müller, K.-S., Mika, S., Rätsch, G., Tsuda, K., Schölkopf, B., 2001, "*An introduction to kernel-based learning algorithms",* IEEE Transactions on Neural Networks, vol. 12, No. 2, pp. 181–201.

Nabeshima K., Suzudo T., Suzuki K., Turcan E., 1998, *"Real-time Nuclear Power Plant Monitoring with Neural Network"*, Journal of Nuclear Science and Technology, vol. 35, No. 2, pp. 93–100.

Venkatasubramanian V., R. Rengaswamy, K. Yin, S.N. Kavuri, 2003a, "*A review of process fault detection and diagnosis Part I: Quantitative model-based methods*", Computers and Chemical Engineering, vol. 27, pp. 293–311.

Venkatasubramanian V., R. Rengaswamy, S.N. Kavuri, 2003b, "*A review of process fault detection and diagnosis Part II: Qualitative models and search strategies*", Computers and Chemical Engineering, vol. 27, pp. 313–326.

Venkatasubramanian V., R. Rengaswamy, S.N. Kavuri, K. Yin, 2003c, "*A review of process fault detection and diagnosis Part III: Process history based methods*", Computers and Chemical Engineering, vol. 27, pp. 327–346.

Widodo A., Yang B., 2007, *"Support vector machine in machine condition monitoring and fault diagnosis"*, Mechanical Systems and Signal Processing, vol. 21, No. 6, pp. 2560–2574.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Experimental design for the evaluation of Critical Heat Flux of small-scale pressurized nuclear reactors

J.P. Duarte & J.R.C. Piqueira
Department of Telecommunications and Control, Polytechnic School, University of São Paulo, São Paulo, Brazil

M.E. Taqueda
Department of Chemical Engineering, Polytechnic School, University of São Paulo, São Paulo, Brazil

ABSTRACT: This paper aims to analyze the Critical Heat Flux (CHF) experimental design for a small-scaled pressurized nuclear reactor. The CHF or Departure from Nucleate Boiling (DNB) is one of the most important thermal-hydraulic safety criteria for pressurized reactors since its occurrence can lead to fuel damage. A 3×3 test section is simulated through COBRAIIIc/MIT-1 code for thirty operational conditions. The results are presented through response surfaces and used to evaluate the DNBR (DNBR ratio) at the hotspot. The lowest DNBR value was 1.587 for the maximum pressure, mass flux and inlet temperature.

1 INTRODUCTION

The Brazilian Navy is building the first nuclear reactor for propulsion in Brazil, the LABGENE (Nuclear Energy Generation Laboratory) ((Natacci and Corrêa 2005, Nascimento et al. 2005, Maragni et al. 1995, Giovedi et al. 2011)), a prototype small-scale pressurized nuclear reactor. One of the most important thermal-hydraulic safety aspects in reactor design is the Critical Heat Flux (CHF), which is under evaluation for this project. CHF occurs when heat transfer mechanisms change and a vapor film is formed on the fuel rods leading to a high temperature increase in a very short period of time (Groeneveld 2011). Therefore, CHF can damage the fuel rods leading to the fission products release into the primary coolant and even to a severe accident by fuel melting.

Although many CHF correlations exist, it is important to perform experiments specifically for each reactor core, once the phenomenon depends on a lot of factors such as: geometry, subcooling, pressure, mass flux, materials, etc. Besides, currently theoretical models cannot predict CHF because of its complexity. Thus, other CHF correlations for small modular reactors have been also researched (Greenwood et al. 2013).

This work evaluated the CHF for LABGENE through experimental design and by simulating the test section under reactor operational conditions through COBRAIIIc/MIT-1 code (Jackson & Todreas 1981). COBRA is a thermal-hydraulic code widely used to evaluate the core of PWRs by means of subchannel analysis. An EPRI (Electric Power Research Institute) correlation (EPRI 1983) is also used to predict CHF, based on the parameter range and previous analysis (Carajilescov & Valente 2011). The geometry of a test section previously designed for CHF experiments consists in 3×3 electrically heated one meter high cylindrical fuel rods. The inlet temperature, mass flow and pressure were the independent variables of the simulated experiments.

The results are presented through response surfaces (Box, Hunter, & Hunter 2005). Aiming at future experimental analysis and licensing, two additional situations were simulated: a 30 cm high shorter test section and one with real power profile.

Section 2 describes the test section as well as some reactor parameters. Section 3 shows the model used through COBRAIIIc and finally, sections 4 and 5 display the results and conclusions, respectively.

2 TEST SECTION

The test section which will be used in the critical heat flux experiments can be seen in Figure 1. Its 3×3 geometry is a fair initial option used for CHF experiments once it can represent the reactor conditions. Rod diameter, rod height, and pitch are the same as in the reactor core. However, the first rod bundle will have a uniform axial heat flux profile. From a uniform power profile, it is still possible to

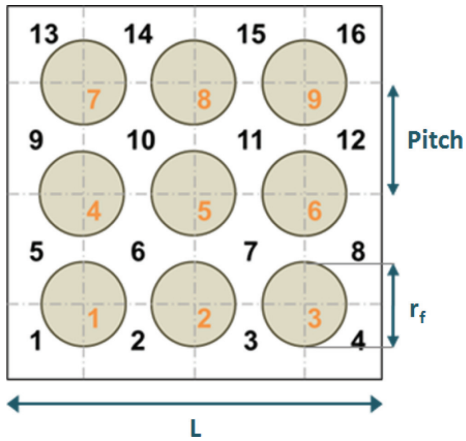


Figure 1. Test section design for CHF experiments.

Table 1. Core reactor parameters.

Parameter	Value
Nominal pressure (MPa)	13.1
Mass flux (kg/s)	454.4
Inlet temperature (°C)	264.15
Average heat flux (MW/m^2)	0.3
Maximum heat flux (MW/m^2)	0.9
Hotspot factor	3.0
Rod diameter, r_f (mm)	10
Pitch (mm)	13
MDNBR[1]	1.5
L (mm)	43.4

[1]Minimum DNB ratio.

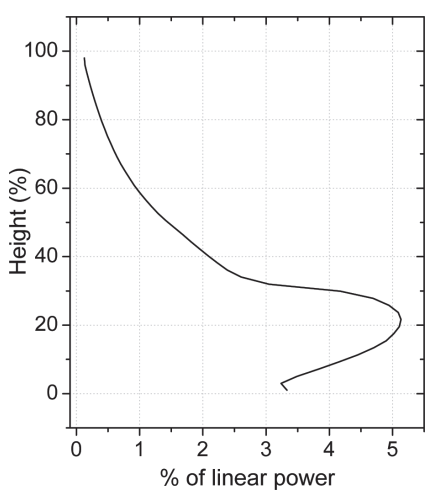


Figure 2. Linear power in the Beginning Of Life (BOL).

calculate a correction factor to predict the CHF in a non-uniform one (Todreas & Kazimi 2012). Core reactor parameters are shown in Table 1.

The rods will be indirectly heated by electrical resistors and rod number 5 will have 10 percent power more than the other ones to induce the DNB (departure from nucleate boiling) at this point.

Once the axial power profile has an uncommon shape (Fig. 2) as compared to commercial PWRs (pressurized water reactors), a shorter test section will be constructed.

3 MODEL

COBRAIIIc is a widely used code for the thermal-hydraulic analysis of nuclear reactor cores. Its approach is based on subchannel analyses where conservation equations are axially solved and coupled through mixing coefficients (Todreas & Kazimi 2001).

The single phase friction model available in COBRAIII is based on the friction factor f and the Reynolds number according to Eq. 1.

$$f = aRe^b + c \tag{1}$$

where a, b and c are specified constants that depend upon the subchannel roughness.

The Armand model was chosen to calculate the two-phase friction multiplier, φ, through Eq.2.

$$\varphi = \begin{cases} 1.0 & \alpha \le 0.0 \\ \dfrac{1-X}{(1-\alpha)^{1.42}} & 0.39 < (1-\alpha) \le 1.0 \\ 0.478\dfrac{(1-X)^2}{(1-\alpha)^{2.2}} & 0.1 < (1-\alpha) \le 0.39 \\ 1.730\dfrac{(1-X)^2}{(a-\alpha)^{1.64}} & 0.0 < (1-\alpha) \le 0.1 \end{cases} \tag{2}$$

where X is the quality and α is the void fraction.

The subcooled void model used is the Levy's one (Jackson & Todreas 1981), which calculates the true quality in terms of the equilibrium quality and the quality started by bubble departure. It is also necessary to choose a turbulent crossflow model. The model used is shown in Eq. 3. The slip ratio between liquid and vapor was considered equal to 1.0.

$$W = aS_kG_k \tag{3}$$

where a is equal to 0.002;

S_k is the gap width;
G_k is the axial mass flux around the gap.

Finally, three parameters were fixed: cross flow resistance equal to 0.5; turbulent momentum factor equal to 0.0; and transverse momentum factor equal to 0.5. These values are typically used for a PWR, once there are no specific values available for the LABGENE.

A sensitivity analysis is needed for the models. However, as we do not yet have experimental data, we have chosen the models we judge more appropriate for the problem among those available in COBRAI-IIc. In particular, the two-phase friction model was compared to the Baroczy model and no significant difference between both models was observed.

3.1 *Critical heat flux*

Two other correlations have been considered earlier for the simulation (Carajilescov & Valente 2011). However, EPRI correlation for CHF (Eq. 4) has shown to be more adequate due to its parameter range for the application to LABGENE. It is worth noting this correlation was chosen for simulation before the experiments. The main goal of the CHF experiments for LABGENE is to formulate a correlation its own.

$$q''_{crit} = \frac{A - x_{in}}{C + \left(\frac{x_e - x_{in}}{q''_L} \right)} \tag{4}$$

where

$$A = P_1 P_r^{P_2} G^{P_5 + P_7 P_r}$$

$$C = P_3 P_r^{P_4} G^{P_6 + P_8 P_r}$$

and
q''_L is the local heat flux in $MBtu/hr - ft^2$;
x_{in} and x_e are the inlet and local qualities;
P_r is the ratio between the pressure and the critical pressure;
G is the mass flux in $M.lbs/hr - ft^2$.

4 RESULTS

Based on the operation conditions, and transient parameters where the non occurrence of DNB is required, an experimental table was proposed. From these values, the CHF was predicted using COBRA. Brent iterative method (Press et al. 2007), was implemented to find the heat flux where the DNBR was equal to 1.0. The results for the two test sections and one with the real power profile (ST1PP) are also presented in Figure 3.

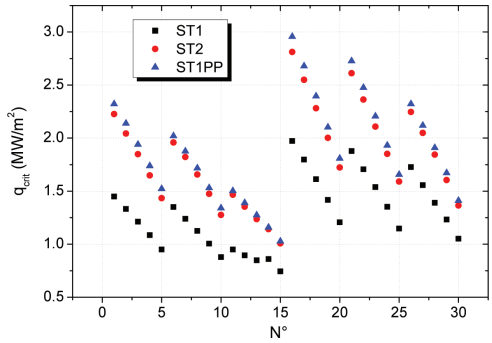


Figure 3. Critical heat flux for thirty simulated points.

Figure 3 shows the CHF behavior for the thirty simulated points. One can note that the two mass flux levels can be easily discriminated as well as the three pressure levels and the five different inlet temperatures.

CHF is approximately linear with the temperature except in the experiments from 10 to 15 for the ST1. This happens because for these operational conditions the simulations indicate CHF occurrence at rod 5(6), 1(1), 1(1), 9(16), 5(7) and 5(7), where the number between parentheses indicates the channel according to Figure 1. All other simulations indicate the DNB occurrence at rod 5 and channel 7. These results are important to foresee specific instrumentation at these rods.

Other germane points are the maximum and minimum CHF values. The maximum value indicates the power needed to perform the experiments and the minimum one indicates critical operation conditions, which are nearer to a boiling crisis.

4.1 *CHF response*

The analysis in this section was performed in order to better visualize the CHF behavior in the established conditions. Through a multi-linear regression one can evaluate the CHF as a function of temperature, pressure and mass flux. The variables were codified for values between –1.0 and 1.0 so that –1.0 represents the minimum value and +1.0 represents the maximum one. The coefficients and their standard errors are shown in Table 2, where quadratic terms proved to be non significant based on p-values greater than 0.10. The regression was performed through STATISTICA™ version 12 (Hill & Lewicki 2006).

The verification that there is no distortion (bias) in the regression was analyzed by the Pearson cor-

Table 2. Regression coefficients.

Factor	Coeff.	Std. error	p value	Cnf. limt 95%
Interc.	1.278	0.012	0.000	1.253/1.304
P (L)	–0.139	0.006	0.000	–0.152/–0.126
P (Q)	–0.007	0.013	0.621	–0.034/0.021
G (L)	0.227	0.005	0.000	0.216/0.238
T (L)	–0.269	0.007	0.000	–0.284/–0.254
T (Q)	–0.015	0.012	0.239	–0.041/0.011
P by G	0.036	0.006	0.000	0.023/0.049
P by T	0.054	0.009	0.000	0.036/0.072
G by T	–0.084	0.007	0.000	–0.100/–0.069

Table 3. Correlation matrix.

	P	G	T	P^2	T^2	P*G	P*T
G	0.00						
	1.00						
T	0.00	0.00					
	1.00	1.00					
P^2	0.21	0.00	–0.00				
	0.27	1.00	1.00				
T^2	0.00	0.00	0.00	0.00			
	1.00	1.00	1.00	1.00			
P*G	0.00	–0.15	0.00	0.00	0.00		
	1.00	0.44	1.00	1.00	1.00		
P*T	0.00	0.00	–0.15	0.00	0.00	0.00	
	1.00	1.00	0.44	1.00	1.00	1.00	
G*T	–0.00	0.00	0.00	0.00	0.00	–0.00	0.00
	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Cell contents: Pearson correlation
P-Value

relation test for the assumed independent factors. The correlation matrix displays the correlation coefficients between factors taken two by two followed by the p-value representing the significance probability of the correlation judged at a specified level of significance α (Box, Hunter, & Hunter 2005).

Table 3 shows the correlation values and p-values for the regression. It can be seen that the variables are practically orthogonal to each other. The three highest correlations had a p-value greater than 0.1 (α) and therefore we cannot say that there is correlation.

Response surfaces for ST1 are presented in Figures 4–9. Each figure shows the unfolded equations for fixed conditions in its caption. These six surfaces show the critical heat flux dependence on two variables while the third one is fixed at the lower or higher value. The orange color indicates the greatest CHF and the dark green indicates the lowest one. For all cases a low temperature suggests we need more heat flux to reach the DNB point. An interesting information to get from response surfaces are CHF contour lines.

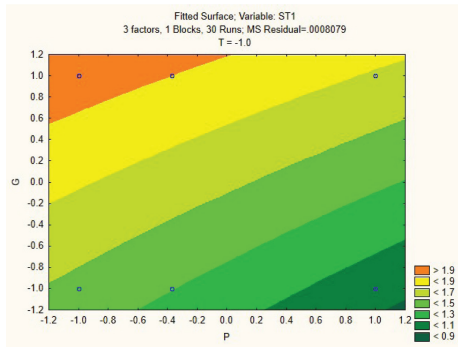


Figure 4. Critical heat flux in MW/m^2 for T = –1.0. $q''_{crit} = 1.55 - 0.19P + 0.31G + 0.04P \cdot G$.

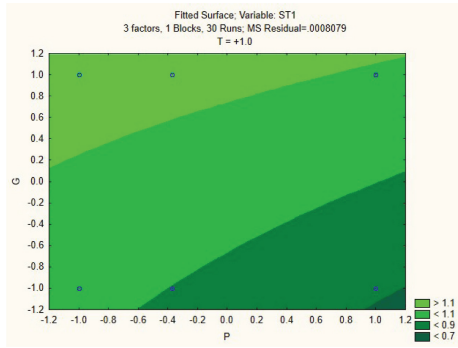


Figure 5. Critical heat flux in MW/m^2 for T = 1.0. $q''_{crit} = 1.01 - 0.09P + 0.14G + 0.04P \cdot G$.

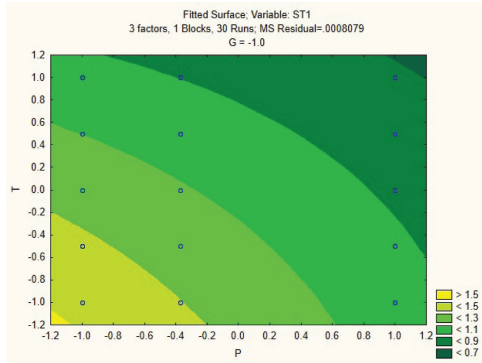


Figure 6. Critical heat flux in MW/m^2 for G = –1.0. $q''_{crit} = 1.05 - 0.18P - 0.18T + 0.05P \cdot T$.

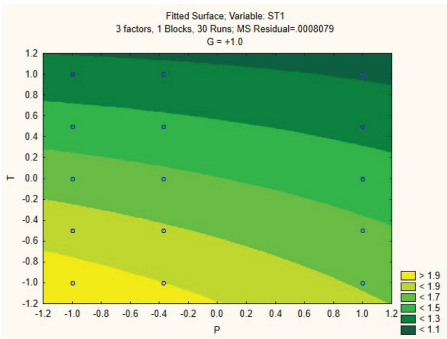


Figure 7. Critical heat flux in MW/m^2 for G = 1.0. $q''_{crit} = 1.51 - 0.10P - 0.35T + 0.05P \cdot T$.

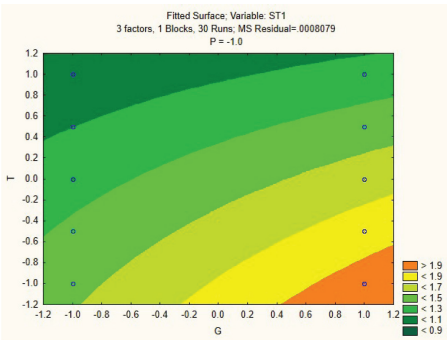


Figure 8. Critical heat flux in MW/m^2 for P = –1.0. $q''_{crit} = 1.42 + 0.19G - 0.32T - 0.08G \cdot T$.

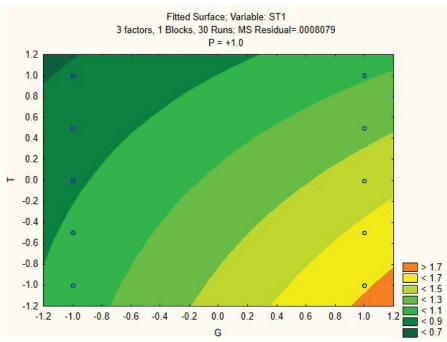


Figure 9. Critical heat flux in MW/m^2 for P = 1.0. $q''_{crit} = 1.14 + 0.26G - 0.22T - 0.08G \cdot T$.

Once we have the critical heat flux simulated for the hotspot, we can evaluate the DNBR given by Eq. 5.

$$DNBR = \frac{q''_{crit}}{q''_{real}} \quad (5)$$

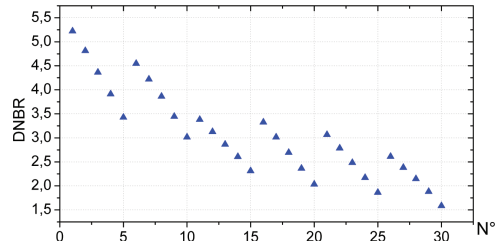


Figure 10. Departure from nucleate boiling for thirty simulated points.

where q''_{real} is given by Table 1 and Figure 2. However, the conditions of the lower mass flux are possible just with 50% power.

The calculated DNBR is shown in Figure 10. The simulations predict a boiling crisis at a height close to 25 cm. All values are above the MDNBR (Table 1), indicating a safe reactor operation. The lowest DNBR value occurs when all the parameters (pressure, mass flux and temperature) reach their maximum values, as expected.

5 CONCLUSION

Critical Heat Flux (CHF) experiments will be performed for the LABGENE with the purpose of creating a specific CHF correlation for it. In this sense, this work presents an initial analysis of the design of experiments which considered 30 operational points that take into account anticipated situations where no boiling crisis occurred. These operational points were simulated by the COBRAIIIc computer code for three cases. The results for the first case are shown by means of response surfaces in order to better visualize the CHF behavior for each condition. Once the CHF was estimated, the DNBR (Departure from Nucleate Boiling Ratio) was also estimated. The lowest DNBR found occurred for the maximum pressure, mass flux, and inlet temperature.

ACKNOWLEDGMENT

Thanks go to São Paulo Research Foundation (FAPESP), University of São Paulo (USP) and Navy Technological Center in São Paulo for their invaluable support and specially to Dr. Marcelo Veloso, Center for Development of Nuclear Technology (CDTN/CNEN).

REFERENCES

Box, G.E.P., J.S. Hunter, & W.G. Hunter (2005). *Statistics for Experimenters—Design, Innovation and Discovery* (2nd ed.). Canada: John Wiley and Sons, Inc.

Carajilescov, P. & B.R. Valente (2011). Analysis system of critical heat flux correlations in water-cooled reactors. *Proceedings of the International Nuclear Atlantic Conference—INAC 2011*. (in Portuguese).

EPRI (1983). Parametric study of chf data, volume 2: A generalized subchannel. Technical Report NP-2609, Electric Power Research Institute.

Giovedi, C., D.S. Gomes, A.Y. Abe, L.T. Hirota, & A.T. e Silva (2011). Fuel performance evaluation for the cafe experimental device. *Proceedings of the International Nuclear Atlantic Conference—INAC 2011*. (in Portuguese).

Greenwood, M.S.S., M.D. Angelis, J. Yang, M. Corradini, & M. Anderson (2013). Study of critical heat flux for a four rod bundle at small modular reactor operating conditions. *Proceedings of The 15th International Topical Meeting on Nuclear Reactor Thermal-Hydraulic, NURETH-15, May 12–17, 2013*, NURETH15-096.

Groeneveld, D.C. (2011). Anomalies and other concerns related to the critical heat flux. *Nuclear Engineering and Design* 241, 4604–4611.

Hill, T. & P. Lewicki (2006). *Statistics: Methods and Applications*. USA: Stat Software, Inc.

Jackson, J.W. & N.E. Todreas (1981). *COBRA IIIc/MIT-2: A Digital Computer Program for Steady State and Transient Thermal-Hydraulic Analysis of Rod Bundle Nuclear Fuel Elements*. US: Energy Laboratory Report No: MIT-EL 81-018.

Maragni, M.G., A. Belchior Jr., & J.A.O. Pessanha (1995). Modeling and steady state reactor inap through relap5/mod2. *Proceedings of "Encontro Nacional de Fisica de Reatores e Termo-Hidraulica"*. (in Portuguese).

Nascimento, J.A. d., L.H. Claro, S. Ono, A.D. Caldeira, A.F. Dias, & W.J. Vieira (2005). Influence of variation in the stainless steel composition in the labgene core reactivity. *Proceedings of the International Nuclear Atlantic Conference—INAC 2005*. (in Portuguese).

Natacci, F.B. & F. Corrêa (2005). Accidental sequences involving the containment of pressurized water nuclear installation (inap). *Revista Brasileira de Pesquisa e Desenvolvimento 4*, 45–48. (in Portuguese).

Press, W.H., S.A. Teukolsky, W.T. Vetterling, & B.P. Flannery (2007). Numerical Recipes—*The Art of Scientific Computing* (3rd ed.). USA: Cambridge University Press.

Todreas, N.E. & M.S. Kazimi (2001). *Nuclear Systems II—Elements of Thermal Hydraulic Design*. US: Taylor and Francis.

Todreas, N.E. & M.S. Kazimi (2012). *Nuclear Systems—Volume 1: Thermal Hydraulic Fundamentals*. Boca Ration, US: CRC Press, Taylor & Francis Group. 1004 p.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The stochastic approach in road network vulnerability analysis

Michal Bíl
Transport Research Centre, Brno, Czech Republic

Rostislav Vodák
Transport Research Centre, Brno, Czech Republic
Palacký University, Olomouc, Czech Republic

ABSTRACT: This paper draws attention to the vulnerability of road networks, when larger numbers of links are interrupted. These situations can arise as a consequence of natural disasters, terrorist attacks or additional random events. The primary aim of the vulnerability analysis is to identify those links whose interruptions have the highest impact on the given network. In order to identify the respective links, a large number of combinations of the links need to be analyzed which is beyond the scope of any computer. In this paper we provide a means of dealing with the problem using methods based on simulated annealing which do not produce the worst-case scenario in general but which enable us to produce scenarios with a sufficiently high impact.

1 INTRODUCTION

Despite the fact that miscellaneous networks can be found practically everywhere, the first papers published by Erdős & Rényi (1959, 1960) appeared in the first half of the 20th century. The boom in networks dates back to the beginning of the 21st century and is connected with a paper by Barabási & Réka (1999). This fact has two causes. The first one involved a limitation due to the slow computational speed of computers. The second limitation was caused by numerous successes in continuum mechanics in physics which assumed that the real world can be viewed as continuous. It began to be clear at the beginning of the 21st century that this approach cannot be applied universally and is completely inappropriate in various areas of physics.

Road networks represent one of the areas. Road networks have a number of features in common with additional networks (telecommunication networks, power grid). Some features are completely different, however. The first one is that road networks are of vital importance for all of society. It is almost impossible to supply people with food and medication without roads. The second one is the relative sparsity of networks when compared, for instance, with the World Wide Web. The number of road links outgoing from a node is rarely higher than 5. This means that the interruption of a small number of links can have a major impact on the functioning of human society.

The robustness and vulnerability of the road networks thus needs to be studied due to the above-mentioned reasons. The robustness enables us to study the resistance of a network to random events such as floods, landslides, etc. The analysis of the vulnerability of a road network provides us with information about those links whose interruptions have the highest impact on the entire network. This impact can consist not only of a prolongation of the shortest paths among several nodes but also the disintegration of the complete network into several parts. The respective events can be caused consciously (terrorist attacks) or unconsciously during repairs to road surfaces.

Numerous papers involve an analysis of the vulnerability of the road networks which only cover the case of one interrupted link or node (Erath et al., 2010; Jenelius et al., 2006; Latora & Marchiori 2004; Sohn 2006; Taylor et al., 2006 Van Knoop et al., 2008). The situation is actually much more complicated and the number of interrupted links is much larger. The primary aim of the administrator of the road network is to avoid the worst-case scenarios caused by interrupted links. This is the reason why there is a need to identify those links whose interruption can lead to these scenarios. The respective combination of the links must be found among the large number of combinations, however. There are, for example, 166,000,000 combinations of three interrupted links in a network with 1000 links. Despite progress in computer science, it is still impossible to analyze all the combinations and process the entire state space. Therefore, certain algorithms based upon random searching in the state space have been developed. The algorithms based upon simulated annealing are presented in this paper.

The paper consists of several parts. A basic algorithm of the simulated annealing is introduced in section 2 along with its modifications and setup. The obtained results are presented in section 3 and discussed in section 4.

2 SIMULATED ANNEALING

The algorithm was developed in connection with issues involving a large state space and with the existence of several local minima of some loss function. The algorithm does not require further assumptions on the loss function as continuity, differentiability and convexity and can also be used in the case of a discrete state space. The state space is obviously discrete and consequently the identification of the minimum of any loss function is extremely difficult as even a small change in the current combination of interrupted links can have a dramatic impact on the value of the loss function.

2.1 *The basic algorithm*

Let us assume that $\theta = (\theta_1, \ldots, \theta_n)$ represents a combination of n-interrupted links and $L(\theta)$ is a loss function which measures the impact of damage on the network. The value of the function is lower while the impact on the network is higher. Let us further denote "temperature" with T. The meaning of the variable will be clarified in the description of the algorithm. The algorithm for simulated annealing has the following form (for more details about the simulated annealing we refer to (Spall, 2003)):

1. Set an initial temperature T, a combination of interrupted links θ_0 and a loss function $L(\theta_0)$.
2. Find a new combination of interrupted links θ and determine $L(\theta)$.
3. If $L(\theta) < L(\theta_0)$, put $\theta_0 = \theta$. If $L(\theta) >= L(\theta_0)$, put $\theta_0 = \theta$ with a probability depending on T.
4. If you are unable to improve the value of L after the given number of iterations, decrease the value of T. If the new value of T is lower than the given limit, it is completed. If this is not the case, return to 2.

There are two key parts in the algorithm. The first one is part 2 where a new combination of interrupted links needs to be found. Since there is a nonzero probability of accepting a worse combination of interrupted links, there is a need to save such a combination of interrupted links which represents the smallest found value of L. The treatment of the second part is presented in the next subsection. The second one is part 3 which makes possible an escape with a certain probability from a local minimum of the loss function L. The probability depends on T and is a decreasing function.

2.2 *The basic setup*

The generation of interrupted links is based upon probabilities which are assigned to all links. There are three approaches to assigning the probabilities to links used in the paper.

1. All links have the same probability.
2. The probability is directly proportional to the length of the link.
3. The probability is directly proportional to the betweeness index of the link (Newman 2010).

The above-mentioned probabilities are used to replace the given number of interrupted links with other links which need to be interrupted. The chosen interrupted links are then assumed not to be interrupted. To obtain the number of interrupted links the following three strategies are used:

a. The maximum number of interrupted links is replaced. This number is equal to the minimum of the number of interrupted and uninterrupted links.
b. The number of replaced interrupted links is random but its value cannot exceed the minimum of the number of interrupted and uninterrupted links.
c. The number of replaced interrupted links depends on temperature T. 4 links are replaced for the range 30–40, 3 links are replaced for the range 20–30, etc.

The loss function can finally be defined. The function should be able to measure the disintegration of the network into several parts which seem to be the most important aspect in the case when greater numbers of links are interrupted. The loss function has the form:

$$L(\theta) = \sqrt{\frac{1}{m}\sum_{i=1}^{m+1}(l_i - \bar{l})^2} \tag{1}$$

where

$$\bar{l} = \frac{1}{m+1}\sum_{i=1}^{m+1} l_i \tag{2}$$

and m are the number of interrupted links and l_i is the number of people living in i-th component. The maximum number of components is $m+1$. If the network disintegrates into a smaller number of components, the further components are assumed up to the number $m+1$ but with zero people living within them. The worst-case scenario is thus the case when m interrupted links can cause the disintegration of

Table 1. The Olomouc region.

Used method	The worst initial value of $L(\theta)$	The best total value of $L(\theta)$	Number of components
1a	272202.813653	270731.713906	3
2a	272202.813653	269446.944966	5
3a	272202.813653	266046.128756	4
1b	272202.813653	252911.956843	2
2b	272202.813653	251991.231980	4
3b	272202.813653	252166.608218	4
1c	272202.813653	252911.956843	2
2c	272202.813653	252105.943310	3
3c	272202.813653	252911.956843	2

Table 2. The Zlín region.

Used method	The worst initial value of $L(\theta)$	The best total value of $L(\theta)$	Number of components
1a	180405.694892	174512.907849	6
2a	180405.694892	167675.112226	10
3a	180405.694892	166539.351550	9
1b	180405.694892	174433.360472	4
2b	180405.694892	167936.961180	9
3b	180405.694892	164893.886086	7
1c	180405.694892	174720.829681	7
2c	180405.694892	169328.173821	7
3c	180405.694892	168104.220931	8

the network into *m+1* components with the same number of people living within them. In this case the loss function is equal to zero. It is positive otherwise. This means the lower value of the loss function the higher damage of the network.

3 RESULTS

We first pay attention to input data. The initial temperature has the value 40 and after 100 iterations without an improvement of the best obtained value of the loss function L it decreases by a value 0.9 until it reaches the value 1. The number of interrupted links is 5 in the case of the Olomouc region and 10 in the case of the Zlín region. The computation was repeated 5 times.

The obtained results are presented in the tables below (see Tables 1 and 2). The used method is denoted by a combination of a digit and a letter which corresponds to the strategies introduced in the previous section. The next two columns indicate the worst initial value of the loss function, which corresponds to the case when the network remains intact, and the best total value of the loss function after 5 computations. In the last column the number of components is mentioned.

In the Table 1 we can see the result for the Olomouc region. In this case the network was adjusted in such a way that there is no dead-end link. It is apparent that there are no major differences among the results apart from the strategy a) which can be caused by the stochastic background of the algorithm. It can be seen that the disintegration of the network into a higher number of components need not represent the worst-case scenario. Moreover, in certain cases the best value of the loss function corresponds to several combinations of interrupted links.

In the second case (Table 2) we can see the results for the Zlín region. In this case dead-end links were not removed. An interesting aspect is that for all distribution of probabilities of the links strategy 3 produced the best results, because it enables the algorithm to refine the obtained results.

4 CONCLUSION

In this paper, several strategies including the method of the simulated annealing were applied to two regions with a different number of interrupted links. The primary difference between the networks was the presence of dead-end links.

Despite the fact that it is impossible to determine such a combination of interrupted links which would lead to a minimum value of the loss function, it is apparent that the used methods were able to improve the value of the loss function and in certain cases find several results corresponding to the obtained value of the loss function. The time of computation does not usually exceed 15 minutes. Improving the obtained results by prolonging the computational time would seem to be plausible. It was also observed that the strategy 3 is suitable if the dead-end links are present. The strategy is unable, however, to produce better results if all the dead-end links are removed.

The situation is interesting in the case of the use of the betweenness index. In the case the links with a larger betweenness index have the higher probability to be interrupted which corresponds more to the real world scenarios where the links with higher transit are more prone to an interruption than other links. This approach leads close to the border between the vulnerability and robustness of networks. Unfortunately, this additional information does not lead to improved results. It was also observed that the number of components of the disintegrated network need not represent the worst-case scenario which is determined by the used loss function.

It would seem apparent that the presented approach contains an unspent potential, because only a minimum of information concerning the structure of the network and about the people living within it was made use of.

ACKNOWLEDGMENTS

This paper was prepared with the help of a project undertaken by the Transport Research Centre (OP R&D for Innovation No. CZ.1.05/2.1.00/03.0064). Access to the CERIT-SC computing and storage facilities provided under the program Center CERIT Scientific Cloud, part of the Operational Program Research and Development for Innovations, reg. no. CZ.1.05/3.2.00/08.0144 is greatly appreciated.

REFERENCES

Barabási, A. & Réka, A. (1999). Emergence of scaling in random networks. *Science* 286: 509–512.

Erath, A., Birdsall, J., Axhausen, K.W., Hajdin, R. (2010). Vulnerability assessment methodology for Swiss road network. *Transportation Research Record* 2137: 118–126.

Erdős, P. & Rényi, A. (1959). On Random Graphs I. *Publicationes Mathematicae* 6: 290–297.

Erdős, P. & Rényi A. (1960). On the evolution of random graphs, *Publications of the Mathematical Institute of the Hungarian Academy of Sciences* 5: 17–61.

Jenelius, E., Petersen, T., Mattsson, L.-G. (2006). Importance and exposure in road network vulnerability analysis. *Transportation Research Part A* 40: 537–560.

Latora, V. & Marchiori, M. (2004). How the science of complex networks can help developing strategies against terrorism. *Chaos, Solitons and Fractals* 20: 69–75.

Newman, M. (2010). *Networks: An introduction*, Oxford University Press.

Sohn, J. (2006). Evaluating the significance of highway network links under the flood damage: an accessibility approach. *Transportation Research Part A* 40: 491–506.

Spall, J.C. (2003). *Introduction to Stochastic Search and Optimization*, Wiley.

Taylor, M.A.P., Sehkar, S.V.C., D'Este, G.M. (2006). Application of accessibility based methods for vulnerability analysis of strategic road networks. *Networks and Spatial Economics* 6: 267–291.

Van Knoop, V., Zuylen, H., Hoogendoorn, S. (2008). The need of spillback modelling when assessing consequences of blockings in a road network. *European Journal of Transport and Infrastructure Research* 8: 287–300.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Analysis of brake testing methods in vehicle safety

A. Bojko, A.I. Fedotov & W.P. Khalezov
Irkutsk State Technical University, Irkutsk, Russia

M. Młyńczak
Wroclaw University of Technology, Wrocław, Poland

ABSTRACT: Safety in automotive engineering depends very much on brake system and its availability for use. That ability is usually tested on stands having cylindrical drums or on stands in form of flat plates. Functionality of brake system means not only slowing down a vehicle, but requires achieving desired result as stopping a vehicle from a given speed on desired distance (Haisler 2007). There are some reports stating discrepancy of brake force measurement using two above mentioned testing methods. Paper presents methodology and results of comparative measurements of braking force on drum and flat stands. The system for experimental testing of phenomena between elastic tire and solid counter surface of diagnostic drum and flat road is shown. Results of experimental tests and analysis of normal and longitudinal stresses in contact point in the two above cases are shown. It has been noticed that distribution and values of normal and longitudinal stresses in the contact area of the tire against flat surface are meaningfully different from that obtained against cylindrical diagnostic brake drum. It is planned to propose assessment index of measurement discrepancy corresponding to hazard of brake testing.

1 INTRODUCTION

Currently, the control of brake systems of motor vehicles is performed under operational conditions as well as in the road and in the test bed conditions (testing stand). Under the conditions of the Russian climate the most effective method of brake system control is said to be stand methods. According to the magazine "*Motor Transport Company*": "*Suggested by various firms stands for assessing the technical condition of the brake system in a government inspection, for example, models LTK and stationary models STS stands Novgorod plant SIPA and foreign company Cartec, can not provide objective indicators of behavior in traffic*" (Kulko 2005, Li et al. 2011).

Studies at the Chair "Road transport" in Irkutsk State Technical University have confirmed the poor quality of assessment of technical condition of vehicles braking system in the diagnosis on a drum dynamometer. Repeatability study showed that the measured values of 40 consecutive braking forces of the same car TOYOTA-COROLLA, on the same bench STM 3500 ranges of 27,9%. The specific braking force varies of ±20% (Fedotov & Boiko 2009).

2 ANALYSIS OF DIFFERENCES IN VEHICLE BRAKE SYSTEM

There are couples of reasons for the large variability of the results of the brake system control on a drum dynamometer few. One of the most important reasons is the difference in tire contact shape on the cylindrical surface of drum stand compared to a flat road surface. The length of the tire contact patch with the cylindrical surface of the drum of 320 mm diameter is 50% less compared to the flat road surface. If the drum diameter decreases from 320 to 202 mm, this difference increases from 50% to 52%.

Width of tire contact against the surface of the drum stand of 320 mm in diameter is 5,5% larger than that against the road surface. With decreasing diameter of the drum from 320 to 202 mm, this difference increases from 5,5% to 13,4% (Fedotov et al. 2009).

3 DESCRIPTION OF LABORATORY BRAKE STAND

Based on the above results, laboratory studies have been conducted on longitudinal and normal reactions at the contact patch of the tire against rolling drum surfaces and flat, road surface. Their ultimate goal is to get a technique that allows transferring stand tests results on road conditions, i.e. predicting the magnitude of the longitudinal reactions of the wheels on the road. Scientific group of Irkutsk State Technical University (ISTU) designed and made measurement unit (Fig. 1), which allows measuring the normal and longitudinal stresses at

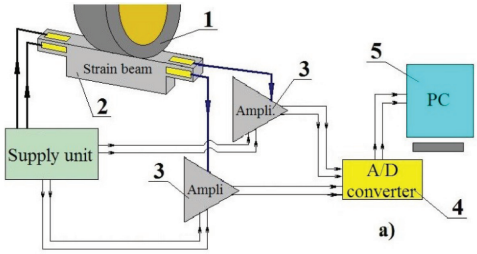


Figure 1. Block diagram of electrical circuit of measurement unit. 1—car wheel, 2—strain gauge bar, 3—electronic signal amplifier unit for longitudinal and normal stresses in the con tact wheel, 4—analog—digital converter, 5—PC.

the contact patch of the tire as on the road (flat surface) and on drum stand (Fedotov et al. 2012). Designed units consist of: strain gauge beams, electronic signal amplifier, Analog/Digital Converter (ADC) and a computer.

3.1 *Measurement of longitudinal and normal stresses on flat surface*

A system for measuring the longitudinal and normal stresses in the flat contact area is shown in Figures 2 and 3.

Flat Surface Testing System (FSTS) consists of an elastic plate 1, on the side surfaces of which the strain gauges 7 are pasted. Strain gauges of the sensor are included in the measuring circuit in a bridge circuit. Plate 1 is attached with two screws 4 to the intermediate support 3, which is attached to the support basement 2. One of the side surfaces of the plate 1 enters into the slot of the support platform of the base 2.

To prevent rotation of the plate 1 in the center of the screws 4 it has a reaction arm 5 connected to the elastic spring 8. This spring is mounted with screws on the plate 6.

The basement of the unit creates a rigid structure 2 (Fig. 4) having installed inside a transducer that while rolling the wheel allows to record two values: normal and longitudinal stresses along the contact patch of the tire.

3.2 *Measurement of longitudinal and normal stresses on drum stand*

Similar structure has Drum Testing System (DTS) recording normal and longitudinal stresses of the tire against the surface of the cylindrical surface of drum stand (Figs. 5 and 6). Running drum 10 has a cylindrical surface and for this purpose special sensor was designed, manufactured and installed in the drum stand. Especially profiled plate 2 fits

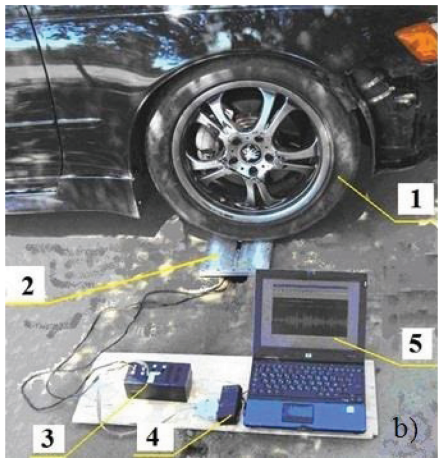


Figure 2. Stress measurement unit in flat contact area.

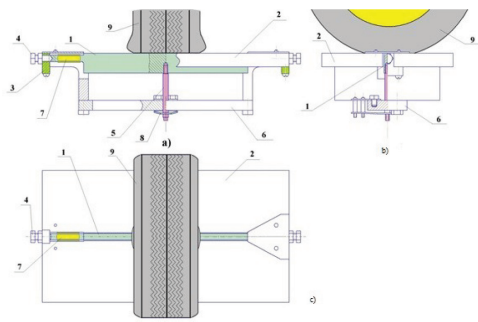


Figure 3. Sensor for measuring stress in flat contact area (road surface): a) front view, b) side view, c) top view.

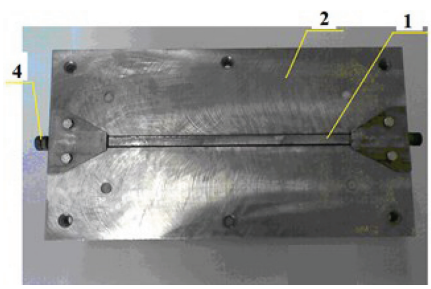


Figure 4. General view of the sensor for measuring stress in the flat contact area (road surface like).

to cylindrical surface of the drum 10 and is bolted to it. Universal elastic strain gauge plate 1 is attached to the plate 2. When the drum rotates the wheel with elastic tire runs cyclically into the built in sensor. The sensor detects the distribution of

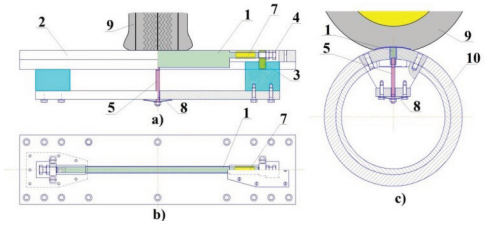


Figure 5. A sensor for measuring contact stress of the tire with the counter surface of the drum: a) front view, b) top view, c) side view.

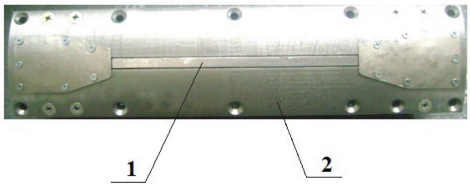


Figure 6. General view of the sensor measuring the stress in the contact of the wheel with the counter surface of the drum: 1—strain gauge plate, 2—base plate.

normal and longitudinal stresses along the length of the contact patch of the tire.

3.3 *Laboratory testing stand*

For laboratory research a stand was designed and manufactured. It is schematically shown in Figure 7. Stand allows defining the voltage at the contact patch of tire supported by the surface of the rolling drum. Wheel with test tire 5 is mounted on pivoted by ball bearing lever 6. Tire presses against the drum 9 with the support of spring 7. Drum 9 is driven by an electric motor 8 through the gearbox 10. Profile of the drum surface corresponds to usual profile of the commercial drum brake testers. Setting a weight on loading arm 4 it is possible to load tire with required value of the normal load. The beam 1 is pivotally mounted on the arm 2 and transmits the normal load to the spring 7 and the tire 5. Along the beam 1 extends an arm 6 which supports the wheel with tested tire 5. Strand 3 is connected to the sensor 11 measuring longitudinal reaction. The sensor 11 can be moved in the vertical direction in case if tested tire is of other size. Disc brake 12 provides brake torque to the wheel. Prior to testing, varying the length of the beam 3, wheel 5 is mounted on a chassis dynamometer 9 so, that the resultant braking force vector is parallel to the axis of the beam 3.

To enhance the range of research it is provided in the design of the stand an apparatus 2 to allow

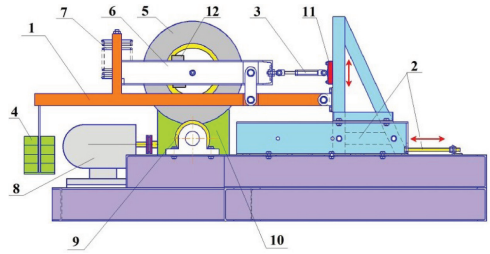


Figure 7. Scheme of the stand to determine the stresses in the tire contact area with cylindrical drum surface.

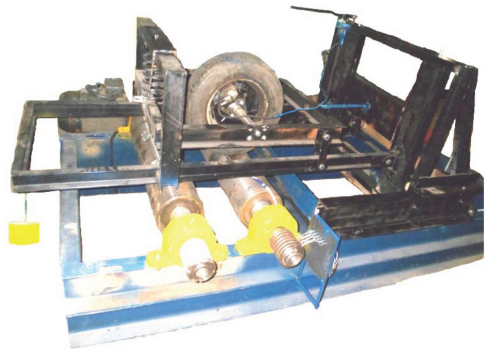


Figure 8. General view of the stand to determine the stresses in the tire contact area with cylindrical drum surface.

longitudinal displacement relative to the center of brake drum. Designed testing system (Fig. 8) allows studying processes occurring in the contact area of tire and drum surface and get diagrams of normal and longitudinal stresses.

It was tested radial tire manufactured by Amtel Planet T-301 of a size 185/65 R14, 86 N. Tread height was measured as 5 mm, which corresponds to the wear level of the wheel of about 30%. Normal wheel load was 3400 N, which corresponds to the weight of the wheel running at front axle on Toyota Fielder. Experiments were carried out at different inflation pressure. The range of pressure was: 0.231, 0,21, 0.19, 0.17, 0.15, 0,13 and 0,105 MPa. The purpose of the research with different pressure was to study on brake properties of the tire.

4 RESEARCH OF STRESSES RESULTS

Experiments were performed both on road and in the test bed conditions in braking mode (full blocked wheel while moved over the sensor surface).

Laboratory experiments were performed on a drum dynamometer (Fig. 8) in the laboratory of "Road Transport Chair" of Irkutsk State Technical University.

The experimental road results were compared with results obtained on laboratory drum stand. Diagrams of distribution of normal and longitudinal stresses along the length of the tire contact area of the flat testing surface were compared with that on cylindrical drum surface.

Comparison of the results of research carried out in a braking wheel (Fig. 9) shows that the shape of diagrams of normal stresses in the road and stand conditions is significantly different. In the road conditions, the length of the tire contact is two times larger than on a braking drum. Inflation pressure varies length of the contact from 110 mm at highest pressure to 160 mm at lowest one at "road conditions" (flat tester) and respectively from 48 mm to 92 mm. The contact length is doubled for flat contact surface.

The numerical values of the normal stresses at the contact area of the tire in the road and stand conditions differ significantly. The maximum value of the normal stresses at the contact patch on a flat tire braking road surface is $\Delta Rz = 0{,}55$ kN and on the cylindrical surface of the brake drum is $\Delta Rz = 1{,}25$ kN, by tire pressure 0,23 MPa. For braking wheel on cylindrical surface having a diameter 0,24 m, normal stress in the contact area ΔRz exceeds the normal stress on a flat road surface about 2,2 times.

The results of studies of the longitudinal stresses in the wheel braking mode (Fig. 10) show that the shape of the distribution diagram of the longitudinal stresses in the road and stand conditions also differ considerably. On a flat road surface diagram of the longitudinal stresses distribution is sinusoidal. In the laboratory, on the cylindrical surface of a drum dynamometer, diagram of normal stress has a shape close to a triangle, and with decreasing of tire pressure it becomes trapezoidal.

The maximum value of the longitudinal stresses in the contact patch on a flat tire braking road surface is $\Delta Rx = 0{,}15$ kN and on the cylindrical surface of the drum stand is $\Delta Rx = 1{,}45$ kN, at tire pressure of 0,23 MPa. When braking wheels with elastic tire on the cylindrical surface of the drum having a diameter of 0,24 m longitudinal stress ΔRx exceeds the longitudinal stresses in the wheel braking on a flat road surface of 9,5 times.

Comparing brake tests performed on flat and drum testers one may notice large difference in contact length between tire and counter surface. Stand with flat counter surface makes double contact length at comparative inflation.

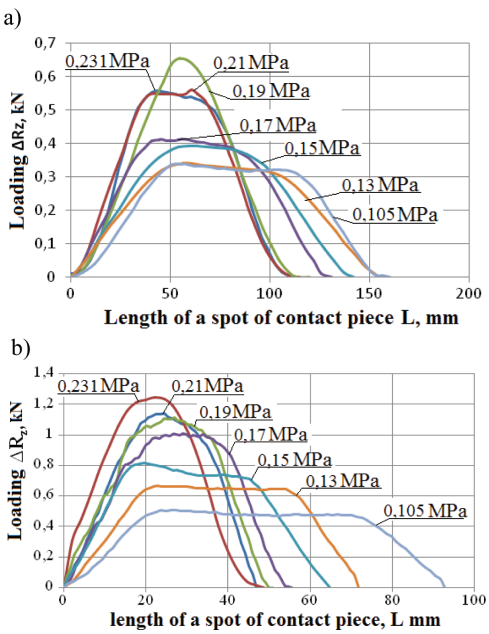


Figure 9. Graph of normal stresses in the tire contact patch while braking a wheel with respect to inflation pressure: a) on a flat road surface, b) on the cylindrical surface of the drum of 0,24 m in diameter.

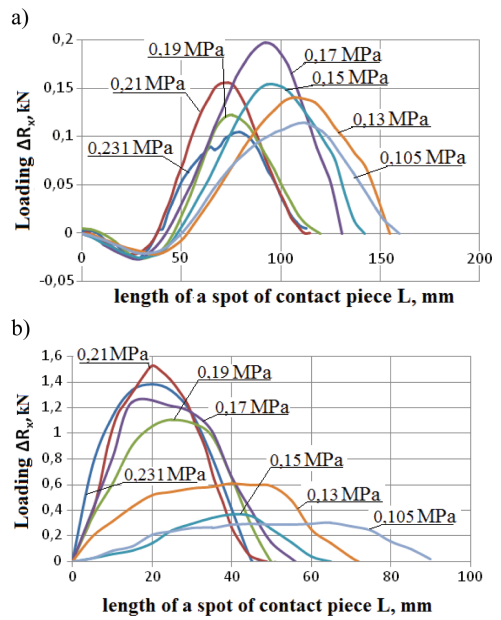


Figure 10. Graph of longitudinal stresses in the tire contact patch while braking a wheel: a) on a flat road surface, b) on the cylindrical surface of the drum of 0,24 m in diameter.

5 CONCLUSIONS

The results of the pilot study suggest the following conclusions:

- shape of distributions of longitudinal and normal reactions at the contact patch of elastic tires against flat and cylindrical surface (in the road and stand conditions) significantly differ both qualitatively and quantitatively,
- braking wheels with elastic tire (tire company Amtel Planet T-301 size 185/65 R14 86 N, normal wheel load was 3400 N) on the cylindrical surface of the drum having a diameter of 0,24 m to the normal stress in the contact exceeds ΔRz normal stress on the flat road surface 2,2 times,
- while braking, the numerical values of the longitudinal stresses ΔRx of tire contact patch with the cylindrical surface of the drum are different from the numerical values of the longitudinal stresses at similar ΔRx wheel braking on a flat supporting surface by 9,5 times,
- with decreasing of pressure in the tire contact patch length increases by more than two times,
- ΔRx of longitudinal stress in the tire contact patch with the cylindrical surface of the drum having diameter of 0,24 m exceeds the longitudinal stresses in the tire contact patch with a flat supporting surface by 35%.

REFERENCES

Fedotov A.I., Boiko A.V., 2009. Effectiveness of control methods bench brake systems in operation. / Proceedings. II International Scientific and Practical Conference "Problems of diagnosis and operation of road transport" Irkutsk Irkutsk State Technical University. p. 115–125.

Fedotov A.I., Boiko A.V., Tsogt D. et al., 2009. Experimental study of the parameters characterizing the interaction of road wheels or castors diagnostic stands. ISTU Herald. no. 4.—Irkutsk: Irkutsk State Technical University. p. 72–77.

Fedotov A.I., Boiko A.V., Tsogt D. et al., 2012. Experimental studies of the interaction of elastic wheel racing drums and expensive. ISTU Herald. no. 9.—Irkutsk: Irkutsk State Technical University. p. 157–163.

Haisler H., 2007. Advanced Vehicle Technology. Oxford, Elsevier.

Kulko P.A., 2005. State Inspection. Problems and solutions/KV Ushakov/Transport company. no. 9. p. 15–19.

Li J., Zha X., Wu D., 2011. The Theoretical Analysis of Test Result's Errors for the Roller Type Automobile Brake Tester. in: Computer and Computing Technologies in Agriculture IV. Nanchang: Springer.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Hilbert-Huang Transforms for fault detection and degradation assessment in electrical motors

M. Rigamonti
Energy Department, Politecnico di Milano, Milan, Italy

S. Rantala
VTT Technical Research Centre of Finland, Tampere, Finland

ABSTRACT: The present work develops a methodology for the analysis of transient signals for fault detection and diagnosis in electrical motors. The objective of this work is the initial development of a Prognostic and Health Monitoring System (PHMS) for the demagnetization of the magnetic field source of a Permanent Magnet Synchronous Motor (PMSM) used in electrical vehicles. The developed methodology is based on the Hilbert-Huang Transform (HHT), a technique which is particularly suitable for processing oscillating transient signals, such as the stator currents typical of automotive electric traction machines. The HHT represents a time-dependent series in a two-dimensional time-frequency domain by extracting instantaneous frequency components within the signal through an Empirical Mode Decomposition (EMD) process. The developed framework has been applied to four transients simulating different levels of demagnetization of the permanent magnet of the PMSM; the obtained results show that HHT enables us to detect and assess the degradation level for a demagnetized core of a PMSM.

1 INTRODUCTION

Permanent Magnet Synchronous Motor (PMSM) machines are attractive for a variety of applications, such as automotive and aerospace drives, because of their excellent efficiency and high power density. This work has been performed within the European project "*Electrical powertrain Health Monitoring for Increased Safety of FEVs*" (HEMIS) which aims at developing a Prognostic and Health Monitoring System (PHMS) for increasing safety and reliability and reducing the maintenance costs of FEVs (Sedano et al. 2013, Baraldi et al. 2013a).

The most significant signatures for fault detection and fault diagnosis of PMSM are the stator currents, which are heavily influenced by several degradation mechanisms typical of these electrical machines, such as permanent magnet demagnetization, stator windings short and open circuits, bearings degradation and rotor shaft eccentricities. Several techniques, such as Fast Fourier Transform (FFT) and advanced Wavelet Analysis, have already been used in order to analyze the motor currents for the identification of incipient failures (Rosero et al. 2006a, b, Gritli et al. 2012). These techniques generally allow performing fault detection and diagnosis, but they are suitable for treating oscillatory signals only in stationary conditions.

Although these represent a common situation in most industrial applications, in this work the focus is on the development of a PHMS for a PMSM used in automotive drives, which typically works under non-stationary conditions. In order to be able to treat those non-stationary signals and to properly extract the meaningful informations, we will apply the Hilbert-Huang Transform (HHT) (Huang et al. 1998, Kizhner et al. 2004) to the stator currents of the PMSM. The HHT represents a time-dependent series, i.e. in this case the stator current, in a two-dimensional time-frequency domain by extracting instantaneous frequency components within the signal through an Empirical Mode Decomposition (EMD) process (Huang et al. 1998, Kizhner et al. 2004, Espinosa et al. 2010, Yan & Gao 2007, Ruiz et al. 2010). The HHT analysis of the stator current signals enables us to identify and compare the instantaneous frequency and the instantaneous amplitude of the Intrinsic Mode Function (IMF) obtained by the EMD process.

As previously noted, there are several typical degradation mechanisms which can affect the PMSM: this work, in particular, will focus on the detection of demagnetization of the permanent magnet of the PMSM, aiming at identifying and assessing the level of demagnetization, i.e. quantifying the degradation (Baraldi et al. 2013b). The developed framework has been finally applied to four transients simulating different levels of demagnetization, showing that the HHT analysis allows the degradation level for a demagnetized

core of a PMSM to be detected and assessed. The remaining part of the paper is organized as follows: Section 2 states the problem; Section 3 describes the methodology; Section 4 shows the obtained results; finally, in Section 5, some conclusions and remarks are provided.

2 PROBLEM STATEMENT

The PMSM can be considered as a combination of a Brushless DC motor (BLDC) and an AC induction motor. They have similar rotor than BLDC, but they are commonly called as brushless AC machine. The permanent magnets, which contain usually rare earth magnetic materials, are located either in the surface of the stator or buried inside to the stator. Since magnetic properties of rare earth materials are highly temperature dependent, too high temperatures inside the motor can cause partial demagnetization of magnets. In order to identify the demagnetization of a PMSM, the most significant signature to be considered is the stator current (Rosero et al. 2006a, b, Gritli et al. 2012). In this study the simulation model of PMSM and inverter has been created in MathWork's Simulink environment with Simscape and SimPowerSystems. There are ready-made models of PMSMs in the library of SimPowerSystems. The model of the 3 phase PMSM was modified so that it was possible to modify its flux linkage. The motor is driven by the PWM inverter with was added to the system. Also some measurements were appended. The model is shown in the Figure 1. Inputs to the model is torque and speed demand. Outputs are different measurements. From the measurements we have considered only the phase α of the stator current.

2.1 *Dataset description*

The dataset consists of four simulated stator current transients (phase α) of a PMSM: one transient represents the normal operating condition, i.e. the permanent magnet is not degraded, while the other three represent the behavior of the stator current under different levels of demagnetization. In these

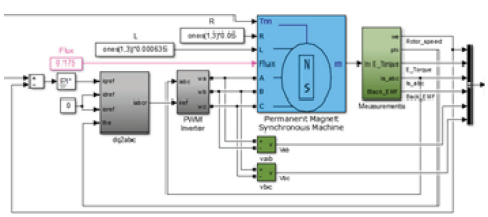


Figure 1. Simulation system of PMSM and inverter.

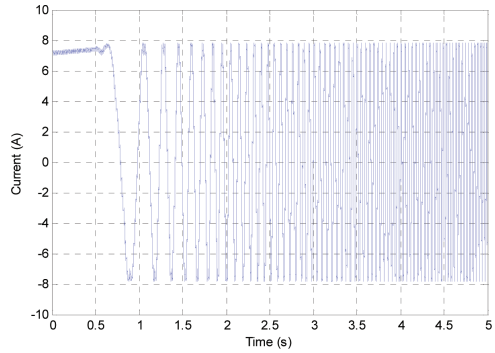


Figure 2. Stator current phase α—20% flux linkage.

simulations the motor speed was increased linearly from 0 rpm to 1800 rpm over 4.5 seconds starting from 0.5 s, in order to represent typical operating conditions of an automotive drive, which are continuously varying. In order to represent the degradation of the permanent magnet, the simulations were performed with different values of the flux linkage, a motor parameter which represents the demagnetization level of the permanent magnet. The three transients representing different levels of demagnetization are characterized respectively by 20%, 50% and 80% of the nominal flux linkage: the lower the flux linkage, the larger the degradation level. Figure 2 shows the phase α of the stator current for the transients representing the most degraded condition, which is characterized by the 20% of the nominal flux linkage value.

3 METHODOLOGY

The proposed approach comprises three steps: pretreatment of the transient to reduce the size of the datasets, EMD to extract the IMFs, and HHT to analyze the IMFs.

3.1 *Data pre-treatment*

To limit the computational requirements, we reduced the size of the original datasets, which were in the order of 2.5 million values in 5 seconds, equal to a sampling frequency of 0.5 MHz. We achieved this by resampling one point in every 25 from the original signal. In doing this, we have tried to lose the least possible information carried by the signal whilst trying to preserve the main functional behavior which characterizes the stator currents. Moreover, in order to further reduce the computational requirements, for each transient we have considered only the time interval in which the rotational speed of the motor increases from 800 rpm to 1600 rpm.

Our dataset is finally composed by four transients of the stator current signal, each one including about 40000 measurements for a time length of 2 seconds. Figure 3 graphically shows the impact of this procedure; the original signal is represented in the bottom-left figure, while the resampled signal is represented in the bottom-right figure. In the upper part of Figure 3 an enlargement of the original stator current signal shows the presence of high-frequency (40 kHz) low-amplitude (0.2 A) internal oscillations that have been lost through the resampling procedure. Although these oscillations may provide some useful information about the degradation of the PMSM, excessive computational requirements prevent their treatment with the techniques described below. However, the results have shown that the majority of the information about the behavior of the degraded PMSM is contained in the principal functional behavior of the stator current signal, which, as shown in Figure 2 bottom-right, has been preserved by our data pre-treatment procedure.

The sampling frequency of the final dataset is then around 20 kHz, which closer to the sampling frequency of a real current sensor than that of the raw simulation data (0.5 MHz).

3.2 *Empirical-Mode Decomposition (EMD)*

An IMF is a function that satisfies two conditions: i) in the whole dataset, the number of extrema and the number of zero crossings must either be equal or differ at most by one; ii) at any point, the mean value of the envelope defined by the local maxima and the envelope defined by the local minima is zero. The EMD extracts the first IMF by the following sifting process (Liu et al. 2006):

1. Find the upper envelope of $x(t)$ as the cubic spline interpolated of its local maxima, and the lower envelope, as the cubic spline interpolated of its local minima.

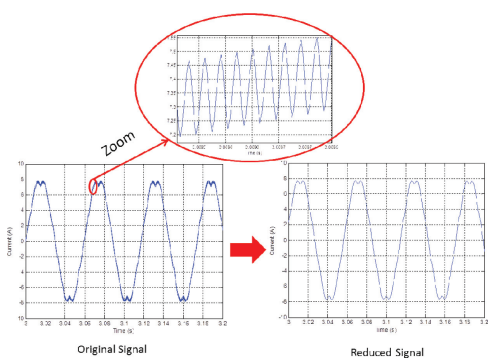


Figure 3. Illustration of the sampling and smoothing procedure used for signal pre-treatment.

2. Compute the envelope mean $m(t)$ as the average of the upper and lower envelopes.
3. Compute

$$h(t) = x(t) - m(t) \tag{1}$$

4. If the sifting result $h(t)$ satisfies the criteria for an IMF, stop. Otherwise, treat $h(t)$ as the signal and iterate on $h(t)$ through steps 1–4.

The EMD extracts the next IMF by applying the aforementioned procedure to the residue

$$r_1(t) = x(t) - c_1(t) \tag{2}$$

where $c_1(t)$ denotes the first IMF. This process is repeated until the last residue $r_n(t)$ has at most one local extreme. The first IMF component from the data contains the highest oscillation frequencies found in the original data $x(t)$.

3.3 *Hilbert-Huang Transform (HHT)*

Once the IMFs have been obtained by means of the EMD method, the Hilbert transform is performed to each IMF component as follows:

$$H\left[c_i(t)\right] = \frac{1}{\pi}\int_{-\infty}^{+\infty}\frac{c_i(\tau)}{t-\tau}d\tau \tag{3}$$

which means that $c_i(t)$ and $H[c_i(t)]$ form a complex conjugate pair, so that an analytic signal z_i is defined as:

$$z_i(t) = a_i(t)e^{j\omega_i(t)} \tag{4}$$

where $a_i(t)$ and $\omega_i(t)$ represent the instantaneous amplitude and frequency, respectively. To transform this temporal-space data to time-frequency space, the Hilbert transform is performed on each IMF component obtained by means of the EMD method as:

$$a_i(t) = \sqrt{c_i^2(t) + H^2\left[c_i(t)\right]} \tag{5}$$

$$\theta_i(t) = \arctan\left(\frac{H^2\left[c_i(t)\right]}{c_i(t)}\right) \tag{6}$$

In this way, the instantaneous frequency $\omega_i(t)$ is given by:

$$\omega_i(t) = \frac{d\theta_i(t)}{dt} \tag{7}$$

After performing the Hilbert transform on each IMF component, we can finally express the original data in the following form:

$$x(t) = \mathrm{Re}\sum_{i=1}^{n} a_i(t)\exp\left(j\int_{-\infty}^{t}\omega_i(t)dt\right) \tag{8}$$

where $Re\{\cdot\}$ denotes the real part of a complex quantity.

Following this procedure, the amplitude and instantaneous frequency for every IMF at every time step are computed. This result can be projected on the time-frequency-energy space, with energy defined as the amplitude squared, enabling us to compare the Hilbert spectra of the simulated currents waveforms.

4 APPLICATION OF THE METHOD AND RESULTS

As described in Section 3.1, our final dataset is composed by $k = 4$ transients of the stator current signal, each one comprising about 40000 measurements. For each transient signal we have performed the EMD obtaining $i = 5$ IMFs $c_{i,k}(t)$, i=1, .., 5, k = 1, .., 4: it has to be remarked that the first IMF is characterized by the highest frequency, while the fifth IMF is characterized by the lowest frequency. For each identified IMF $c_{i,k}(t)$, we have computed the Hilbert Transform by means of Eq. 3. Then, using Eq. 5 we have computed the instantaneous amplitude $a_{i,k}(t)$; finally, applying first Eq.6 and then Eq. 7 to each $c_{i,k}(t)$ we have computed the instantaneous frequency $\omega_{i,k}(t)$ for each IMF of each transient, i=1, .., 5, k = 1, .., 4. Figure 4 shows the Hilbert spectrum of the four considered transients, which are characterized by an increasing value of flux linkage, i.e. decreasing degradation level. The 3D space of the Hilbert spectrum is represented on a 2D figure, using a color scale in order to represent the amplitude of the obtained IMF. Notice that the color scale is the same for all the subfigures of Figure 4.

In order to highlight the most energetic IMFs, i.e. the IMFs characterized by the largest amplitude, we have decided to assign the black color to amplitude values close to zero and to use a black background with the intent of hiding the low energy IMFs. The effects of this choice are clearly noticeable: in the upper-left subfigure of Figure 4, the instantaneous frequency of the first IMF is a large band whose average increases from 100 Hz to 150 Hz, and is characterized by a dark red color, which represents a low amplitude. In the other three subfigures of Figure 4, the functional behaviors of the instantaneous frequencies of the first IMFs are almost the same, but it is not possible to notice them because they are characterized by a very dark color which makes them indistinguishable from the black background color. It is possible to notice the presence of these IMF frequencies only because they cover

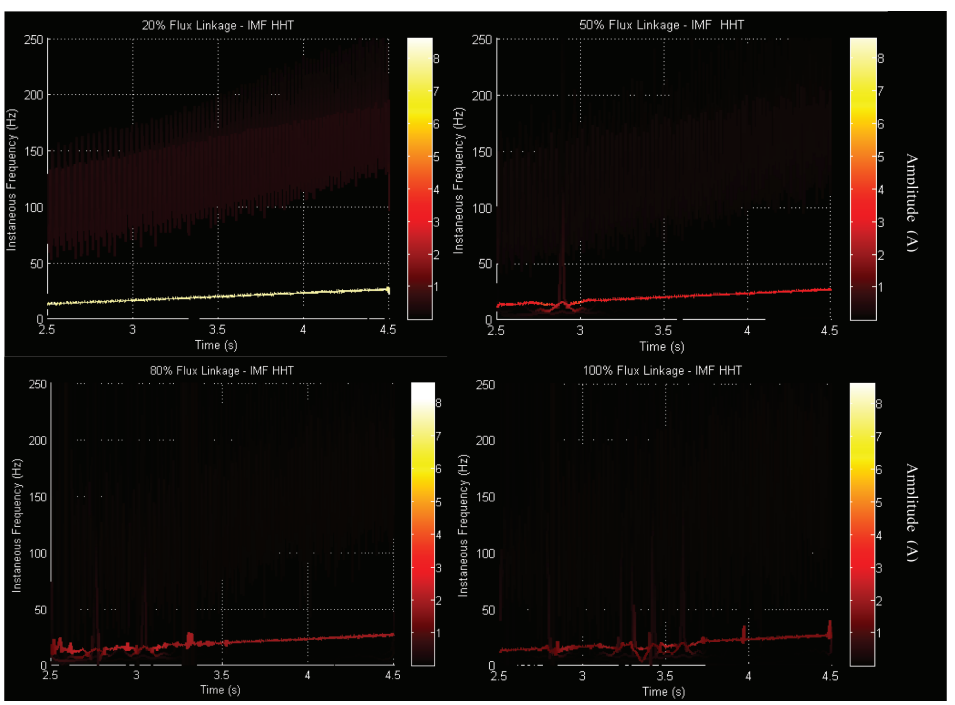


Figure 4. Hilbert spectrum for 20%, 50%, 80%, 100% flux linkage.

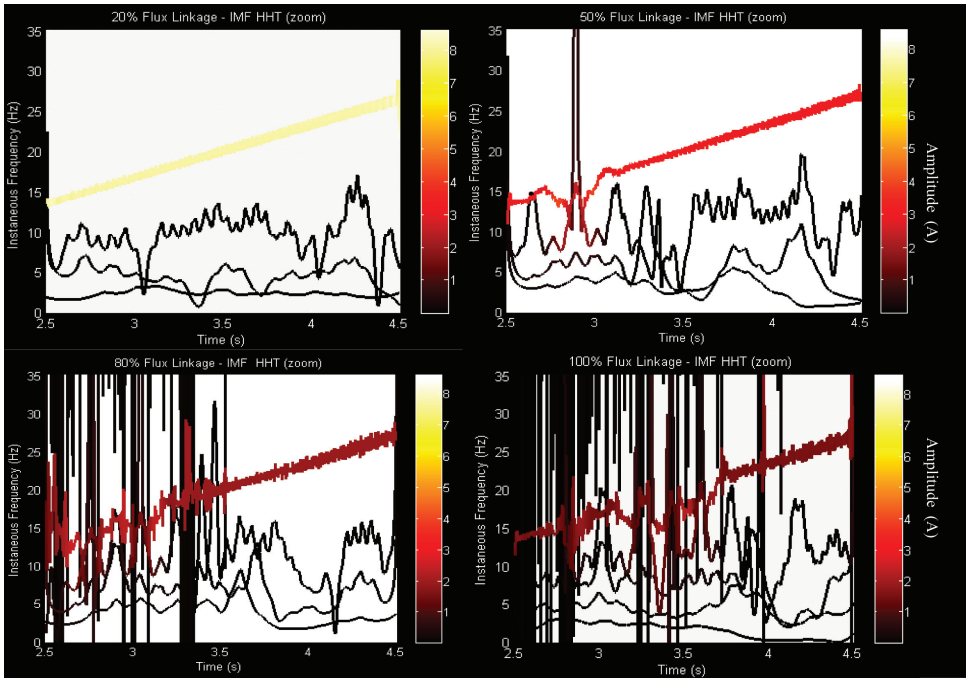


Figure 5. Enlargement of the Hilbert spectrum for 20%, 50%, 80%, 100% flux linkage.

the white grid of the figure: this means that the energy levels of these IMFs are very low. However, the main difference highlighted by Figure 4 is the amplitude of the instantaneous frequencies of the second IMFs, which are all represented by a line continuously increasing from 15 Hz to 28 Hz. Although their functional behaviors are almost the same, they are characterized by different constant amplitude values, increasing from the 1.5 A of the nominal condition (dark red, bottom-right), to the 7.8 A of the most degraded condition (yellow, upper-left). Thus, using the Hilbert spectrum of the second IMFs it is possible to clearly distinguish between healthy and degraded conditions of the permanent magnet of the PMSM; furthermore, based on amplitude of these spectra it is also possible to distinguish and classify the different degradation levels. From a physical point of view, these results can be considered as expected: in fact, if the permanent magnet of a PMSM is demagnetized (i.e. the internal magnetic field is lower than in the nominal case), a larger stator current will be needed in order to produce the same acceleration. Figure 5 shows an enlargement of Figure 4; in addition to the second IMF spectrum, it is also possible to observe the spectra of the third, fourth and fifth IMFs. Their functional behaviors can be considered comparable, even if their shapes are not exactly the same as found for the second IMF.

Their amplitudes are very close to zero, resulting in a very dark coloration which represents their low energetic significance. It is important to point out that the oscillating effects appearing in the two bottom subfigures of Figure 5 are mainly due to computational and numerical errors of the MATLAB code used for the HHT computation and do not provide any information about the demagnetization of the PMSM permanent magnet. Notice that also in this case the color scale is the same for all the subfigures of Figure 5.

5 CONCLUSION AND FUTURE WORK

In this work we analyzed four simulated stator current transients representing different levels of permanent magnet demagnetization in a PMSM, at 20%, 50%, 80% and 100% of the nominal value Since these transients represent an automotive drive linearly accelerating from 0 rpm to 1800 rpm during 5 seconds, we decided to analyze the Hilbert spectra of these signals resorting to the HHT analysis described in Section 3, which has been developed for treating non-linear and non-stationary oscillating signals (Kizhner et al. 2004). This technique can be divided in two steps: i) EMD and ii) HHT. In addition, a preliminary data reduction step was required in order to limit the computational

requirements for the analysis. The resulting Hilbert spectra have been compared in order to detect and assess the degradation level of the PMSM permanent magnet. It has been shown that, in this case, the most significant components are the Hilbert spectra of the first and second IMFs. Although the functional behavior of the signals is similar, it is possible to distinguish between the different levels of degradation by focusing on the amplitudes of the IMFs; in particular, the larger the demagnetization of the motor, the larger the amplitude of the corresponding IMFs of the stator currents. The results obtained suggest significant opportunities for the improvement of the methodology. In particular, a possible next step for this work is the development of a classification tool based on the "brightness" difference between the Hilbert spectra of the signals: the rationale behind this consideration is that the brightness difference, which is due both to the amplitude and the frequency differences, is representative of the energy difference between two signals. Thus, if we represent the Hilbert spectrum as in Figure 4, we can develop an automatic tool for the PHMS which, based on the HHT analysis, will be able to distinguish and automatically classify the PMSM degradation due to the field source demagnetization.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Community's Framework Programme (FP7/2007-2013) under grant agreement n° 314609. The authors are grateful for the support and contributions from other members of the HEMIS project consortium, from CEIT (Spain), IDIADA (Spain), Jema (Spain), MIRA (UK), Politecnico di Milano (Italy), VTT (Finland), and York EMC Services (UK). Further information can be found on the project website (www.hemis-eu.org).

We also express our gratitude to Dr. Alastair Ruddle of MIRA for his careful revision of the paper.

REFERENCES

Baraldi, P., Barbisotti, F., Capanna, R., Colombo, S., Rigamonti, M., Zio, E., 2013a. Assessment of the performance of a fully electric vehicle in presence of a prognostic and health monitoring system. *Chemical Engineering Transactions*, 33, pp. 787–792.

Baraldi, P., Zio, E., Mangili, F., Gola, G., Nystad, B.H., 2013b. Ensemble of Kernel Regression Models for Assessing the Health State of Choke Valves in Offshore Oil Platforms. *International Journal of Computational Intelligence Systems*, on-line.

Espinosa, A.G., Rosero, J.A., Cusidó, J., Romeral, L. & Ortega, J.A. 2010. Fault detection by means of Hilbert-Huang transform of the stator current in a PMSM with demagnetization. *IEEE Transactions on Energy Conversion* 25(2), art. no. 5404255: pp. 312–318.

Gritli, Y., Rossi, C., Casadei, D., Zarri, L. & Filippetti, F. 2012. Demagnetizations diagnosis for Permanent Magnet Synchronous Motors based on advanced Wavelet Analysis. *Proceedings—2012 20th International Conference on Electrical Machines, ICEM 2012*, art. no. 6350219: pp. 2397–2403.

Huang, N.E., Shen, Z., Long, S.R., Wu, M.C., Shih, H.H., Zheng, Q., Yen, N.C., Tung, C.C. & Liu, H.H. 1998. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. *Proc. R. Soc. A, Math., Phys. Eng. Sci.,* vol. 454: pp. 903–995.

Kizhner, S., Flatley, T.P., Huang, N.E., Blank, K., Conwell, E. & Smith, D. 2004. On the Hilbert-Huang transform data processing system development. *IEEE Aerospace Conference Proceedings* 3: pp. 1961–1978.

Liu, B., Riemenschneider, S. & Xu, Y. 2006. Gearbox fault diagnosis using empirical mode decomposition and Hilbert spectrum. *Mechanical Systems and Signal Processing* 20 (3): pp. 718–734.

Rosero, J.A., Cusido, J., Garcia, A., Ortega, J.A. & Romeral, L. 2006a. Study on the permanent magnet demagnetization fault in permanent magnet synchronous machines. *IECON Proceedings (Industrial Electronics Conference)*, art. no. 4153043: pp. 879–884.

Rosero, J.A., Cusido, J., Garcia, A., Ortega, J.A. & Romeral, L. 2006b. Broken bearings and eccentricity fault detection for a permanent magnet synchronous motor. *IECON Proceedings (Industrial Electronics Conference)*, art. no. 4153044: pp. 964–969.

Ruiz, J.-R.R., Garcia Espinosa, A., Romeral, L. & Cusidó, J. 2010. Demagnetization diagnosis in permanent magnet synchronous motors under non-stationary speed conditions. *Electric Power Systems Research* 80 (10): pp. 1277–1285.

Sedano, B., Ruddle, A.R., Unane, I., Low, L., Astigarraga, D., Ibarra, I., Cerro, I., Galarza, A., 2013. HEMIS: electrical powertrain health monitoring for increased safety of FEVs. *Chemical Engineering Transactions*, 33, pp. 781–786.

Yan, R. & Gao, R.X. 2007. A tour of the tour of the Hilbert-Huang transform: An empirical tool for signal analysis. *IEEE Instrumentation and Measurement Magazine* 10(5): pp. 40–45.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Volatility regime switching and jump-diffusion process for prognosis: Case of equity price modeling

H. Ghamlouch, M. Fouladirad & A. Grall
CNRS UMR 6279, Institut Charles Delaunay, Université de Technologie de Troyes, Troyes, France

ABSTRACT: Data modeling is a critical step in working with real dataset in order to characterize the collected data and their dynamics. Accurate data modeling is needed in many domains for prognosis, forecasting, passage-time prediction, and other data based analysis. In this document we give an application of financial data modeling within the framework of asset price forecasting and risk prediction. Having the price evolution of different equity indexes from different countries for almost 20 years, the aim of our project is to suggest a suitable model describing the dynamics of these indexes. Several types of asset price modeling were considered and improved over years. The work in this paper is focused on stochastic processes. Comparing the volatility behavior of different indexes, the external environment is divided into three states. The transition between these three states is controlled by an external covariate following a Markov chain. At each state the price of the index is considered to follow a jump-diffusion process with Log-Uniform Jump Amplitude. Combining the Markov chain and the jump-diffusion process the resulting model will represent the price variation behavior and can be used for price forecasting and risk prediction.

1 INTRODUCTION

In engineering, as in many domains, system design and surveillance requires the collection and analysis of different types of information. Data analysis forms the fundamental work in system understanding and performance evaluation (working conditions, reliability evaluation, risk-based decision-making ...). However, working with real data may introduce signals that cannot be modeled exactly by an analytic expression or in a deterministic way (noise waveforms, biological signals, temperature histories, communication signals, stock prices ...). Considering the random evolution of collected data over time, a good representation of their dynamic would be a stochastic process (Wiener, Gamma, stochastic differential equations ...). In general, stochastic processes are suitable tools to model the system behavior by taking into account its dynamic evolution and the influencing random phenomenon. Stochastic calculus and control play a significant role in various disciplines of engineering (Lin, de Weck, & MacGowan 2008), physics, biology (Giraudo & Sacerdote 1997) and finance (Bhar, Colwell, & Xiao 2013, Zhao, Rong, & Zhao 2013) ...

Besides their probabilistic behavior and non-deterministic general dynamics, an additional factor that may appear in real data variation is "jumps". Jumps are formed by the relatively large fluctuation (positive or negative variation) with respect to the mean and variance of the actual variation distribution. One important type of stochastic process that has the ability to describe the general behavior of data evolution as well as the particular large fluctuations is the jump-diffusion process. Taking into consideration the changes in the influencing environment, this type of stochastic model is proposed in this paper with a financial application.

Using real data, we are trying to find the suitable stochastic model. The collected dataset consists of the daily closing prices for 13 equity indexes from different countries. Starting from 1th January 1993 until 11th January 2013, the corresponding data series for each index forms 5000 daily points. In a preliminary study we found that the probability distribution of the log-returns follows a combined density function of Normal and Laplace distribution, which is consistent with the previously mentioned proprieties of real data. In section 2, the model that we propose to use for the description of the dynamic of equity indexes is presented. First the data evolution is represented and briefly descried in order to clarify the chosen model motivation. Afterwards the two essential parts of the proposed model are represented: the economic environmental is divided into three states (calm, normal and agitated) controlled by an external covariate that follows a Markov Chain, and the price evolution of different index at each state is considered to follow a log-normal diffusion, log-uniform jump

amplitude stochastic process. The jump-diffusion process description and estimation method of the process parameters are given. In the section 3 case studies are represented, giving the technical consideration of the calibration method. Real data evolution and simulated data from the chosen model are compared.

2 STOCHASTIC MODEL AND DATA EVOLUTION

In Figure 1 we show the values of daily evolution (called log-returns) of four different collected data series (SPX Index, CAC Index, DAX Index and SMI Index). In order to decide which model is the best to describe the data dynamic, we have toexamine the variation of the growth rate and the volatility of the collected data with respect to time. Visually, the return variance is not constant over the time. In addition the variance behavior is found to be similar for different indexes. Taking the period of 20 years (from Jan. 1993 to Jan. 2013), we found that the log-return variance ups and downs are almost simultaneous for a large number of indexes (9 different indexes). Another important factor appears in this figure which called "jumps". Jumps are formed by the relatively large value of return (positive or negative return) with respect to the mean and variance of the actual return distribution. These jumps appear in several instants of the overall period. Figure 1 shows that jumps (or shock) arrive randomly in time and are distributed over the whole period.

The model that we propose will take into consideration both of these observations. This model consists of an external factor controlling and relating the volatility behavior of different indexes and a jump-diffusion stochastic process that reflect the jump phenomena in addition of the normal diffusion variation of each index.

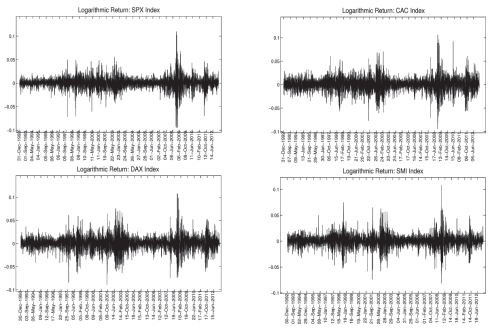


Figure 1. Daily log-returns of four different indexes from different countries.

2.1 *Environment state and Markov chain*

We study first the correlation between volatility behaviors of the 14 equity indexes. The study is based on the relative periodic standard deviation STD (with 1 period = 3 months) of different equities with respect to the STD of their log-return distribution for the 20 years period. For 9 over 14 indexes we found a strongly correlated STD behavior i.e. the relative STD increases (and decreases) appear simultaneously for this 9 indexes, which shows that the volatility of daily returns distribution may be related to an external factor that will be called the "*environment state factor or ES factor*". We suggest that a sub-period ES can be represented by a simple Markov Chain of three states. The states that represent the three different states of the ES factor are defined by the following:

- Calm: Relative STD of return less than 1.
- Normal: Relative STD of return between 1 and 2.
- Agitated: Relative STD of return greater than 2.

Transitions between the three states and the average duration in each state are defined by the Markov chain transition matrix and duration vector and are given in section 3.

2.2 *Log-normal diffusion log-uniform jump amplitude model*

Taking the data of only one specific index, the overall period is divided into smaller sub-period of 3 months. According to the relative STD of log-return distribution during one sub-period, this latter is associated to one of the three different ES. For each ES an appropriate stochastic model is associated to describe data evolution in this state.

Let $S(t)$ be the variable representing our concerned data at time t. $S(t)$ is supposed to satisfy a Markov, continuous-time, geometric Stochastic Differential Equation (SDE). A classical model of stochastic process is the BS (Black & Scholes) log-normal diffusion process. The BS model follows a basic stochastic differential equation given by:

$$dS(t) = \mu S(t)dt + \sigma S(t)dW(t) \quad (1)$$

where μ and σ are two constant parameters that represent respectively the growth rate and the volatility of the process and $W(t)$ is a standard wiener process.

BS model is widely used in finance where the log-return of asset price is considered to be normally distributed (Platen & Health 2006). However, equity returns distribution presents several realistic properties not found in the ideal BS model: (1) the presence of jumps represented by large random fluctuations such as crashes or sudden upsurges, (2) the log-return distribution are skewed,

and (3) the distribution of log-returns has a positive excess kurtosis with respect to the normal distribution i.e. the shape of the distribution has a more acute peak around the mean and fatter tails.

To model these phenomena, different modification of the Black & Scholes model have been proposed. The most two common models are the stochastic volatility model (see Hull White process (Hull & White 1987)), CIR process (see (Cox & Ross 1976)) and Ornstein-Uhmenbeck process (see (Heston 1993, Stein & Stein 1991)) and the jump diffusion model.

In Jump-Diffusion models a space-time Poisson process is added to the usual geometric Brownian motion in order to give the possibility of large fluctuations called jumps. Using a Poisson process for the jump timing and a log-normal distribution for the jump-amplitudes (Merton 1976) introduced the jump-diffusion model in financial modeling in order to describe the market crashes and rallies. Later on, (Kou 2002) proposed a jump-diffusion model with a log-double-exponential process for the jump-amplitudes. One important application of jump diffusion models is given by (Chernov, A.Ronald Gallant, & Tauchen 2003) where the jump process is added to a stochastic volatility model.

In this work, the chosen model to describe the dynamic of the data during one state will be the log-normal diffusion log-uniform jump amplitude model introduced by Hanson and al. (Hanson, Westman, & Zhu 2002) and described by the following SDE:

$$dS(t) = S(t)[\mu_D dt + \sigma_D dW(t) + (e^J - 1)dP(t)] \quad (2)$$

starting at $S(0) = S_0$, $S_0 > 0$, and where μ_D is the drift coefficient associated with the diffusion, σ_D is the diffusive volatility, $W(t)$ is the one-dimensional stochastic Weiner process, $(e^J - 1)$ is the Poisson jump amplitude and $P(t)$ is the standard Poisson process with joint mean and variance $E[P(t)] = Var[P(t)] = \lambda t$ which marks the arrival times of shocks.

The index log-return $d\ln(S(t))$ can be transformed to a simpler jump-diffusion Stochastic Differential Equation (SDE) upon use of the stochastic chain rule (Platen & Health 2006),

$$d[\ln(S(t))] = \mu_{lnD} dt + \sigma_D dW(t) + JdP(t), \quad (3)$$

where $\mu_{lnD} = \mu_D - 0.5\sigma_D^2$ can be called the log-diffusive (ld) drift and J is the log-return jump-amplitude. Note that the finite log-return jump-amplitude is supposed to respect $(e^J - 1) > -1$ in order to avoid complete investment loss (Hanson, Westman, & Zhu 2002).

Considering Hanson and al. studies (Hanson & Westman 2002a) (Hanson & Westman 2002b) and the comparison in (Hanson & Zhu 2004) between the use of normal, double exponential and uniform distribution, the jump-amplitudes in the log-return modelare assumed to be uniformly distributed on $[Q_a, Q_b]$, with $Q_a < 0 < Q_b$ which yields a mean $\mu_J = (Q_a + Q_q)/2$ and variance $\sigma_J^2 = (Q_b - Q_a)^2/12$.

$$J \sim U(Q_a, Q_b) \quad (4)$$

We assume also that the model parameters $\mu_{lnD}, \sigma_D^2, \mu_J, \sigma_J^2$ and λ are constant (time independent).

Numerical discretization of this model is needed. Taking $dt \to \Delta t$ we define the discrete stock log-return increment of the jump-diffusion process 2 as:

$$\Delta \ln S(t) = \ln S(t + \Delta t) - \ln S(t) \quad (5)$$

The basic moments of the stock log-return increment in (5) are given in Appendix 1. The increment probability distribution of the model is detailed in Appendix 2.

2.2.1 *Parameter estimation*

The object of this step is to find a Jump-Diffusion model that describe fairly the dynamic of the index log-returns. Considering a log-normal diffusion, log-uniform jump amplitude log-return model, the five parameters $\{\mu_J, \sigma_J^2, \mu_{lnD}, \sigma_D^2, \lambda\}$ have to be estimated. Let $M_1^{(sp)}$ and $M_2^{(sp)}$ be the empirical moments (mean and variance) of real log-return dataset $\Delta[\ln(S^{(sp)})]$ defined by:

$$\Delta[\ln(S_i^{(sp)})] = \ln(S_{i+1}^{(sp)}) - \ln(S_i^{(sp)}), \quad (6)$$

Two constraints are used to reduce the number of free parameters, which are the following mean and variance constraints:

$$M_1^{(sp)} = E[\Delta[\ln(S(t))]] \quad (7)$$

$$\text{and } M_2^{(sp)} = Var[\Delta[\ln(S(t))]] \quad (8)$$

where $E[\Delta[\ln(S(t))]]$ and $Var[\Delta[\ln(S(t))]]$ are the theoretical moments (mean and variance) given by equations (15) and (16) in Appendix 1.

Therefore if only the three jump parameters $\{Q_a, Q_b, \lambda\}$ are estimated,the parameters $\mu_J, \sigma_J^2, \mu_{lnD}$, and σ_D^2 can be deduced from equations (7) and (8) as follows

$$\mu_J = (Qa + Qq)/2 \quad (9)$$

$$\sigma_J^2 = (Qb - Qa)^2/12 \quad (10)$$

$$\mu_{lnD} = (M_1^{(sp)} - (\lambda \Delta t \mu_J))/\Delta t \quad (11)$$

$$\sigma_D^2 = [M_2^{(sp)} - (\lambda \Delta t)(\mu_J^2 + \sigma_J^2)]/\Delta t \quad (12)$$

Thus we have a three dimensional global minimization problem for a complex density function (19). In literature two optimization functions has been proposed and used for this problem (Hanson, Westman, & Zhu 2002, Hanson & Westman 2002a). Both of these objective functions are based on the division of the log-return domain into $N^{(bin)}$ bins and the calculation of theoretical and empirical bin frequencies. The weighted least squares function (χ^2 fit) is given by (Hanson, Westman, & Zhu 2002) as follows:

$$\chi^2 = \sum_{i=1}^{N^{(bin)}} \omega_i \cdot (f_i^{(jd)} - f_i^{(sp)})^2 \quad (13)$$

where ω_i is the weight of the ith bin, $f_i^{(sp)}$ is the ith empirical bin frequency and $f_i^{(jd)}$ is the ith theoretical jump-diffusion bin frequency corresponding to the same sample size $N^{(sp)}$ of the real data set (see Appendix 3).

Note that an unweighted least square function was also used in parameter estimation of jump-diffusion process (Hanson & Westman 2002a, Hanson & Westman 2002b).

The second used objective function is the Multinomial Maximum Log-Likelihood function (MML). This function is derived in (Hanson, Westman, & Zhu 2002) based on the assumption that the simulation distribution of a bin frequency is a multinomial distribution. The optimization function can be written as the following minimization objective:

$$-\sum_{i=1}^{N^{(bin)}} \left[f_i^{(sp)}(x_p) \ln(f_i^{(jd)}(x_p)) \right] \quad (14)$$

where x_p is the unknown parameter vector.

3 CASE STUDY

As we mentioned in section 2.1 the period of 20 years is divided into sup-periods according to the environment state "*ES*". The transition between different states is controlled by an external covariate which follow a Markov Chain model. The Markov Chain is constructed by three states (N1, N2 and N3) that represent respectively the Calm, Normal and Agitated ES. Considering the nine indexes influenced by this factor, the transition matrix between these states and the average duration in a state are defined by the following matrix and vector:

$$T = \begin{pmatrix} 0.846 & 0.141 & 0.013 \\ 0.51 & 0.432 & 0.058 \\ 0 & 0.8 & 0.2 \end{pmatrix}$$

$$D = \begin{pmatrix} 6.49 & 1.76 & 1.25 \end{pmatrix}$$

The objective of the next step is to find, for one equity, the jump-diffusion model suitable to each state. Considering the *ES classification* we can separate the data of one equity into three sets that correspond to the three ES (*Calm*, *Normal* or *Agitated*). Parameter estimation is done using the dataset formed of equity log-return belonging to the same *ES*.

Model calibration is done using the numerical Nelder-Mead optimization which serves to find the minimum of one of the objective functions cited in section 2.2. The three objective functions, weighted least square function (13), unweighted least square function and multinomial log-likelihood function (14), have been tested.

3.1 *Estimation constraint*

As seen in section 6 the three free parameters to be estimated for the jump-diffusion model are Q_a, Q_b and λ. However some constraint are needed in order to define the variation domain of each parameter and therefore to guarantee reasonable and realistic solutions for the wanted model. The first constraint derives from the fact that the number of jumps in one year cannot exceed the number of trading days. Other constraints are chosen to prevent the jump amplitude at a time t to exceed the rang of [–65%,+100%] of the price at this time. Finlay, one nonlinear constraint is needed. Considering equations (9) to (12) that permit to reduce the number of free parameters from 5 to 3, the nonlinear constraint is needed to keep positive the value of σ_D^2. No constraint is needed for σ_J^2 since $(Q_a - Q_b)^2$ is always positive.

To allow necessary boundary and nonlinear constraint to be respected a constrained Nelder-Mead optimization is used.

3.2 *First guess*

For a good global optimization method the results must be independent of the choice of parameter starting values (first guess). However a reasonable choice of starting values is needed to reduce the calculation time. Six different combinations of starting values are chosen to ensure that the optimization algorithm is converging to the same minimum. The chosen sets take into consideration the coverage percentage of the majorities of sample values. In the following, the convergence of the optimization method has been tested starting from six different *first guess* combination.

3.3 *Results*

For each equity price evolution, the log-return dataset is calculated using equation (6). Data classification is done by separating the time interval into sub-periods of 3 months. A sub-period *SubP* is considered to be in one of the three Markov chain states ($N1$, $N2$ and $N3$) as follows:

- If $V[\Delta \ln(S_i^{(sp)}))]_{SubP} < V[\Delta \ln(S_i^{(sp)}))]_{1993-2013}$, the log-return values of the sub-period *SubP* are added to the equity *Calm ES dataset* represented by $N1$.
- If $V[\Delta \ln(S_i^{(sp)}))]_{1993-2012} \leq V[\Delta \ln(S_i^{(sp)}))]_{SubP} < 2 * V[\Delta \ln(S_i^{(sp)}))]_{1993-2013}$, the log-return values of the sub-period *SubP* are added to the equity *Normal ES dataset* represented by $N3$.
- If $V[\Delta \ln(S_i^{(sp)}))]_{SubP} \geq 2 * V[\Delta \ln(S_i^{(sp)}))]_{1993-2013}$, the log-return values of the sub-period *SubP* are added to the equity *Agitated ES dataset* represented by $N3$.

Using the six different *First Guess* for the parameter set $\{Q_a, Q_b, \lambda\}$ we optimize the three different objective functions (weighted mean square, unweighted mean square and multinomial maximum likelihood). We found that the unweighted mean square objective function gives the best results in terms of convergence. Kolmogorov-Smirnov test and Q-Q plot are used to test the statistical resemblance between the real log-return distribution and simulated-data distribution resulting from the estimated model. Statistical tests show that the use of unweighted least square objective function leads to the best estimated parameters in terms of statistical comparison between real and simulated data.

Table 1 shows the estimation results for the Calm ES period of the SPX Index equity price,

Table 1. Summary of estimated parameters of log-normal diffusion, log-uniform jump amplitude process for SPX Index in the *CalmES* period using three objective functions and three different starting values. The Kolmogorov-Smirnov distance *k2stat* is also represented.

	Start. values	*Calm*			
Obj. func.	$[Q_a, Q_b, \lambda]$	Q_a	Q_b	λ	*k2stat*
Unweighted χ^2	[–0.008, 0.009, 123:58]	–0.01557	0.01454	92.99	0.02262
Unweighted χ^2	[–0.0388, 0.0275, 15:12]	–0.01557	0.01454	92.99	0.03648
Unweighted χ^2	[–0.0108, 0.0119, 138, 96]	–0.01557	0.01454	92.99	0.02627
Weighted χ^2	[–0.008, 0.009, 123.58]	–0,00541	0,00000	103,98	0.04305
Weighted χ^2	[–0.0388, 0.0275, 15.12]	–1,00000	0,70000	0,01	0.03356
Weighted χ^2	[–0.0108, 0.0119, 69.48]	–0,00541	0,00000	103,98	0.04196
MML	[–0.008, 0.009, 123.58]	–0,02421	0,01848	15,53	0.05217
MML	[–0.0388, 0.0275, 15.12]	–0,02421	0,01848	15,53	0.03612
MML	[–0.0108, 0.0119, 69.48]	–0,02418	0,00000	8,06	0.05801

Table 2. Summary of estimated parameters $\{\mu_J, \sigma_J^2, \mu_{ln}D, \sigma_D^2, \sigma_D^2, \lambda\}$ of log-normal diffusion, log-uniform jump amplitude process for *SPX Index*, *CAC Index* and *DAX Index* in *Calm*, *Normal* and *AgitatedES* periods using the unweighted χ^2 objective function.

		Estimated parameters				
Equity	State	μ_J	σ_J^2	μ_{lnD}	σ_D^2	λ
SPX Index	*Calm*	–0,00051	0,00008	0,19178	0,00504	92.99
SPX Index	*Normal*	–0,00148	0,00028	0,17502	0,02165	81,98
SPX Index	*Agitated*	–0,00304	0,00125	–0,27323	0,06356	105,27
CAC Index	*Calm*	–0,00144	0,000217	0,20807	0,01936	48,92
CAC Index	*Normal*	–0,0017021	0,0007097	–0,014317	0,05349	55.86
CAC Index	*Agitated*	–0,004096	0,002356	–0,48741	0,22769	37,70
DAX Index	*Calm*	–0,00179	0,000139	0,36491	0,0122	78,24
DAX Index	*Normal*	–0,00637	0,000415	0,38841	0,0451	56,97
DAX Index	*Agitated*	0,006465	0,00234	–0,7541	0,2021	13.87

using the three proposed objective functions and starting from different chosen parameters set. This result shows that the unweighted least square function is more stable in terms of convergence. For both the weighted least square and MML functions the convergence may change with the change of *first guess* and tends to reach the limits of the field of variation of some parameters. In Table 2 the estimated parameters for the three ES periods of three different equities (*SPX Index*, *CAC Index* and *DAX Index*) are represented.

Table 3. Statistical comparison between the simulated data from the estimated model and real log-return data set for three equities (*SPX Index*, *CAC Index* and *DAX Index*) for the *Calm*, *Normal* and *Agitated ES* periods.

Equity	State	*k2stat*	*%skewness*	*%kurtosis*
SPX Index	*Calm*	0,0262	–68,66	–11,18
SPX Index	*Normal*	0,0258	24,514	–18,68
SPX Index	*Agitated*	0,04792	–296,85	–25,05
CAC Index	*Calm*	0,01090	18,55	–2,88
CAC Index	*Normal*	0,0343	–620,92	–7,49
CAC Index	*Agitated*	0,07633	–98,79	6,90
DAX Index	*Calm*	0,0215	–7,56	–7,13
DAX Index	*Normal*	0,0359	16,14	–12,89
DAX Index	*Agitated*	0,0322	–76,61	1,26

Table 3 shows the results of Kolmogorov-Smirnov distances for different equities and states, and the difference in statistical proprieties (Skewness and Kurtosis) of simulated data from the estimated model with respect to those of the real dataset. Note that the Kolmogorov-Smirnov test always leads to the null hypothesis H0 which means that the distribution of the simulated data is

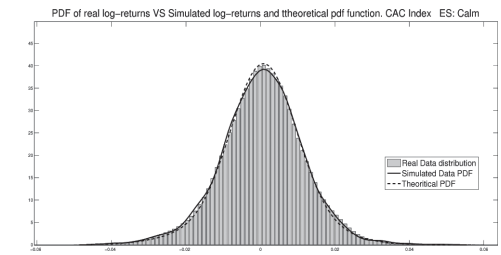


Figure 2. PDF comparison between real log-return and simulated log-return for *CAC Index* in *Calm* State.

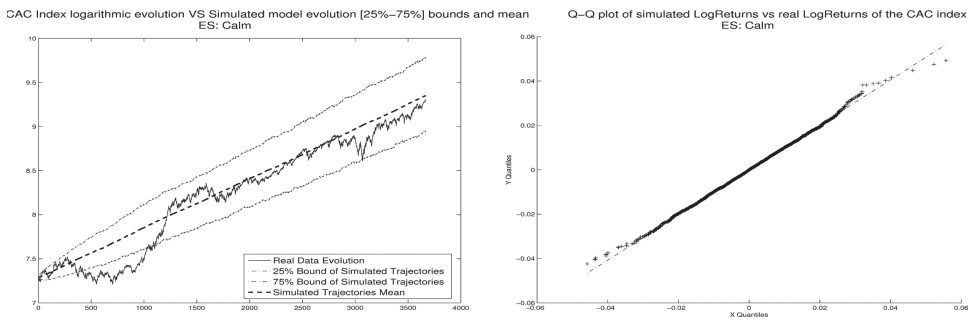


Figure 3. Data evolution comparison between real *CAC Index* log-price and simulated jump-diffusion process for *Calm* State (on left) and the Q-Q plot of these two data set (on right).

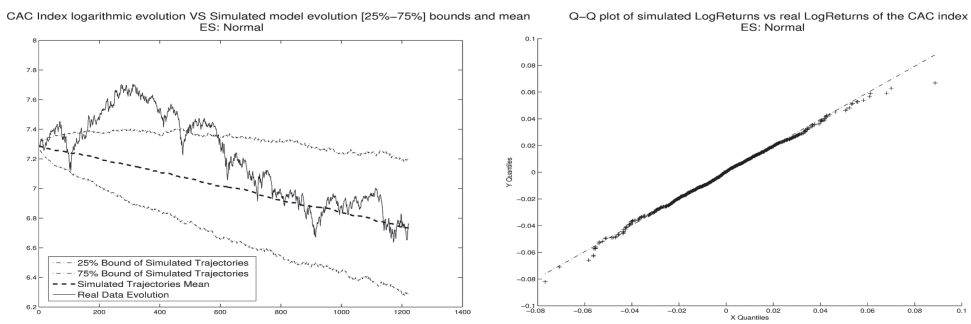


Figure 4. Data evolution comparison between real *CAC Index* log-price and simulated jump-diffusion process for *Normal* State (on left) and the Q-Q plot of these two data set (on right).

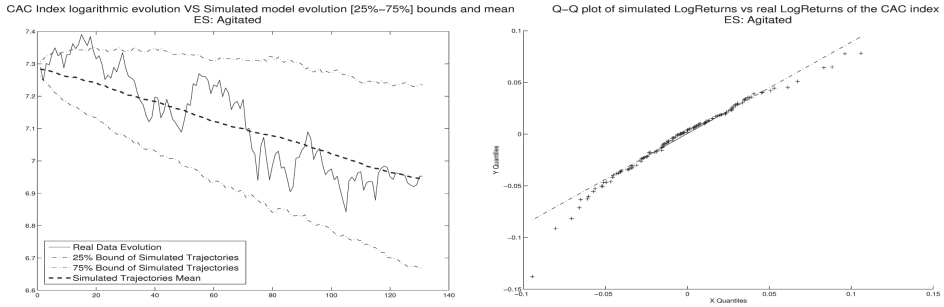


Figure 5. Data evolution comparison between real *CAC Index* log-price and simulated jump-diffusion process for *Agitated* State (on left) and the Q-Q plot of these two data set (on right).

quit similar to the distribution of real log-returns. We also notice a small difference in the kurtosis coefficient between real and simulated data while in some cases the skewness coefficient of the simulated data shows an important deviation from the skewness coefficient of the real dataset. In Figure 2 the Probability Density Function (PDF) is given for both real dataset *CalmCACIndex* and simulated data from the estimated model as well as the theoretical PDF of the calibrated model. Figure 3 shows on the left the evolution of the equity price considering only the *Calm ES CAC Index* data and a the [25% 75%] bounds of 500 random simulated data evolution using the estimated jump-diffusion model. On the right a Q-Q plot for the real dataset (*CalmCACIndex*) and the estimated dataset is represented. Similarly, Figure 4 (Fig. 5) shows the comparison between the evolution of real *NormalCACIndex* (*AgitatedCACIndex*) dataset and simulated data from the estimated model, as well as the Q-Q plot between this two dataset.

4 CONCLUSION

The *log-normal diffusion, log-uniform jump amplitude process* has been used in many paper to solve optimal consumption and portfolio optimization and control (Hanson & Westman 2002a) (Hanson & Westman 2002b). Hanson and Westman (Hanson & Westman 2002b) use a yearly decomposition of log-returns in order to estimate the appropriate parameters for their jump-diffusion model. The difference of model parameters between different years is noticeable. A reasonable division of the time domain is proposed according to the volatility behavior of log-return values. The estimation of the model parameters for the three predefined environment states is done using a numerical minimization method (constrained Nelder-Mead) for a least square objective function. The results show that the estimated model is suitable for modeling the real dataset in terms of the probability distribution. Estimated models show statistical resemblance to real data distribution which is more important in terms of the kurtosiscoefficient than the skewness coefficient. A future work is needed to test the goodness of fit between the estimated model and the log-price evolution, to find and adjust the weak points where the model does not adequately reflect the log-price dynamics. Thus, we can benefit from the estimated model in order to propose new solutions for financial control, risk-based decision-making and prognostics.

APPENDIX 1

The basic moments of the stock log-return increment in (5) are given by the following:

$$M_1^{(jd)} = E[\Delta[\ln(S(t))]] = (\mu_{lnD} + \lambda\mu_J)\Delta t, \quad (15)$$

$$M_2^{(jd)} = Var[\Delta[\ln(S(t))]] \simeq [\sigma_D^2 + \lambda(\sigma_J^2 + \mu_J^2)]\Delta t. \quad (16)$$

APPENDIX 2

Increment distribution for jump-diffusion models is studied is (Synowiec 2012) for different type of jumps. In (Hanson & Westman 2003) the probability density for the log-normal diffusion, log-uniform jump amplitude increment $[\ln(S(t))]$ is derived for the case of time dependent parameters. This probability density is used in (Hanson, Westman, & Zhu 2002) with the modified form as follows:

$$\begin{aligned}\mathbb{P}[d\ln(S(t)=x] &= \mathbb{P}[dP(t)=0]\cdot\phi^{(n)}(x;\mu_{lnD}dt,\sigma_D^2) \\ &+ \sum_{k=1}^{\infty}\mathbb{P}[dP(t)=k] \\ &\cdot\frac{\Phi^{(n)}(x-k\cdot Qb, x-k\cdot Qa;\mu_{lnD}dt,\sigma_D^2 dt)}{k(Qb-Qa)}\end{aligned} \quad (17)$$

for $-\infty < x < +\infty$, where the Poisson distribution $p_k(\lambda dt)$ is specified by (18) and $\Phi^{(n)}(x, y; \mu_{lnD} dt, \sigma_D^2 dt)$ is the integral of the normal density function $\phi^{(n)}(x; \mu_{lnD} dt, \sigma_D^2)$ between x and y.

$$\mathbb{P}[dP(t) = k] = exp(-\lambda dt)(\lambda dt)^k / k! \tag{18}$$

The derivation of this probability is based on the triad random variable $\xi + \eta \cdot \zeta$ which forms the $d \ln S(t)$ model, with diffusion $\xi = \mu_{lnD} dt + \sigma_D dW(t)$, jump amplitude $\eta = J$ and jump-time index $\zeta = dP(t)$ process.

For $\Delta t \to 0^+$ the probability density defined in (17) can be asymptotically approximated for the discrete case as

$$\begin{aligned} &\mathbb{P}[\Delta \ln(S(t))] \sim \phi^{(jd)}(x) \\ &\quad \equiv (1 - \lambda \Delta t)\phi^{(n)}(x; \mu_{lnD} \Delta t, \sigma_D^2 \Delta t) \\ &\qquad + (\lambda \Delta t) \frac{\Phi^{(n)}(x - Q_b, x - Q_a; \mu_{lnD} \Delta t, \sigma_D^2 \Delta t)}{(Qb - Qa)}. \end{aligned} \tag{19}$$

APPENDIX 3

In 13 $f_i^{(jd)}$ represent the ith expected bin frequency after $N^{(sp)}$ simulation of the theoretical jump-diffusion process is:

$$f_i^{(jd)} = N^{(sp)} \cdot \int_{x_i}^{x_{i+1}} \varphi_i^{(jd)}(x) dx. \tag{20}$$

The bin weights in 13 are chosen as the normalized theoretical values:

$$\omega_i = (1/\sigma^2_{f_i^{(jd)}}) / \sum_{j=1}^{N^{(bin)}} (1/\sigma^2_{f_i^{(jd)}}), \tag{21}$$

where

$$\sigma^2_{f_i^{(jd)}} = N^{(sp)} \cdot [1 - f_i^{(jd)} / N^{(sp)}]^2 \cdot f_i^{(jd)}. \tag{22}$$

ACKNOWLEDGMENT

This work was supported by the Regional Council of Champagne-Ardenne (RCCA) and the European Regional Development Fund (ERDF) in the framework of RISK PERFOM project.

REFERENCES

Bhar, R., D.B. Colwell, & Y. Xiao (2013, August). A jump diffusion model for spot electricity prices and market price of risk. *Physica A: Statistical Mechanics and its Applications 392*.

Chernov, M., E.G.A. Ronald Gallant, & G. Tauchen (2003). Alternative models for stock price dynamics. *Journal of Econometrics. 116*.

Cox, J.C. & S.A. Ross (1976). The valuation of options for alternative stochastic processes. *The Journal of Financial Economics 3*.

Giraudo, M.T. & L. Sacerdote (1997). Jump-diffusion processes as models for neuronal activity. *Biosystems 40*.

Hanson, F.B. & J.J. Westman (2002a, May). Optimal comsimption and portfolio control for jump-diffusion stock process with log-normal jumps (corrected). *Proceedings of American Control Conference*.

Hanson, F.B. & J.J. Westman (2002b, December). Portfolio optimization with jump-diffusions: estimation of time-dependent parameters and application. *Decision and Control, Proceedings of the 41st IEEE Conference 1*.

Hanson, F.B. & J.J. Westman (2003). Jump-diffusion stock-return model with weighted fitting of time-dependent parameters. *Proceedings of 2003 American Control Conference 3*.

Hanson, F.B., J.J. Westman, & Z. Zhu (2002, August). Jump-diffusion stock return models in finance: Stochastic process density with uniform-jump amplitude. *Proceedings of the 15th International Symposium on Mathematical Theory of Networks and Systems, 7 pages,(invited paper)*.

Hanson, F.B. & Z. Zhu (2004, 14–17 December). Comparaison of market parameters for jump-diffusion distribution using multinomial maximum likelihood estimation. *Proceedings of 43nd IEEE Conference on Decision and Control*. invited paper.

Heston, S.L. (1993). A closed-form solution for options with stochastic volatility with application to bond and currency options. *The Review of Financial Studies 6*.

Hull, J. & A. White (1987). The pricing of option on assets with stochastic volatilites. *Journal of Finance 42*.

Kou, S.G. (2002). A jump diffusion model for pricing. *Management Science 48*.

Lin, J., O. de Weck, & D. MacGowan (2008, April). Modeling epistemic subsurface reservoir uncertainty using a reverse wienerb jumpdiffusion process. *Journal of Petroleum Science and Engineering 84–85*.

Merton, R. (1976). Option pricing when undelying stock returns are discontinuous. *J. Financial Economics 3*.

Platen, E. & D. Health (2006). *A benchmark approach to quantitative finance*. Springer.

Stein, E. & J. Stein (1991). Stock price distributions with stochastic volatility: An analytic approach. *Review of Financial Studies 4*.

Synowiec, D. (2012, October). Jump-diffusion models with constant parameters for financial log-return processes. *Computers and Mathematics with Applications 56*.

Zhao, H., X. Rong, & Y. Zhao (2013). Optimal excess-of-loss reinsurance and investment problem for an insurer with jump-diffusion risk process under the heston model. *Insurance: Mathematics and Economics 53*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Performance evaluation of Emergency Response Plans using a Multi-State System approach

C. Girard
CNRS, G-SCOP, University Grenoble Alpes, Grenoble, France
Ecole Nationale Supérieure des Mines, FAYOL-EMSE, SEPIT, Saint Etienne, France

E. Piatyszek
Ecole Nationale Supérieure des Mines, FAYOL-EMSE, SEPIT, Saint Etienne, France

P. David & J.-M. Flaus
CNRS, G-SCOP, University Grenoble Alpes, Grenoble, France

ABSTRACT: Emergency Response Plans in case of natural or industrial disaster have to be assessed before being triggered. But it appears that there is no much works on how to assess these plans. Some tried to assess robustness but only considering two states: complete functioning or total failure. In this paper, we propose to assess Emergency Response Plan by looking its performance. It is used Multi-State System approach, for two reasons. The first is that Multi-State System approach allows to study more than the two binary states of functioning or failure, the second is that it includes probability to be in each state. Using a model-based approach to analyze Local Emergency Response Plan will systemize the analysis and allow to deal with a high variety of engaged resources. It has been chosen to work with Function-Interaction-Structure modeling method.

1 INTRODUCTION

Events threatening our societies happen in more and more complex contexts (Lewis & Mioch, 2005) and have highest frequency and intensity (United Nations 2011). United Nations ask its members to build organization to face these events. However, there is no consensus on how to assess such organization. Models have been used (Flaus 2010, Kolen et al. 2012, Robert et al. 2008, Robert, unpubl.) to capture complexity of organization where threatening events occur in order to understand crisis management mechanisms.

Consequences modeling model (Robert et al. unpubl.) and critical infrastructures model (Robert et al. 2008) have been developed to show interactions between critical infrastructures and the domino effects of consequences. Consequences and critical infrastructure models are part of work on organizational resilience (Hémond & Robert 2013) that identify needs in assessing Emergency Plan but do not treat this aspect.

Several levels of Emergency Response Plan can be considered: national, regional and individual scale (Calixto & Larouvere 2010). In this study, we will consider Local Emergency Response Plan (LERP) which is the third level in the Emergency Response Plan: Individual. It is the most important, because it is the first organizational response set up in case of emergency due to its proximity to happening event.

Plans are collection of procedures to describe organizational management in case of a threatening event and identify resources to set up to face such an event. Resources of LERP can be categorized as human resources (i.e. head quarter and field staff), technical resources (i.e. transportation means, alert means), organizational resources (procedure) and informational resources (i.e. message, order) as resources in Industrial Emergency Response Plan (IERP) (Karagiannis et al. 2010).

Also LERP contains a risk analysis part to describe threatening events which can occur in local territory. They are design to ensure warning alert, information protection and support to local population. Plans are not designed to anticipate all possible scenarios but have to be as flexible as possible to adapt to the occurring event (Perry & Lindell 2003).

Currently, potential problems are identified a posteriori thanks to feedback analysis (Karagiannis et al. 2010). A key issue is to identify potential problems of these plans before their deployment. It is necessary to know if the designed plan will

be efficient in case of emergency. Indeed, knowing ERP efficiency in its design phase gives visibility to decision makers on the possible disruptions. It allows setting preventive actions to enhance the plan before it is triggered.

However, an a priori ERP assessment is not easy due to its complexity (Flaus 2010) and it seems that local authorities do not see emergency planning as a priority (de Souza 2000, Henstra 2010). The complexity of ERP comes from resources variability in terms of type, geographical position and organizational owners. To understand all links between resources and missions it is needed to model Emergency Response Plan (that describes crisis management) at a good level of description. Works in this field are increasing (Jain & McLean 2003). Modeling an Emergency Response Plan allows a better first-aid response, knowledge of consequences before they happen, activities continuity where the event is not happening, traffic management and victims allocation to hospitals.

In previous work (Karagiannis et al. 2010) develop a method laying on models to assess robustness of Emergency Response Plan in industrial context. This method is based on questionnaires to assess probability of resource failure modes, organize and combine them in a Fault-Tree (FT) specific to each category (human, technical, organizational and informational). In this way plan failure scenarios can be built. Authors developed also a resource taxonomy for Emergency Response Plan to build patterns of Fault-Tree. A limit of this work is that it considered for model elements (both resource and function) only two binary states and so does not take into account partial failures of these elements, specifically function element. As it can be noticed in real world many elements of a system may have more than two possible states of failure. Moreover, these states may be qualified by a real value (not only 0 and 1).

For example, during an evacuation phase, 150 individuals have to be evacuated by ERP elements with 200 individuals capacity. With Boolean approach function failure is considered as a binary event. It is so complicated to get partial failure for modeled function evacuation: x% of individuals evacuated, because only two binary states (0: 0 individual evacuated or 1: 150 individuals evacuated) are considered. Another example can be given by an uncompleted coverage of the alert zone. Alert may not be spread in the entire zone which is described in ERP, because of several causes.

To solve these problems, it is proposed in this paper to use Multi-State System (MSS) approach in order to be able to deal with partial degradation of model element. Multi-State System approach has been summarized by Lisnianski & Levitin (2003) and Natvig (2010).

Next section, described the proposed approach to assess Emergency Response Plan by taking into account function partial failures.

2 METHODOLOGY FOR EMERGENCY PLAN ASSESSMENT

What is expected by decision maker is information about mission accomplishment. While previous works were able to only give information of complete functioning or failure, this work propose to give a view for decision maker for a mission to be in more than the two usual binary states $\{0,1\}$.

In this section, it is exposed methodology employed to assess Local Emergency Response Plan leading to give for each planned mission couples of mission states and probability to be at these mission states. First step of the proposed method is to handle complexity of the real world problems using model. Knowing interactions between model elements (resource and function), second step is to characterize resources to take into account in a different way the expression of functioning state. This will allow in a third step to better characterize function states, for example to have more than the two usual functioning or failure state $\{0,1\}$.

2.1 *First step: Handle complexity by using model*

2.1.1 *Concepts*

The first step of the proposed methodology is to handle the complexity of interactions between the elements of the organization in crisis time (Flaus 2010). Each element of the organization can be seen as a resource in the model and missions are expressed as functions.

Modeling method FIS (for Function Interaction Structure) (Flaus 2011) have been used to assess robustness of Industrial Emergency Response Plan using Fault Tree (Karagiannis et al. 2010). This modeling method links systems that realize functions by using resources.

By describing element of the model, it is possible to follow disruption propagation in all systems.

Work has been done on the description of Local-ERP thanks to the FIS modeling method (Girard et al. 2013). A meta-model of LERP has been designed by studying building guide (DDSC 2009) and LERPs from different towns of various size, and exposal risks. Thanks to this meta-model, generic system, functions and resources have been identified to describe a LERP.

This method is used to model LERP but with the current characteristics, it is not enough to assess Emergency Response Plan, because it does not take into account partial failure.

2.1.2 *Example*

Instance of the model is given following the generic model described in Girard et al. (2013) and laid on Function-Interaction-Structure modeling method. It has been chosen to illustrate example on a specific function of model: Evacuate.

Evacuate, is defined to move 150 individuals from A to B. Resources to set up the function are defined as follow:

- R01: 1 evacuation procedure, without any evacuation procedure the function is less performed. A lack of procedure will not lead to the function to be not fully performed. In fact it will be less efficient performed. We consider that an expert reasoning shows that if there is a lack of procedure, function will be complete at 20% whereas 100% if the procedure exists.
- R02: Population informed for evacuation
- R03: Population evacuated
- R04: Staff member
- R05.01: Bus with capacity of 75 individuals
- R05.02: Bus with capacity of 75 individuals
- R05.03: Bus with capacity of 50 individuals
- R06: Gathering point, without any gathering point function is not performed. In fact individuals do not know where buses will pick them up
- R07: Itinerary

Instance can be described by scheme at Figure 1.

This model instance is described with the FIS modeling method. Reader can notice a resource pool (evacuation vehicle: buses), that shows resources having the same goal in the Evacuate function. The buses pool is made up of 3 buses with different characteristic values (capacity). In the following paragraphs P_1 will be also used to describe this resource pool.

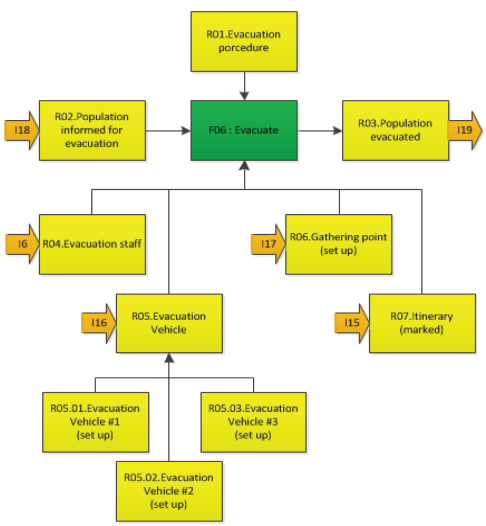


Figure 1. Instance of FIS modeled function evacuation.

Complexity of real world resource interactions can be modeled to handle it. Next step is so to enhance resource characterization to take into account in a different way expression of functioning and failure state to better characterize function states.

2.2 *Second step: Resource characterization*

2.2.1 *Concepts*

Each resource is characterized with two states complete functioning or total failure, but we introduce a different way from previous works to define functioning states. In fact, in this work we are taking into account the function demand.

We propose to give a different value regarding function demand for resource. A resource is so characterized by two state values: total failure performance (l) and complete functioning performance (m) defined regarding a function demand written W. "m" denotes the maximum service the resource can accomplish regarding function demand and "l" the minimum service.

Definition 1:

For all resource j, it exists two states corresponding to the state $g_{j,i}$ where i is state number $i \in \{1,2\}$ (Lisnianski & Levitin 2003, Natvig 2010).

$$g_i = \{g_{j,1}, g_{j,2}\} \tag{1}$$

with $g_{j,1} = l$ and $g_{j,2} = m$.

Then using previous works (Karagiannis et al. 2010), it is possible through resource taxonomy to generate failure modes and Fault-Tree structure as degradation assessment approach developed for industrial Emergency Response Plan. Fault-Tree is used to obtain probability of total failure state. Probability to be at this failure state is obtained via questionnaires developed in these previous works giving elementary events probabilities and via probabilities computation through the tree structure. By opposition since it is possible to access to total failure probability, it is possible to have an access to functioning probability.

Generic failure modes that composed Fault-Tree have been identified for LERP in Girard et al. (2013).

Definition 2:

Probability to be at state $g_{j,i}$ at instant t is given by the set (Lisnianski & Levitin 2003, Natvig 2010).

$$p_j(t) = \{p_{j,1}(t), p_{j,1}(t)\}$$

where

$$p_{j,i} = \Pr\{G_j(t) = g_{j,i}\} \tag{2}$$

At this step for each resource and each of their participation to function, it is defined values "*l*" and "*m*" of complete dysfunctioning and functioning states and the probability to be in these states.

2.2.2 *Example*
State values for each states are:

– *l* if element is in total failure
– *m* if element is fully working

An example for resource in buses pool can be illustrated as follow:

$$m = \frac{Capa_i}{W} \tag{3}$$

with
$Capa_i$ Capacity of element i and W the function demand

$Capa_1 = Capa_2 = 75$ and $Capa_3 = 50$
W = 200

Results for example are given in Table 1. Because of the chosen instance, R02, R03 R06 and R07 are defined in $\{0,1\}$ whereas R05 resources in resource pool P_1 are in $\{0,m\}$. R01 (the evacuation procedure) is coded in $\{l,1\}=\{0.2,1\}$ since experts judge that 20% of the mission is realized if R01 is missing.

In the following example, it will be used the next probability:

$p_{R01,1} = 0.3$, $p_{R01,2} = 0.7$

$p_{R05.01,1} = 0.2$, $p_{R05.01,2} = 0.8$

$p_{R05.02,1} = 0.2$, $p_{R05.02,2} = 0.8$

$p_{R05.03,1} = 0.3$, $p_{R05.03,2} = 0.7$

$p_{R04,1} = 0.05$, $p_{R04,2} = 0.95$

$p_{R06,1} = 0.2$, $p_{R06,2} = 0.8$

$p_{R07,1} = 0.15$, $p_{R07,2} = 0.85$

Table 1. List of state values by resource ID.

Resource ID	State values
R01	{0.2,1}
R02	{0,1}
R03	{0,1}
R04	{0,1}
R05.01	{0,0.50}
R05.02	{0,0.50}
R05.03	{0,0.33}
R06	{0,1}
R07	{0,1}

In this subsection it has been described characterization changes of resources from states defined in $\{0,1\}$ to state defined in $\{l,m\}$. Probability to be at each state can be obtained from Fault-Tree for state value "*l*" and "*m*". The third step is to deduce function states from the resource analysis, with more than the two usual binary states.

2.3 *Third step: Function characterization*

2.3.1 *Concepts*
For each function, participating resources' states $\{l,m\}$ are combined to give possible function states.

For the modeled function, it exists a mathematical function to compute the states and probability to be at each state, this is relative to Multi-State System theory (Lisnianski & Levitin 2003). A node characterized by its mathematical function models resource assembly to complete modeled function. As in Fault-Tree, nodes like AND, OR and K/N can be expressed, as well as more specific nodes, directly related to a function.

Definition 3:

$$G(t)=\phi(G_1(t),G_2(t),\ldots,G_n(t)) \tag{4}$$

The output $G(t)$ characterizes the state of the function in time t. In this paper we considered G functions as constant in time. ϕ characterizes the computation function for a given node.

2.3.2 *Example*
With the instance described in the previous section, we propose for the "Evacuate" function an initial event graph of Multi-State propagation in Figure 2.

Behavior at node 1 and 2 for the function "Evacuate" will be described in paragraphs below.

Mathematical computation functions for each node (1 and 2) are respectively described in Table 2 and Table 3.

At node 1, states of all resources used in resource pool P_1 are assessed. Evacuation vehicle #1, #2 and #3 are indexed respectively by *b1,b2,b3*. States are so given by the function ϕ_1. Node 1 models that each evacuation vehicles (buses) of pool P_1 participates to the evacuation function as evacuation means.

$$\begin{aligned} G_{p1}(t) &= \phi_1(G_{b1}(t),G_{b2}(t),G_{b3}(t)) \\ &= G_{b1}(t) + G_{b2}(t) + G_{b3}(t) \end{aligned} \tag{5}$$

states for P_1 are defined as:

$$G_{p1}(t) = \{0.00,0.33,0.50,0.83,1.00,1.33\} \tag{6}$$

At node 2, all resources used in the function Evacuate are assessed. All resources previously

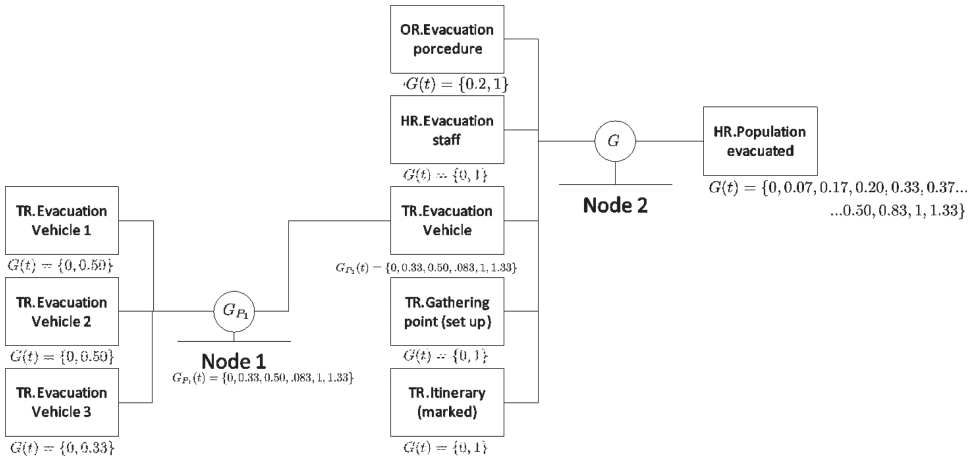


Figure 2. Performance propagation tree for resolved node 1 and 2.

Table 2. States value at node 1.

$G_{b1}(t)$	$G_{b2}(t)$	$G_{b3}(t)$	$G_{P1}(t)$
0.00	0.00	0.00	0.00
0.00	0.00	0.33	0.33
0.00	0.50	0.00	0.50
0.00	0.50	0.33	0.83
0.50	0.00	0.00	0.50
0.50	0.00	0.33	0.83
0.50	0.50	0.00	1.00
0.50	0.50	0.33	1.33

Table 3. State values at node 2.

$G_1(t)$	$G_2(t)$	$G_3(t)$	$G_4(t)$	$G_{P1}(t)$	$G(t)$
0.20	0.00	0.00	0.00	0.00	0.00
0.20	0.00	0.00	0.00	0.33	0.00
0.20	0.00	0.00	0.00	0.50	0.00
0.20	0.00	0.00	0.00	0.83	0.00
0.20	0.00	0.00	0.00	1.00	0.00
0.20	0.00	0.00	0.00	1.33	0.00
…	…	…	…	…	…
0.20	1.00	1.00	1.00	0.00	0.00
0.20	1.00	1.00	1.00	0.33	0.07
0.20	1.00	1.00	1.00	0.50	0.10
0.20	1.00	1.00	1.00	0.83	0.17
0.20	1.00	1.00	1.00	1.00	0.20
0.20	1.00	1.00	1.00	1.33	0.37
…	…	…	…	…	…
1.00	1.00	1.00	1.00	0.00	0.00
1.00	1.00	1.00	1.00	0.33	0.33
1.00	1.00	1.00	1.00	0.50	0.50
1.00	1.00	1.00	1.00	0.83	0.83
1.00	1.00	1.00	1.00	1.00	1.00
1.00	1.00	1.00	1.00	1.33	1.33

un-described by node 1 (evacuation staff, gathering point, itinerary) except evacuation procedure, are characterized by binary sates $G_i(t) = \{0.00,1.00\}$, for $i = 1,3,4$. From the modeled instance $G_2(t) = \{0.20,1.00\}$. Evacuation staff, evacuation procedure, gathering point, itinerary are indexed respectively by *1,2,3,4*. Node 2 models the entire interaction for evacuation resources to the evacuation function.

This mean that all elements are necessary for function success, ϕ_2 is defined as follows:

$$G(t) = \phi_2(G_1(t), G_2(t), G_3(t), G_4(t), G_{P1}(t)) = G_1(t) \times G_2(t) \times G_3(t) \times G_4(t) \times G_{P1}(t) \quad (7)$$

This node is characterized by a product mathematical function. Indeed as all resources are necessary for the modeled function to be realized, it is represented as AND-gate. Concretely, if we take the evacuation procedure, it gives a kind of completion percentage in terms of number of evacuees. Buses combine this with an evacuation capacity. Other resources are viewed as switches. If the gathering point, or itinerary, or evacuation staff are unavailable, the function can not be realized.

Table 3 shows all possible performance states for the presented function. Intermediate values give the result $G(t)=0.00$.

Thus, with all combinations of performance states it is possible to access to all functional performance state in which the modeled function (in this case "Evacuation") could be.

Even if resource are defined by binary states, it is considered not only $\{0,1\}$ as state values but $\{l,m\}$. In this way function can be characterized by multi-state. In this case, if we refer to the Multi-State System theory, LERP are now considering as non-homogenous MSS with binary elements. It

allows having more information at function state for decision makers. They will better know with the developed approach the functions of their Emergency Response Plan.

As it has been written before, it is possible through model and thanks to Fault-Tree pattern to access to the probability of total failure state of a resource and in opposition to get the probability of its complete functioning state. Because goal of this paper is to present assessment method, it is used arbitrary probability values for each resource state, instead of probability coming from Fault-Tree Assessment and questionnaire. The computation rules are extracted again from Multi-State System theory.

By using the table of states for pool P_1 combined with probability in section 2.2.2, Table 4 can be filled.

Probability of each element in a row is multiplied. This is corresponding in a Fault-Tree to an And-gate. For each identical output state coming from different associations of element performance states, probability is summed. This is corresponding in a Fault-Tree to an Or-gate.

For each state of P_1, probabilities are:

$$G_{P1,1} = 0.00,\ p_{P1,1} = 0.01$$
$$G_{P1,2} = 0.33,\ p_{P1,2} = 0.05$$
$$G_{P1,3} = 0.50,\ p_{P1,3} = 0.08$$
$$G_{P1,4} = 0.83,\ p_{P1,4} = 0.30$$
$$G_{P1,5} = 1.00,\ p_{P1,5} = 0.11$$
$$G_{P1,6} = 1.33,\ p_{P1,6} = 0.45$$

A bar chart of probabilities repartition for each state is given by Figure 3.

With the probabilities given in section 2.2.2 and the previous probability computation result, probabilities at node 2 are the following:

$$G(t) = 0.00,\ p_{G(t)=0.00} = 0.36$$
$$G(t) = 0.07,\ p_{G(t)=0.07} = 0.01$$

Table 4. States crossing probabilities at node 1.

$G_1(t)\,(p_{1,i})$	$G_2(t)\ (p_{2,i})$	$G_3(t)\ (p_{3,i})$	$G_{P1}(t)\ (p_{P1,i})$
0.00 (0.2)	0.00 (0.2)	0.00 (0.3)	0.00 (0.01)
0.00 (0.2)	0.00 (0.2)	0.33 (0.7)	0.33 (0.05)
0.00 (0.2)	0.50 (0.8)	0.00 (0.3)	0.50 (0.03)
0.00 (0.2)	0.50 (0.8)	0.33 (0.7)	0.83 (0.11)
0.50 (0.8)	0.00 (0.2)	0.00 (0.3)	0.50 (0.05)
0.50 (0.8)	0.00 (0.2)	0.33 (0.7)	0.83 (0.19)
0.50 (0.8)	0.50 (0.8)	0.00 (0.3)	1.00 (0.11)
0.50 (0.8)	0.50 (0.8)	0.33 (0.7)	1.33 (0.45)

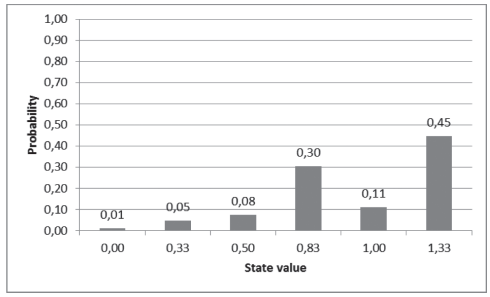


Figure 3. Probabilities of performance rates at node 1.

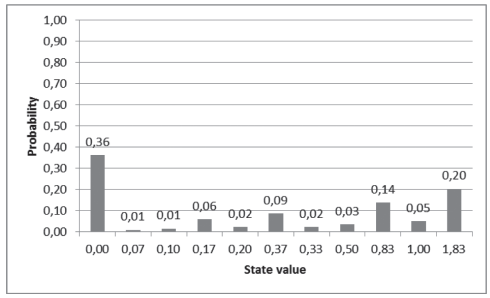


Figure 4. Probabilities of performance rates at node 2.

$$G(t) = 0.10,\ p_{G(t)=0.10} = 0.01$$
$$G(t) = 0.17,\ p_{G(t)=0.17} = 0.06$$
$$G(t) = 0.20,\ p_{G(t)=0.20} = 0.02$$
$$G(t) = 0.33,\ p_{G(t)=0.33} = 0.02$$
$$G(t) = 0.37,\ p_{G(t)=0.37} = 0.09$$
$$G(t) = 0.50,\ p_{G(t)=0.50} = 0.03$$
$$G(t) = 0.83,\ p_{G(t)=0.83} = 0.14$$
$$G(t) = 1.00,\ p_{G(t)=1.00} = 0.05$$
$$G(t) = 1.33,\ p_{G(t)=1.33} = 0.20$$

A bar chart of probabilities repartition for each state is given in Figure 4.

In the end we can better described function with a range of state it can take and a probability to be at each state described. For example, it can be considered state where more than 80% of population can be evacuated. In the instance described in this paper the probability to obtain this performance is 39%.

3 CONCLUSION

In this paper it has been presented how to use Multi-State System (MSS) with Function-

Interaction-Structure (FIS) modeling Method to assess Local Emergency Response Plan (LERP).

Because commonly failure modes are seen as binary events, it is not enough to assess LERP. Multi-State System approach has been chosen to deal with partial failures of LERP.

Thanks to previous work, we laid on a generic model of LERP to assess and propose propagation mechanisms of Multi-State through a model. Laying on a generic model will allow having a quick access to homogenous resource information.

Performance assessment (via MSS approach) makes possible to determine performance (G) of a function regarding demand (W). With probability assessment (and Fault-Tree patterns obtained with generic model), the probability to be at total failure state can be given and so the probability to be in the opposite state for a resource. But instead of considering state in $\{0,1\}$, we consider in $\{l,m\}$, enabling more relevant analysis of resource participation. As for example being capable of analyzing partial function realization even with a complete dysfunctioning resource, analyzing over performance in case of redundant resources and partial execution evaluation.

This is a new result because even if we considered binary state for resources, at modeled function level we are now considering Multi-State.

By using the model-based proposed performance propagation event graph, it is easy to follow performance propagation in a LERP model.

Further work can be done by implementing the proposed approach in a software which already implement FIS formalism for risk assessment. The proposed approach could be implemented to help building and computing all state relations at node. Another perspective can be to consider more than only two binary states for being more precise in modeling and considering a homogenous (or non) MSS with multi-state elements. This model integrating Multi-State system could also be used to simulate LERP performance behaviors.

ACKNOWLEDGMENT

This works received a founding from the Région Rhône-Alpes (FRANCE).

REFERENCES

Calixto, E. & Larouvere, E.L. 2010. The regional emergency plan requirement: Application of the best practices to the Brazilian case. *Safety Science* 48(8): 991–999.

DDSC. 2009. *Plan Communal de Sauvegarde—Guide pratique d'élaboration*. Asnières-sur-Seine.

De Souza, A.B.J. 2000. Emergency planning for hazardous industrial areas: a Brazilian case study. *Risk Analysis* 20(4): 483–493.

Flaus, J.-M. 2010. Modélisation de systèmes organisationnels pour l'analyse des défaillances: Application au plan communal de sauvegarde. In *8ème Conférence Internationale de MOdélisation et SIMulation. Hammamet, 2010*.

Flaus, J.-M. 2011. A modelling framework for model based risk analysis. In *European Safety and Reliability Conference (ESREL 2011), Troyes 2011*.

Girard, C., David, P., Piatyszek, E., & Flaus, J.-M. 2013. Emergency Plans Modeling: Toward An Assessment Tool. In *European Safety and Reliability Conference 2013 (ESREL 2013), Amsterdam, 29 September-2 October 2013*.

Hémond, Y. & Robert, B. 2013. Assessment process of the resilience potential of critical infrastructures. *International Journal of Critical Infrastructures* 9(4), 29p.

Henstra, D. 2010. Evaluating Local Government Emergency Management Programs: What Framework Should Public Managers Adopt? *Public Administration Review* 70(2): 236–246.

Jain, S. & McLean, C. 2003. A framework for modeling and simulation for emergency response. *Proceedings of the 2003 International Conference on Machine Learning and Cybernetics, Xi'an, 2–5 November 2003*.

Karagiannis, G.-M., Piatyszek, E., & Flaus, J.-M. 2010. Industrial emergency planning modeling: a first step toward a robustness analysis tool. *Journal of Hazardous Materials*, 181(1–3): 324–334.

Kolen, B., Kok, M., Helsloot, I., & Maaskant, B. 2012. EvacuAid: A Probabilistic Model to Determine the Expected Loss of Life for Different Mass Evacuation Strategies During Flood Threats. *Risk Analysis* 33(7): 1312–1333.

Lewis, D. & Mioch, J. 2005. Urban Vulnerability and Good Governance1. *Journal of Contingencies and Crisis Management* 13(2): 50–53.

Lisnianski, A. & Levitin, G. 2003. *Multi-State System Reliability*. Singapore: World Scientific Publishing Co. Pte. Ltd.

Natvig, B. 2010. *Multistate Systems Reliability Theory with Applications.*Wiley Seri. Chichester: Wiley, 1st Edition.

Perry, R.W. & Lindell, M.K. 2003. Preparedness for Emergency Response : Guide- lines for the Emergency Planning Process. *Disasters* 27(4): 336–350.

Robert, B., De La Lande De Calan, R., & Morabito, L. 2008. Modelling interdependencies among critical infrastructures. International Journal of Critical Infrastructures. *International Journal of Critical Infrastructures* 4(4): 392–408.

Robert, B., Morabito, L., & Debernard, C. (unpubl.). Simulation and anticipation of domino effects among critical infrastructures. *International Journal of Critical Infrastructures* X(Y).

United Nations. (2011). *General assembly AG/11047 from 28/01/2011, New York, January 2011*.

This page intentionally left blank

Human factors and human reliability

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The model of a pilot competency as a factor influencing the safety of air traffic

J. Skorupski
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

M. Wiktorowski
33rd Polish Air Force Base, Poland

ABSTRACT: The level of safety in air transport is affected by many factors: the widely understood human factor, technical factor and environmental factor. The aim of the research is to develop indicators for quantitative assessment of the flight crew status in the context of its impact on the safety of air traffic. The paper presents a new definition of a flight crew status of a formal nature. The proposed approach takes into account functional dependencies between the various factors influencing the air crew status. These dependencies are hardly definable and partly subjective, so the research concerning them belongs to the area of uncertain information analysis. We propose to use fuzzy inference methods using expert knowledge for this analysis. The paper gives a detailed description of the new fuzzy local model of a pilot competence, which is expressed by the linguistic variable values. They are influenced by the pilot's experience, training process and the Crew Resource Management (CRM). A fuzzy inference system corresponding with the model was built. Some examples of membership functions of linguistic variables and sample fuzzy inference rules are presented in the paper. This system was used for the model experiments, which led to the interesting results. These include finding the relationships between the experience of the pilot, the various elements of the pilot training process and the flight crew status. The obtained results allow, among others, to optimize the process of flight crew selection to specific tasks, and to optimize the process of a pilot training.

1 HUMAN FACTOR IN THE AIR TRAFFIC MANAGEMENT SYSTEM

The very important problem in the Air Traffic Management (ATM) is to maintain the control subsystem's ability to interact with the controlled objects in order to achieve the intended objectives. The efficiency of this interaction is affected by many factors like suitable communication or surveillance systems reliability. As well the control subsystem as the controlled objects (aircraft) are strongly human-related and in this paper particular attention will be given to a flight crew as the human component of the air traffic. The crew's ability to proceed with basic tasks of managing flight as aircraft control and positive two-way communication process with air traffic controllers is one of crucial factors determining the main goal—maintaining the flight safety at assumed level. This ability is to a great extent dependent on a crew selection or, saying more widely, on a crew resource management at the air carrier's level. This paper presents the method of flight crew status assessment, particularly the crew competency as one of the most important elements.

Problems concerning human factor's role in the air traffic safety are the point of interest of scientists of different domains. The paper (Afrazeh & Bartsch 2007) presents human reliability as the human ability to perform the task in given frames, covering all the physical and psychological skills, experience and personal characteristics. The other one (Dekker 2006) states that the whole human performance of people taking part in aviation transportation process is located in a specific context that consists of the aircraft and its equipment type, weather, air traffic and other Performance Shaping Factors—PSF. They were incorporated in (Swain & Guttman 1983) as the set of factors affecting human capabilities. They are divided to internal ones—like stress, fatigue, knowledge, personality, experience, and external ones—such as ergonomics, educational programs, organizational structure, motivation and procedures (Pei-Hui 2011).

According to system approach to air traffic safety problem, the human factor is placed in the center of interest. However, the other important factors that influence the operational risk in

direct or indirect manner are not omitted. There are two most popular system models of human factor in the air traffic safety. One of them is the SHELL model (Edwards 1972; Hawkins 1993) and the second one—the Reason's model (1990). The first model describes the threats connected with interface between human and environment, software, hardware and other human. The second one presents dependencies among different areas of operations which can include different safety gaps.

The attempt to analyze flight crews and air traffic controllers using fuzzy sets theory was introduced in (Lower et al. 2013). The likelihood of an incident to accident transformation was analyzed assuming adverse human operation.

The literature analysis shows the most common way to divide human factors to four groups: physical, physiological, psychological and external conditions. Physical factors can be expressed in the form of health, growth and strength. The physiological ones include the access to oxygen, changes in pressure, perception capabilities, disorientation, fatigue, biorhythm disturbances, diet and alcohol effects. The psychological factors are: information processing and selection, error management, personality, self-discipline, motivation, operation under pressure, situational awareness, perception, safety awareness, threat identification, decision making and judgment of situation, attention distribution, coping with stress, interpersonal communication, leadership, adaptation capabilities, training, skills and experience. Finally the external conditions consist of workload and task demand, also the all meanings of culture (connected with profession, organization and safety) are included.

The literature mentioned above however, doesn't try to assess quantitatively the one given flight crew status in the context of the actual flight safety. In (Skorupski & Wiktorowski 2013) a proposal of the mathematical fuzzy inference model with the quantitative crew status assessment as the result is introduced. The estimation is expressed by linguistic variable value where the way leading to the final result takes into consideration many of the essential factors connected with crew's before flight preparation. The calculations consider also the operational and organizational environment influence. The model can become the base for creation of a decision support system that could be useful for people responsible for crew management process.

This paper is the extension of our previous work. It shows how the very important parameter—pilot's training—affects pilot's competency. It also shows how this relationship can be assessed quantitatively with the use of fuzzy sets theory.

The paper is organized as follows. In section 1 a short literature review on human factors in ATM is presented. Section 2 contains the short introduction to air carrier tasks connected with the crew resource management. In section 3 the literature review and general idea of fuzzy inference system for air crew status assessment is given. Section 4 presents one of the most important elements of this system—the local model, where the linguistic variable *Competency* is introduced. Then, in section 5 detailed description of training (represented by linguistic variable *Training*) as the very important part of competency model is given. Section 6 presents and discusses some experiments' results, that can be useful in everyday aircrew management. In section 7 a summary and concluding remarks are presented.

2 AIRLINE OPERATORS' TASKS IN THE AREA OF CREW RESOURCE MANAGEMENT

According to The Annex 6 of Chicago convention, the Safety Management System (SMS) was introduced. This triggered the situation where the airline operators are obliged to manage the safety, covering their all activities including every single flight. First of all, SMS deals with threat identification, ineligible events effects mitigation and risk estimation. The goals listed above can be assisted by the proposed model of the flight crew status in the context of safety. The risk connected with conducting the whole process of flight by the given crew will be easier to estimate in objective and quantitative way. The research of some flight operators (airlines) functioning in the area of SMS was presented in (Pei-Hui 2011). It was to be said that the idea of SMS was realized only partly, therefore some changes at the operational level are to be made. The model and the fuzzy inference system for the flight crew assessment, presented in the following sections, are going to work at the same level. Nowadays the risk management cards are widely used for the operational risk assessment, but they are not sufficient. The discussed model application can possibly extend the risk assessment idea by the whole human factor problem consideration. The flight crew assessment based on the presented method may improve crew resource management and planning process and in result will make the operators able to maintain high level of operational readiness especially in the area of crew availability.

3 THE FUZZY MODEL OF THE FLIGHT CREW STATUS ASSESSMENT IN THE CONTEXT OF AIR TRAFFIC SAFETY

The problem of the flight crew status estimation in the context of proper flight task realization

concerns the human factor that is hard to analyze in exact manner. That's why the problem is located in the area where the information is imprecise and uncertain. Therefore the fuzzy logic approach is used in this elaboration.

There are many papers that suggest the usage of the fuzzy logic methods and tools in the area of air traffic management. One of the most interesting (Hadjimichael 2009) describes the expert system that was created to assist the take-off and landing risk assessment. The human factor was taken into consideration however the problem was much simplified. The problem of flight crews duty hours planning was undertaken in the paper (Teodorovic & Lucic 1998). Psychological aspects of pilot's behavior where analyzed in (Wanyan et al. 2011). The research (Xianfeng & Shengguo 2012) includes the attempt of airport security assessment where the human factor was partly taken under consideration. The other examples of fuzzy methods utilization in the area of air traffic management can be found in (Babic & Krstic 2000) and (Netjasov 2004). The other technology sectors also use the fuzzy methods in risk assessment of key elements damage (Torshizi & Parvisian 2012), as well as human factor influence on reliability of system (Bertolini 2007).

In this research we are concentrated on hierarchic fuzzy structure creation considering any possible factors which can influence the crew (not single pilot) ability to perform the flight. We try to consider all the physical, physiological, psychological factors as well as the external conditions. The created model that is still being developed as well as its computer implementation in SciLab can be used to support the decision making process in crew selection.

The fuzzy set A we define as follows (Kacprzyk, 1986):

$$A = \left\{ \left(x, \mu_A(x) \right) : x \in X, \mu_A(x) \in [0,1] \right\} \tag{1}$$

where μ_A is the membership function of this set.

As a linguistic variable we define the variable which is expressed by words or sentences that we call linguistic values of linguistic variable. Our models assume that linguistic variables have *low, average* and *high* values.

The trapezoidal membership function for *low* value with trapezoidal shape and parameters (a,b,c,d) is defined as follows:

$$\mu_{low}(x;a,b,c,d) = \begin{cases} 0, & x < a = b \\ 1, & b \le x \le c \\ \dfrac{d-x}{d-c}, & c < x \le d \\ 0, & x > d \end{cases} \tag{2}$$

For value *average*:

$$\mu_{avg}(x;a,b,c,d) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a < x \le b \\ 1, & b < x \le c \\ \dfrac{d-x}{d-c}, & c < x \le d \\ 0, & x > d \end{cases} \tag{3}$$

For *high* value:

$$\mu_{hgh}(x;a,b,c,d) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a < x \le b \\ 1, & b < x \le c \\ 0, & x > c = d \end{cases} \tag{4}$$

In the reasoning process we use the input values fuzzification block, then inference block that uses a set of fuzzy rules, and finally defuzzification block of output values. The set of rules is being created with experts' opinions, in this case aircraft pilots and people responsible for Safety Management System (SMS) organization. As a inference rule for local models we will use the fuzzy rule *modus ponens*, as below (Kacprzyk 1986):

$$\begin{aligned} &I : x = A \Rightarrow y = B \\ &P : x = A' \\ &C : y = B' \end{aligned} \tag{5}$$

where I denotes implication, P—premise, C—conclusion. This rule gives us opportunity to conclude about the successor based on the predecessor logical value. The implication is treated as a fuzzy relation which means that A' doesn't have to be equal to A and B' doesn't have to be equal to B. It's fairly enough when A' is similar to A and this way B' is similar to B.

In the fuzzy inference systems the parameters listed below were chosen for determination of linguistic variable values concerning *CRM, Training* and *Experience*

– s-norm of maximum type:

$$\mu_{A \cup B}(x) = \max\left(\mu_A(x), \mu_B(x) \right) \tag{6}$$

– t-norm of minimum type:

$$\mu_{A \cap B}(x) = \min\left(\mu_A(x), \mu_B(x) \right) \tag{7}$$

– implication of algebraic product type:

$$\mu_{A \to B}(x,y) = \mu_A(x) \cdot \mu_B(y) \tag{8}$$

– rules aggregation of algebraic sum type:

$$\mu_{A\oplus B}(x) = \mu_A(x) + \mu_B(x) - \mu_A(x)\cdot\mu_B(x) \quad (9)$$

– defuzzification of center of gravity type:

$$Z^* = \frac{\int \mu_B(z)\cdot z dz}{\int \mu_B(z) dz} \quad (10)$$

The literature shows many different factors that influence human activity but only the most effective ones on flight crew performance were chosen for the analyses. We can point out three the most important factors describing the flight crew status. The first of them is competency (which among the others covers skills, experience and knowledge), the second one is situational awareness (that is determined mainly by communication and information processing) and the last one—motivation—the psychological side of performance (especially shows the difference between the actual results of activity and the theoretical abilities). The Figure 1 presents dependence scheme of the factors listed above.

The lack of situational awareness is one of the most important reasons of aviation negative events: incidents, serious incidents and accidents. The awareness is dependent on quality of information processing and communication, where the last one is strongly connected with competency and motivation. Information processing is dependent on fatigue and competency as well. As we can see the connections and dependencies are strongly complicated. This fact causes difficulties in the research and makes us to use expert estimated data, which are subjective and imprecise. Also that was the reason to use the fuzzy method in the research (Zadeh & Kacprzyk 1992).

The model of relations showed at Figure 1 determines the structure of local models. The every rectangle at this figure symbolizes the linguistic variable which is the output of a local fuzzy model with many inputs. The example of local models for *Competency* estimation will be shown in Chapter 4.

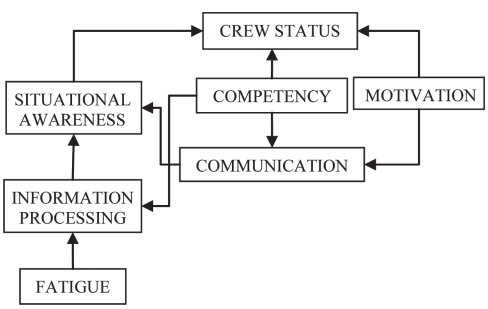


Figure 1. The general fuzzy model of factors that have influence on flight crew status.

4 THE FLIGHT CREW STATUS ASSESSMENT METHOD—LOCAL MODEL COMPETENCY

In this section we will concentrate on the local model destined to estimate the linguistic variable *Competency* which is the key factor for crew status assessment. That's because the *Competency* influence the linguistic variable of crew status directly and indirectly through the inputs to *Communication* and *Situational awareness* as well. Contributory factors of aviation events analysis indicate the last two factors are frequently direct reasons of flight incidents or belong to the circumstances that are conducive to negative events.

The linguistic variable *Competency* is determined by three input variables (Fig. 2): *Training, Experience* and *CRM* (Crew Resource Management), assumed as the ability of the crew to cooperation. We assumed the variable *Competency* will accept three values: *low, average* and *high*.

The three input variables influence the *Competency* in different manner. We assume the *Experience* has the highest weight because it mirrors crew flight capabilities with reference to their performance on current and the previous types of aircraft as well. The variables *Training* and *CRM* affect the *Competency* with the information about the so-called pilots currencies (length of breaks in flying) and important trainings participation which are

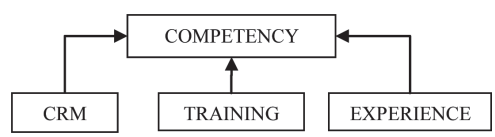


Figure 2. The local model *Competency*.

Table 1. The example of some fuzzy reasoning rules for *Competency*.

Rule	*CRM*	*Training*	*Experience*	*Competency*
10	*Average*	*High*	*Low*	*Low*
13	*Average*	*Average*	*Low*	*Low*
14	*Average*	*Average*	*Average*	*Average*
17	*Average*	*High*	*Average*	*Average*
18	*Average*	*High*	*High*	*High*
24	*High*	*Average*	*High*	*High*

especially key factors for young pilots. For more experienced pilots trainings and in-flight or simulator checks secure the safety from routine and conviction about their excellence that can become dangerous.

The Table 1 presents several fuzzy reasoning rules used in the fuzzy inference system for determining the *Competency.*

5 THE METHOD UTILIZATION EXAMPLE—TRAINING ASSESSMENT IN THE CONTEXT OF HIGH LEVEL OF CREW COMPETENCY

Between the others, the linguistic variable *Training* characterizes a member of flight crew in the area of currency in flying, and also accepts three linguistic values: *low, average* and *high*. One of the determinants can be the time that has passed since the last flight. The other one is the time (in months) since the last simulator training which is valuable index in relation to crew capabilities to cope with flight emergencies. Usually once a year every pilot is subjected to pass the checkride (an examination during flight) which causes the need to update and refresh his knowledge and this way improves his general professional performance in routine flights. That's why we can accept the time since the last checkride as the next *Training* determinant.

According to EU-OPS the every airline operator is responsible for implementation of procedures that guarantee their flight crews have all the proper licensees, suitable trainings, experience and are eligible to fulfill all the pilots duties (European Commission, 2008). Generally the every pilot is supposed to complete the aircraft class rating and aircraft type rating. Any change of operator by a pilot, forces him to complete the proper courses and trainings before he/she starts to fly without supervision.

The young pilots after completing suitable tests should execute minimum four flights under supervision in maximum 21 days period and 6 takeoffs and landings on simulator (sometimes the number of the operations can be flexible). The captains should have proper experience and they are obliged to complete aircraft commander training for multicrew operations that consists of:

- simulator training;
- captains airline training;
- captains skills examination;
- airports and en-route knowledge and competency training;
- CRM training.

Pilots should maintain their currencies (not to exceed maximal time between flights). The general rule is minimum 3 takeoffs and landings in the period of 90 days, but the period can be extended up to 120 days in cases pilots fly under supervision. When the break is longer, the compulsory additional flight under supervision or simulator training is required (European Commission, 2008). Not earlier than after 2 years of continuous flight operations, the periods of time listed above can be changed by the proper aviation authorities. In such cases ATQP (alternative training and qualification programme) and LOE (line oriented evaluation) allow the time spaces between checkrides to be extended to 12 months, and between emergency management checks-up to 24 months.

According to the previous assumptions and with respect to the flight crews operational rules we chose the input variables for linguistic variable *Training*:

- The period of time since the last flight: the *Pause* linguistic variable accepts three fuzzy values *low, average* and *high.* It's defined on the universe of discourse equal to the real numbers from the interval [0,90] days.
- The period of time since the last simulator training: the *Simulator* linguistic variable accepts three fuzzy values *low, average* and *high*. It's defined on the universe of discourse equal to the real numbers from the interval [0,12] months.
- The period of time since the last checkride in flight: the *Checkride* linguistic variable accepts three fuzzy values *low, average* and *high*. It's defined on the universe of discourse equal to the real numbers from the interval [0,24] months.

The Figure 3 shows the example of *Training* fuzzy model using the three listed above fuzzy variables as inputs. The Table 2 presents the trapezoidal membership functions parameters (a,b,c,d) of input variables while the trapezoidal membership functions parameters of output variable are shown in Table 3.

The factors listed above are searched for the importance and weigh that they have on *Training* and the results were taken into consideration in fuzzy reasoning rules creation. We assume the *Pause* is the most important. Pilots have to rely on their knowledge and experience and also they have to take care of the learnt good skills and habits. The longer the time since the last flight the faster proper skills and habits are forgotten. Less important are *Simulator* and *Checkride* while still they influence the output variable value. Some of the fuzzy reasoning rules are shown in Table 4. They were defined on the basis of expert evaluations. The group of experts consisted of pilots, safety managers and persons responsible for investigating the causes of air accidents.

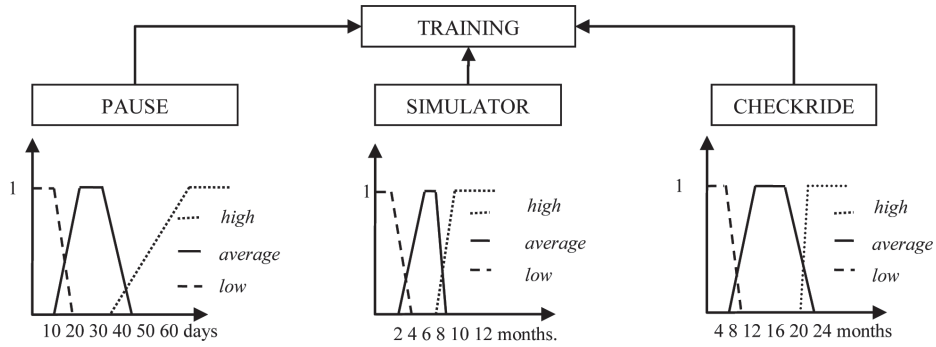


Figure 3. The local fuzzy model of linguistic variable *Training*.

Table 2. The (*a*,*b*,*c*,*d*) parameters of trapezoidal membership functions of input linguistic variables for *Training* model.

	a	*b*	*c*	*d*
Pause				
Low	0	0	10	20
Average	10	20	30	40
High	30	60	90	90
Checkride				
Low	0	0	4	8
Average	6	12	16	20
High	18	20	24	24
Simulator				
Low	0	0	2	4
Average	3	6	7	8
High	7	9	12	12

Table 3. The (*a*,*b*,*c*,*d*) parameters of trapezoidal membership functions of output linguistic variable for *Training* model.

Training	*a*	*b*	*c*	*d*
Low	0	0	1	2
Average	1	2	3	4
High	3	4	5	5

Table 4. The examples of fuzzy reasoning rules for *Training* local model.

Rule	*Pause*	*Simulator*	*Checkride*	*Training*
4	*Low*	*Average*	*Low*	*High*
6	*Low*	*Average*	*High*	*High*
7	*Low*	*High*	*Low*	*Average*
17	*Average*	*High*	*Average*	*Average*
21	*High*	*Low*	*High*	*Low*
25	*High*	*High*	*Low*	*Low*

6 THE RESULTS DISCUSSION

The example results of fuzzy inference system simulation for linguistic variable *Training* estimation, obtained with a computational tool created in SciLab 5.4 environment are shown on Figure 4.

In the case of *Training* and *Simulator* relationship (Fig. 4a) we can see in the results that the pilots with relatively short break from the last flights (up to 20 days) may extend the time between simulator trainings up to 6–7 months. The more frequent simulator trainings don't improve the *Training* value, which equals to 4.3 (the *high* linguistic value). For pilots with longer break from last flight (40 days and more) the simulator trainings should be organized more often (after about 3 months). The longer break results with the drop of *Training* value even to 0.8 (the *low* linguistic value). The observation is similar to intuitional approach but the model results give us quantitative assessment. The above experiment result can be treated as the element of the model validation process.

On the other hand the *Training* and *Checkride* relationship analyses (Fig. 4b) reveal a little amazing results. The simulation experiments results show, the *Checkride* in most cases doesn't influence the *Training* at all. This concerns the cases when the break from the last simulator training is longer than 1.5 month for any value of break in flights practicing. The only case (showed on Fig. 4b) the *Checkride* influence on the *Training* value, exists when a pilot has long break in flying (60 days or more) and the time from the last simulator training is shorter than 1 month. Then the checkride makes sense, but only if the break from the last one is more than 18 months. The observation is interesting because it indicates the checkride every 6 or 12 months (as requested by the regulations) may be needless because it doesn't improve the *Training* variable. In case the check-rides are to be continued they should be scheduled maximum every

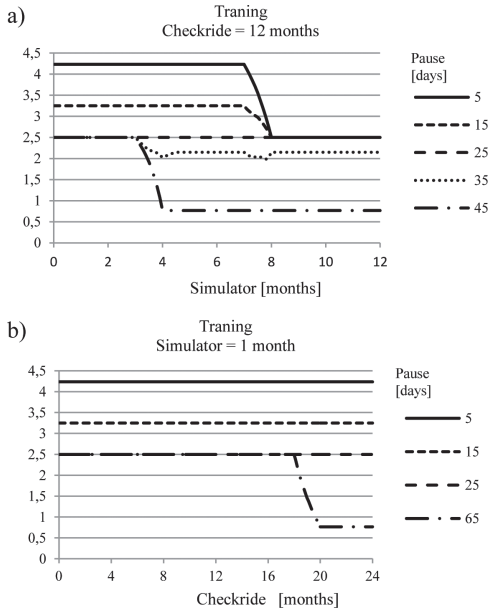


Figure 4. *Training* correlation with: a) *Simulator,* b) *Checkride.*

16–17 months. However further verification of the model, system and the results should be continued.

7 SUMMARY

The flight operators crew resources management is one of the most important factors that influence the air transport safety. The proper crew selection process is one of the key elements. The crew should have optimal performance that among the others mirrors their competency, motivation, communication skills or situational awareness. Those features are not constant and depend on many different factors such as current crew predisposition to perform the safe flight. The crew selection and assessment process in the context of flight safety is significantly difficult due to the imprecise, uncertain and incomplete information. In such a case the expert systems based on the fuzzy sets theory can become the meaningful and helpful assistance. The presented example of the fuzzy inference system assures the possibility of the presented approach utilization in flight operator assistance by crew reliability improvement.

REFERENCES

Afrazeh, A., Bartsch, H. 2007. Human reliability and flight safety. *International Journal of Reliability, Quality and Safety Engineering* 14(5).

Babic, O., Krstic, T. 2000. Airspace daily operational sectorization by fuzzy logic. *Fuzzy Sets and Systems* 116: 49–64.

Bertolini M. 2007. Assessment of human reliability factors: A fuzzy cognitive maps approach. *International Journal of Industrial Ergonomics* 37(5): 405–413.

Dekker, S. 2006. *The field guide to understanding human error*. Ashgate Publishing Ltd.

Edwards, E. 1972. Man and machine: Systems for safety. *Proc. of British Airline Pilots Associations Technical Symposium*, British Airline Pilots Associations, London.

European Commission 2008. Commission regulation (EC) No 859/2008 of 20 August 2008 amending Council Regulation (EEC) No 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane. *Official Journal of the European Union* L 254/1.

Hadjimichael, M. 2009. A fuzzy expert system for aviation risk assessment. *Expert Systems with Applications* 36: 6512–6519.

Hawkins, F., Orlady, H. 1993. *Human factors in flight* (2nd ed.). Avebury Technical.

Kacprzyk J. 1986. *Fuzzy sets in system analysis*. Państwowe Wydawnictwo Naukowe, Warsaw.

Lower, M., Magott, J., Skorupski, J. 2013. Air Traffic Incidents Analysis with the Use of Fuzzy Sets. in: L. Rutkowski et al. (Eds.): *ICAISC 2013, Part I, LNAI* 7894: 306–317. Springer, Heidelberg.

Netjasov, F. 2004. Fuzzy expert model for determination of runway in use case study: Airport Zurich. *Proceedings of the "1st International Conference on Research in Air Transportation ICRAT 2004"*, Zilina, Slovakia: 59–64.

Pei-Hui, L. 2011. *Safety Management and Risk Modelling in Aviation: The challenge of quantifying management influences*. Delft University of Technology, PhD thesis, 2011, http://repository.tudelft.nl/view/ir/uuid%3A3b293559-81ed-4450-aa78-005bbd9054f1/ (04.2013).

Reason, J. 1990. *Human Error*. Cambridge University Press, 1990.

Skorupski, J., Wiktorowski, M. 2013. The problem of crew status assessment in the context of air traffic safety. *Prace Naukowe Politechniki Warszawskiej. Transport* 96: 401–411.

Swain, A., Guttman, H. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque.

Teodorovic, D., Lucic, P. 1998. A fuzzy set theory approach to the aircrew rostering problem. *Fuzzy Sets and Systems*, 95(3): 261–271.

Torshizi, A., Parvizian, J. 2012. A Hybrid Approach to Failure Analysis Using Stochastic Petri Nets and Ranking Generalized Fuzzy Numbers. *Advances in Fuzzy Systems*, 2012, doi:10.1155/2012/957697.

Wanyan, X., Zhuang, D., Wei, H., Song J. 2011. Pilot attention allocation model based on fuzzy theory. *Computers & Mathematics with Applications* 62(7): 2727–2735.

Xianfeng, L., Shengguo H. 2012. Airport Safety Risk Evaluation Based on Modification of Quantitative Safety Management Model, International Symposium on Safety Science and Engineering in China. *Procedia Engineering* (43): 238–244.

Zadeh, L., Kacprzyk J. 1992. *Fuzzy logic for the management of uncertainty,* Wiley.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Human Dependability Model for space application—the HuDeM project

T.M. Stene
NTNU Social Research, Trondheim, Norway

S.O. Johnsen
SINTEF, Trondheim, Norway

S. Ophof
ARGOTEC, Turin, Italy

ABSTRACT: This paper will present the HuDeM (Human Dependability Model) project financed by the European Space Agency (ESA). The project has focused on developing a Human Dependability Model to be applicable for space activities and projects. The project is based on relevant perspectives from other industries like aviation, petroleum, nuclear and railways. Human Dependability is described as the contribution of the human in a space system to safety and reliability, a subject to reduce the incidence of human error and minimize its effects. Existing literature suggests that there is a trend towards an understanding and acknowledgement of the importance of humans in accidents and recoveries. In addition to propose a Human Dependability Model, the project validated the implementation of one proposed method. The initial validation is based on a case study. The validation method focuses primarily on the use of scenarios and checklists. This paper will outline and discuss some experiences and key challenges.

1 INTRODUCTION

1.1 *Developing a human dependability model for space activities and projects*

In 2012 ESA initiated a one year project to review human dependability and identify relevant practices from other industries.

In general, the project is related to space control centres, integration facilities, and launch bases. Such technical infrastructures are all operated by human, and may constitute:

- Flight Segments: Manned Space Station and/or Modules; Satellite/Spacecraft etc.
- Ground Segments: Control or Test Centre; Launch Base etc.
- Recovery segments: Ground Vehicles; Ground Teams etc.

Even if the focus primarily is on activities and projects related to control centres human operated system in general are relevant.

1.2 *The consortium*

In defining a human error avoidance program, the Consortium constitutes three partners: NTNU Social Research, SINTEF and ARGOTEC. The former has been project manager and prime contractor.

NTNU Social Research has eight units, and the two involved in this project are CIRiS and Studio Apertura. CIRiS contribute, through the N-USOC (Norwegian User Support and Operations Centre), on a daily basis to support and operate research facilities and experiments on-board the International Space Station (ISS). The N-USOC is an important contributor during planning, development, integration and execution of the different experiments that utilizes the ESA Columbus laboratory on-board ISS. In addition to safety research in the petroleum sector, Studio Apertura has experience from sectors like transport and critical infrastructures. Many of the projects are of a cross-disciplinary character, often focusing on the interplay between formal and informal elements of organizations.

SINTEF is the largest independent research organization in Scandinavia. The research covers a diversity of domains; petroleum and energy, health, information and communications technology, marine activities, materials science and applied chemistry, technology management and building/construction. The Safety and Reliability department has expert knowledge in risk and reliability, having several publications in the field of human reliability, human errors, risk indicators, risk control methods and systems engineering.

ARGOTEC has experience from space operations through development of software displays, implementation of crew training as well as training and simulations for flight controllers, the company has identified and adopted processes and principles which contribute to the mitigation of human errors. In particular, the validation of the proposed methodology is based on experiences in the space domain.

1.3 *Key questions*

Although we have presented some background information for selecting one particular method applicable to space, this paper primarily describes the "initial validation" of the most central method in the HuDeM project.

Thus key questions in this article are:

- What human dependability methods are significant for control centre?
- How to validate a proposed human dependability model for space application?

2 THE HuDeM PROJECT

2.1 *The objective and tasks*

The main objective of the HuDeM project was to define a human dependability model, in addition to develop an analytical methodology and procedural approach for space system applications with emphasis on spacecraft operations and astronaut activities.

The HuDeM project covers the following five tasks: (1) Identification, Survey and Evaluation of the Most Meaningful Domains for Deriving a Consistent Human Dependability Model Applicable to Space Projects and Activities, (2) Definition of the Methodology for Development of Human Dependability Model(s), (3) Implementation of the Proposed Methodology, (4) Definition of the Analyses for Human Errors Identification and Avoidance, and (5) Management.

The objective of the tasks was respectively: (1) to investigate current existing practices in the industrial domain which use and apply human dependability approaches to their systems/activities. Literature from the following domains is used; aviation, nuclear power plants, oil/gas and railway. (2) To define a human dependability methodology suitable for space applications. (3) To define a human error avoidance program (methodology), in addition to validate the methodology with an example from ISS payload development, integration and operation (USOC). (4) To define the qualitative and qualitative analyses for human errors identification and avoidance or mitigation. (5) Project management.

2.2 *Experience form several domains*

In the first phase of the project experiences from other high technology industries like aviation, nuclear, marine and petroleum industry. In addition a survey in the space domain was conducted (see Johnsen & Stene, 2014).

Major accidents and mishaps have multiple systemic origins, i.e. origins and causes related to multiple factors such as technology, organisations, human factors and the interplay between them.

2.3 *Theoretical approach*

Human dependability encompasses the risk of human errors, but also the human capacity to perform well, even beyond expectations, and to anticipate and solve problems. Consequently the project addresses both human error and how it can be avoided, as well as how one can depend on humans to create safety in space operations. Thus, the project also includes theories and perspectives from resilience engineering and High Reliability Organizations (HRO).

To understand the ability of humans to perform safely in high technological organizations, it is necessary to study human action in light of technology and the organizational context. Errors do not happen in isolation, and there is a strong relationship between these factors. Consequently, human dependability is seen from a so called Man-Technological-Organisation (MTO) or Human-Organization-Technology (HOT) perspective in the project (Johnsen, Stene & Kongsvik, 2014).

When reviewing experiences from other industries, the development has gone from the perspective of "human errors" to looking at major accidents as having multiple interrelated causes from organisation, technology and human factors. Thus a key finding is the need to establish taxonomy to understand accidents and recoveries based on a causal chain avoiding to blame the human element if the causes were due to organisational or technical issues, as suggested by Dekker (2002).

In aviation, the taxonomy called Human Factors Analysis and Classification System (HFACS) has been established; see Shappell & Wiegmann (2000), to understand accidents based on several factors than mere human error. The HFACS taxonomy are based on the "Swiss Cheese Model" from Reason (1997), looking at accidents as unsafe acts based on preconditions, unsafe conditions and organisational influences, in order to avoid blaming the human element. However, the HFACS method has no exploration of resilience, and should be extended to cover resilient acts, based on preconditions of resilience, resilient conditions and High Reliable Organisational influences.

The HFACS method was initially developed to avoid mishaps in naval aviation, and has later been applied in several other domains similar to the space domain. Hence, it seems well suited to ESA. However, it should be adapted to the space environment. It consists of a comprehensive analysis of previous accidents, also identifying lacks in barriers that are more remote from the incident itself, as management or supervision or organisational causes Thus, taxonomy such as HFACS could be adapted and implemented in order to have an empirical background to implement and work with tools such as Human Reliability Analysis (HRA).

2.4 *Human dependability methods*

The project primarily focuses on control centre activities. The HuDeM project describes several theoretical perspectives and methodological approaches, and goes in depth of one particular human factor based approach—CRIOP—and both task 2 and 3 is dedicated to this.

CRIOP is Human Factors (HF) based method to verify and validate the ability of a human operated system to function reliable and safely during crises and during normal operations. CRIOP has been funded by the research council and it is a freely available method see, Aas et al. (2009), also www.criop.sintef.no. CRIOP is based on HF standards such as ISO 11064—"Ergonomic design of control centres".

CRIOP is performed to avoid accidents, based on risk analysis, and to build and support resilience (i.e. where resilience is considered as the ability to handle surprises and continue operations).

Good practice checklists, discussion in an expert team and exploration of scenarios are central elements. *Check lists* cover seven elements: Organisation and management. Procedures, work descriptions and workload, Competence and training, Communication/distributed situational awareness, Working environment, Layout, and Control and safety systems. The checklists explores key human factors (safety) issues in each area, i.e. when discussing control systems the use of alarms is explored and a question is the existence of an "alarm philosophy", and performance issues of alarm handling such as the acceptable number of alarms pr. hour.

Scenarios are used to highlight unwanted incidents, potential accident or loss of science in a particular project or activity. The scenarios are based on findings from the checklist, discussion with the design team to identify conditions where there are some unease or based on discussing key root causes from known documented accidents. The scenarios with errors and recoveries are modelled by using a simple STEP analysis, where critical steps are identified, selected and discussed in a workgroup meeting constituting *key stakeholders*: experts from management, operators, safety experts, designers and human factors experts. The purpose is to support both "bottom up" and "top-down" processes. Results, i.e. mitigating actions, are prioritized by experts in collaboration—ensuring that key issues are discussed and prioritised by different perspectives.

In addition to CRIOP, task 1 and 4 (see 2.1) of the HuDeM project describe several methods relevant for studying human dependability. In the following we mention relevant qualitative and quantitative methods.

Qualitative methods emphasized are Operational Condition Safety (OCS) and Operational Conditions in Control Room Organisations (OCCO). The OCS method is developed and frequently used in the petroleum industry. It is a counterpart to methods mapping the processing plant's technical safety condition. Five of seven elements constituting the whole OCS method in the petroleum sector, is operationalised to control room settings for space application; called OCCO. Prior to this project, a pilot study had operationalised four elements: Competence, Procedures and documentation, Communication and Management (Fossum et al., 2014). During the HuDeM project, a fifth element was added: Change management. Thus, two elements remain to be operationalised for space application: Work practice and Workload and practical working environment.

Quantitative methods emphasized are HRA methods based on a proposed set of selection criteria. We suggest SPAR-H as a simple and usable method for space. The method is developed for the US Nuclear Research commission. The method is applicable for selected scenarios to evaluate probabilities and areas of great concern for the space domain. SPAR-H accounts for the context associated with Human Failure Events (HFEs) by using Performance Shaping Factors (PSF) (Gertman et al. 2005).

3 VALIDATION OF THE METHODOLOGY

3.1 *Participants*

In addition to the consortium, the SPACE-CRIOP workgroup mainly included participants from one of ESA's control centre. N-USOC (Norwegian User and Operations Centre) is supporting biological experiments on-board ISS.

3.2 *Initial validation*

Validity assessment of the method is based on control centres within ESA and their collaboration

with space flights. The CRIOP method is in accordance with the European Cooperation for Space Standardization (ECSS) regulations.

Phases 0–2 of the CRIOP main phases are covered in the validation: (0) Preparation and organisation, (1) General analysis including checklists, (2) Scenario analysis, (3) Actions and (4) implementation and follow up.

The initial validation focuses primarily on the scenario and checklist methods. In addition to a real incident that occurred during real-time ISS operations, the validation includes a selection of standard checklist items as recommended in the general CRIOP method.

3.3 *Validation criteria*

The initial validation process aims to achieve the same analysis of real world ISS (International Space Station) operations anomalies by using the SPACE-CRIOP method. The CRIOP method should be able to identify weak points related to safety in advance of a real time operation.

In the project, we have used actual anomaly reports to validate the method. If the method is valid for the space domain, the identified weak points should be similar to actual anomalies cases from the real world.

Identified root causes to anomalies were used to find relevant validation cases. The project covers a survey, included in task 1, to identify meaningful anomalies during human spaceflight operations (Johnsen & Stene, 2014). The anomaly reports were related to control centres supporting ISS operations.

One of the registered anomalies was selected as suitable test scenario.

Validation criteria are:

- The *checklist process* was expected to identify similar causes to anomalies as the survey in task 1
- The *scenario process* was expected to identify weak points in line with the actual problems/ root causes according to the specific anomaly report.

4 RESULTS

In addition to results according to the stated validation criteria, this chapter presents experience with the validation process.

4.1 *The validation process*

The CRIOP method developed for the petroleum sector is used as a basis for development of a Human Dependability Model for space.

The purpose was to validate the methodology process and to test the specific results related to the checklists and scenarios. Thus, the project covers the first three of the following steps: (0) Preparation, (1) General analysis, (2) Scenario analysis, (3) Action and (4) Implementation and follow up.

The facilitator, in this case from Argotec, is in charge of the process. The facilitator chairs the meetings, provides all documentation and coordinates the discussion. The facilitator also selects the scenario and makes sure everything is performed within the time-limits.

Preparation and organisation phase: The scenario is briefed and all necessary documentation collected. During a teleconference the most applicable checklist items are selected. The final list included 34 relevant items.

Further, the scenario is briefed and discussed.

General analysis—Checklists: During a one day workshop the selected checklist items are discussed with all participants. Finally a prioritised list of the most important items is created.

Scenario analysis: The second day of the workshop is devoted to two scenario runs. All parties involved in designing the scenario and take a passive role. It is important that the involved people are not familiar with the specifics of the chosen scenario. In order to make a general process validation, the sequence is closed with a final debrief.

4.2 *Scenario selection*

The N-USOC participants in the validation are responsible for a biological payload (EMCS) onboard ISS. For the validation we chose a similar payload in ESA's Columbus laboratory. The German control centres MUSC is responsible for the Biolab payload (see Fig. 1). Both EMCS and Biolab allow biological and bio-medical experiments investigating the effects of e.g. weightlessness on plants.

We wanted to choose a scenario that was not known in advance to the participants, but where we had identified some anomalies and root causes. We chose the Waico experiment using Biolab.

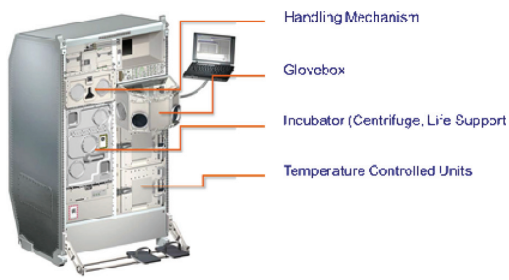


Figure 1. Caption of a typical figure.

Here the effect of gravity on the coiling of the roots was observed. Important information about the experiment set-up:

– Biolab contains two rotors inside its incubator that can simulate different levels of gravity. The Waico experiment required 4 different gravity levels and therefore required 2 separate runs. Each run contains 8 experiment containers on the rotors
– Video is taken every day to follow the growth
– Runs take 10–14 days

There were not enough resources to download all experiment containers to ground in cold stowage. Therefore crew was required to take high definition images to select prime samples.

The anomaly report for this scenario occurred during a rerun of the second Waico run. A rerun was required, because the Biolab handling mechanism failed to supply an Experiment Container (EC) with enough fixative at the end of Waico #1. The anomaly describes a failure from the crew to take pictures of a desirable quality, making it impossible for the scientist on ground to select the prime samples. Investigation following the anomaly showed a lack of crew training with this camera as the prime cause.

Using this scenario has several advantages for the initial validation. Firstly Biolab is very similar to the EMCS payload NUSOC is familiar with from their operations. Therefore, only a high level introduction to the payload and experiment is required to achieve the desired level of knowledge in the participants. Participants can explore the scenario from their own experience, requiring only a minimal amount of role-play. This ensures that the result will be more realistic.

Secondly, the anomaly is easier to include in a scenario. For the scenario we can take one run from start to finish with all the main activities as they were performed. All participants will be already familiar with the details of these activities and the actors involved, even though they have no intimate knowledge of Biolab and the failure.

4.3 *Validation criteria 1: Identification of weak points (relevant items form the checklist)*

An early phase of the CRIOP process is to pick relevant items from the total checklist. In our validation, the checklist items from CRIOP included potential incidents. These items were similar to the root causes identified in the survey.

The walk through of the 34 selected checklist items, in addition to prioritising the items, resulted in the following six most significant issues:

1. Alarm systems
2. No clear responsibility
3. High/Low mental workload

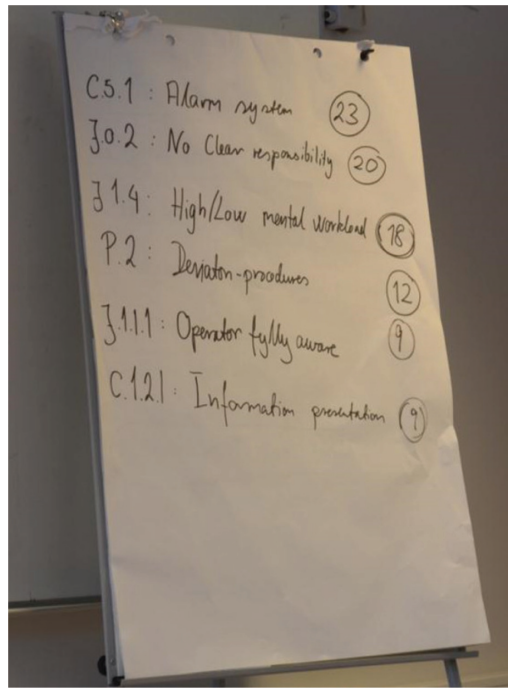


Figure 2. A selection of the flipcharts describing the key issues and their assigned priorities.

4. Deviation from procedures
5. Awareness of responsibilities
6. Information in graphs and telemetry

The list of the most significant issues is very similar to the survey results in task 1. The list of key root related to anomaly causes identified was:

A. Parallel tasks
B. Simple, repetitious tasks
C. Lack of domain knowledge on other systems
D. Long hours
E. Teleconferences on console
F. Lack of team support
G. Procedures

The only item not covered in the survey was the alarms (prioritized issue 1). Thus, the checklist method can be seen as validated. It helps to bring up similar issues that were brought up in an anonymous survey, together with some issues that are unique to the specific control centre.

4.4 *Validation criteria 2: Identification of critical steps in the experiment*

In order to validate the scenario method, the participants should at least identify the training of taking the pictures as a critical item,

since it has a strong impact on the entire Waico experiment.

As a secondary requirement, the participants were expected to indicate issues that were already indicated in the survey.

By going through the steps and actors involved in the scenario, the flow in Figure 3 was created. This was used to identify critical steps in this scenario. The specifications of critical actions should be describes as precise and objective as possible.

For each critical issue the group identified barriers for mitigation of risks. Only issues related to human dependability were considered. Figure 4 show the identified issues. It is worth commenting that the possible issues at step 5 are in accordance with anomalies reported in the Waico experiment.



Figure 3. Complete flow of the Waico scenario.

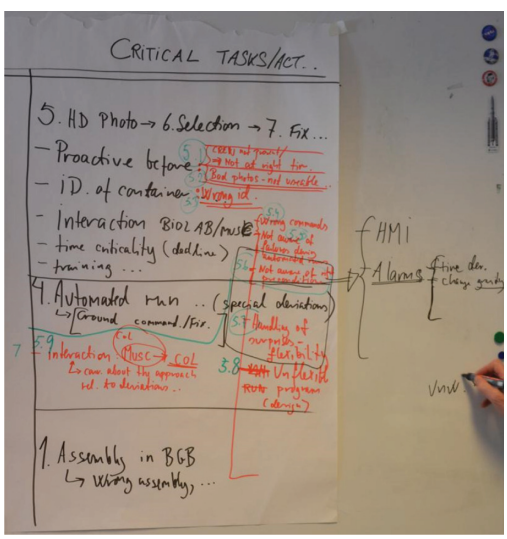


Figure 4. Critical issues identified and analysed.

In this scenario workshop, training was one barrier that should be empathized to cope with this critical step.

It can therefore be assumed that the run of this scenario would have resulted in the same conclusion as the analysis of the anomaly afterwards. This is a strong case for the validity of this method.

Interestingly, the time criticality of the fixation and the stowage afterwards was also identified as a critical issue to be checked. This time criticality is what eventually leads to the requirement of a second Waico experiment, since there was not enough time to recover from the fixation error that occurred in Waico #1.

The results from this study indicate that the method would have possibly mitigated the occurrence of both anomalies. Therefore from this perspective the method is regarded as validated.

5 CONCLUSION

5.1 *Human dependability study*

This paper describes an implementation of the SPACE-CRIOP method from start to finish. The application of the method is originally developed and applied in the petroleum sector. Deviations from the standard are clearly stated. Thus, results from the initial validation can be used as a guide to the practicalities of implementing and facilitating the method.

The project gives a good understanding of how the method may work in space control room settings.

5.2 *Recommendations—theoretical and methodical approach*

In addition to describe common pitfalls, suggestions are gives on how to improve results and implements lessons learned.

Recommendations are given to ensure the applicability of the method for space application. We have suggested that an improvement of human dependability should be based on the following prerequisites:

- Improved understanding of human errors and human recoveries
- Model errors and recoveries through scenario analysis and practice as described in the CRIOP method
- Selection of a HRA method based on a rigorous set of selection criteria—suggesting SPAR-H as a simple and usable method

– Explore the suggested methods in design and operation to support human dependability as a result of improved design and operations, based on best practices in human factors in organisation, technology and humans.

5.3 *Recommendations—process performance*

The preparation is done via telecom in this case, but should be performed in a face-to-face meeting in a normal SPACE-CRIOP process.

The selection of checklist items was very useful, but quite a long process. A longer meeting would help to relieve some of the time pressure.

In addition, it was agreed that a teleconference is not sufficient for a preparation meeting. A meeting face to face would facilitate a less formal feeling, would improve the ability to collaborate on drawings and other inputs, remove problems with sound quality and similar and have an overall positive effect on the quality of the discussions.

However, the item list selected was in the right range of size, the scenarios where selected, the schedule finalized and all questions clarified, so the meeting met its objectives.

Finally, it was clear that a facilitator needs to be familiar with the method, or receive some sort of training, to be able to chair this meeting. Specific domain knowledge of the control center is however not required.

FURTHER WORK

The suggested methods should be used and evaluated, in order to ensure that human dependability is increasing. Further, the methods should be used as early as possible—in design, through engineering; building and operation.

The results from the analysis performed by CRIOP, OCCO and SPAR-H may influence human dependability. We suggest that further work in the space domain perform several pilot projects exploring CRIOP, OCCO and SPAR-H.

REFERENCES

Aas, A.L., Johnsen, S.O. & Skramstad, T. 2009. CRIOP: A Human Factors Verification and Validation methodology that works in an industrial setting. Lecture Notes in *Computer Science*. Volume 5775.

Dekker, S.W.A. 2002. Reconstructing human contributions to accidents: the new view on error and performance. *Journal of Safety Research 33* (3): 371–385.

Fossum, K., Berg, C.H., Kongsvik, T., Almklov, P. & Johnsen, S.O. 2014. Monitoring human and organizational factors in spaceflight operations. *Safety, Reliability and Risk Analysis: Beyond the Horizon*, (Eds) Steenbergen et al. Taylor & Francis Group, London, pp 277–283.

Gertman, D., H.S. Blackman, J. Marble, J. Byers, L.N. Haney, and C. Smith. 2005. The SPAR-H Human Reliability Analysis Method, NUREH/CR-6883, Washington DC: U.S. Nuclear Regulatory Commission.

Johnsen, S.O., Stene, T.M. & Kongsvik T.Ø. 2014. Human dependability in space control operations—a HOT perspective. *Safety, Reliability and Risk Analysis: Beyond the Horizon*, (Eds) Steenbergen et al. Taylor & Francis Group, London, pp 67–74.

Johnsen, S.O. & Stene, T.M. 2014. Improving human resilience in space and distributed environments by CRIOP. *Safety, Reliability and Risk Analysis: Beyond the Horizon*, (Eds) Steenbergen et al. Taylor & Francis Group, London, pp 293–302.

Reason, J. (1997). *Managing the risks of Organizational Accidents*. Ashgate.

Shappell, S.A. & Wiegmann, D.A. 2000. *The Human Factor Analysis and Classification System—HFACS.* DOT/FAAM/AM-00/7. Office of Aviation Medicine, U.S. Department of Transportation Federal Aviation Administration. Washington, DC 200591.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Towards safer air traffic: Optimizing ATC controller workload by simulation with reduced set of parameters

B. Számel & G. Szabó
Department of Control for Transportation and Vehicles, Budapest University of Technology and Economics, Hungary

ABSTRACT: The workload of air traffic controllers plays a crucial role in the safety and efficiency of air traffic as it is the prime factor to determine airspace capacity. Workload is the result of traffic complexity which can be described by different sets of parameters. In order to find a small, yet reliable set of complexity parameters that describe controller workload in the Hungarian Air Traffic Control system, a study with multiple steps was conducted and the results are presented in this paper. Information on the most important complexity factors was aquired from experts through interviews and questionnaires and as a result, different sets of parameters were created. To validate the method for gathering information as well as the applicability of complexity factors for airspace capacity estimation, a neural network based model was used. The results indicate that even smaller sets of parameters can be helpful in estimating workload.

1 INTRODUCTION

The safety of air traffic can be defined as the optimal operability (and the probability of maintaining it) of airspace and aerodrome movements under given circumstances. This level of operability is the result of the complex actions of human and technological factors concerned with air transportation. Owing to its complexity, air traffic safety has many different aspects, which led to different approaches in the research area of analyzing and improving it. These approaches may involve the following:

- Mathematical modeling and/or simulation of the movement of aircraft and air traffic flows (e.g. Skorupski (2010) presents a quantitative description for air traffic safety based on the incidence rate of disturbed flights)
- Modeling or simulating automation systems and the behavior of human operators in aircraft or in ATC (Air Traffic Control) (e.g. Inoue et al. (2010) present a model of knowledge in ATC operations, Yemelyanov (2009) introduces a complex method for modeling operator performance and analyzing error)
- Analysis of the effect of design, implementation and maintenance on the reliability of technical system elements
- Analysis of the effect of regulations, training and work environment on the performance of humans in the system (e.g. Martinie et al. (2010) propose an integrated model of the ATC system and operator training)

In our present study, we introduced a functional relationship diagram showing technical and human subsystems affecting air traffic safety at ATC side, then we focused on the human operators in the system of ATC and their impact on the safety (and efficiency) of air traffic. We examined the factors that influence the workload of air traffic controllers working in the Flight Information Region (FIR) of Budapest (BUD) and analyzed how different sets of such factors can be used to predict the optimal number of controllers needed to handle a certain traffic situation.

In Section 2, we provide a brief description of the structure of a general ATC system and the safety analysis techniques related to the system elements focusing on human components. In Section 3, a method is presented for the determination of the set of air traffic complexity parameters to be used for sector capacity estimation. In Section 4 we summarize the results of a neural network based sector capacity estimation model with different sets of complexity factors as input parameters and in Section 5, we give final conclusions.

2 HUMAN FACTORS IN THE SYSTEM OF ATC

When talking about the different parties involved in air transportation, a key area related to the safety of the entire system is Air Traffic Control (or Air Traffic Management in a broader scope). The system of Air Traffic Management consists

of various technological and human components. We created a model to show the components and their relationship. The model can serve as a basis for investigation of a given component malfunction. Figure 1 shows this model with some simplification and thus presents a brief overview of the most important and most common components involved in the Air Traffic Control department of a general ATM system. The safety of ATC is affected by the reliability of both the technological elements and the humans operating the system.

Examining the contribution of technology to the safety of the entire system is usually done by applying safety-, reliability- and risk analysis techniques developed in past decades. Technical system components can be broken down into subcomponents, the structure of which can be unambiguously defined (i.e. what kind of input data they receive, what functions they use to process data and what kind of output data they provide). For example, a primary radar data processing unit may get the time of transmission and time of reception (obtained using a digital timer) of an analogue electromagnetic pulse along with the sign of a digital counter that is reset after each turn period of the antenna and provide digital signs correspondent to the difference of the two times (thus the distance of the aircraft) and the counter's value (thus the azimuth angle). This makes the applicability of traditional safety and risk analysis methods such as failure mode and effects analysis possible, taking into account different function degradations and malfunctions.

When it comes to the estimation of human reliability, the available methods are not as straightforward as those applied for technological systems. Problems are brought on by the fact that human behavior is influenced by lots of different factors that are hard to describe using formal methods (mainly factors that belong to the area of psychology, medicine or social science). This makes the performance of human operators barely predictable and therefore traditional safety analysis methods inapplicable.

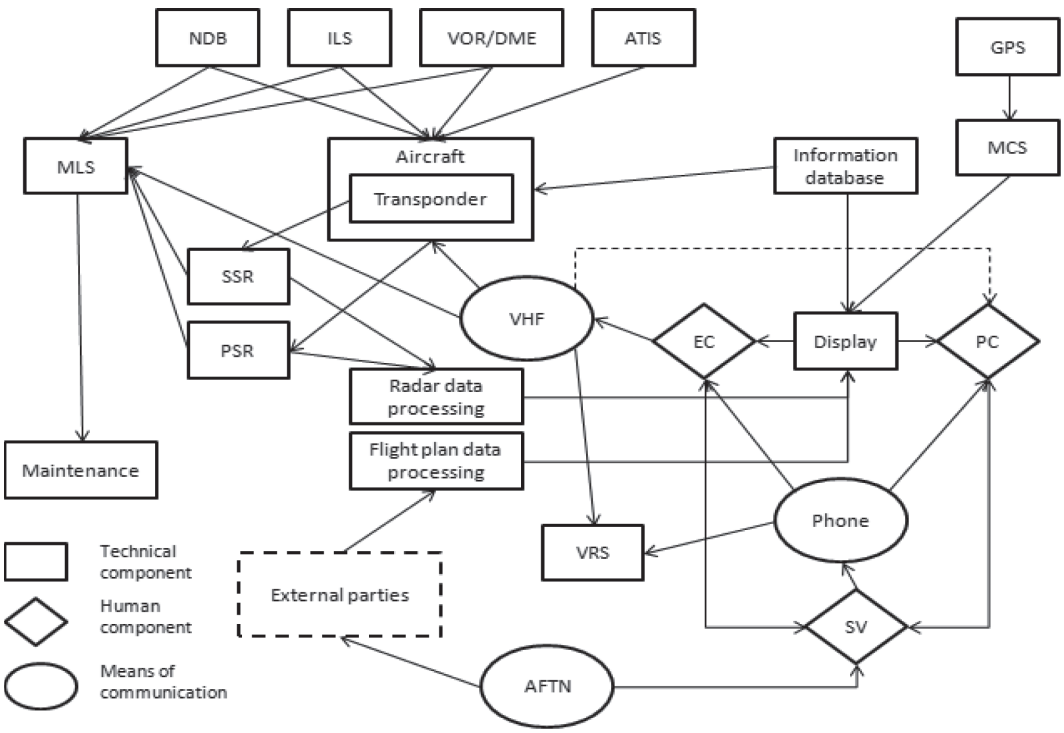


Figure 1. Structure of the ATC system (abbreviations: EC: Executing Controller, PC: Planning Controller, SV: Supervisor, VHF: Very High Frequency (radio), AFTN: Aeronautical Fixed Telecommunication Network, PSR: Primary Surveillance Radar, SSR: Secondary Surveillance Radar, ILS: Instrument Landing System, VOR/DME: VHF Omni-directional Radio Range and Distance Measuring Equipment, NDB: Non-directional Beacon, ATIS: Automatic Terminal Information System, MLS: Microwave Link System, VRS: Voice Recording System, MCS: Master Clock System, GPS: Global Positioning System).

The above statement however does not mean that there are no similarities between the analysis of the impact on safety for humans and for technology. The work of a human operator can also be broken down into a functional group of macroscopic actions (i.e. externally observable actions, not cognitive ones that are executed "inside" the operator) like gathering certain information, processing it and executing actions. For example, in the case of an air traffic controller in a common work situation, there is a traffic monitoring activity which means gathering visual information from the display and audio information from communication with pilots. Based on this, the controller executes actions by issuing orders to aircraft. This enables some kind of analysis for human reliability (e.g. when analyzing operator error, the erroneous macroscopic activity can be determined), but the retrievable information is insufficient as the most important causes of human behavior (and human error) dwell within the microscopic cognitive processes.

Modeling the microscopic information processing activities for humans is much harder than it is for technological elements but there are several methods developed for the task. The most well known models of cognitive human behavior include the information processing model in Wickens (1992), the Step Ladder Model presented in Rasmussen (1986), the Generic Error Modelling System in Reason (1987), the Contextual Control Model and Simple model of Cognition in Hollnagel (1993) and the model of situational awareness in Endsley (1999).

When modeling or analyzing operator error or performance in order to aid the improvement of system safety, it is usually not enough to uncover the area of human cognition which is responsible for the erroneous behavior (e.g. by using one of the above mentioned models). In most cases, the root cause of human error (or a certain type of human behavior) does not lie solely in the problems of the operator's information processing, as human behavior is always influenced by environmental effects which are usually called Performance Shaping Factors (PSFs) in literature. PSFs may include the operator's inner conditions (e.g. hunger or fatigue), hardware environment (quality and condition of equipment used), organizational issues (e.g. regulations, work atmosphere), social environment (e.g. operator's interpersonal relations) etc. An example for the classification of PSFs (for nuclear power plant operators) is given in Blackman et al. (2008).

When it comes to the analysis of the performance of operators in safety critical systems, perhaps the most emphasized of PSFs is workload (as seen in e.g. the operator performance model of Strenzke & Schulte (2011)). In the case of air traffic controllers, workload can be defined (according to Flynn et al. (2005)) as the amount of time in a certain time interval that the controller spends on activities directly related to controlling air traffic (i.e. gathering information, interpreting situations, developing and executing plans). Using this definition, workload can be measured in absolute time (mostly in minutes) or relative time. The latter is a percentage value representing how big a part of work time is spent on the above activities (e.g. 30 minutes in an hour equals to a 50% workload level).

While operator workload is an important factor in every safety related area, in the case of ATC it is even more essential. In the present state of air transportation systems worldwide, the capacities of airspaces are determined by the capacity of the local ATC center. The capacity of ATC centers is in turn based on the level of traffic that controllers can handle, which is heavily influenced by the controller workload generated by the given traffic level. The rule of thumb dictates that the larger the traffic, the higher the workload and although some doubt it (Stager & Hameluck (1990)), higher workload leads to more frequent and more severe controller errors. This means that if the workload generating characteristics of certain air traffic situations could be calculated, then it could be decided whether the given situations can be handled by ATC with controller workload not reaching an undesired level or not. In other words, this would enable determining how many air traffic controllers (airspace sectors) would be optimal to handle the given traffic in a safe and efficient way.

It is also worth noting, that not only high levels of workload can lead to more controller errors but very low workload situations as well. The presence of different PSFs is one explanation for this. It is assumed, that if an air traffic controller works under medium or high workload, then he or she will not pay attention to other internal or external effects that could otherwise hinder work efficiency. When workload drops however, these other factors may become predominant and cause error. Further problems can occur at low workload situations, if it is not obligatory for air traffic controllers to guide flights using only the standard routes in the airspace. If regulations allow and there are not many aircraft present in their sector, controllers will often direct flights to waypoints on non-standard routes. Doing so however means that the flight requires constant attention from the controller until it reaches a standard route again. This, of course leads to increase in workload in situations that would normally induce only a moderate workload level.

Earlier in this Section, we mentioned that larger traffic leads to higher workload. It is important

to state, that large traffic does not simply mean a large amount of aircraft in this context. It means instead, that the traffic is hard to handle for controllers due to the number of aircraft as well as the complexity of both traffic and the airspace.

3 METHOD FOR SELECTING COMPLEXITY PARAMETERS

3.1 *Querying experts' opinions*

There is an enormous number of possible parameters to describe the complexity of air traffic and airspace sectors. This makes it necessary to narrow the set of parameters to a level at which they still provide a good description about the controller workload caused by the given traffic situations but do not lead to unnecessarily complicated and time consuming calculations in mathematical models and simulation.

The first step in determining the optimal set of complexity parameters is figuring out which are the characteristics of air traffic that active air traffic controllers find the most burdensome. In order to realize this, we first made an interview with an expert in the topic of organizing air traffic control as well as the characteristics of the airspace and air traffic in Hungary. The interview was unrestricted, so first we avoided using guidewords and yes or no questions and simply asked, what are the factors of air traffic and airspace that have the biggest impact on controller workload and therefore decisions about the sector configuration to use.

The interview served a double purpose. The first and more obvious one was helping us filter the set of all possible complexity factors we gathered from past studies (e.g. Gianazza & Guittet (2006), Kopardekar & Magyarits (2002) or Christien & Benkouar (2003)), thus generating a smaller set that was not hard to use for the remainder of the survey. The second purpose was to get some guidance for describing complexity factors with words as well as mathematical formulae. For example, the fact that the interviewed expert mentioned descending aircraft among the first workload generating factors and talked about climbing aircraft much later indicates that the number of descending and climbing aircraft should be used as two different complexity factors instead of using only the number of aircraft changing altitude.

In the second step, we broadened the scope of the experts whose opinions were taken into consideration while narrowing the list of parameters using the information gathered in the first step. After the interview, the following parameters of the airspace and air traffic seemed to be the major factors to influence controller workload.

- Number of climbing aircraft
- Number of descending aircraft
- Direction of aircraft movement relative to one another
- Variability of aircraft velocity
- Relative number of arriving, departing and cruising aircraft
- Number of aircraft pairs flying on crossing routes
- Smoothness of the distribution of aircraft in the airspace (flatness of traffic density)
- Number of pilot requests
- Number of intersection points of standard routes
- Number of available flight levels
- Number of special (e.g. military) airspaces used in the given sector or its neighboring sectors
- Weather
- Congestion of frequency
- State of technological system components

Based on this list, a questionnaire was created and given to several air traffic controllers and supervisors. The average experience of controllers to provide answers was 24.3 years and the average experience of supervisors was 5.6 years.

The substantive part of the questionnaire contained the possible air traffic complexity factors listed above and the respondents were required to rate them subjectively (relying on their own experience) based on two aspects. The first aspect was the extra workload generated by the unfavorable state of the given parameter. The respondents were asked to mark each parameter with a number from 1 to 5 based on their thoughts about the workload generated (with 1standing for no or very low workload and 5 for very high workload).

The second aspect was the variability in the values of the given factor. The respondents were once again asked to give marks from 1 to 5 depending on the variability of the parameters. A mark of 1 meant that the parameter's value could be considered constant; 2 meant that the value is not constant but changes significantly only 1–5 times a day; 3 meant that the value changes every 1–2 hours; 4 meant that the value can change multiple times in an hour; 5 meant that the value changes randomly and its change is hard to predict.

This information was necessary in order to determine whether it is important to take the given factor into consideration for the rest of the research process. If a complexity factor has a high impact on workload but its value does not change frequently or greatly, then it should not be used in sector capacity estimation models. One reason behind this is the fact that air traffic controllers will probably adapt to the presence of the given factor which would result in lesser influence on workload.

We also assumed that controllers can even adapt to frequent changes in complexity factor values at a certain level, if the changes are predictable. This is why we asked the respondents to give 5 (the mark representing the worst case) to parameters the changes of which are not regular. The respondents were informed about the aim of the questionnaire and received detailed instructions about providing the answers properly. Although we could not establish personal contact with all the air traffic controllers and supervisors that filled the questionnaire, the feedbacks indicated that the questions, the instructions and the additional information were clear and professional.

3.2 *Results of the questionnaire*

The results obtained from the questionnaire are presented in Table 1. The table shows the mean value and standard deviation of the marks given to the different workload affecting parameters. The parameters are the same as those listed above but this time we used shorter names for the sake of simplicity.

It is worth noting that some of the complexity parameters used had a similar meaning to others and in some cases, a logical relationship can be found between two parameters. For example, arriving and departing aircraft increase complexity because they are usually descending and climbing aircraft respectively and the frequency in the given sector gets overloaded when there are bad weather conditions or failure in technology. These parameters were left in the list for two reasons. Reason number one was that we did not want to combine complexity factors that were stated as different during the interview, regardless if they differed only slightly. Reason number two was the will to create an opportunity to check the coherence of answers given in the questionnaire.

3.3 *Creating final set of parameters*

The results of the questionnaire showed us that the parameters with similar or relational meaning received similar ratings, so the respondents had probably given thought-out answers instead of random marks.

The results summarized in Table 1 indicate that the most important complexity factor according to air traffic controllers is unsurprisingly weather with a mean value well above 4 in both categories. Other major factors based on the mean value of extra workload rating are the numbers of climbing and descending aircraft, the relative number of arriving, departing and cruising aircraft, the aircraft pairs on crossing routes (i.e. pairs with a possibility of conflict), the smoothness of the distribution of aircraft, the number of route intersections, the available flight levels, the number of active special airspaces, the congestion of frequency and the state of technological system components. Density, intersections, flight levels and state of technology however received a mean value below 3 for variability so these can be considered factors that are easier to adapt to than others, therefore they are less significant. The complexity factors that do not seem to have much relevance

Table 1. Ratings of complexity factors based on subjective opinions.

	Extra workload		Variability	
Parameter	Mean	Deviation	Mean	Deviation
Climbing aircraft	3.71	0.53	3	0.88
Descending aircraft	3.57	0.58	3.14	1.15
Relative heading	2.29	1.03	2.43	1.63
Speed variability	2.57	1.05	3	1.25
Arriving/departing/ cruising aircraft	3.86	0.97	3.57	1.23
Aircraft pairs on crossing routes	3.57	0.85	3.43	1.37
Flatness of density	3.71	0.53	2	1.25
Pilot requests	2.86	0.75	3.43	0.85
Route intersections	3.43	0.58	2.43	1.51
Available FLs	3.29	0.82	2.43	1.51
Special airspaces	3.57	0.85	3.29	1.5
Weather	4.57	0.58	4.29	1.03
Frequency congestion	3.71	0.82	3.57	1.22
State of technology	3.14	1.31	2.71	1.84

to controller workload in Hungarian airspace are the variance of aircraft speed and heading and the number of pilot requests.

The standard deviation for the extra workload generated by the different factors is small (does not exceed 1 in most cases), so most answers were close to one another indicating that controllers have a uniform opinion about the complexity factors' effect on workload. In the case of variability, the deviation values are much greater in general (this time they are above 1 for almost every parameter). This indicates that the answers were not as unified as they were to the question about extra workload. The reason behind this may either be that controllers' opinions differed more on this question or more probably, the meaning of variability was not clear (regardless of the information provided to the questionnaire) and/or it was not easy to estimate the variability of different complexity factors.

The primary goal of the information acquiring process about complexity factors was to use them as parameters for mathematical modeling of the relationship between air traffic characteristics and controller workload. The aim of such a model in turn was serving as a basis for a decision support tool that would help supervisors in making decisions about the optimal sector configuration for various traffic situations.

With the above aims in sight, it was necessary to consider other aspects beside the opinion of ATC experts when trying to determine which would be the optimal set of parameters to be used in the model. One of these aspects was the issue of predictability. An automated decision support system could not be operable without receiving reliable information about the anticipatory values of complexity factors in the near future. In the case of our research, this meant that only parameters with confidently predictable values could be taken into consideration. This resulted in the exclusion of the number of pilot requests and the state of equipment from the parameters (which is hard to predict even though the ATC system is equipped with diagnostics tools) as well as the most important workload affecting factor: weather.

The latter decision may seem neglect, but it is important to note, that weather is hard to predict even on short terms and hard to describe by mathematical formalization that would be essential for usage in automated decision support (although there may be methods to do so, like modeling thunderstorm areas as restricted airspaces and treating them similarly). We can also assume that supervisors would not rely on decision support systems when weather conditions in the airspace are harsh.

The other complexity factors were more or less included in our first set of parameters to be used for modeling. The term "more or less" refers to the fact that some of the parameters were used with a meaning slightly different from what can be presumed from the name that was used in the earlier list while others were included implicitly as parts of other complexity factors. For better understanding, the actual complexity parameters that were included in our largest parameter set are listed below with a short explanation, where needed:

- Number of aircraft
- Number of climbing aircraft
- Number of descending aircraft
- Percentage of climbing aircraft among all aircraft
- Percentage of descending aircraft among all aircraft
- Standard deviation of aircraft velocity (to represent variability in aircraft speed)
- Flatness of traffic density (indicates whether the aircraft are distributed equally in the given sector or they are concentrated in small, high density areas)
- Divergence of traffic (to represent relative heading and speed of aircraft)
- Convergence of traffic (to represent relative heading and speed of aircraft)
- Insensibility of traffic divergence (the insensibility of divergence to changes in aircraft speed and heading)
- Insensibility of traffic convergence (the insensibility of convergence to changes in aircraft speed and heading)
- Number of aircraft pairs on crossing routes with the possibility of conflict
- Number of intersections of standard routes
- Sector volume (geographical area of a sector multiplied by the standard flight levels in the sector)
- Number of available flight levels
- Number of temporary restricted airspaces (TRAs) (in the given sector as well as its neighboring sectors)
- Number of climbing aircraft in Budapest Terminal Maneuvering Area (TMA) (to represent if the given traffic situation has a "departing" nature)

Traffic density, divergence, convergence and the insensibility of divergence and convergence were calculated using the formulae presented in Delahaye & Puechmorel (2000). Relative heading of aircraft were included implicitly in convergence and divergence. The proportion of departing, arriving and cruising aircraft is represented by climbing and descending aircraft as well as by climbing aircraft in the TMA. When calculating the number of aircraft pairs on crossing routes, only those were considered, where both aircraft would reach the

intersection point in no more than 720 seconds with a time difference less than 90 seconds (based on the current speed and heading).

4 MODEL CREATION AND RESULTS WITH DIFFERENT SETS OF COMPLEXITY PARAMETERS

4.1 *Data and structure of the neural networks*

In order to examine the applicability of the complexity factors introduced in Section 3, we decided to use a neural network based approach similar to the one seen in Gianazza & Guittet (2006). To provide input data to our networks, air traffic data of the Hungarian airspace was obtained for two days in the past (29th July 2011 and 30th July 2012) and a few more hours from 25th October 2012 when military TRAs were in use. We took snapshots of the radar data every 30 minutes for the two full days and every 10 minutes for the time when TRAs were open. After taking these samples, we had radar data for 107 different air traffic situations which included a wide variety of traffic levels.

Based on the radar data and data regarding sector structure of the airspace, values of the complexity factors listed in Section 3 were calculated for the different traffic situations. Calculations were made for the entire airspace, for elementary sectors (sectors that cannot be split) and for sector blocks that are currently used in Hungarian ATC.

The input values of the neural network were obtained by applying principal component analysis on the set of complexity parameter values. We had 17 principal components in the case of elementary sectors and sector blocks, and 15 principal components in the case of the entire airspace (sector volume and intersections of standard routes were constant, therefore the principal component analysis was performed on a set of only 15 parameters).

The output values of the networks were numbers indicating the optimal state of the given sector in the given traffic situation. Still sticking to the path laid by Gianazza & Guittet (2006), sectors had two or three possible states. The airspace could be split or armed, elementary sectors could be armed or merged and sector blocks could be split, armed or merged. Each possible state was represented by a node in the output layer of the neural network that could take on a real value between 0 and 1. In an ideal case, the node of the optimal state would have a value of 1 and the other or others 0. In practice however, error can never be completely eliminated during the training of a neural network and in some cases it is hard to tell even for experienced human supervisors what the optimal state of a sector would be. These problems usually lead to values between 0 and 1 on two or more output nodes. In such a case, the node with the greatest value is considered the node of the optimal state.

For the training of our neural networks we needed information about the optimal state of sectors in reality, which required supervisory know-how. Once again active supervisors with high experience were asked to state their opinions about different traffic situations and tell what the best sector configuration would be for the safest and most efficient control. To achieve this, they were shown radar pictures of the historical air traffic data of the traffic situations in scope. Although the situations were shown in chronological order, they were asked to look upon them "out of context" and tell what the optimal configuration would be if the given situation lasted for a long time and not only a couple of minutes as it was the case in some situations.

Neural networks were trained by using about 80% of the available data, while the remaining 20% was used as query data. For the training we used off the shelf software which prevented us from fully recognizing or modifying training logic, but network size and training parameters were still settable. The networks had twice as many hidden layer nodes as input nodes and the training of a network was considered complete once at least 95% of the output nodes' values was within 5% range of the expected value. Time limit for training was also used to avoid too long training periods. Validation of the networks was done using both query data and the same data that had been used for training.

4.2 *Results of the neural networks*

In order to examine how the results of a neural network analysis depend on the set of parameters used as input, we performed our analysis for three different sets of parameters. The first and largest one (named Set A) contained every complexity parameter described in Section 3. The second set (Set B) was created by removing the least significant parameter (according to the subjective opinion of experts), which was relative heading. Since relative heading was present in Set A as a latent parameter included in divergence and convergence, these parameters were the ones to be excluded (along with their corresponding insensibility values). Set B therefore had 13 parameters (11 in the case of the entire airspace). The third set (Set C) was obtained by the exclusion of the second least important parameter: the standard deviation of aircraft velocity. We also removed the percentage of climbing and descending aircraft as these parameters seemed to be redundant. This resulted in 10 parameters for Set C.

For the analysis of the applicability of neural network modeling for sector capacity estimation in Hungarian airspace, we examined the reliability of the results by comparing the results calculated by the network with those provided by supervisors. Results of a certain network for a certain set of parameters in a certain sector type (i.e. airspace, elementary sector or sector block) can be characterized by the percentage of results that were correct (equal to those obtained from supervisors).

The neural network calculations using Set A provided the results summarized in Table 2. Calculations were done with different amounts of principal components, but Table 2 lists only the results obtained using the maximum amount. The "Validation data" column shows what type of data was used for validation of the network with Q standing for query data and T standing for training data.

As it is seen in Table 2, the results for sector blocks are far from satisfactory. This is a problem that may have several causes (e.g. the geometrical diversity of different sector blocks or the quality of the neural network planning software used) which are out of the scope of this paper and are to be dealt with in another research project. To eliminate the problem temporarily, a smaller set of sector blocks was considered, which involved only the West (W) and East (E) sector blocks, each built up of five elementary sectors. For the neural networks of Set B and Set C these were the only sector blocks used by default.

Tables 3 and 4 show the neural network results for Set B and Set C respectively.

Tables 2–4 show us that although there is a slight decrease in the accuracy of neural network results when the number of input parameters (complexity factors) is reduced, the results can still be considered satisfactory as they rarely drop below 80%. The seemingly strange increase in accuracy in the case of sector blocks in Table 3 can be explained by the parameters we used for training our networks. In both cases, training was stopped after the fixed time limit but since Set C had a simpler network (due to the lower number of input parameters) its training was probably in a more advanced state already than it was for Set B.

Table 2. Results of neural network calculations for Set A.

Sector type	Validation data	All (%)	Split (%)	Armed (%)	Merged (%)
Airspace	Q	100	100	100	–
Airspace	T	100	100	100	–
Elementary	Q	96.5	–	56.3	99.5
Elementary	T	97.8	–	81.8	99
Block	Q	57.2	69.9	4.6	59.7
Block	T	72.2	88.5	8.1	77.7
Block W&E	Q	95.2	100	91.7	83.3
Block W&E	T	97.7	100	92.1	100

Table 3. Results of neural network calculations for Set B.

Sector type	Validation data	All (%)	Split (%)	Armed (%)	Merged (%)
Airspace	Q	100	100	100	–
Airspace	T	95.5	95	100	–
Elementary	Q	82.1	–	82.4	82.1
Elementary	T	88.1	–	86.7	88.2
Block W&E	Q	73.8	82.6	63.6	62.5
Block W&E	T	96.9	98.7	97.5	86.7

Table 4. Results of neural network calculations for Set C.

Sector type	Validation data	All (%)	Split (%)	Armed (%)	Merged (%)
Airspace	Q	100	100	100	–
Airspace	T	100	100	100	–
Elementary	Q	93.5	–	75	95
Elementary	T	93.8	–	73.9	95.3
Block W&E	Q	82.9	85.2	81.2	66.7
Block W&E	T	93.8	97.2	94.6	78.9

5 CONCLUSIONS

In an attempt to enhance the safety of air traffic control in Hungarian airspace, we conducted a study to examine the possibility of using a neural network model as a basis for a supervisory decision support tool that would be able to estimate the optimal number of ATC sectors for a given traffic situation based on its complexity. Data about the importance of different complexity parameters was gathered using a simple method that focused on finding out the subjective opinions of ATC experts. To validate our method, we used neural network calculations with different sets of complexity parameters.

The results obtained using reduced parameter sets indicated that the complexity factors that air traffic controllers did not find important are not important indeed, so the method used for gathering information on complexity factors was proven suitable. It was also proven that complexity factors that are calculated through complicated mathematical formulae (divergence, convergence and insensibility) are not indispensable for neural network

calculations with satisfactory results. This makes it inadvisable to use such parameters in a decision support tool as they would only lead to lower software performance with not much increase in reliability.

As the method of selecting complexity factors seems to be proven adequate, it is advisable to use it in similarly themed studies in the future. The reduced sets of complexity parameters seem to lead to a similar outcome as the full set when used in neural network calculations, therefore it is worth considering to use these instead.

ACKNOWLEDGMENT

The authors would like to return thanks to AMKMA (Foundation for the Hungarian Transportation Engineering Education) for supporting the project presented in this article and Hungaro-Control Hungarian Air Navigation Services Co. for providing radar data and contributing to the selection of complexity factors by consultation.

REFERENCES

Blackman, H.S., Gertman, D.I., Boring, R.L. 2008. Human Error Quantification Using Performance Shaping Factors in the SPAR-H Method. *Proceedings of the 52nd Annual Meeting of the Human Factors and Ergonomics Society*, New York, NY, USA.

Christien, R., Benkouar, A. 2003. Air Traffic Complexity Indicators & ATC Sectors Classification. *Proceedings of the fifth USA/Europe Air Traffic Management R & D Seminar,* Budapest, Hungary.

Delahaye, D., Puechmorel, S. 2000. Air traffic complexity: towards intrinsic metrics. *Proceedings of the third USA/Europe Air Traffic Management R & D Seminar,* Naples, Italy.

Endsley, M.R. 1999. Situation Awareness and Human Error: Designing to Support Human Performance. *Proceedings of the High Consequence Systems Surety Conference*. Albuquerque, NM, USA.

Flynn, G.M., Benkouar, A., Christien, R. 2005. Adaptation of Workload Model by Optimisation Algorithms and Sector Capacity Assessment. *EEC Note No. 07/05.*

Gianazza, D., Guittet, K. 2006. Evaluation of air traffic complexity metrics using neural networks and sector status. *Proceedings of the 2nd International Conference on Research in Air Transportation, ICRAT 2006,* Belgrade, Serbia and Montenegro.

Hollnagel, E. 1993. *Human Reliability Analysis: Context and Control*. Academic Press, London, UK.

Inoue, S., Aoyama, H., Nakata, K., Furuta, K. 2010. Managing ATC expertise based on distributed cognition analysis. In: *Reliability, Risk and Safety* (Ale, Papazoglou & Zio. (Ed)), Taylor & Francis Group, London, UK: 1993–1999.

Kopardekar, P., Magyarits, S. 2002. Dynamic density: measuring and predicting sector complexity [ATC]. *Proceedings of the 21st Digital Avionics Systems Conference*, Irvine, CA, USA.

Martinie, C., Palanque, P., Navarre, D., Winckler, M. 2010. A formal approach supporting effective and efficient training program for improving operators' reliability. In: *Reliability, Risk and Safety* (Ale, Papazoglou & Zio. (Ed)), Taylor & Francis Group, London, UK: 1828–1835.

Rasmussen, J. 1986. *Information Processing and Human-machine Interaction:* An Approach to Cognitive Engineering. Elsevier Science, New York, NY, USA.

Reason, J. 1987. Generic Error-modelling System: A cognitive framework for locating common human error forms. *New Technology and Human Error*. Wiley, Chichester, UK.

Skorupski, J. 2010. Air traffic smoothness as a measure of air traffic safety. In: *Reliability, Risk and Safety* (Ale, Papazoglou & Zio. (Ed)), Taylor & Francis Group, London, UK; 707–713.

Stager, P., Hameluck, D. 1990. Ergonomics in air traffic control. *Ergonomics* 33(4): 493–499.

Strenzke, R. & Schulte, A. 2011. Modeling the Human Operator's Cognitive Process to Enable Assistant System Decisions. *Proceedings of the 21st International Conference on Automated Planning and Scheduling*, Freiburg, Germany.

Wickens, C. (1992). *Engineering Psychology and Human Performance (Second Edition)*. Harper-Collins, New York, NY, USA.

Yemelyanov, A.M. 2009. Modeling and Decision Support for Analysis of Operator Errors in Complex Systems. *Journal of Computers* 4(4): 319–329.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Human reliability test and identification of HCR model basic parameters for multi-factor "Meta-Operation"

Yi Yang
China Astronaut Research and Training Center, Beijing, China
School of Reliability and Systems Engineering, Beihang University, Beijing, China

Xin Chen & Jianli Zhang
China Astronaut Research and Training Center, Beijing, China

Rui Kang
School of Reliability and Systems Engineering, Beihang University, Beijing, China

ABSTRACT: There are the very important problems about the lack and veracity of the basic data in Human Reliability Analysis (HRA). In order to resolve the problems, the task process operations in manned spaceflight are analyzed, and "Meta-Operation" is defined. The eleven kinds of "Meta-Operations" are given which cover both the rule type and skilled cognitive type, including six operations for one person, five operations for two persons, then classify the process of tasks related to the multi-factor. According to these eleven kinds of "Meta-Operation", the test environments and the groups of experimental persons are designed. Through five different groups of experimental persons, over ten thousand valid experimental data are obtained. The analysis of these experimental data reveals that there is no significant difference among the different groups at the "Meta-Operation" level. From the analysis, the eleven kinds of Human Cognition Reliability (HCR) model basic parameters are gotten.

1 INTRODUCTION

At all times, HRA is regarded widely in the fields of nuclear power human operations, fighter operations and astronaut operations. The foreign and domestic scholars have focused a growing amount of research efforts in this direction [He X.H., et al., 2007, Huang J., Huang X.R. and Shen Z.P., 1999, Li B.F., Song B.F. and Xue H.Q., 2005, Thomas A.B., 2012, etc]. Yang Yi, Liu Weibo & Kang Rui (2012) researched into the overview of human reliability which has produced basic models to solve certain problems and assess complex manipulation task reliability, especially for "Meta-Operation". The work has laid a solid foundation for further study in the field of Human Reliability Analysis. However, due to the particular nature of different manned missions, data tends to be unreliable and limited. Solutions to the problems of Human Reliability Analysis must satisfactorily solve the problems arising from limited and unreliable sample data. So Yang Y., Chen S.G., Zheng W.X. & Kang R. (2013) gave the "Meta-Operation" of the single-factor of one person, the test environment, the valid experimental data, and the parameter estimates of HCR (Weibull distribution). This paper further attempts to use the results of "Meta-Operating" analysis to identify the multi-factor of one person and multi-person for "Meta-Operation", and design appropriate test environment for reliability data accumulation, obtain the test data and the parameter estimates of the multi-factor HCR, thus developing the ability to evaluate complex task operation reliability.

2 MULTI-FACTOR "META-OPERATION" ANALYSIS

Using the results of Yang Yi, Liu Weibo & Kang Rui (2012), the single factor in feeling can be divided for visual expression, listening comprehension, smell and touch, classification can sort out two factors at the same time, such as visual and smell, visual and listening, visual and touch, and so on, classification can sort out three and four factors at the same time. A single factor, two factors, three factors and four factors constitute the basic classification judgment. The same way considers the classification of body movement, which can be divided into the upper limb movement, lower limb movement, upper and lower limb coordination

Table 1. Meta-Operation summary in the manned space mission operations.

Operation test content	Factors	Meta operational motion
Suit A worn operation	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Suit B worn operation	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Suit C worn operation	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
open/close doors operation	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Piping layout operations	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Two players together remove a seal operation	Vision-Hearing-Touch (three factors)	Upper limb movement
Two players together install a seal operation	Vision-Hearing-Touch (three factors)	Upper limb movement
Two players together a seal adjustment	Vision-Hearing-Touch (three factors)	Upper limb movement
Two players together measuring	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Two players remove/install beams together	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs
Two players together install floor block operation	Vision-Hearing-Touch (three factors)	Coordinated action of upper and lower limbs

actions, etc. The classification of the judgment is combined with the body movements' classification. All of the contents of the specific procedures for the flight event classification are given, the classification reflects the operation types, also is the base of main model.

2.1 *Building method of "Meta-Operation" set*

With the increase of task difficulty, the type of Meta-Operation also increased, from simple single-factor type into multi-factor of one player type, such as: the operation of filling in, switching operations, pick and place operations, connectors join operations, extravehicular suits worn operation, physiological clothing and protective clothing worn operation, cabin clothes worn operation, open/close doors operation and pipeline connection operation and so on.

For complex manned space mission, we need to consider more than two players in collaborative multi-factor "Meta-Operation" type. For example, in typical operation of replacing the door seals, "Meta-Operation" type include two players together remove seal ring operation, two players collaborative installation seal ring operation, two players at the same time to adjust the position operations and so on.

According to astronauts normal flight manuals and operating instructions in a certain manned space mission, action items astronauts were to be carried out are detailed analyzed and generalized from the beginning to the spacecraft to return astronauts landing, 11 kinds of Meta-Operation includes: clothing worn operation, open/close doors operation, piping connection operation and some collaborative operations, see Table 1.

3 MULTI-FACTOR "META-OPERATION" PERSONNEL RELIABILITY TEST

Yang Yi, Chen ShangGuang, Zheng WeiXing & Kang Rui (2013) detailed analysis of personnel operating activities during manned spaceflight missions, known as "Meta-Operations". Using "Meta-Operation" the basic categories, and combining related the main operating classification in the multi-factor test of one player and two players, we can determine the main type of operation and the main equipment. It can be seen that personnel operations involved in the upper and lower limb coordination actions. All types of multi-factor are shown in Table 2.

Aimed at the above operations, these main factors are considered in the test:

a. Suit A, B, C worn operation;
b. Open/close doors operation;
c. Piping layout operation;
d. Two players collaboratively a seal operation;
e. Two players collaboratively measuring operation;
f. Two players collaboratively remove/install beams;
g. Two players together install the block.

The testing environmental and implementation can straightway use the results of Yang Yi, Chen ShangGuang, Zheng WeiXing & Kang Rui (2013).

Table 2. Personnel operation factor.

Categories	Subclass of similar operation time	HCR type
The upper and lower limb coordination actions for one player	Suit A worn operation Suit B worn operation Suit C worn operation Opening/closing doors operation Pipeline connection operation	Regular skill
The upper and lower limb coordination actions for two players	Two players together remove a seal Two players collaborative installation a seal, Two players at the same time to adjust the seal positions Two players together measuring Two players remove/install beams together Two players together install the block operation	Regular skill

4 MULTI-FACTOR TEST PARAMETERS IDENTIFICATION

4.1 *HCR model*

In order to carry out the personnel operating reliability analysis in complex task, we have already arranged the experiments of "Meta-Operation", and obtained a large amount of data. If these data can be used for predicting the personnel operating reliability in complex task, we must determine the each reliability of "Meta-Operation". According to the reliability model in the HRA, we considered HCR model has the standard expression form and clear meaning. Especially it could reflect the comprehensive effect of cognitive rules. So we selected HCR model as the basic paradigm of "Meta-Operation" reliability model.

He X.H., et al. (2007) illuminated in the detail that Weibull distribution is the most broad model in the HRA. Then Assuming the time to complete a "Meta-Operation" meets Weibull distribution, then

$$R(t)=\begin{cases}\exp\left\{-\left(\dfrac{t-\gamma}{\eta}\right)^{\beta}\right\} & t\geq\gamma\\ 0 & t<\gamma\end{cases} \tag{1}$$

where $R(t)$ is the probability for completing a "Meta-Operation" at t. γ is location parameter, η is dimension parameter, β is shape parameter.

Furthermore, we can get that

$$\ln\left[\ln\frac{1}{R(t)}\right]=\beta\ln(t-\gamma)-\beta\ln\eta \tag{2}$$

In order to reduce the inherent time differences, the operation time to completion is normalized. Standardized time is defined as $t/T_{0.5}$, where t is the operation completion time for the operator to complete a certain operation time.

$$T_{0.5}=\gamma+\eta(\ln 2)^{1/\beta} \tag{3}$$

Using $T_{0.5}$ to normalize the processing operations time, we get:

$$R(t)=\begin{cases}\exp\left\{-\left(\dfrac{(t/T_{0.5})-C_{\gamma}}{C_{\eta}}\right)^{\beta}\right\} & t/T_{0.5}\geq C_{\gamma}\\ 0 & t/T_{0.5}<C_{\gamma}\end{cases} \tag{4}$$

where $C_{\gamma}=\gamma/T_{0.5}, C_{\eta}=\eta/T_{0.5}$, β is constant.

Through the test, we can use fitting method to get estimated values of the above parameters. For the same set of test data in ascending order, $t_1, t_2, t_3, \ldots, t_N$, $R_i=i/N+1$ is the estimation of the operating task when t_i complete probability value. By the preceding definitions, we have:

$$\ln R(t)=-\left(\frac{t-\gamma}{\eta}\right)^{\beta} \tag{5}$$

$$\ln\left[\ln\frac{1}{R(t)}\right]=\beta\ln(t-\gamma)-\beta\ln\eta \tag{6}$$

According to the equation (2) and test data we can get the fitted values of β, η and γ by the method of least squares. Then, the fitted values of $T_{0.5}$, C_{γ} and C_{η} can be obtained.

4.2 *Multi-factor test data identification results for one player*

Tables from 3 to 8 provide HCR model parameter identification results of the clothing worn operation test, open/close doors operation test and piping connection operation test.

Figures 1 to 6 reveal the estimated probability curve of tests 1 though 6. Grouping trends were similar according to probability estimation value curves. The analysis of the parameters identified in

Table 3. Suit A test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	1	5.5382	30.50521	29.55141	0.033839	1.032276
B	1	5.3891	30.32803	29.33364	0.034091	1.033899
C	2	5.8246	29.29097	29.5043	0.067787	0.992769
D	1	5.4256	31.39999	30.34854	0.032951	1.034646
E	10	3.836	22.00437	29.99891	0.333345	0.733506

Table 4. Suit B test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	0.1	2.1094	11.18234	9.498512	0.010528	1.177273
B	0.1	2.2091	11.08352	9.488804	0.010539	1.168063
C	0.1	2.3409	11.01348	9.517048	0.010507	1.157237
D	0.1	2.2977	10.66045	9.188391	0.010883	1.160208
E	0.1	2.3524	10.51664	9.099112	0.01099	1.155787

Table 5. Suit C test result.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	1	4.2511	20.0228	19.36854	0.05163	1.033779
B	1	3.8042	20.82753	19.91421	0.050215	1.045863
C	1	3.8999	20.28324	19.46353	0.051378	1.042115
D	1	4.4776	20.30609	19.70987	0.050736	1.03025
E	1	3.9582	20.88451	20.03719	0.049907	1.042287

Table 6. Opening the door test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	2	4.8219	13.3915	14.41116	0.138781	0.929245
B	1	4.7486	15.06411	14.94495	0.066912	1.007973
C	2	5.5649	13.76479	14.88727	0.134343	0.924601
D	4	4.366	11.45429	14.53183	0.275258	0.788221
E	0.1	5.2828	15.47154	14.53435	0.00688	1.064481

Table 7. Closing the door test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	0.1	2.5405	2.77504	2.502165	0.039965	1.109056
B	0.1	2.4789	2.7526	2.474211	0.040417	1.112516
C	0.1	2.4587	2.780678	2.495518	0.040072	1.114269
D	0.1	2.5032	2.710474	2.441235	0.040963	1.110288
E	0.1	2.5798	2.845172	2.568294	0.038936	1.107807

Table 8. Piping test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	0.1	2.9151	6.131169	5.506668	0.01816	1.113408
B	0.1	2.6653	6.005007	5.33337	0.01875	1.125931
C	0.1	2.6426	6.296576	5.580993	0.017918	1.128218
D	0.1	2.6698	6.031005	5.357245	0.018666	1.125766
E	0.1	2.4048	5.869399	5.139541	0.019457	1.142008

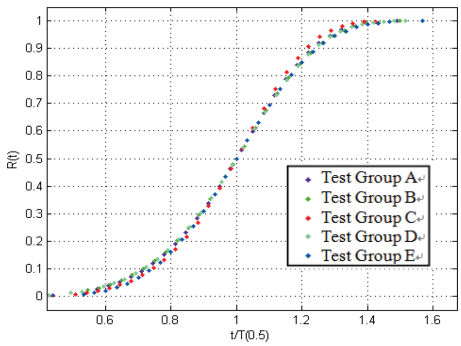


Figure 1. Suit A test results plot.

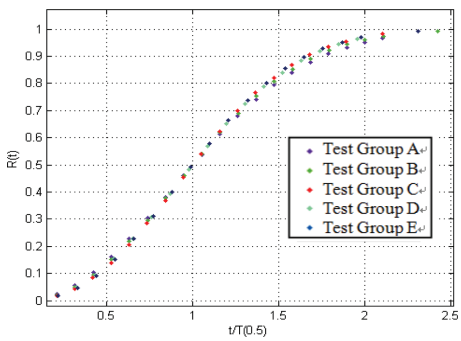


Figure 2. Suit B test results plot.

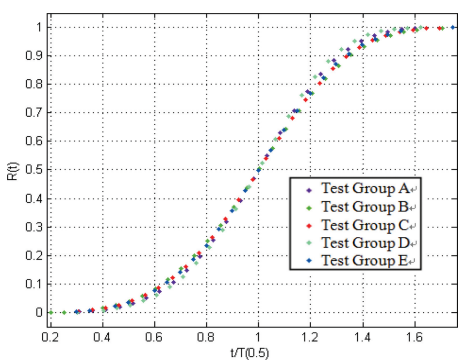


Figure 3. Suit C test results plot.

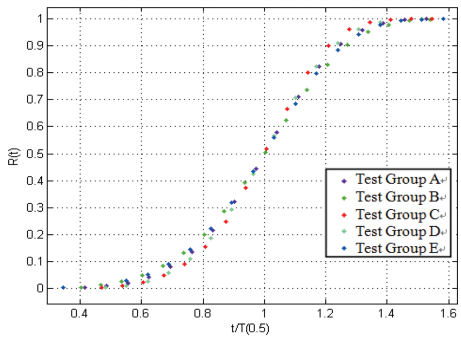


Figure 4. Opening the door test result plot.

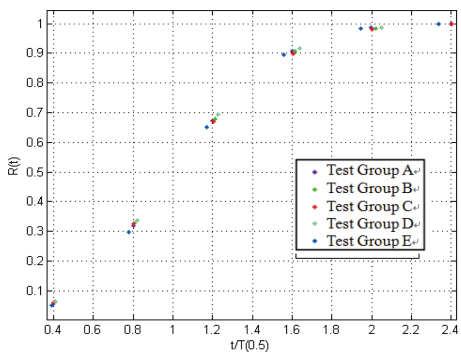


Figure 5. Closing the door test results plot.

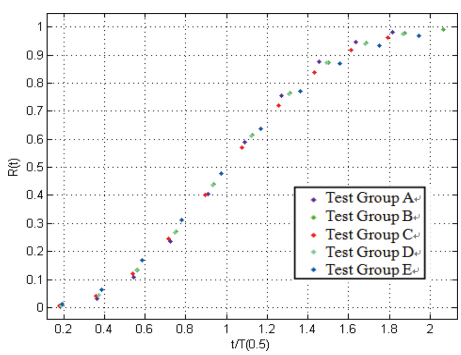


Figure 6. Piping test results plot.

the table showed that individual areas also showed some differences, but the fundamental differences reflect the different team level, then from the evaluating requirements the differences are acceptable. The results can be used as the base for human reliability evaluation.

4.3 *Multi-factor test data identification results for two players*

Tables from 9 to 14 provide HCR model parameter identification results of two players together removing a seal test, two players together installing a seal test, two players together to adjust the seal position test, Two players together measuring test, Two players removing/installing beams test together, and Two players together installing the block test.

Figures from 7 to 12 give the curves of probability evaluation for the 6 experimental data. From the curves, the differences are small among the different groups and conditions. The results of parameters identification are concentrative, and then can be used as the base for human reliability evaluation.

Table 9. Removing a seal test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	1	2.4749	15.42312669	14.299795	0.069931	1.078556
B	0.1	2.5317	15.9328797	13.885103	0.007202	1.14748
C	1	2.97977	15.27040996	14.502756	0.068952	1.052932
D	1	2.67883	14.91158556	14.004494	0.071406	1.064771
E	1	2.90505	14.81501167	14.058683	0.07113	1.053798

Table 10. Installing a seal test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	1	2.58438	22.14255872	20.214338	0.04947	1.095389
B	1	2.59879	20.47266982	18.779253	0.05325	1.090175
C	0.1	2.18057	22.65948106	19.253127	0.005194	1.176925
D	1	2.98954	21.48277842	20.003639	0.049991	1.073944
E	1	2.54926	21.05907221	19.23846	0.051979	1.094634

Table 11. Adjusting the seal position test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	0.1	2.20384	4.943493325	4.2859543	0.023332	1.153417
B	0.1	2.4319	5.345193443	4.697255	0.021289	1.13794
C	0.1	2.57934	5.132969662	4.5529302	0.021964	1.127399
D	0.1	2.38456	5.111641194	4.4832462	0.022305	1.140165
E	0.1	2.09418	5.125638206	4.4025491	0.022714	1.164243

Table 12. Measuring test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	0.1	2.51154	2.837130869	2.5518296	0.039188	1.111803
B	0.1	2.52122	2.72238465	2.4539853	0.04075	1.109373
C	0.1	2.62686	2.927562538	2.6462431	0.037789	1.106309
D	0.1	2.59385	2.770126214	2.5050379	0.03992	1.105822
E	0.1	2.4055	2.739257428	2.4520661	0.040782	1.117122

Table 13. Removing/installing beams test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	6	6.00048	47.16110615	50.366187	0.119128	0.936364
B	9	5.13898	43.72106427	49.710929	0.181047	0.879506
C	16	4.41244	37.3204727	50.345225	0.317806	0.741291
D	20	3.87183	32.90621034	49.933624	0.400532	0.658999
E	1	6.15427	52.244943	50.223826	0.019911	1.040242

Table 14. Installing the block test results.

Test group	γ	β	η	$T_{0.5}$	C_γ	C_η
A	2	4.37036	8.224182415	9.5624859	0.209151	0.860046
B	1	4.681	9.098225526	9.4129056	0.106237	0.966569
C	1	4.00082	9.401211026	9.5780963	0.104405	0.981532
D	1	3.96278	9.152692862	9.3439956	0.107021	0.979527
E	2	4.20637	8.071108134	9.3974973	0.212823	0.858857

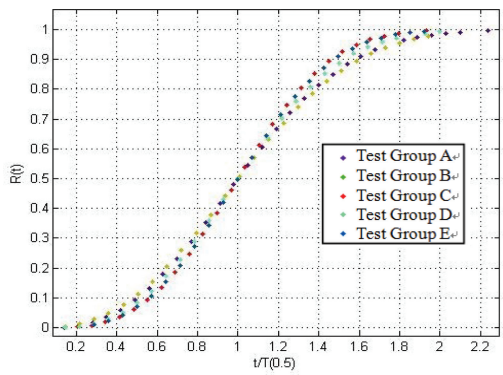


Figure 7. Removing a seal test results plot.

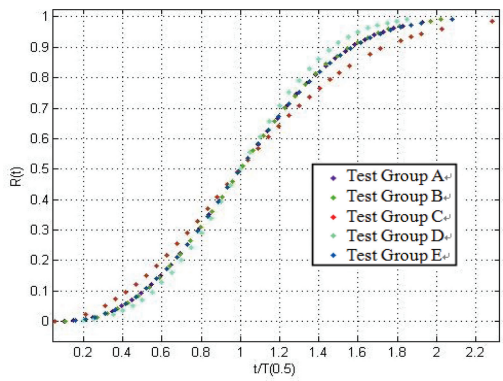


Figure 8. Installing a seal test results plot.

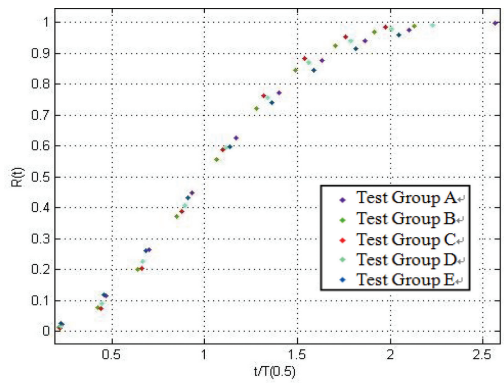


Figure 9. Adjusting the seal position test results plot.

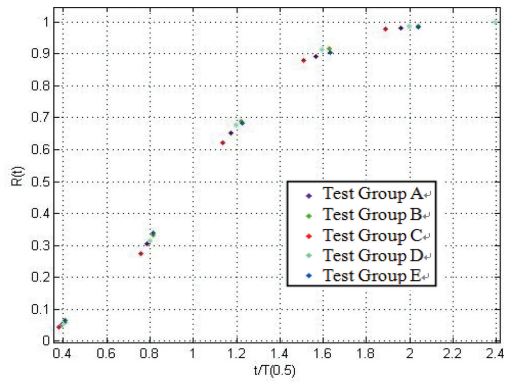


Figure 10. Measuring test results plot.

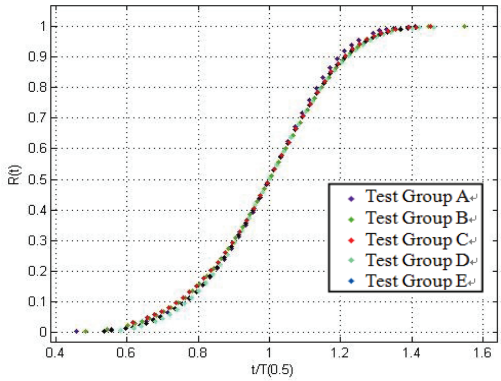


Figure 11. Removing/installing beams test results plot.

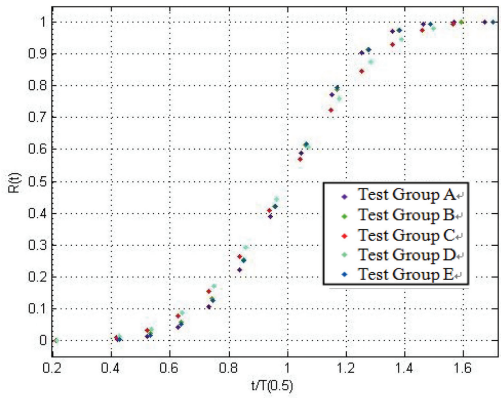


Figure 12. Installing the block test results plot.

5 CONCLUSION

The study is just a simple study attempting to put forward the basic method of human operation reliability testing and parameter identification for multi-factor, given the 11 categories of the test as well as test data. Compared the test results with the data of engineering, the tests are coincident. Because of the lack for the data of engineering, the statistical consistency cannot been given, the data also must be got together. However the results of parameter identification, experimental design and data processing method are scientific and reasonable. The study's results can support the study of the complex task of reliability assessment, as comparisons of task execution differences between personnel need further analysis, and further work will be required to expand this subject.

ACKNOWLEDGMENT

This work was supported in part by the grant of permission from National Natural Science Foundation of China (61104132) and Director of the Foundation (SJ201002). Finally, the authors would like to thank the Associate Editors and anonymous reviewers for their insightful comments.

REFERENCES

Fujita Y. and Hollnagel E., 2004, Failure without Errors: Quantification of Context in HRA, *Reliability Engineering and System Safety*, 83, 145–151.

He X.H., et al., 2007, Human Reliability Analysis of Industrial Systems: Principles, Methods and applications, Tsinghua University press, Beijing, China.

Huang D.S., 2005, Manned Space Environment stress and Hunman Reliability, The 7th Man-machine-environment System Engineering Academic Meeting.

Huang J., Huang X.R. and Shen Z.P., 1999, The second generation method of reliability analysis of the new progress, *Journal of Engineering of the South*, 13, 138–149.

Kim M.C, Seong P.H. and Hollnagel E., 2006, A Probabilistic Approach for Determining the Control Mode in CREAM, *Reliability Engineering and System Safety*, 91, 191–199.

Li B.F., Song B.F. and Xue H.Q., 2005, Analysis on Theoretical Issues in Study of Human Reliability in System Safety, *China Safety Science Journal*, 15, 21–23.

Thomas A.B., 2012, Avoiding Human Error in Mission Operations-Cassini Flight Experience, AAIA Guidance, Navigation, and Control Conference, Minneapolis, Minnesota.

Wang D.H. and Huang W.F., 1996, Human Reliability in Manned Spaceflight, *Space Medicine & Medical Engineering*, 9, 295–301.

Wang W.H., 1998, A Literature Survey and Review on Human Reliability Analysis In man-machine Systems, *Journal of Systems Engineering,* 13, 29–45.

Wondea J., Jinkyun P., 2007, Analysis of an Operators' Performance Time and Its Application to a Human Reliability Analysis in Nuclear Power Plants, *IEEE Transactions on Nuclear Science*, vol. 54(5).

Yang Y., Chen S.G., Zheng W.X., Kang R., 2013, Human Reliability Test and Identification of HCR Model Basic Parameters for Single Factor "Meta-Operation", *Chemical Engineering Transactions*, Vol 33.

Yang Y., Liu W.B. and Kang R., 2012, The Model Framework of Human Reliability For Complicated Spaceflight Mission, Prognostics & System Health Management Conference, Beijing, China.

Zhang L., et al., 2005, The Operator Reliability Experiment at Qinshan Nuclear Power Plant by the Simulator, *Engineering Science*, 7, 41–46.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Statistical analysis of past accidents and a methodology (MEDIA) for Human and Organizational Factors assessment in process industries

M. Ahmad & M. Pontiggia
D'Appolonia S.p.A., Milan, Italy

M. Demichela
Politecnico di Torino, Turin, Italy

ABSTRACT: This paper presents a statistical analysis of past accidents occurred between 1983–2013 reported to European Major Accidental Reporting System (EMARS) across seven industries for Human and Organizational Factor (HOF) assessment. The main purpose of this analysis is to provide guidelines for the HOF analysis and its quantification in chemical process industries. Five identified organizational factors have been chosen as performance shaping factors for human actions/interventions which are quantified using analysis of past accidents. The relation between organizational and human factors is developed and quantified using a newly developed methodology MEDIA.

A case study is carried out for a pig launcher that is widely used in oil and gas facilities during pigging operations. Failure Mode, Effects and Criticality Analysis (FMECA) approach is used to identify the potentially critical human actions/interventions based on guided brainstorming. After that, these identified actions/interventions analyzed using conventional FMECA approach and MEDIA. FMECA can provides a qualitative results, while MEDIA can provides quantitative results and also demonstrates the influence of an organization on human reliability.

1 INTRODUCTION

1.1 *Statistical analysis of past accidents*

One of the concerns during Human and Organizational Factor (HOF) assessment in process industries is the absence of a database for HOF quantification. Therefore, for an effective HOF assessment, it is required to rely on an authentic source for quantification. In this work, it was decided to rely on data from past accidents for HOF quantification. IEC Standard (2009, p. 15) also illustrates the use of relevant historical data to predict the probability of occurrence for events in future.

European Major Accidental Reporting System (EMARS) is selected to recover the historical data of accidents for 30 years from 1983 to 2013. The EMARS was established by the EU's Seveso Directive 82/501/EEC in 1982. The purpose of this reporting system is to facilitate the exchange of lessons learned from accidents and near misses involving dangerous substances in order to improve chemical accident prevention and mitigation of potential consequences (EMARS). At the moment, only accidents are considered in this analysis with a possibility to add near misses in future.

Reporting an event to EMARS is compulsory for EU member states when a Seveso establishment is involved and the event meets the criteria of a "major accident". This criteria of major accident has been defined in the annex VI of the Seveso III Directive (2012/18/EU) and also highlighted below:

- Dangerous substances involved;
- Injury to the person and damage to real estate;
- Immediate damage to the environment;
- Damage to property;
- Cross-border damage.

In this analysis seven different types of industries have been considered to increase the number of accidents and available accidental data. These seven types of industries have been selected due to similarities in their organizational and operative structures. The following self explanatory industrial types as reported in EMARS have been considered in this analysis:

- Petrochemical/Oil Refineries;
- Chemical installations—ammonia;
- General chemical manufacture (excluding H2, SO_x, NO_x, F_2, Cl, NH_3 & CO);
- Wholesale and retail storage and distribution (excluding LPG);
- Production of basic organic chemicals;
- LPG production, bottling and distribution;
- Power supply and distribution.

A preliminary assessment is used to identify those accidents caused by the HOF. Once these accidents have been identified, a detailed analysis was carried with HOF action taxonomy. Accidents were classified according to their major root causes, after reading accidental reports from EMARS. Table 1 illustrates the factors used for the accidental classification. In the first column, plant's operational conditions are listed and in subsequent columns HOF are highlighted.

During the accidental analysis it was also examined if an accident was caused solely either by human error or by an organizational fault or by both.

1.2 *New HOF assessment methodology: MEDIA*

Method for Error Deduction and Incident Analysis (MEDIA) is a newly developed taxonomy based HOF risk quantification technique (Ahmad et al. 2014) and shown in Figure 1. MEDIA is based on newly developed HOF taxonomy which is illustrated in Table 1. At present, only organizational factor is considered as a Performance Shaping Factor (PSF) for human actions.

MEDIA assumes that humans inherit a tendency to make errors even in an ideal working condition, these errors entitle as inherit human error in MEDIA. It also assumes that human reliability fluctuate with the given organizational characteristics. Meanwhile, effect of Safety Instrumented Functions (SIF) is also important to consider in overall HOF assessment by using their risk reduction factor. Guidelines of these safety function and their risk reduction is provided in IEC Standard (1999).

1.2.1 *Organizational factor*

In MEDIA five organizational factors are considered as illustrated in Table 1. Øien (2001) described

Table 1. Criteria for accident classification.

Plant's operational stage	Human factor taxonomy	Organizational factor taxonomy
Normal	Monitoring (M)	Training (T_O)
Start up	Control room	Design (D_O)
Shut down	Actions (A)	Procedures (P_O)
Maintenance	Communication (C)	Management (M_O)
	Manual on-field (F) operations	Safety culture (C_O)
	Reporting (R)	

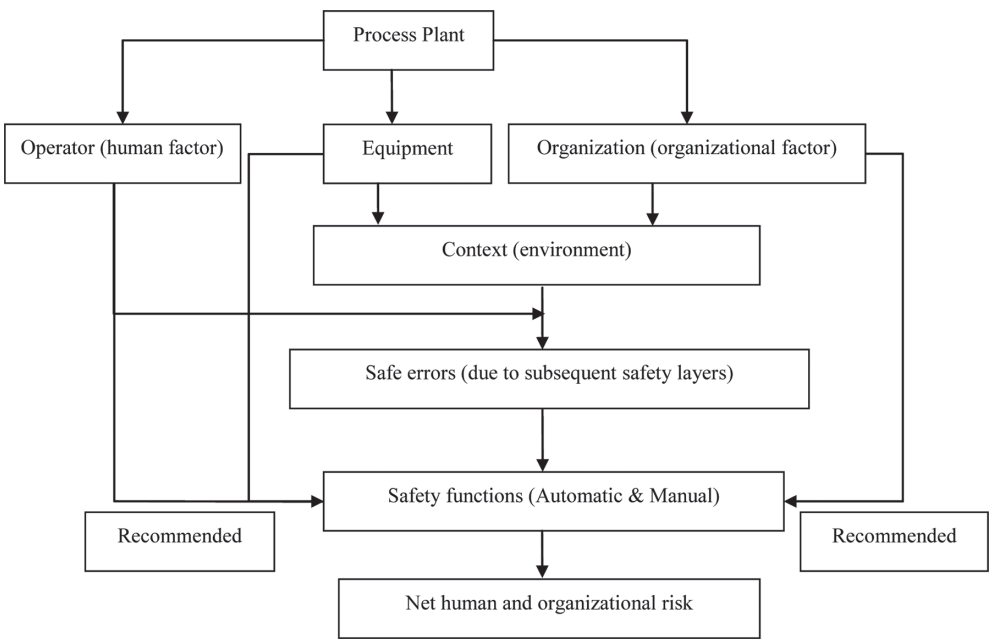


Figure 1. Method for Error Deduction and Incident Analysis (MEDIA) framework.

six organizational factors in his model. During accidental analysis all the Organizational Factors (OF) leading to accidents are recorded and listed in Table 3. OF can be assessed in an organization/company using safety audit/review procedures in order to assign them a level. During proposed safety audit/review, points mentioned in Table 3 will be examined in an organization to check if precautionary measures are in place to minimize the effect of an organization on human actions. If an organization meets all the criteria, then its level is defined by a lower number than if it does not meet these criteria.

Table 3 only illustrates the points that were directly involved in an accident but not those organizational aspects which were improved after the accident.

1.2.2 *Human factor*

In human factor analysis five human factors are considered based on an action based taxonomy as shown in Table 1. A Similar taxonomy is used in SPEAR and reported by Stanton et al. (2005). For each of the factors inherit error frequency/year/plant was calculated based on the accidental analysis. Table 4 shows the basic human errors that led to an undesirable situations during past accidents.

1.2.3 *Quantification of organizational effect on human behavior*

The effect of an organizational characteristics on human behavior is the main feature of this methodology. It is also reported by Daniellou et al. (2011) that organizational factors can influence the human actions. Accidents were observed in a way to account for all the human failure and number of times these failure were caused due to an organizational factor. This quantification analysis can provides the limits to what extent organization can influence the human behavior and cause an accident.

2 STATISTICAL ANALYSIS OF PAST ACCIDENTS

In this section the results of the analysis are presented. Table 2 shows the main features of this analysis. In this analysis 470 accidents from 30 years were considered, of which 90 of them caused by the HOF as mentioned in EMARS database.

It was also recorded if an accident is caused solely either by HF, OF or by both factors. The determination of causal factors to an accident is based on subjective judgment after reviewing the detail report of an accident.

Table 4 lists all the human actions that have led to accidents in the past. Therefore, during a human factors assessment an analyst can know what kind of potential failure events can happen and can consider them accordingly. Since all the human actions are grouped into five main classes, therefore frequencies of human failures are determined across these five classes.

Table 2. Features of accidental analysis.

Description	Number
Time duration (years)	30
Total no. of accidents	470
No. of times HOF involved	90
Accidents in petrochemical/oil refineries	27
Accidents in ammonia installation	2
Accidents in gen. chem. production plants	42
Accidents in wholesale and retail storage and distribution	5
Accidents in organic chemical production installation	6
Accidents in LPG production, bottling and distribution	1
Accidents in power supply and distribution	7
Accidents caused solely by Human Factor (HF)	11
Accidents caused solely by Organization Factor (OF)	17
Accidents caused by both Human and Organizational (HOF)	62

2.1 *Plant's operational stage*

As mentioned earlier, all possible plant stages are considered in this analysis, since risk can be associated with each of the operational stages of the plant as illustrated in Table 1.

Figure 2 shows that major share of accidents (about 67%) occurred during the normal operating conditions while maintenance operations caused about 23% of accidents. Start up operations also led to a noticeable fraction of accidents.

This analysis proposes to consider not just normal operating conditions but also other conditions during the plant's life.

During HF analysis potential failure events can be identified by considering different plant's operational stages and frequencies of events can be adjusted accordingly.

2.2 *Human and organizational factor quantification*

In order to perform integrated HOF assessment, it is important to identify and quantify the effect of different organizational factors on human factors. Table 5 illustrates the effect of different organizational factors on human actions.

Table 3. Organizational factors audit/review points.

Organizational factors	Description
Training	To provide training about most hazardous scenarios;
	To provide training to workers for daily operations;
Design	To check equipment requirements and specifications (e.g. flanges, heat exchangers);
	To provide necessary interlocks (verification of shutting time provided by interlocks);
	Risk should be calculated for all the operations and incorporate during design phase (i.e. loading op.);
	To consider Periodic maintenance of units and adjusted accordingly in design phase of a plant;
	To consider potential human errors and included in design phase of plant;
	To consider vibrations of units and pipelines due to diversions;
	To provide redundancy (e.g. double alarms and interlocks) for high risk operations (e.g. loading and unloading operations);
	To consider proper type/class of an equipment (e.g. pumps, heat exchangers) depending upon the operations and involved substances;
Procedures	To provide necessary operational procedures for operators;
	To provide proper procedures for the start-up operations (i.e. need to consider metrological conditions if seems influencing);
	To provide procedures for carry out maintenance/modifications operations (i.e. procedures to provide work permits to consultants);
	To provide updated operative procedures for the potential hazardous substances and also for the critical operations (e.g. cleaning of high flammable liquid tanks);
	To provide strict procedures for hot work applications (i.e. maintenance and normal operations);
Management	To ensure plant's manning level as considered during the risk assessment;
	To verify knowledge about properties of all the chemicals use in a plant and their potential propagation to certain explosive scenarios (e.g. domino effect);
	To ensure the handling and communication of process modifications (e.g. management of change) to all involved parties;
	To ensure steps to adopt enhanced (latest) safety and performance standards;
	To ensure that Periodic maintenance/inspection of equipments is devised with care;
	To ensure safety and proper management during contractors' work (i.e. normal, maintenance operations) to issue work permit to contractors;
	To ensure necessary communication between different parties involved in different phases of a plant;
Safety culture	To ensure the development and maintaining of safety culture across a facility.

Table 4. Human factor analysis points.

Human factors	Description
Monitoring	Monitoring of vibrations (i.e. vibration in pumps);
	Visual checks for leaks;
	Monitoring of automated safety functions (e.g. not disarmed);
	Constant monitoring of high pressure alarms and indicators;
	Supervision for potentially wrong sequence of operations;
Control room actions	Unintentionally change (i.e. increase or decrease) in plant parameters (i.e. pressure, temperature and flow etc);
Communication	Communication between shifts;
	Communication among and between operators and supervisors;
	Communication between control room operator and manual on-field operator;
Manual on-field operations	Repetition of an action;
	Manual operation of valves;
	Switch-off an alarm unintentionally/intentionally;
	Error of commission (i.e. wrong valve, wrong fluid, wrong equipment etc);
	Error of omission (i.e. violations, slips);
	Error to recover from a faulty state;
	Operator left valve open/close after an operation;
Reporting	Not informing management about the state of a component/accident.

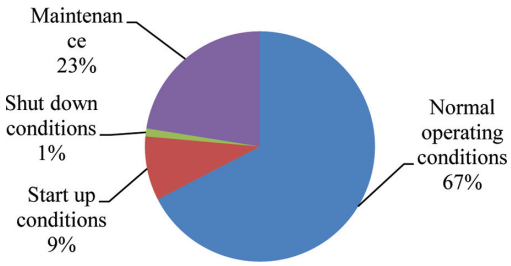


Figure 2. Accidents in different operational stages of a plant caused by HOF.

Table 5. Effect of organizational factors on human factors.

	Organizational factors				
Human factors	T_O	D_O	P_O	M_O	C_O
Monitoring	0.44	0.30	0.36	0.34	0.33
Control room actions	0.00	0.00	0.04	0.00	0.00
Communication	0.33	0.09	0.13	0.09	0.00
Manual on-field operations	0.88	0.60	0.77	0.43	1.00
Reporting	0.11	0.04	0.00	0.00	0.00

Table 6. Human factor inherit error frequencies, HEP and organizational influencing factor.

Human factors	Inherit human error (event/plant/year) (HEP)	Human error probability factor (PSF*)	Organizational influencing
Monitoring	4.96E-04	6.38E-02	3.2
Control room actions	7.09E-05	4.26E-03	1
Communication	2.13E-04	2.55E-02	3
Manual on-field operations	6.38E-04	1.17E-01	5.1
Reporting	7.09E-05	6.38E-03	2

*PSF: Performance Shaping Factor.

Table 5 quantifies the conditional occurrence of human factor errors given the faulty organizational factors. For example: in column 2 and row 1, 0.44 shows that in past accidents whenever there was a problem with the "Training (T_O)", this scenario had 44% potential to led to an error in "Monitoring" activates performed by operators and subsequently caused an accident.

Since organizational "Training (T_O)" has great effect on the "Monitoring" activities, therefore in order to improve the operator's "Monitoring" activities, "Training (T_O)" of operators should be improved.

Table 5 also shows that all five organizational factors had a huge influence on "Manual on-field operations" in a plant. Therefore "Manual on-field operations" errors can't be reduced without proper organizational improvement.

On the other hand, "Control room actions" did not showed much influence from organizational factors except from the "Procedures (P_O)".

Hence, this analysis can provide quantification estimates of organizational influence on the human actions. After this analysis, industrial human actions can be improved by improving the right kind of organizational factor.

Table 6 demonstrates the human error frequencies which had led to notifiable accidents without having any influence from organizational factors (as per EMARS accidental reports); therefore these human error are called inherit human errors.

Table 6 provides the inherit error frequencies for different kinds of human actions. These inherit human error frequencies are calculated by considering only the accidents caused solely by human failures without any involvement of organizational factors.

Organizational influencing factor in Table 6 shows the number of times inherit human error frequencies can be increased considering a conservative approach.

3 HUMAN AND ORGANIZATIONAL FACTOR ASSESSMENT

In this section, the "Method for Error Deduction and Incident Analysis" (MEDIA) methodology is applied to human and organizational factors assessment. A combination of Failure Mode, Effects and Criticality Analysis (FMECA) and MEDIA will be presented for pigging operations. Risk quantification of this assessment is based on the results of statistical analysis of past accidents as explained in section 2.

3.1 *A case study: Pig launcher (pigging operation)*

Pigging operations are used in oil & gas sector for pipeline cleaning. A pigging operation consists of launching and receiving traps. In this study only

launching trap (launcher) is considered for HOF assessment. Figure 3 shows the pig launcher in a simple process flow diagram. Launching operation consists of number of properly sequenced human actions like purging, pressurization, venting, scraper loading and launching. Valves used in this operations are provided with an interlock therefore minimizing the risk of HOF failures.

A sample FMECA worksheet is used for the HOF analysis as reported in Table 8. In order to screen the risk through FMECA, a risk matrix is used extracted from IEC Standard (2000, p. 24) as shown in Table 7. Risk matrix in Table 7 ranks the risk according to frequency and consequence of failures and classify it in terms of high, medium and low risk.

FMECA sheet is slightly modified in order to use MEDIA along with conventional method for risk analysis as shown in Table 8.

In order to calculate the HOF risk through MEDIA, Equation 1 (Ahmad et al. 2014) is used.

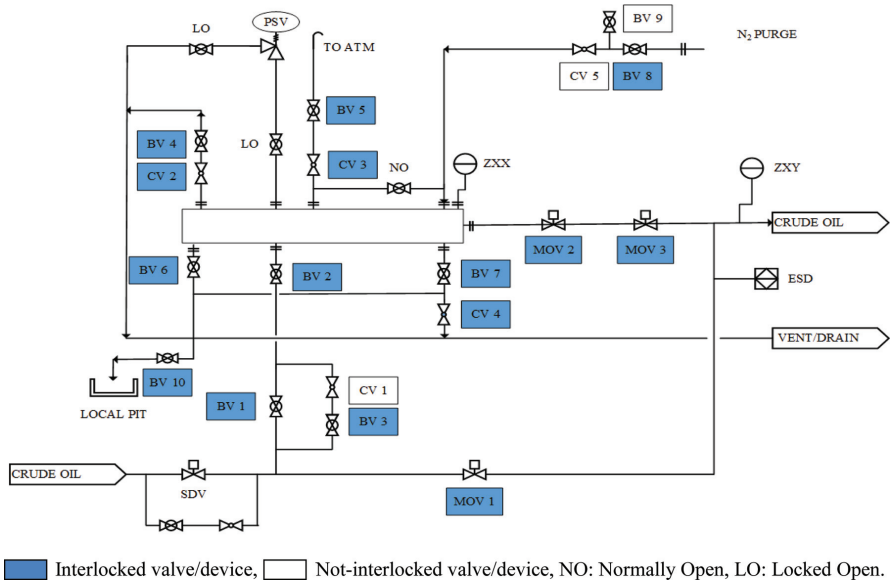


Figure 3. Pig launcher of a pigging operation.

Table 7. Risk matrix use in FMECA.

Consequence					Increasing probability			
Severity rating	People	Assets	Environment	Reputation	A	B	C	D
					Occurred in E&P industry	Occurred in operating company	Occurred several times a year in a company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero effect	LR	LR	LR	LR
1	Slight injury	Slight damage	Slight effect	Slight effect	LR	LR	LR	LR
2	Minor injury	Minor damage	Minor effect	Limited impact	LR	LR	MR	MR
3	Major injury	Local damage	Local effect	Considerable impact	LR	MR	MR	HR
4	Single fatality	Major damage	Major effect	Major national impact	MR	MR	HR	HR
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact	MR	HR	HR	HR

*LR: Low Risk (manage for continued improvement); MR: Medium Risk (incorporate risk-reducing measures); HR: High Risk (fails to meet screening criteria).

Table 8. HOF assessment through FMECA and MEDIA.

Task/action class	Potential failure of task	Plant's state	Potential effect (s) of failure (local)	Severity	Occurrence	Risk (from matrix)	Human Error Prob. (HEP) Table 6	Updated HEP (plant's state)	$Risk_{HOF}$ (Eq. 1) P = 0	$Risk_{HOF}$ (Eq. 1) P = 1
Monitoring	1: Fails to detect rupture of crude oil pipeline.	Normal	Potential explosion event	1	B	LR	6.38E-02	4.27E-02	4.24E-05	1.82E-04
	2: Fails to detect pressure rise in crude oil pipeline.	Pigging	Damage of pipeline	2	B	LR	6.38E-02	1.47E-02	1.46E-05	6.24E-05
	3: Fails to identify by-passed ESD.	Normal + abnormal	Fails to provide shut-down when req.	3	B	MR	6.38E-02	6.38E-02	6.33E-05	2.71E-04
Control room actions	4: ESD by-passed unintentionally/ intentionally.	Normal + abnormal	Fails to provide shut-down when req.	3	B	MR	4.26E-03	4.26E-02	1.21E-06	2.59E-06
Communication	No credible tasks have been identified									
Manual on-field operations	5: CV 5 unintentionally open.	Pigging	Un-controlled pressurization	1	C	LR	1.71E-01	3.93E-02	5.02E-05	2.15E-04
	6: CV 1 unintentionally close while BV-1 is also close.	Pigging	Require more time for pigging	1	B	LR	1.71E-01	3.93E-02	5.02E-05	2.15E-04
	7: BV 9 unintentionally open during purging.	Pigging	N2 release to atmosphere	1	B	LR	1.71E-01	3.93E-02	5.02E-05	2.15E-04
	8: Wrong position of scraper during launching.	Pigging	Damage of launcher	1	B	LR	1.71E-01	3.93E-02	5.02E-05	2.15E-04
Reporting	9: Not informing management about a problem.	Pigging	Effects the pigging op.	2	B	LR	6.38E-03	1.47E-03	2.08E-07	8.91E-07

$$Risk_{\mathrm{HOF}} = E \cdot e^{\mathrm{P}.\ln(X/E)} \cdot \left(\sum_{i=1}^{4} (N\ I\ Si \cdot i) \cdot R \right) \qquad (1)$$

where:
E = Inherit human errors (ev/plant/year);
P = Probability of human action failure given organizational characteristics, $0 \le P \le 1$;
X = Total number of human errors (ev/plant/year);
i = No. of safety layer associated to human actions;
$N\ I\ Si$ = Number of human action associated to ith safety layer;
R = Human Error Probability (HEP).

Equation 1 is developed using definition of risk (i.e. frequency × consequence). Number of factors were identified and recorded while conducting the analysis of past accidents with regard to HOF. These factors relate together in Equation 1 using iterations in order to ensure the theoretical concepts behind MEDIA.

1st term in Equation 1 represents the frequency as listed in Table 6, while 2nd term is the calibration term for this model which also consider the organizational influence through "*P*" value. The last term in this equation is the consequence term which involves the characteristics of a specific plant by taking into account the number of human interventions at each safety layer and also the failure probability of these human interventions.

In this analysis all the potential human interventions are categorized into five main classes as identified in Table 8.

Nine potential human interventions have been selected for further analysis. HOF risk is evaluated qualitatively by using the conventional risk matrix approach as indicated in Table 8 column 7. On the other hand, same interventions are also evaluated quantitatively using MEDIA approach as indicated in columns 10 and 11 of Table 8.

3.2 *MEDIA HOF risk quantification*

HOF risk can be quantified using Equation 1 as proposed by MEDIA. MEDIA also accounts for the criticality of an action by considering the associated safety layer of an action. Figure 4 illustrates the HOF risk associated to nine identified potentially critical human actions for zero organizational influence on human actions. X-axis shows the number of an action and Y-axis shows the obtained risk.

Action 3 has the highest associated risk since failure of this action had led to extensive accidents in the past. While, lowest risk is obtained for action 9 which is associated to "reporting" failure to management. Risk from action 5 to action 8 almost remains the same since it all involved the manual on-field operations.

3.3 *Comparison of risk at different levels of organization*

As mentioned earlier, an organization has an influence on human reliability, therefore in Figure 5 MEDIA model will be tested against four organizational influence levels to see the final obtained risk.

Figure 5 illustrates the effect of an organization on human actions. Associated risk to human actions increases as the influence of an organizational increases as represents by "P" values.

The curve with minimum level of organizational effect (P = 0) has lowest risk, while curve with the maximum level of organizational effect (P = 1) has the highest risk. The extent of change in risk with change in organizational level is determined by the calibration term in Equation 1. This calibration term is calculated from the analysis of past accidents across selected five type of human factor taxonomy.

Therefore, MEDIA model can provide consistent results against different influencing levels of an organization.

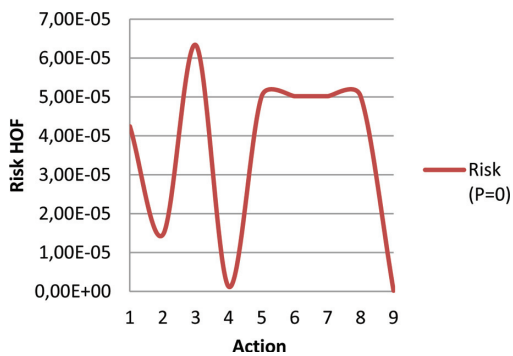


Figure 4. Chart of human factor risk with zero organizational influence.

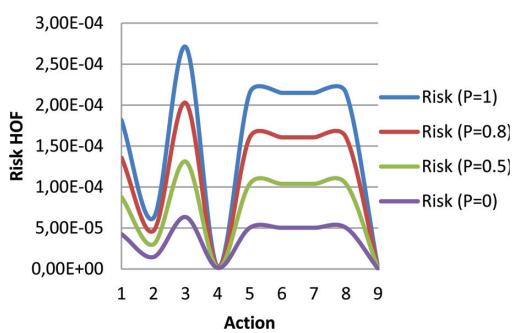


Figure 5. Chart of human factor risk with four organizational influencing levels.

4 DISCUSSION

It is very important to consider HOF in overall risk management. Major hurdle in HOF analysis arise due to lack of human unreliability database. Statistical analysis of past accidents can provides good estimates for potential human failures and effect of an organization on the outcome of human actions.

The statistical analysis of past accidents (1983–2013) confirmed the importance of organizational influence on human actions.

"Design" and "procedures" organizational factors have high degree of influence on human actions. Meanwhile, output from "Manual on-field" human actions has maximum tendency to be influenced from organizational factors.

Concluding the statistical analysis of past accidents, frequencies and probabilities of human failure were obtained for selected human factor taxonomy. This analysis is strongly based on data obtained from past accidents, therefore it will provide the fewer estimates of HOF errors compare to normal operational situation where near-miss events are also an important aspect to be considered.

In the second part of this study, a newly developed methodology "MEDIA" is applied to a case study.

Primarily, MEDIA is a methodology to quantify the human failure actions based on the past accidental database. At the same time, MEDIA also provides an added value to the analysis since it can also incorporate the organizational influence on human actions. This methodology is developed keeping in mind today's practical constraints posed by lack of information flow from a company to an outsource contractor about HOF analysis. P&ID's, cause & effect diagrams and organizational & human factor reviews can provide the necessary information for MEDIA human factor analysis, however results can be more precise with any other relevant information depending upon company's regional or international standards.

Various organizational factors have different influence on different kinds of human actions. Therefore, this analysis can provides the information about the right kind of organizational factor to be improved in order to improve the human factor.

Furthermore, in future it is expected to include the guidelines to use HOF as an extra safety barrier in order to optimize the existing resources.

REFERENCES

Ahmad, M. Pontiggia, M. & Demichela, M. 2014. Human and organizational factor risk assessment in process industry and a risk assessment methodology (MEDIA) to incorporate human and organizational factors, *Chemical Engineering Transactions*, 36, 565–570 DOI:10.3303/CET1436095.

Daniellou, F. Simard, M. & Boissières, I. 2011. Human and organizational factors of safety: a state of the art, *Institute for an Industrial Safety Culture*, Toulouse, France, http://www.FonCSI.org/cahiers/, accessed 11.09.2013.

EMARS (European Major Accident Reporting System), *Major Accident Hazards Bureau*, European Commission https://emars.jrc.ec.europa.eu/id=4, accessed 20.10.2013.

IEC Standard, 2000, ISO 17776: Petroleum and natural gas industries—Offshore production installation—Guidelines on tools and techniques for hazard identification and risk assessment, *International organization for standardization*, Geneva, Switzerland.

IEC Standard, 2009, IEC/FDIS 31010: Risk management—Risk assessment techniques, *International Electrotechnical Commission*, Geneva, Switzerland.

IEC Standard, 1999, IEC 61511-1: Functional safety: Safety instrumented systems for the process industry sector, *International Electrotechnical Commission*, Geneva, Switzerland.

Stanton, N.A. Salmon, P.M. Walker, G.H., Baber, C. & Jenkins D.P. 2005. *Human factors methods: a practical guide for engineering and design*, Ashgate Publishing Group, Oxon, GBR.

Øien, k. 2001. A framework for the establishment of organizational risk indicators, *Reliability Engineering and System Safety*, 74:147–167.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Predictive Human Error Analysis in Permit To Work system in a petrochemical plant

M. Jahangiri
Department of Occupational Health, School of Health, Shiraz University of Medical Sciences, Shiraz, Iran

F. Zare Derisi & N. Hobobi
Student Research Committee, Shiraz University of Medical Sciences, Shiraz, Iran

ABSTRACT: Permit To Work (PTW) is a means of safety system to coordinate different work activities. However, it may be susceptible for human error. The purpose of this study was identification and analysis of human errors in PTW system using Predictive Human Error Analysis (PHEA) technique. The most important identified errors were; inadequate isolation of process equipments, inadequate labelling of equipment, and delay in starting the work after issue the work permit, improper gas testing, inadequate site preparation measures etc. Finally for preventing and recovering from the identified errors, site work permit form and its procedure was revised.

1 INTRODUCTION

According to industrial accident's investigation 60 to 90% of all accidents have directly been caused by human errors (Brazier et al. 2000). Increasing interest in this area has arisen partly from occurrence of a number of major accidents such as Flixbrough (1974), Seveso (1976), Tree Mile Island (1974), Bhopal (1984), Chernobyl (1986) and many other accidents where human error has played a significant role.

Human error defined as any situation in which an operator fails to do an activity within the tolerance of the system that can result in unacceptable or undesirable results (Roger et al. 2001).

Permit to work (P.T.W) is a formal written system to control certain types of work which are identified as potentially hazardous. This system may need to be used in high-risk jobs such as hot works, confined space entry, carrying hazardous substances, and electrical or mechanical isolation. In this system, responsible persons should assess the work and check safety at all stages. Moreover, permits are effectively a means of communication between site management, plant supervisors and operators, and those who carry out the work. The people doing the job sign the permit to show that they understand the risks and precautions necessary.

Although P.T.W is an integral part of a safe system of work and can help to properly manage the wide range of activities, it may be susceptible for human error itself. The purpose of this study was identification and analysis of human errors and proposing proper solutions for prevention of errors and reduction of theirs consequences in a petrochemical plant.

2 METHOD

In this cross-sectional study, permit to works system procedure in a petrochemical plant were studied for potential human errors. For this purpose, in the first stage occupational tasks in P.T.W procedure were analyzed using Hierarchal Task Analysis (HTA) (Stanton 2004).

Task analysis is description of the observable aspects of operator behaviour at various level of details together with some indications of the structure of the task (Embery 2000).

HTA is a systematic method to describe how work is organized in order to meet the overall objective of the job. It involves identifying in a top down fashion the overall goal of task, then various subtasks and the condition under which they should be carried out to achieve the goal (Stanton 2000). In this study all tasks that were selected as critical and susceptible to human error consequences were analyzed by HTA method and its information was gathered through observation method, interviewing with workers and reviewing procedures and documents.

In the second stage, Predictive Human Error Analysis (PHEA) technique was used for

predicting and analysis of human errors in each task. In PHEA worksheets, all possible errors in the selected occupational tasks were predicted and proper solutions for their preventing were determined. This technique is systematic and easy to learn and recommended for chemical process. Moreover, it is based upon HTA and error taxonomy and predict errors and their consequences (CCPS 2004, Brazier 2000).

Error classifications in PHEA are as follows (Kirwan 1997);

– Action errors (e.g. pressing a button or pulling a switch): Action too late/early; action too fast/ slow; action in wrong direction; action too little/much; wrong action on right object, action omitted, action incomplete
– Retrieval errors (e.g. getting information from a screen or manual): information not obtained; wrong information obtained; information retrieval incomplete.

Checking errors (e.g. conducting a procedural check): check omitted; check incomplete; right check on wrong object; wrong check on right object; checking too late/early.

Selection errors (e.g. choosing one alternative over another): selection omitted; wrong selection made.

Information communication errors (e.g. talking to another party): information not communicated; wrong information communicated; information communication incomplete.

In PHEA, each task analysed step by step in term of error type, error description and error consequences. Moreover, error reduction strategy and proper solutions for prevention and recovering from errors were determined and presented in PHEA worksheets.

3 DISCUSSION

Table 1 shows the hierarchical task analysis of P.T.W system procedure in the studied petrochemical plant. As it can be seen, 11 main tasks and 4 subtasks were identified in HTA process. Task No. 3 (Inspecting the workplace and complete the checklist section in the permit) had 4 subtask including venting process equipments from flammable and toxic materials, lock out and tag out the electrical equipment, cleaning the work area from flammable material and isolation of process equipment.

A sample of PHEA worksheet for prediction of human errors in each task has been presented in Table 2. As shown, in PHEA worksheets, apart from errors and their description, consequences of error occurrences and error reduction strategy for each task are determined. Error types and frequency of predicted errors in permit to work system in the studied petrochemical plant has shown in Table 3.

Table 1. Hierarchical task analyses of work permit system in the studied petrochemical plant.

1. Site inspection
2. Description of hot/cold work
3. Site preparation
   3.1. Venting process equipments from flammable and toxic materials
   3.2. Lock out and tag out the electrical equipment
   3.3. Cleaning the work area from flammable material
   3.4. Isolation of process equipment
4. Flammable gas testing
5. Oxygen and toxic gas testing
6. Specify the protective devices in the permit
7. Specify safety measures in the permit
8. Showing work area to operator
9. Site inspection by shift control
10. Signing the permit
11. Validation and revalidation after shift handover

Totally 67 errors were identified in all permit to work system tasks including 28 action error, 23 checking error, 8 retrieval error, 5 selection error and 3 information communication error.

Some of the most important errors identified in the PHEA worksheets were; inadequate isolation of process equipments, inadequate labelling of equipment, delay in starting the work after issue the work permit, improper gas testing, inadequate site preparation measures etc. 32% of predicted errors, were related to inadequate isolation of process equipments and hazardous energy source which are one of the main causes of accidents in process industries.

For preventing and recovering from identified errors, proper solutions were proposed. These solutions were mainly focused to;

1. Training: Inadequate training has been found to be one of the failures relating to the operation of P.T.W system (HSE, 2005). Effective training is essential to achieve quality and consistency in the use of the permit-to-work system. Some of human errors identified in the PHEA worksheets, were because of inadequate and shortcomings in training programs. Therefore, training needs in P.T.W system were determined specifically for each task in PHEA worksheets.
2. Work procedures: Studies have showed that 11 to 24% industrial accidents occurred due to lack and weaknesses related in procedures (Peterson 1996). Rasmussen's classified these errors as rule based errors (Kirwan 1997). In this study, some of human errors identified in the PHEA worksheets, were because of shortcomings in

Table 2. Sample of PHEA worksheet for prediction of human errors in permit to work system.

Task step	Error code	Error description	Error consequences	Control strategy
6. Specify required protective equipment in the permit	A3	Operator does not specify required protective equipment the permit	Workers may not use the protective equipment specified in the permit	Training and check the permit by supervisor
	A6	Operator specify required protective equipment too much	Unnecessary protective equipment specify in the permit and workers may not use tem	Training and check the permit by supervisor Revision of work permit form
	A7	Operator forgot to specify some of required protective equipment in the permit	Workers may not use all required protective equipment	Training and check the permit by supervisor

*For error codes refer to Table 3.

Table 3. Predicted human errors in permit to work system in the studied petrochemical plant.

Error types	Code	Description	No. of predicted errors
Action errors	A1	Action too late	–
	A2	Action too early	–
	A3	Action omitted	17
	A4	Action too fast	1
	A5	Action too slow	–
	A6	Action too much	1
	A7	Action too little	1
	A8	Action incomplete	8
	A9	Action in wrong direction	–
	A10	Wrong action on right object	1
Checking errors	C1	Checking too late	5
	C2	Checking too early	1
	C3	Right check on wrong object	2
	C4	Check incomplete	7
	C5	Checking omitted	8
Retrieval errors	R1	Information not obtained	5
	R2	Wrong information obtained	–
	R3	Information retrieval incomplete	3
Information communication errors	I1	Information not communicated	1
	I2	wrong information communicated	–
	I3	Information communication incomplete	2
Selection errors	Sel1	Selection omitted	1
	Sel2	Wrong selection made	3

P.T.W procedures. For this reason, proper solutions were proposed for revising P.T.W procedures and work permit form.

3. Hardware change in equipment design: The most effective way for preventing human errors is design plants and working methods to remove opportunities for error or provide opportunities for recovering them (Kletz 2000). Therefore for some of errors identified in PHEA worksheet, measures including labelling and colouring of process equipments, installing acoustic telephone booths for better communication in the site etc were proposed.

Finally for preventing and recovering from the identified errors, site work permit form and its procedure were revised totally.

4 CONCLUSIONS

Permit To Work (P.T.W) is a means of safety system to coordinate different work activities, but

it may be susceptible to human error. Predictive Human Error Analysis (PHEA) technique could be applied for prediction and analysis of human errors and providing proper solutions for preventing and recovering from the identified errors. These solutions could be in the area of training, labeling of equipments, coloring pumps and process equipments, installing acoustic telephone booths in the site for better communication etc.

REFERENCES

Brazier, A. Richardson, P., Embery, D. 2000. Human factor Assessment of safety critical tasks. London: Health and Safety Executive. Available at; *www.hse.gov.uk/research/.../oto99092.pdf.*

CENTER FOR CHEMICAL PROCESS SAFETY CCPS. 2004. Guidelines For Preventing Human Error In Process Safety. First Edition. United States, Wiley-Aiche.

Embery, D. 2000. Task Analysis Technique, Human Reliability Associate. Available at *www.humanreliability.com/articles/Task%20Analysis%20Techniques.pdf.*

Health and Safety Executive HSE. 2005. Guidance on permit-to-work systems. Available at: *http://www.hseni.gov.uk/hsg250_guidance_on_permit_to_work_systems.pdf.*

Kirwan, B. 1997. A Guide to practical human reliability assessment. London: Taylor and Francis.

Kletz, T. 2002. *An Engineering View of human error*. Third edition. London: Taylor & Francis.

Peterson, D. 1996. *Human error Reduction and safety management.* Third Edition. United States, International Thoams Publishing.

Stoelsnes, R.R., Gudmestad, O.T. and Bea R.G. 2001. On the Importance of Human and Organizational Factors in Design, Construction and Installation of Engineered Systems. *Proceedings of the Eleventh International Offshore mid Polar Engineering Conference Stavanger, Norway*, June 17–22, 2001.

Stanton, N., Hedge, A., Brookhuis, K., Eduardo Salas, E., Hendrick, H.W. 2004. *Handbook of Human Factors and Ergonomics Methods*. Los Angeles; CRC Press.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Anticipating impacts of change on individual behaviors within a perspective of safety management

T. Côte, E. Rigaud & E. Garbolino
Mines ParisTech, CRC Sophia Antipolis, France

ABSTRACT: Technological or managerial changes aim improving a dimension of performance of sociotechnical systems, generally productivity, profitability or quality. In some circumstances changes can affect, as a side effect, system safety properties and facilitate occurrence of crisis situations or by decreasing system ability to mitigate crisis situations. Anticipating potential consequences of change on sociotechnical systems safety properties requires knowledge, method and tools covering the complexity of sociotechnical system. Objective of this paper is to present and apply a methodological framework aiming supporting the identification of impact of a change on individual and collective behaviors within the perspective of safety management.

1 INTRODUCTION

Organizational changes, defined as a "process of radical or marginal transformation of structures and skills that punctuates the process of evolution of organizations" (Grouard et al. 1998) or "any relatively permanent modification in a subsystem of the organization, provided that such modification can be observed by its members or people who are related to this system" (Collerette et al. 1997) are omnipresent in enterprises.

Among the diversity of these changes, some are injunctions coming from the strategic apex with a strong constraint of realization and relatively weak margins of manoeuvre (Autissier et al. 2012). Consequences are the launch of change management project aiming to transform the organisation as whished by the strategic apex.

Changes can affect safety performance. Several examples can be found where new technologies, new rules, new work organisation led to system failure, misunderstanding of situation by agent, creation of new system dependencies, loose of flexibility, etc.

Technology assessment (Westrum 1991) aims considering the potential consequences of new technological system. Several methods and tools exist to support such assessment. In the context of safety and security, brainstorming, expert groups and traditional risk assessment methods such as FMECA (Failure Mode, Effects and Criticality Analysis) are often used with the purpose of identifying potential risks related to the adoption of a new technology.

Objective of this paper is to present initial results of a research project aiming to understand and improve safety management tasks to be achieved during change processes.

First section is related to the presentation of the context of the project. Second section aims describing basis of the framework currently developed. Third section presents an inventory of dimensions to be considered by the assessment of potential consequence of a change on socio technical system safety performance. Fourth part describes a module aiming to support assessment of consequences of change on system situation awareness performance.

Some lessons of the realization of assessment on different cases are summarized in the conclusion and perspectives of development are presented.

2 CONTEXT OF THE RESEARCH

Occurrence of a change can affect safety performance of a system. In order to prevent them, risks analyses are conducted. In some industry like train transportation, studies is mandated by a regulation, in other industries studies are voluntary done.

In order to define the context of the project, empirical studies are conducted to understand practices and issues related to the realization of those studies.

A set of studies is conducted in order to understand safety issues of change management. Main results of those studies are:

– **Impact of change on safety performance is a key issue for safety management systems.** Changes occur everyday (new tools, new technology, new organization of work, etc.). Management of

related safety issues is mandatory or voluntary done.
- **Absence of global methods.** Analyses are done using methods like brainstorming; experts group or with the application of risks analysis methods but no global methodological guideline exist.
- **Technological dimension are well considered, study of human and organizational factors has to be improve.** Anticipation of potential technological failures well considerate but analyses of consequences of a change on human and organizational factors has to be improved.
- **Analyses are generally realized to late.** Risks analyses are considered by change management people as constraints and therefore are planned near the end of the process. Consequences are tensions when safety manager identify potential risks and ask to revise the change process.
- **Decisions are trade-off between conducting change and maintaining safety.** When change management process has to be modified for safety issues, a trade off between the two dimensions is searched between change and safety managers.
- **Safety management does not consider all changes.** There are rules to decide if an event is considered as a change and consequently studied by risk analyses.

Those empirical results structure methodological development in order to provide a method aiming to support change management based risk analyses with the finality to improve the consideration of human and organizational factors.

3 THE IMPACT FRAMEWORK

The IMPACT method aims providing a set of recommendations for a change process management before, during and after its realisation. It is based on a risk analyses approach. Consequences are identified through the application of an assessment strategy that is defined alongside an examination of the change considered.

Methodological guidelines support the application of the different steps to be achieved and a toolbox offers data acquisition processes and performance indicator assessment guidelines.

3.1 *Methodological guidelines*

The IMPACT method is structured with four phases.

- **Phase 1**: *General Outline*. Definition of an assessment strategy based on the description of the change studied, the system impacted and the selection of assessment modules.
- **Phase 2**: *Consequence identification*. Application of assessment modules with the perspective of identifying potential pacts of the change.
- **Phase 3**: *Risks and opportunities analysis*. Evaluation of risks and opportunities of each consequence.
- **Phase 4**: *Recommendations for decision-making*. Definition of recommendations for change management process and system safety management.

In order to support the application of the method a toolbox has to be developed.

3.2 *IMPACT toolbox*

The IMPACT toolbox aims to be constituted of two types of guidelines: data collection processes and performance indicator assessment processes.

A preliminary survey supports the identification of dimensions to be considered by process of definition of modules.

Three types of data collection processes are suggested:

- **Risk assessment**. Traditional risk assessment processes based on different methods (FMECA, HAZOP, THERP, CREAM, etc.).
- **Focus groups**. Focus groups is an approach that consists of asking a group of people about their feelings, opinions, and beliefs concerning an idea, a concept, a product, etc.
- **Simulation**. Simulation can be an efficient way to identify the consequences of a change on a system. Simple role-playing games or more elaborate simulations using technological facilities such as bridge, flight or crisis management simulators can be used in order to acquire information about the consequence of a change by, for example, comparing the execution of a given scenario with and without the application of the change.

Two levels of safety performance indicators are suggested based on the safety I versus Safety II theoretical context (Hollnagel 2014).

- **Safety I based consequences**. Consequences related to failure of a dimension of the system (technological, human or organizational) including change acceptance, non-technical skills definition and assessment; research and development activities, e.g. situation awareness, decision-making, communication, teamwork, leadership, stress, fatigue (Flin et al. 2008); control performance assessment (Hollnagel & Woods 2005); and risk governance e.g. pre-assessment, management, appraisal, characterization, evaluation and communication (Renn & Walker 2008).
- **Safety II based consequences**. Consequences related to capabilities of a system to sustain

required operations under both expected and unexpected situations. It includes resilience capabilities e.g. Respond, Learn, Monitor and Anticipate (Hollnagel et al. 2011); HRO abilities, e.g. Preoccupation with failure, Reluctance to simplify interpretations, Sensitivity to operations, Commitment to resilience, Deference to expertise (Weick & Sutcliffe 2001); Efficiency Thoroughness Tradeoff model i.e. Work ETTO, Psychological ETTO, and Organizational ETTO (Hollnagel 2009).

Research and development activities are conducted with the perspective of developing a first prototype of assessment module dedicated to the assessment of impact of change on human behaviour.

4 HUMAN—BASED CONSEQUENCES OF CHANGE ASSESSMENT INDICATORS

Objective of the module is to support assessment of potential impact of a change on the diversity and complexity of individual behaviors. Two preliminary assessment modules are considerate:

- **Societal and practical acceptance of change impacts assessment.** This module aims assessing the potential of the change to be at the origin of rejection by people for general or practical concerns.
- **Individual characteristics impacts assessment.** This module aims assessing the potential of the change to affect individual characteristics (stress, fatigue, etc.) and behaviors (observe, interpret, plan, etc.).

For each dimension, a list of preliminary indicators is proposed.

4.1 *Societal and practical acceptance of change conceptual model*

Societal and practical acceptance of change issues concern mainly innovative technology and are related to the question of acceptance of a technology.

4.1.1 *Societal acceptance of a new technology*

Societal acceptability is related to the potential of an innovation to be at the origin of a social problem. Social problem can be defined as "a condition that undermines the well-being of some or all members of a society and that is usually a matter of public controversy" (Macionis 2005) or as "the activities of individuals or groups making assertions of grievance and claims with respect to some putative conditions" (Spector & Kituse 1977). Social problem life cycle can be structured with six phases (Best 2008):

- **Claims making**. People make claims that there is a social problem, with certain characteristics, causes and solutions.
- **Media coverage**. Media report in claims makers so that news of the claims reaches a broader audience.
- **Public reaction**. Public opinion focuses on the social problem identified by the claims makers.
- **Policymaking**. Lawmakers and others with the power to set policies create new ways to address the problem.
- **Social problem work**. Agencies implement the new policies, including calls for further changes.
- **Policy outcomes**. There are various responses to the new arrangements.

In order to assess the potential of a change to be at the origin of social problems, a set of dimensions are considered. Table 1 presents dimensions that are considered.

4.1.2 *Practical acceptability of a new technology*

Practical acceptability is related to the perception by users of the utility of a technology for achieving their goals. This perception can be studied "a priori", assessment is based on the subjective representation of the technology and characterized its acceptability. It can be studied with an experimental use of the technology and characterized its acceptation. Finally it can be studied once

Table 1. Societal acceptance indicators.

Indicators	Description
Privacy	Concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention'
Confidentiality	Status accorded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorised individuals or organisations with a need to know"
Safety	Condition of being protected against physical, social, spiritual, financial, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event, which could be considered non-desirable.

integrated in users activities and characterized its appropriation (Terrade et al. 2009).

In order to assess the potential of acceptability, acceptance and appropriation of a change a set of dimensions are considered (Table 2).

Dimensions to be considerate by a diagnostic of a change potential of acceptance or of reject by society and end users have been presented in this section. These dimensions can be used, as basement by data collection processes.

4.2 *The individual perspective*

This is related to the presentation of a set of factors to be used for the diagnostic of potential impacts of a change on individual functions and characteristics.

Four individual functions are firstly considerate: Observe, Interpret, Plan and Communicate. Then individual characteristics of human stress and fatigue are discussed.

4.2.1 *Observe, interpret, plan and communicate*

Observation function aims gathering information by perception in the current situation (Endsley 1995, Flin et al. 2008). Failure modes of observation process are (Hollnagel 1998):

- **Observation can be missed**. A signal, an event or a measurement is missed.
- **A false observation can be made**. A response is given to an incorrect stimulus or event, an event or some information is incorrectly recognized or mistaken for something else.
- **Wrong identification can be made**. A signal or a cue is misunderstood as something else, the identification of an event or some information is incomplete or incorrect.

Information gathered by the observation process has to be processed to make sense of the situation in order to understand what is going on and the significance of data observed (Flin et al. 2008). Failure modes of interpretation process are (Hollnagel 1998):

- **Diagnosis is false**. Diagnosis of the situation is incorrect or incomplete.
- **Reasoning is false**. Induction or Deduction reasoning process lead to invalid results, Selection among alternatives is achieved with using incorrect criteria, hence leading to incorrect results.
- **Decision is false**. Agents are unable to make a decision; decision is wrong, decision does not completely specify what to do.
- **Interpretation is delayed**. Identification is not made in time or not made fast enough.
- **Prediction is incorrect**. A change not anticipated occurred, event developed in the main as anticipated but some side effects has been missed, speed of development has been misjudged.

Interpretation and prediction of the evolution of the events to be controlled information is used for planning decisions and actions to be performed (Flin et al. 2008). Failure modes of planning process are (Hollnagel 1998):

- **Plan is inadequate**. Plan is not complete, does not contain all the details needed or is wrong.
- **Selection of goals is wrong**. Priorities followed are wrong and goals have been wrongly selected.

Communication refers to the exchange of information, feedback, response, ideas and feelings. Failure modes of communication process are (Hollnagel 1998):

- **Communication failed**. The message or the transmission of information did not reach the receiver, the message was received, but it was misunderstood.
- **Information is missing**. Information is not being given when it was needed or requested, the information being given is incorrect or incomplete, there is a misunderstanding between sender and receiver about the purpose, form or structure of the communication.

4.2.2 *Stress and fatigue*

Stress is a "particular relationship between the person and the environment that is appraised by the person as taxing or exceeding his or her resources and endangering his or her well-being" (Lazarus et al. 1984). Two types of stress are considered (Flin et al. 2008). Acute stress is sudden, novel, intense and of relatively short duration. It disrupts goal-oriented behaviour and requires a proximate response (Salas et al. 1996). Chronic stress is related to reactions of individuals of the variability of its environment such as an increase of the

Table 2. Practical acceptance indicators.

Indicators	Description
Utility	Utility is related to the total or partial correspondence between functions provided by the innovative system and actual and future users' needs.
Usability	Usability is related to a set of dimensions characterizing the ease of use of system functionalities (efficiency, ease of learning, man machine interface, errors prevention, satisfaction, etc.).
Acceptability	Acceptability is related to users' attitude and the correspondence between users' values and the innovative technology properties.

demand or a perception of having not enough time or resource to perform goals correctly.

With the perspective of assessing impact of change on stress of individual, source, symptoms and effects of stress are considerate (Flin et al. 2008).

Factors related to activities, demands, individual perception or work and general environment of the individual can create stress (Table 3).

Stressor Factors can create both individual and organisational symptoms. (Table 4).

Effects of stress can also be both individual and organisational. (Table 5).

All these indicators can be used to assess potential impacts of a change on the stress of individuals.

Fatigue can be define as "the state of tiredness that is associated with long hours of work, prolonged periods without sleep, or requirements to work at times that are 'out of synch' with the body's biological or circadian rhythm" (Caldwell et al. 2003). With the perspective of assessing impact of change on individual's fatigue, cause and effects of fatigue are considerate (Flin et al. 2008).

All these indicators can be used to build assessment process for assessing potential impacts of a change on human performance variability.

Table 3. Stressors factors.

Indicators	Description
Job demands	Too much, or too little time to complete tasks
	Too little or too much training for the job
	Boring or repetitive work, or too little to do
	Working environment (temperature, noise, etc.)
Control	Lack of control of work activities
	Lack of involvement in decision making
Superviser/ manager	Lack of support from manager and co-workers
	Unrealistic goals
Relationships	Poor relationships with others
	Bullying, racial or sexual harassment
Role	Uncertainty about work objectives and lack of clarity about responsibilities
	Staff feeling the job requires them to behave in conflicting ways
Change	Uncertainty about what is happening at work
	Fears about job security
	Restructuring of the job
Home: work interface	Family problems
	Dual-career marriages
	Life crises

Table 4. Symptoms factors.

Indicators	Description
Individual	Behavioral (absenteeism, abuse of drugs or alcohol, hostile behavior, apathy, distracted, etc.)
	Emotional (anxiety, cynicism, depression, irritability, etc.)
	Somatic (decline in physical appearance, chronic fatigue, infections, health complaints, etc.)
	Thinking (lack of concentration, reduced attention, difficulty in remembering, failures in planning, etc.)
Organizational	High absenteeism
	High labor turnover
	Poor quality control

Table 5. Effects of stress factors.

Indicators	Description
Individual	Physical ill-health
	Mental ill-health
	Burn out
Organizational	Apathy
	Chronically poor performance
	Frequent/severe accidents
	Prolonged strikes

Table 6. Fatigue cause and effect factors.

Indicators	Description
Cause of fatigue	Long hours of work
	Lack of sleep
	Stress
	Temperature extremes
	Noise
	Physical work
	Vibration
Effect of fatigue	Cognitive performance (reduced ability to cope with unforeseen rapid changes, less able to adjust plans, tendency to adopt more rigid thinking and previous solution, acceptability of lower standards of performance, etc.)
	Motor skills (less coordination, poor timing, etc.)
	Communication (difficulty in finding and delivering the correct word, speech is less expressive, etc.)
	Social (become withdrawn, more acceptance of own errors, less tolerant of others, neglect smaller tasks, less likely to converse, increasingly irritable, distracted by discomfort, etc.)

Next section will be dedicated to the presentation of a set of data collection process that can be used to structure assessment.

5 HUMAN—BASED CONSEQUENCES OF CHANGE ASSESSMENT MODULES

Indicators characterized in the precedent sections are used for realizing assessment modules.

Three types of assessment are considered:

- **"Before change" assessment**. Identification of potential consequences of change on system safety performance is realized before the occurrence of the change. Identification process of potential impact is based on systems' experts and end users perceptions of the change and of its potential consequences.
- **"During change" assessment**. Identification of potential consequences of change is realized during the change management process. Identification is based on the study of systems' experts and end users perceptions after the start of the change process or on the conduct of a pilot study.
- **"After change" assessment**. Identification of potential consequences of change is realized after the change management process. Identification is based on the study of systems' experts and end users perceptions after the change.

Two types of methods are proposed for building the assessment modules. Focus Group for studying impacts of change before, during and after the conduct of the change and human factors assessment methods for assessing impacts of changes during and after the conduct of the change.

5.1 *Focus group*

Focus groups are structured, attentively moderated group discussions that reveal a target audience's conscious preferences, recalled experiences, and stated priorities (Goodman et al. 2012).

Focus groups are good for finding desires, motivations, values and firsthand experience; Understanding fundamental issues and perceptions; Get attitudes and perceptions, thoughts and feeling; Identify and prioritize features of a product and Brainstorming.

Focus groups are not good for getting general information on usability as this can vary much among individuals and getting numerical results, which can be generalized, to a larger public.

The organization of a Focus Group requires defining:

- **The schedule**. In order to be successful, a focus group requires time for preparation and time for data analysis. The definition of a schedule allowing appropriate time for each step is important.
- **The target audience and scope**. The selection of the people that will participate to the focus group and the definition of the groups are important to have a climate allowing free exchanges and discussions.
- **The topics**. The definition of the topics of the focus group, based on the strategy of assessment will support the writing of the discussion guide that will help the animation of focus group.

With the perspective of identifying consequences of change, focus group can be used to get people perceptions about the new technology, the new organization or the new regulation. Organizing Focus Groups with representative of the different activities of a domain allows collecting elements about their perception about the pertinence of the change, the potential change resistances forces or the complementary actions to be followed in order to support the change process.

Focus group dedicated to the identification of potential consequences of change can be completed with the application of specific human factors assessment methods

5.2 *Human factors assessment methods*

Various human factors assessment methods can be applied with the perspective of identifying consequences of changes. Situation awareness measurement techniques and discusses in this section.

Situation awareness is related to the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future (Endlsey 1995a). Different methods exist for studying situation awareness three approaches are presented thereafter.

SART (Situation Awareness Rating Technique) method (Taylor 1990) aims to assess ten dimensions related to situation awareness: Familiarity of the situation, complexity of the situation, focusing of attention, variability of the situation, information quantity, arousal, instability of the situation, information quality, concentration of attention and spare capacity.

Participants of the assessment perform a scenario and at key moments they are asked to rate the ten dimensions with a scale of one (low) o seven (high).

SAGAT (Situation Awareness Global Assessment Technique) method (Endsley 1995b) aims to assess three key dimension of situation awareness: Perception of the elements, Comprehension of their meaning and Projection of future status. A set of questions is defined after a task analysis and participants are asked to answer to them during freezes time of a simulation scenario.

SACRI (Situation Awareness Control Room Inventory) method (Hogg et al. 1995) is an adaptation of SAGAT method to assess situation awareness in control rooms. Assessment is based on three types of questions: Comparison between the current situation with that of the recent past, Comparison between the current situation with normal operations and Prediction of future situation developments.

5.3 *Preliminary experimentations*

Experimentation has been conducted with preliminary version of the method and of assessment modules.

First application was the study of a prototype of 3D chart for transport industry. Diagnostic of technology acceptance issues with focus group sessions and a set of simulation for assessing potential impacts on human factors in general and more specifically on operator situation awareness were conducted (Rigaud et al. 2012).

Second application was the study of the use of drones to monitor pipeline threats. Study of technology acceptance issues with focus group sessions and the potential of occurrence of emerging risks with role games were conducted (Zarea et al. 2013a, Zarea et al. 2013b).

Experimentations demonstrate the relevance of the approach. Nevertheless, dimensions to be improved have been identified related to the definition of experimentations protocol and of the use of the data collected to define recommendation for the change management process.

6 CONCLUSION AND PERSPECTIVES

Finality of this paper is to present preliminary results of a research project aiming to understands risks analysis during change issues and to develop a methodological framework to support assessment in helping to take in consideration human and organizational factors.

A methodological framework structured with four main phases is proposed. Application of the method is based on a set of data collection and performance modules. Current status of the development of the modules is discussed in the paper with the identification of dimensions to be considered for assessing impacts of a change on human performance and with the definition of an assessment framework aiming to support the assessment of impact on change on the Situation Awareness non technical skill before, during after the change conduct process.

Next phases of the work are the development and the experimentation of equivalent module for other non-technical's skills and for organizational capabilities.

ACKNOWLEDGMENTS

Authors wanted to thanks industrial partners of the Industrial Chair on Safety and Resilience of Mines ParisTech: SNCF, TOTAL, GDFSUEZ and AFNOR and to the "Provence Alpes Cotes d'Azur" region.

REFERENCES

Autissier D., Bensebaa F., Moutot J.M., 2012. "Les strategies de changement: l'hypercube du changement gagant", Dunod.

Best J., 2007. "Social Problems" W.W. Norton & Co.

Collerette P., Delisle G. and Perro R., 1997. Le changement organisationnel: Théorie et pratique. Presse de l'Université du Québec, p. 173.

Endsley M.R. 'Measurement of situation awareness in dynamic systems', Human Factors, 37, pp. 65–84.

Endsley M.R. 'Toward a theory of situation awareness in dynamic systems', Human Factors, 37, pp. 32–64.

Flin R., O'Connor P. & Chrichton M., 2008. Safety at the sharp end. A guide to non-Technical Skills, Ashgate, United Kingdom.

Goodman E., Kuniavsky M. & Moed A., 2012. "Observing the user experience, A practitioner's guide to User Research", Morgan Kaufmann.

Grouard, Benoit et Meston, Francis, 1998. L'Entreprise en mouvement: conduire et réussir le changement. Dunod, 336 p.

Hogg D.N., Folesso K., Strand-Volden F. & Torralba B., "Development of a situation awareness measure to evaluate advanced alarm systems in nuclear power plant control room", Ergonomic, 38(11) pp. 2394–2413.

Hollnagel E., 1998. Cognitive Reliability and Error Analysis Method, CREAM, Edition Oxford: Elsevier Science.

Hollnagel E., Pariès J., Woods D.D. & Wreathall J., 2011. Resilience Engineering in Practice. Ashgate Studies in Resilience Engineering.

Hollnagel, E., 2009. The ETTO Principle: Efficiency-Thoroughness Trade-Off. Why Things That Go Right Sometimes Go Wrong. Ashgate: Farnham, UK.

Hollnagel, E. & Woods, D.D., 2005. Joint Cognitive Systems: Foundations of Cognitive Systems Engineering: An Introduction to Cognitive Systems Engineering. Boca Raton: CRC Press.

Lazarus, Richard S. et Folkman, S., 1984. Stress, appraisal, and coping. New York: Springer, 445 p.

Macionis J.J., 2005. "Social Problems" (2nd ed.), Upper Saddle River, NJ: Pearson Prentice Hall.

Renn, O. & Walker, K.D., 2008. Global Risk Governance: Concept and Practice Using the IRGC Framework. Dordrecht: Springer.

Rigaud E., Lützhöft M., Kircher A., Schroder-Hinrichs J.W., Baldauf M., Jenvald J., & Porathe T., 2012. «Impact: More Than Maritime Risk Assessment », Procedia—Social and Behavioral Sciences, Volume 48, pp. 1848–1854.

Salas E., Driskell J.E. & Hughes S., "Introduction; the study od stress and human performance. In Driskell J. and Salas E.(eds). Stress and Performance (pp. 1–46). Hillsdale, NJ:Lawrence Erlbaum.

Spector M. & Kituse J.L., 1997. "Constructing social problems". Menlo Park, CA: Cummings.

Taylor R.M., "Situational Awareness Rating Technique (SART): The development of a tool for aircrew systems design", un Situational Awareness in Aerospace Operations (AGARD-CP)478, pp 1–17., Neuilly sur Seine, France: NATO-AGARD.

Terrade, F., Pasquier, H., 2009. Reerinck-Boulanger, J., Guingouain, G. & Somat, A. L'acceptabilité sociale: la prise en compte des déterminants sociaux dans l'analyse de l'acceptabilité des systèmes technologiques. *Le Travail Humain, 72*, 383–395.

Weick, K.E. & Sutcliffe, K.M., 2001. Managing the unexpected: assuring high performance in an age of complexity. San Francisco.

Westrum, R., 1991. Technologies and Society. Belmont, California: Wadsworth Publishing.

Zarea M., Pognonec G., Lecchhi M., Lana J.A., Sohlbach M., Scholtz A., Rigaud E., & Mazri C., «Anticipating Risks of Innovative Safety Barriers: Findings on an Automated Aerial Surveillance System», Proceedings of the 5th IntegRisk Conference 'Horizon 2020: From Integf-Risk Radar to the European Emerging Risk Radar'.

Zarea M., Pognonec M., Schmidt C., Schnur T., Lana J., Boehm C., Buschmann M., Mazri C., & Rigaud E., 2013. «First steps in developing an automated aerial surveillance approach». *Journal of Risk Research,* 16 (3–4), 407–420.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Modeling and assessment of Performance Shaping Factors in construction

Y. Xenidis & K. Giannaris
Department of Civil Engineering, Aristotle University of Thessaloniki, Thessaloniki, Greece

ABSTRACT: Human reliability is a key issue for ensuring safety in all industries; however, while it has been thoroughly studied in other industries, limited research has been conducted in the construction industry. This paper constitutes a first step towards the development of a methodology for identifying, analyzing and calculating the significance of Performance Shaping Factors (PSFs) in the context of worksite operations of civil engineering projects. The adopted approach differs from the established methods, in terms of architecture and concept. The method classifies PSFs in three categories, namely organizational, human and environmental and maps with the help of network analysis their relations in respect with the occurrence of a specific human failure incident. The method's last stage is to quantify the significance of each PSF to the occurrence of the human error. It is anticipated that further development of this method will allow HRA's successful application in the construction industry.

1 INTRODUCTION

Human reliability is a critical parameter for safety and security in all industries. It is estimated that 70%–90% of all types of failures in all types of activities are directly or indirectly related to human error (Li et al. 2012). In the nuclear industry human-induced failures are 90% of the total recorded failures (French et al. 2011); this percentage is more than 80% for the chemical and petrochemical industry (Kariuki & Löwe 2007, French et al. 2011, El-Ladan & Turan 2012), 80%–90% for the marine and offshore industry (El-Ladan & Turan 2012, Kounavos 2012, Sundaramurthi & Smidts 2013), 60%–90% for the aviation industry (French et al. 2011, El-Ladan & Turan 2012), and 75% for infrastructure such as water supply, dams, buildings and bridges (French et al. 2011, Kounavos 2012).

Although automation would be expected to reduce the effect of human reliability on production processes, simply because it limits both the presence of humans and their level of impact on production, it seems that the exact opposite happens. On the one hand, the complexity and power of technological, automated and information systems is constantly raising, thus hardening their use and increasing the requirements for employees with special knowledge, skills and training to operate these systems; on the other hand, the increased level of control of several processes, which is achieved due to automation exceeds by far the level of control of the rest, human-dominated, processes, thus rendering the latter more critical than in the past. Therefore, Human Reliability Assessment (HRA) remains a critical parameter in production processes.

The last 50 years extensive research has been conducted with regard to HRA, focusing on various aspects, such as definition and modeling of human error, data and information collection and evaluation, HRA techniques, etc. (Groth & Swiler 2013, Kirwan et al. 2008). Several tools and methods have been developed, broadly grouped in three generations (Bell & Holroyd 2009). ATHEANA, CREAM, HEART, OHPRA, and THERP are some of the most applied HRA methods. Despite, the extensive research on the field, the following issues remain challenging and even controversial for researchers and practitioners (Groth & Swiler 2013, Colombo & Demichela 2008, Kennedy et al. 2007, Trucco & Leva 2007):

- Quality of Data. It is widely accepted that various data are required in HRA, which need to be retrieved from various sources such as related data and knowledge bases, experiments, and analysis of the organizational and behavioral structure of the specific organizations investigated per case. So far, a methodology for the integration of data sources for HRA has not been achieved, thus retaining the use of methods, which deal only with a small part of the data required for HRA.
- Inefficiency of exerts' judgments. Data inconsistency and fragmentation frequently renders

experts' judgments as an alternative for conducting HRA. The lack, however, of a robust methodology for the definition and quantification of the various parameters involved results to uncertain outcomes that depend on the experts involved, and the method adopted.
- Lack of consistent human error definition. Human error is defined in many similar yet distinct manners, thus resulting to the lack of a consistent approach for identification and, consequently, taking of response measures.
- Lack of integration of framework factors. It is acknowledged that human error is heavily affected by the working environment, the organizational structure and culture, and cognitive reasons. The difficulty in quantifying these factors results to their indirect introduction in the assessment of human reliability; moreover, these factors are, frequently, introduced to the analysis after the human error quantification stage, thus leading to an inconsistent consideration of the interdependencies between the factors that affect human error.
- Inefficiency in the presentation of human error root-causes. The identification and presentation of the root-causes of human errors would considerably improve HRA, because it would allow deeper understanding of the error-making process, more accurate quantification of the contributing factors, and less subjectivity in the analysis. The difficulties in the systematic and clear mapping of the cause-and-effect relations between technological, human and environmental factors in an error-making process has resulted to their partial inclusion in current HRA methods.
- Inadequate inclusion to the analysis of the positive impact from health and safety measures and proactive human actions. HRA methods, systemically, tend to overlook the effect of precautionary measures, actions and behaviors in the error-making process. This results to the exclusion from HRA of a significant part of the analysis, which renders the whole approach incomplete.
- Inadequate modeling of Errors of Commission (EoC). The number of inappropriate actions or performance failures by humans that may result to human errors, the difficulty of tracking down the impact of such events to an error-making process, and the difficulty to clearly identify the context wherein EoCs occur has resulted to their incomplete and inadequate modeling in current HRA methods.

The challenge to deal with the abovementioned issues motivated the research effort presented in this paper; however, HRA methods' improvement was not the single goal to pursue in this research. A literature review revealed that HRA methods are scarcely applied in the construction industry, which is an unexpected observation given that construction is: a) the sector with the worst performance in terms of occupational safety and health, worldwide (Eurostat Statistics Explained 2014, OSHA 2014), and b) a field of activity where human errors are by far the first reason for the occurrence of failures and accidents (Health and Safety Executive 2003).

Construction industry processes differ significantly from chemical, nuclear or aviation industry processes, where current HRA methods are mainly applied. A construction site is completely different from a nuclear or chemical plant in the following terms:

- Construction works are not automated, since normal construction equipment is mainly operated by humans.
- Construction site conditions are dynamic in nature and develop rapidly, thus limiting the capacity to response, in case of failures or accidents. Moreover, construction site conditions, are mainly determined by the performance and actions of the construction site personnel; in most of the cases, these actions and performance are neither standard, nor predictable due to the nature of the work that allows even for ordinary workers a certain level of initiative in everyday practice.
- Construction sites are open systems, which are affected by factors that very often are not controllable (e.g. supply chains) and even not predictable (e.g. weather).

Based on all the above, it is inferred that the application of HRA in construction industry is a challenging task, since it requires innovation to, concurrently: a) form an approach that will try to overcome the various inherent deficiencies of existing HRA methods, and b) apply it on a field where little, if any, experience is available. This paper is a step in performing this challenging task that focuses on the identification and modeling of Performance Shaping Factors (PSFs) in construction. The remaining of this paper is organized in the following way: Section 2, provides some necessary background in HRA that sets the theoretical framework of this research. Section 3 presents the proposed method for modeling PSFs in construction, while Section 4 presents a demonstration example of the method. The conclusions of this work are presented in Section 5.

2 BACKGROUND IN HUMAN RELIABILITY ASSESSSMENT

HRA has attracted much interest from researchers and practitioners, which have formed a theoretical

and methodological background that is not always clear even with regard to the fundamentals (e.g. definitions). This is normal, especially when the field is highly complicated and involves many uncertainties. In these cases, any new attempt to apply HRA requires first a brief review of the existing working definitions. Subsections 2.1 and 2.2 serve this requirement.

2.1 *Definition and classification of human error*

Error is probable in any human activity, just because human actions are highly unforeseen and interactive in every context, thus creating the condition for errors to occur (El-Ladan & Turan 2012). The occurrence of a human behavior largely depends on the interpretation of the environment, the available information, the existing constraints and the motivation of the individual (Monferini et al. 2013). In this context, several definitions have been assigned to human error (Moriyama and Ohtani 2009, Kounavos 2012). A working definition in the context of this paper is that "human error is any human activity that solely or in combination with other activities increases the probability of occurrence or the consequence of a risk". It must be noted that this definition expands the usual interpretation of error from something directly associated to some sort of failure to something that could potentially result to a failure. This context allows considering as errors, all those actions that may not be perceived in this way at the time of their occurrence, but have an undoubted impact on the forthcoming failure. This is very valuable, especially, for the construction industry, where the lack of standardized production procedures often conceals the factors that contribute to the occurrence of an error.

Human error is classified based on type, consequence, failure modes, root-causes, etc. Some of those classes of error are (Moriyama & Ohtani, 2009, Kim & Park 2012, Kounavos 2012):

- Random vs. systemic, depending on whether the error is caused by random factors or the functional mode of the system.
- Internal vs. external, depending on whether the error is caused by cognitive functions or environmental factors.
- Obvious vs. hidden, depending on whether the error's consequence is directly perceived or in a relatively long period after the error's occurrence.
- Procedural vs. organizational, depending on whether the error is caused by a deviation from a course of action or organizational inefficiencies.
- Errors of Omission vs. Errors of Commission, depending on whether the error is caused by the omission of some planned actions or the commission of some redundant or inappropriate actions.

It is obvious that an error belongs simultaneously in various classes (i.e. systemic, internal, hidden, organizational, EoC) and that may be an obstacle for an efficient modeling in the context of HRA. This is the reason why these classifications constitute—in most of the cases—significant parameters in the development of a theoretical or methodological approach for HRA.

2.2 *Performance shaping factors*

Performance Shaping Factors (PSFs) are used to describe the various situational, organizational and personal causes that influence human behavior. They are defined and, even, named differently in the context of different HRA methods (Kim & Jung 2003, Petkov et al. 2004, Marhavilas et al. 2011) and this prevents from establishing a credible and widely accepted group of PSFs for general application. Therefore, it is common practice for researchers or practitioners to form the appropriate group of PSFs in a customized manner depending on the HRA model's requirements, the field of application and the analysts' approach (Kim & Jung 2003, Groth & Mosleh 2012).

While PSFs vary between different HRA methods, certain issues concerning the selection and use of them are quite common in every approach. These issues include (De Ambroggi & Trucco 2011):

- The definition of PSFs according to the level of analysis. In some cases, PSFs are not distinct in clarifying by definition whether they correspond to individual or team errors. This results to inclusion of PSFs of different level of analysis in the same model, which normally should be avoided.
- The interdependencies between PSFs. In all cases, many PSFs interact with other PSFs by affecting either their weights or directly their values. The type as well as the level of interdependency between two or more PSFs needs to be considered in the analysis.
- The existence of latent PSFs. Some PSFs are very hard to identify, mainly because they are hardly quantifiable. These latent PSFs can be measured indirectly through certain behaviors and actions that correspond to them.
- The connection between PSFs and failure mechanisms. In many cases, PSFs are, falsely, considered as error causes, while, in fact, they are measures of a condition.
- The scarcity of certain PSFs. In some cases, certain PSFs are met so rarely that no data exist for them with regard to their level of influence.

In these cases experts' judgments are the only source of useful information.
– The inherent properties of certain PSFs. In many cases, PSFs have by definition a positive or negative content that, respectively, influences the analysis; therefore, depending on the PSFs used in a particular method, this may be biased.

The knowledge of the issues concerning PSFs facilitates their proper introduction in the HRA method, which is proposed in this paper.

3 A METHOD FOR HUMAN RELIABILITY ASSESSMENT IN CONSTRUCTION

As mentioned in Sections 1 and 2, a major source of inefficiencies in HRA methods is the appropriate modeling of PSFs, which is a difficult task, in the first place. This research proposes: a) a systematic identification of the organizational, environmental and personal factors that have an impact on human errors in construction, and b) an evaluation procedure concerning the significance of each one of these factors. Subsections 3.1, 3.2 and 3.3 present the proposed method in this research.

3.1 *Identification and parameterization of performance shaping factors in construction*

In this research PSFs are organized in three major groups, namely organizational, situational and personal factors. This categorization is consistent with the standard approach for grouping PSFs, which has been applied in many previous cases (Marhavilas et al. 2011).

In complex situations the influences between PSFs may or may not be reciprocal. For example, while an organization factor affects the performance of a construction crew, the opposite does not happen. This means that, while the significance of the construction crew PSFs could be moderated by appropriate treatment of the organizational PSFs, the opposite is not feasible (Hallbert et al. 2004). Therefore, in the context of this research two types of influences are considered: a) those between PSFs in the same category, and b) those between PSFs from different categories according to the hierarchy shown in Figure 1.

The specific PSFs included in each one of those categories are not strictly defined. Unlike most other methods, it is considered that the PSFs set should not be standardized, but left free for the analyst to define it according to the situation in hand and a specific method, which is presented in subsection 3.3. This approach is considered effective given: a) the absolute lack in the literature of PSFs for the construction industry, and b) the characteristics of construction projects as presented in Section 1. As a working PSFs set, this research has adopted the one presented by Li et al. (2012), which with some slight modifications was evaluated as the most sufficient between the investigated sets for use in the construction industry.

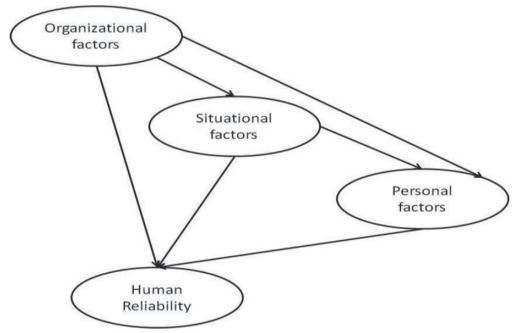


Figure 1. PSFs influence hierarchy.

3.2 *Construction of the performance shaping factors' influence tree*

PSFs influence the occurrence of a human error and their interaction determines the respective mode of failure. This can be represented by an influence tree, which requires the definition of the potential error. The selection of the appropriate PSFs from the respective set may follow the procedure of fault or event trees. The procedure has two stages, namely the pre-selection and the selection stages.

The pre-selection stage involves the selection of PSFs based on the evaluation of the analyst with regard to the influence they have to the investigated error. The following requirements must be met at this stage:

– All PSFs must refer to the same time band. The various PSFs present a different scale of reference in terms of development over time; however, it is ineffective for any method to include PSFs that are inaccurately defined in the analysis' period of reference.
– All PSFs are introduced to the analysis in a neutral state. This state is either the normally anticipated effect of the PSF or a state of zero effect, if the PSF does not fall in the first category.

The selection phase is conducted, based on the following assumptions:

– Human reliability has a high top boundary value. This assumption allows the consideration of behavior determinants (i.e. feelings, circadian rhythm), which are completely irrelevant to the

working environment, but, which may easily have an impact to an error occurrence.
– The error is known or considered as known in advance (i.e. prior to the analysis).
– The state of all PSFs can be evaluated; since the error is known or considered as known, a certain value for each influencing PSF should be, also, assigned to it.

The rules applied to select the appropriate PSFs in the analysis are the following:

– The selection includes only those PSFs, which have a direct impact to the downstream nodes. Those PSFs may be included in any one of the three categories as long as this category is prior (upstream) to the one where the node under investigation lies in.
– The selection includes only PSFs that at their final state, i.e. after the influences of other PSFs have been taken into account, is remote from the neutral state.

The selection follows a bottom-up approach, i.e. a direction from the error to the sources of its occurrence. When all PSFs of a certain category (e.g. personal) are identified, those of them, which have a negative influence to the error occurrence, are distinguished in two classes: a) Class A, which includes those PSFs that worsen the condition of the PSFs they affect, and b) Class B, which includes those PSFs that fail to exercise their positive influence to PSFs they affect. The transition to the upper PSFs level involves only those PSFs of the first class, while the rest PSFs are mapped for completeness but are not introduced into the network's calculations.

The final outcome of this process is a network like the one presented in Figure 2.

In the network of Figure 2: a) the circle represents a PSF with a positive influence to the connected PSF, while the rectangular represents a PSF with negative influence to the connected PSF, b) the solid line arrows represent a connection between PSFs of Class A, while the dashed arrow represents a connection of Class B.

Note that in Figure 2, PSF9 appears twice one with a negative and one with a positive effect to PSF7 and PSF4, respectively. The multiple appearance of a PSF in the network is feasible, since this PSF, in each repetition, is related with a different PSF. The potential of multiple appearances of a PSF at the same hierarchical level necessitates the measurement of the frequency of appearances at a certain condition (i.e. positive or negative) in the same time band.

Another issue is the importance of the influence a PSF exerts to another PSF. The importance measure of a PSF responds to the question of how much does one appearance of a PSF influences the frequency of appearance of the downstream PSF. The multiplication between a PSF's frequency and importance measures provides the measure of significance of this PSF.

The simple network described in Figure 2 could become much more complicated under specific circumstances, such as the following:

– A PSF could appear in multiple duplicates in several relations. All these duplicates are unified upstream at a single node as in Figure 3.
– Three PSFs could constitute a loop in the network. Loops should not appear in the network; therefore multiple duplicates of a node should be introduced, according to the example of Figure 4.
– A PSF could appear in multiple states in the network. In this case, the PSF is not introduced in duplicates, but for each state a different node is introduced.
– Several PSFs may have similar definition or function in the network. For example "Time Availability" may refer to several network parts with a different content in each one of these parts. This situation should be avoided by properly defining each PSF in the first place.

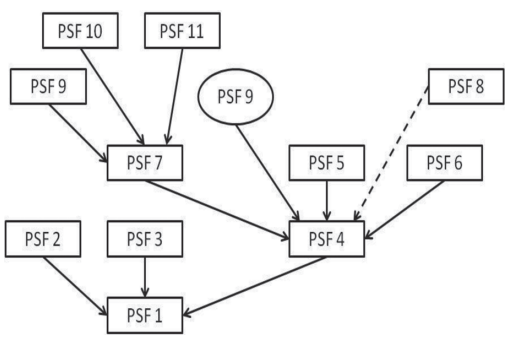


Figure 2. An example of a PSFs influence tree.

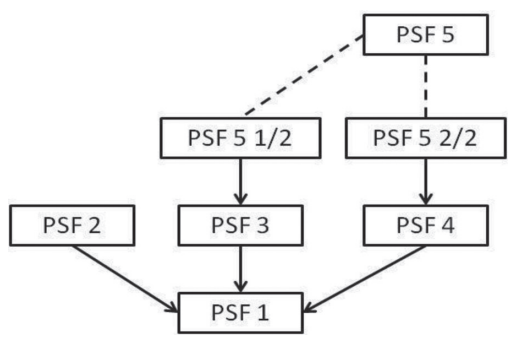


Figure 3. An example of a PSFs influence tree.

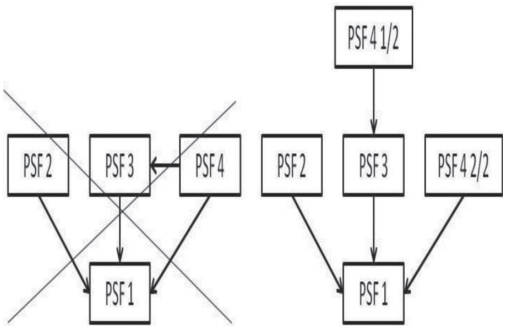


Figure 4. False and correct networks with regard to loops.

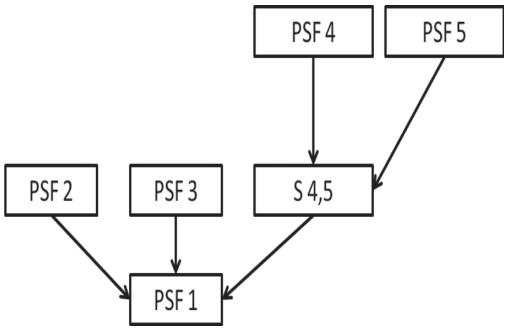


Figure 5. Representation of a situational node in the network.

– Several PSFs may have a decisive contribution to the failure mode of a downstream PSF, in such a way that their omission could automatically cancel this failure mode. This situation is tackled by introducing another type of node to the network, namely the "situational (S) node", whose frequency is the product of the multiplication of the frequencies of the converging nodes and importance is defined according to frequency measure. A case of a situational node in a network is presented schematically in Figure 5.

3.3 *Assessment of the significance of each performance shaping factor*

The quantification part of the proposed method is related to the assessment of the significance of the various PSFs that are included in the network. For this purpose an assessment card as shown in Figure 6 is filled for each PSF.

In the assessment card cells (1) to (3) are filled according to the developed network. It should be noted here that the copy number is the unique number of the specific duplicate of the PSF, which

(1) Ref. No	(2) PSF Name	(3) Duplicate Number
(4) Linguistic Description of Importance		(6) Linguistic Description of Frequency per Time Unit
(5) PSF State		(7) PSF Frequency per Time Unit
(8) Relative Importance (%)		(9) Product (7) x (8)
(10) Nodal Relative Significance		(11) Total Relative Significance

Figure 6. The PSF assessment card.

is presented in the form x/n, where x is the number of the duplicate and n is the amount of the duplicates for the particular PSF. Cells (4) to (7) are filled based on expert judgment, previous experience or available data, while cells (8) to (11) are calculated in the following way:

– The relative importance of a PSF (cell 8) is determined after the application of the AHP method, where experts compare the influence of a PSF to the downstream PSF's to determine which one of the latter is mostly influenced by the calculated PSF. The calculated influence, which has the form of a percentage, constitutes the relative importance of the PSFs that converge at a single node.
– The PSF's significance is calculated as the product of the values in cells (7) and (8), according to the proposed definition in subsection 3.2.
– The convergence of several PSFs at a node requires the determination of the specific PSF's significance; therefore, the calculated value in cell (9) is divided by the sum of all significance values of the PSFs that converge at the node. This new value (cell 10), which again has the form of a percentage, constitutes the PSF's nodal relative significance.
– The total relative significance for each PSF (cell 11) is calculated according to the network by multiplying each PSF's nodal relative significance with the total relative significance of the connected downstream PSF. In this way, the total significance of each PSF is determined up to the point of the error occurrence (the first node in the network).

In the assessment of the PSFs significance it should be noted that:

– The significance of a PSF with multiple duplicates is the sum of the values of significance of each duplicate.
– Situational nodes are also assessed with the same card, but the propagation of the total significance is inversely proportional to the parent nodes' frequency values. This is because of the method's orientation to the chances of dealing

with the potential error, which renders the rarest between, e.g. two causes of error, as more significant than the other.

4 AN APPLICATION EXAMPLE OF THE PROPOSED METHOD

The method's application is presented in a hypothetical example for demonstration.

Suppose that the seal of an equipment device, which is sensitive to water, is left open as a result of human negligence. This is the case of a human error that could evolve to a risk occurrence and the proposed method seeks to identify the reasons for this source of risk.

For the example, suppose that ten PSFs are identified as contributors to the human error occurrence. The time band is set to eight working hours, and the identified PSFs are presented in the corresponding network of interdependencies in Figure 7.

Each PSF is defined in terms of content and state. For example the "Maintenance planning" PSF's neutral state is set to "Normal operation", while the real state met, based on the example, is "Slightly problematic". All the PSFs in the network are defined in the same way.

The determination of the states for each PSF modifies the network as shown in Figure 8.

The updated network introduces the "Language understanding" PSF, as positive, instead of negative influencing factor for the downstream PSF.

Once the network is finalized, the next step is to fill the assessment cards of all active PSFs. An indicative card for the PSF "Level of Noise" is presented as an example in Figure 9.

The results of the total relative significance of all PSFs as they are derived from the assessment cards are summarized in Figure 10.

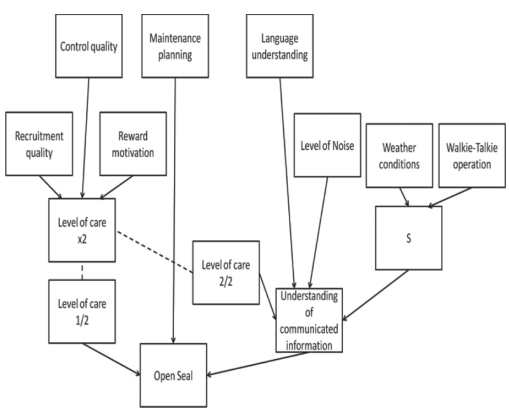


Figure 7. The network of the demonstration example.

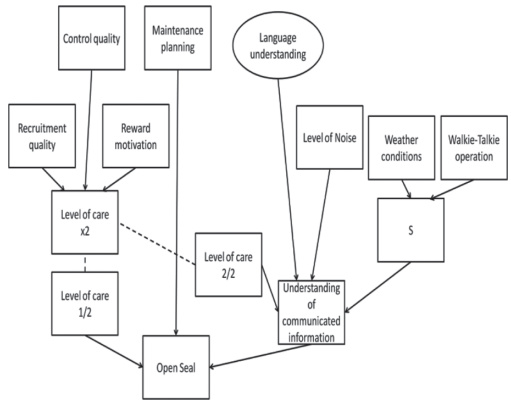


Figure 8. The modified network after the determination of states for each PSF.

4	Level of Noise	-
Noise often causes a slightly problematic communication		The site is noisy 4 hours per day
Noisy		0,5
39%		0,195
42%		19,95

Figure 9. An example of a filled assessment card.

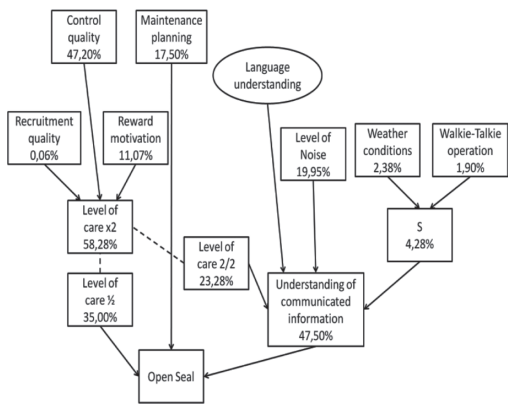


Figure 10. The final results of the PSFs' significance in the network.

As shown in Figure 10, the level of care is the most important factor and is mostly influenced by the quality of control in the site. Therefore, to avoid similar future human errors the construction manager should pay attention to the quality of control processes in the site, in order to minimize the risks from the lack of care on behalf of the workers.

5 CONCLUSIONS

Current HRA methods despite their evolution since the first generation are, still, far from being considered as accurate or generally applicable. Especially in the construction industry, which is characterized by complexity in the production process, current HRA methods are inefficient and, therefore, inadequate.

Taking into consideration the accumulated knowledge on the field, this paper proposes a method to model and assess performance safety factors in construction. The method comprises three basic steps, namely the identification of the PSFs, the creation of the network of interactions between the identified PSFs, and the assessment of the PSFs significance, in terms of impact to the downstream connected PSFs.

This method tries to tackle several issues that current HRA methods have inadequately treated; however, it still requires further development to achieve this goal. The method's current disadvantages are the heavy computational effort that may be required in the case of a very complicated network and the huge dependence on the initial development of the influence network. Moreover, a refinement of the assessment process may be required especially with regard to certain parts of the modeling, such as the copies or the situational factors.

Further improvements and research that will entail the method's performance in real cases and the algorithmic approach for the solving of the network are planned in this ongoing research, which intends to provide a new human reliability assessment method for application in the construction industry.

REFERENCES

Bell, J. & Holroyd, J. 2009. *Review of human reliability assessment methods*. London: Health and Safety Executive.

De Ambroggi, M. & Trucco, P. 2011. Modelling and assessment of dependent performance shaping factors through Analytic Network Process. *Reliability Engineering & System Safety*, 96(7): 849–860.

El-Ladan, S.B. & Turan, O. 2012. Human reliability analysis—Taxonomy and praxes of human entropy boundary conditions for marine and offshore applications. *Reliability Engineering & System Safety*, 98(1): 43–54.

Eurostat Statistics Explained 2014. *Health and safety at work statistics.* [online] Available at: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Health_and_safety_at_work_statistics#. [Accessed 06 April 2014].

French, S., Bedford, T., Pollard, S.J.T. & Soane, E. 2011. Human reliability analysis: A critique and review for managers. *Safety Science*, 49(6): 753–763.

Groth, K.M. & Mosleh, A. 2012. A data-informed PIF hierarchy for model-based Human Reliability Analysis. *Reliability Engineering & System Safety*, 108: 154–174.

Groth, K.M. & Swiler, L.P. 2013. Bridging the gap between HRA research and HRA practice: A Bayesian network version of SPAR-H. *Reliability Engineering & System Safety*, 115: 33–42.

Hallbert, B., Gertman, D., Lois, E., Marble, J., Blackman, H. & Byers, J. 2004. The use of empirical data sources in HRA. *Reliability Engineering & System Safety*, 83(2): 139–143.

Health and Safety Executive 2003. *Causal factors in construction accidents*. London: Health and Safety Executive.

Kariuki, S.G. & Löwe, K. 2007. Integrating human factors into process hazard analysis. *Reliability Engineering & System Safety*, 92(12): 1764–1773.

Kim, J. & Park, J. 2012. Reduction of test and maintenance human errors by analyzing task characteristics and work conditions. *Progress in Nuclear Energy*, 58: 89–99.

Kim, J.W. & Jung, W. 2003. A taxonomy of performance influencing factors for human reliability analysis of emergency tasks., *Journal of Loss Prevention in the Process Industries* 16(6): 479–495.

Kirwan, B., Huw Gibson, W. & Hickling, B. 2008. Human error data collection as a precursor to the development of a human reliability assessment capability in air traffic management. *Reliability Engineering & System Safety*, 93(2): 217–233.

Kounavos, M. 2012. *Human error and human reliability assessment methods*. MSc thesis, Thessaloniki: Aristotle University of Thessaloniki.

Li, P., Chen, G., Dai, L. & Zhang, L. 2012. A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks. *Safety Science*, 50(7):1569–1583.

Marhavilas, P.K., Koulouriotis, D. & Gemeni, V. 2011. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009. *Journal of Loss Prevention in the Process Industries*, 24(5): 477–523.

Monferini, A., Konstandinidou, M., Nivolianitou, Z., Weber, S., Kontogiannis, T., Kafka, P., Kay, A.M., Leva, M.C., and Demichela, M. 2013. A compound methodology to assess the impact of human and organizational factors impact on the risk level of hazardous industrial plants. *Reliability Engineering & System Safety*, 119: 280–289.

Moriyama, T. and Ohtani, H. 2009. Risk assessment tools incorporating human error probabilities in the Japanese small-sized establishment. *Safety Science*, 47(10): 1379–1397.

Occupational Safety & Health Administration (OSHA) 2014. *Top ten most frequently cited standards.* [online] Available at: https://www.osha.gov/Top_Ten_Standards.html [Accessed 06 April 2014].

Petkov, G., Todorov, V., Takov, T., Petrov, V., Stoychev, K., Vladimirov, V. & Chukov, I. 2004. Safety investigation of team performance in accidents. *Journal of hazardous materials*, 111(1–3): 97–104.

Sundaramurthi, R. & Smidts, C. 2013. Human reliability modeling for the next generation system code. *Annals of Nuclear Energy*, 52: 137–156.

Trucco, P. & Leva, M.C. 2007. A probabilistic cognitive simulator for HRA studies (PROCOS). *Reliability Engineering & System Safety*, 92(8): 1117–1130.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, *ISBN 978-1-138-02681-0*

The impact of the use of subcontracting on organizational reliability and safety

C. Guers, C. Martin & J.L. Wybo
Centre de Recherche sur les Risques et les Crises (CRC), Mines ParisTech, Sophia Antipolis, France

ABSTRACT: Subcontracting has become very widespread in contemporary socio-technical systems. It takes many forms and leads us to think again about the nature of the workforce. This article takes a new look at organizational boundaries in terms of the concept of businesses that are extended through subcontracting and its implications for safety culture. First we present a comprehensive, state of the art typology of the current forms of subcontracting, which have been developed to meet the needs of productive organizations. Then we focus on the effects of this type of indirect management on the effectiveness and reliability of organizations and more specifically, the workforce.

1 INTRODUCTION

Since the beginning of the twentieth century, we have seen a change in the way businesses are organized. Until the end of the 1970s an integrative model dominated. Under this model companies themselves were responsible for most of the manufacturing of the final product and all production functions were integrated. In the early 1970s, companies became large corporate networks (a multi- or poly-cellular model). The contracting company headed the network; it was only responsible for a very limited part of production/manufacturing and was surrounded by a network of suppliers/partners.

This new model can be seen as offering the best prospects in an increasingly unstable economic context. Nowadays it takes many forms: the extended organization (Benchimol 1993; Capraro & Baglin 2002; Perez 2007; Defelix & Picq 2013), the fragmented organization (Hatzfeld 2000; Berger 2005), the network organization (Veltz 2000; Roy & Audet 2002; Rorive 2005; Morley 2005; Mazaud 2006; Pesqueux 2008), the shared organization (Abdul-Nour, Jacob, Julien & Raymond 2003), the enhanced organization (Moreau 2003) or the agile organization (Barrand, Gumb, Badot, Benameur, Blum *et al*. 2010). These new forms are all examples of not only a more flexible and efficient organization, but also new organizational boundaries, a new way of occupying space and new governance mechanisms. They consist of a national and international exterior space and an internal space that is fragmented due to the diversity of actors and skills. In this kind of organization, production is distributed in an orderly manner between partner companies.

These changes in the way businesses operate are fundamentally changing the organization. They are likely to accentuate certain types of organizational risks related to the management of a fragmented workforce distributed across a network, and extended by a constellation of actors (subcontractors, co-contractors or partners). It is important to understand these new organizational forms in order to be able to better predict these changes and anticipate the risks associated with them. The internal organization of a company can become a source of threat. Organizational reliability is based on the strategies of actors who shape production on a daily basis given the organizational constraints they face. In this context, this article examines how the constraints faced by the extended organization can be a source of reliability or risk. The aim is to help organizations that have decided to use subcontractors to improve reliability, and control safety- and security-related risks in the context of relevant research, particularly management systems.

Specifically, we ask how the strategies implemented by individuals shape the efficiency, reliability or risk of extended productive organizations. In the first part of the article we define subcontracting, its different forms and motivations. In the second part we define the extended organization, its characteristics and the risks that are associated with it. Finally, we show the impact of this ambivalent mode of organization on the effectiveness and reliability of the workforce.

2 SUBCONTRACTING

There is no question that subcontracting is one of the key characteristics of the operation of these new

productive organizations and the subcontractor can be thought of as a fully-fledged actor in the system. While the phenomenon of subcontracting is not new, its popularisation is. This phenomenon means two things: On the one hand it has become both widespread and commonplace; the subcontractor cascade has become common practice in many companies. On the other hand it has been extended into a growing number of business operations. In the 1970s it concerned simple tasks such as cleaning and security; since the 1980s it has extended in some companies to the entire production process (the hollow firm). The internal organization and working conditions of companies in many sectors have thus completely changed.

2.1 *Subcontracting and outsourcing*

Subcontracting is one form of outsourcing. A report by the French Social and Economic Council distinguishes between subcontracting and outsourcing in terms of the length of the relationship and the transfer of ownership (activity substitution), "It could therefore be said that subcontracting, unlike outsourcing, partially concerns the provision of a service in a given time and not necessarily over many years and—most importantly—does not imply that the activity was previously undertaken internally. Outsourcing is further distinguished from subcontracting in that it tends to lead to long-term change (by subtraction from the original company to an economic third party) in the boundaries of the company and the structural configuration of its resources. It could be called a 'contractualised' and 'monetised' handover of a function or activity previously included in the internal mode of governance."[1]

The concept of semi-integrated subcontracting (Houssiaux 1957) is based on the principle of substitution and the transfer of ownership of a specific piece of work; however it implies that there are ongoing and stable links. According to Barthélemy (2007, p. 12), the difference between subcontracting and outsourcing is based on the obligations of the service provider. Outsourcing is based on an obligation to provide results; the service provider takes entire responsibility for the management of the outsourced activity. In the case of subcontracting, the client is responsible for the management of the outsourced activity and the service provider merely provides production resources. Nevertheless, subcontractors are also obliged to produce results, and can be seen as the intervention of an external agent on at least three levels: the definition of work, its resources and the procedures put in place to achieve a specified outcome. In some cases, highly-qualified subcontractors may participate in drawing up specifications (Chaillou 1977).

Nevertheless, the difference between outsourcing and subcontracting remains ambiguous. Intercompany links are varied and in many cases go beyond official definitions, which give an incomplete picture of labour relations, "a little like concrete can mask the girders it supports" (Jounin 2006). In a very general and basic way, we define subcontracting[2] as an operation that consists, for a company A, of the delegation to a company B of a task or a function that Company A does not want to or cannot undertake itself.

2.2 *The various forms of subcontracting*

In order to understand the different forms that subcontracting can take within organizations, Chaillou (1977) proposed a typology, in which time is a fundamental characteristic for understanding the relationship between businesses. He distinguishes short-term subcontracting (comparable to occasional, cyclical troubleshooting) and long-term activities that can be compared to permanent, structural or semi-integrated subcontracting that is more akin to outsourcing (Houssiaux in Baudry 2013). The contract frames the length of the relationship between the client and the subcontractor.

At the same time, it is vital to identify areas where subcontracting can be used: on-site, internally or externally. External subcontracting may be local or abroad, known as offshore or delocalized outsourcing (Niang 2013). This practice runs the risks found in both outsourcing and offshoring (Geyer 2007) – loss of control and ownership of one or more delegated activities. In this case, it is up to the organization to decide whether it is in its interests to expand its borders. Ponnet (2011) also distinguishes between the activities carried out on the contractor's premises and those performed externally. She noted that maintenance work is semi-integrated and carried out at the contractor's production facilities.

In cases where subcontracting is carried out in the organization's country of residence, it is

[1]Social and Economic Council (*Conseil économique et social), Conséquences sur l'emploi et le travail des stratégies d'externalisation des activités,* The Official Journal (*Les éditions des journaux officiels*), 2005, p.92.

[2]The French law of 31 December 1975 defines subcontracting as "the operation by which a business entrusts, through a subcontract and under their responsibility, to another person called a subcontractor, all or part of the execution of a business contract or a public tender concluded with the client."

more like classical subcontracting or nearshore outsourcing (Quelin 2007).

When the work is carried out onsite by a foreign contractor, and the subcontractor's company is located in a different country to that of the client, the term onshore outsourcing is used (Samaganova 2008). *In situ* subcontracting is also subject to risk. Jounin (2006) gives examples of field observations where employees of various local companies coexist and work together to achieve the same production objectives. This is an illustration of a constellation of actors where the new interactions fundamentally change the organization's reliability, the division of work and teamwork modalities.

Although subcontracting practices vary from one organization to another, there are two main scenarios that are widely used. In the first scenario the company does not have sufficient production resources and therefore delegates certain functions that cannot be undertaken internally. This is known as 'speciality' subcontracting, where the contractor calls upon a specialist who has the equipment, materials and expertise that meets the needs of the purchaser, because the latter does not have or may not wish to acquire them, for their own strategic reasons[3]. Specialty subcontractors or specialised suppliers (Houssiaux in Baudry 2013) carry out specific operations using their own methods. Their activity is complementary to that of the organization. In the same vein, Barthélemy and Donada (2007) argue that companies are motivated by rapid access to resources and skills that are not available internally. It allows the organization to focus on its main activity (Mazaud & Lagasse 2009) and to delegate ancillary activities. Specialization is subjective and varies depending on the organization as, "their point of reference is their own technical ability" (Chaillou 1977). A specialist is someone who is as (or more) capable than the company itself, while others are seen as 'capacity' subcontractors (see below). Chaillou differentiates specialty subcontracting from 'supply' subcontracting which concerns, "the definition and study of methods to be used to perform a given piece of work." This type of subcontracting involves a high degree of specialization that makes it possible to define functions on the basis of specifications that target a specific need of the client company. This enables the client company to optimize its internal resources.

In the second scenario, the company is able to produce the good or service itself, but instead it delegates the work. This is called 'capacity' subcontracting. In this case, the contracting company, which can produce the product itself, employs another company (either occasionally due to a temporary spike in production or technical problem or on a more or less ongoing basis) because it wants to maintain its own capacity through the use of external production capacity[4]. These capacity subcontractors can also be called consignment manufacturers (Houssiaux in Baudry 2013); they perform simple tasks as directed by the contracting company or client and very often their activities compete with that of the organization.

Although in theory there are several types of subcontracting, in practice it is difficult to identify them. According to Jounin (2007), in the public construction sector, the boundary between capacity subcontracting and specialty subcontracting is blurred. For example, subcontracting in building industry activities is mainly based on workers and intermediate consumption, "some of the girders are supplied by the contractor, while their main tools are supplied by the general business" (such as the crane). In this case, Houssiaux talks about 'community' subcontracting, in which the activity, the execution of work or the finished product are collective.

2.3 *Motivations for the use of subcontracting*

We have highlighted the different forms of subcontracting, which correspond to the different needs and strategies of organizations. According to Houssiaux (in Baudry 2013) capacity subcontracting is mainly used to reduce or limit production costs. Business owners can create competition between different service providers to get better rates. This idea is not new; Williamson in 1975 looked at corporate collaboration through market relations from an economic point of view. Transaction costs theory (Ghertman 2003) argues that the organization chooses between doing things themselves, or having them done, depending on the cost of acquiring a product or service on the market compared to the cost of internal production. Barthélemy and Donada (2007) noted that the use of subcontracting allowed organizations to be more flexible by transforming fixed costs into variable costs, which made it easier for them to cope with market fluctuations. According to Quélin and Duhamel (2002) the economic factor is closely related to the quality function. A company delegates not only for reasons of quality and efficiency, but also cost.

[3]The French National Institute for Statistics and Economic Studies (INSEE) definition is as follows: Following the application of the *Nomenclature d'Activités Françaises* on 1 January 2008 (second revision), in the manufacturing sector primary contractors *sensu stricto* are only those who provide raw materials. Conversely, subcontractors *sensu stricto* are only those who receive raw materials.

[4] INSEE definition (op. cit.)

For some companies in some cases, subcontracting is primarily explained by performance issues in the workplace. Finally, subcontracting can be a way to transfer risks and responsibilities associated with production to a third party. Statistics show that accidents occur more often among the employees of subcontractors (Algava & Amiras 2011) compared to the employees of contractors, but it must not be forgotten that some companies outsource their riskier activities, particularly in the industrial sector (Thébaud-Mony 2000).

Other organizations transfer social risks through subcontracting (Puech 2004; Barthélemy 2007, p. 67). In this case, it is a way to avoid excessively high social costs; the imposition of new constraints, loss of benefits, lower wages and lack of resources can result in disenchantment with the organization. Subcontracting can enable the company, in deteriorating market conditions, to take measures that have a negative impact on the subcontractor without having to deal with the consequences. This is not an intentional process, but an adjustment mechanism in response to market fluctuations.

In addition to these quantitative, qualitative and social advantages of subcontracting, we can add a further strategic and opportunistic motivation. These concern situations where the company is faced with uncertainty concerning the market or its products and wishes to test a company or its staff before integrating them or buying the company. In practice, although the extended, outsourced organization has become a dominant trend, other organizations are moving in the opposite direction and are seeking to strengthen their classical "hierarchical and pyramidal centralization" through internalisation policies (Veltz 2000). This raises the question of the acquisition of certain subcontractors. The motivations for the use of subcontracting are not always rational, and are likely to be the result of poor strategic choices. Subcontracting is by nature ambivalent. While it offers various benefits to the organizations and can form part of an extension strategy, this extension can sometimes be a disadvantage and pose a risk to production.

3 ORGANIZATIONS EXTENDED BY THE SUBCONTRACTOR NETWORK

Rorive (2005) provides a typology of six types of corporate network. Of these six, five are driven by the use of partners, suppliers, joint contractors, subcontractors or distributors. It could therefore be said that many organizations extend themselves through outsourcing, and more specifically subcontracting.

For Veltz (2000, pp. 174–175) the term corporate network is both overly polysemic and restrictive. He defines this new form of organization as "a network of cellular models" made up of "a relatively compact and traditional central core surrounded by a periphery of suppliers and distributors structured in successive layers." Three elements characterize this type of organization and mark a break with the integrated organizational model: market-oriented decentralization, the contract and multi-functionality.

3.1 *Market-oriented decentralization*

Market-oriented decentralization concerns the distribution of activities across relatively autonomous units. These subsets are subject to strict targets coupled with the systematic evaluation of their results (rather than a precise definition of procedures). According to Veltz (2000) this management mode is a consequence of Taylorism where goals become more important than the means: "specialization according to goals and products impacts on specialization according to processes, resources and technical knowledge". This phenomenon can be observed in many organizations and has spread to many industries. This market-oriented decentralization can be a risk for organizations. If goals are too general and vague, they must be broken down into operational and individualisable sub-goals (Simon 1983). Otherwise, individuals may take decisions that have an adverse impact on the organization and it becomes difficult to control the consequences. Herbert Simon (1983) points out that the goals and objectives of an organization can be perceived differently by different members of the organization and these different perceptions are likely to harm the overall coherence of these new organizations.

3.2 *The contract*

The increasing use of the contract is a fundamental element of the relationships between the different units in the cellular network organization. For Veltz (2000) the contract leads to "very diverse relationships, legal forms, styles and constraints". He stresses that 'hierarchy' and 'contracts' are in no way antithetical" and takes the example of Japanese supplier chains. In these chains, the ability to mobilize networks of relationships is based on a clearly defined, prescribed hierarchy that forms the basis for the organization (Magaud & Sugita 1993).

An extension of the commercial function is found in new organizations through contracts that mobilise remote resources. The characteristic feature of this type of organization is that it is able to extend its scope for action while reducing its legal exposure. Many economists have highlighted the trend towards "vertical disintegration" (i.e. a reduction in direct production units legally owned by the company). This makes it possible to

indirectly extend and share production by mobilising a network of actors and skills. This market-driven vertical disintegration usually involves a reduction of the salaried workforce and non-strategic or ancillary activities (such as administration, cleaning or security) for the lead company.

Demmou (2011) noted that there has been a significant decrease in manufacturing jobs since the 1980s. The partial outsourcing of industrial activities to the service sector explains 20–25% of the decrease in the salaried workforce[5]. On the other hand, market orientation and the use of contracts have encouraged the creation of "complex mini-businesses rather than divisions created along the lines of traditional functional departments" in organizations (Veltz 2000, p. 178). Contractual relationships become one of the keys to the expansion of the organization. Coase (1937, p. 23) highlighted this point in other terms when he wrote, "a firm becomes larger as additional transactions (which could be exchange transactions co-ordinated through the price mechanism) are organized by the entrepreneur and becomes smaller as the abandons the organization of such transactions". The contract, whether between two individuals or two companies, allows the organization to expand both on a spatial and skills level. However, it cannot alone organize collective action, contrary to what the transactional approach (also known as agency theory) suggests[6].

There are a variety of mechanisms to coordinate production activities, the contract is not the only incentive mechanism (Baudry 1992). The mobilization of remote productive resources may pose management and control problems within the extended organization.

3.3 *Multi-functionality*

The organization distributes distinct functions across its network of partners, suppliers, joint contractors, subcontractors or distributors. This is the case at Airbus Toulouse (France), which divides tasks between Airbus and its network of suppliers. Production processes are distributed across the manufacturer's internal sites. Airbus is the prime example of the "lead network firm"; it delegates its non-strategic sub-functions in order to focus on its core activities.

However, the firm also uses strategic, lead subcontractors, who play an intermediate role and use their own subcontractors. Mazaud and Lagasse (2009) found "a high degree of segmentation" in Airbus suppliers. There is a division of labour between the company leading the network and its network of suppliers. Few authors have looked at its modalities. This multifunctional character of the organization means that it can carry out several simultaneous activities, improve performance and be more responsive to the needs of its customers. One example is the cooperation model that Airbus operates with its suppliers, which enables it to simultaneously develop several aircraft at different sites. However, while this multi-functionality enables organizations to focus on their specialty, it can also, in certain cases, lead to the loss of skills and control of overall production (Nogatchewsky & Donada 2005; Barthélemy 2007 p. 65).

These three features (market-oriented decentralisation, the contract, multi-functionality) make it possible to characterise and understand ambivalence in organizations that are extended by subcontracting. Such organizations grow around a base unit or an autonomous decision-making centre, which structures activities and their deployment, and ensures the overall coherence of peripheral activities.

The base unit forms the foundation for all other activities. This central core lies at the heart of direct and indirect cooperation with a constellation of partners, who undertake functions designed to achieve an ultimate goal. According to Capraro and Baglin (2002), the extended business "has to set the standard for all partners in design and production excellence, which must unite the efforts of numerous partners to achieve shared success in the extended company." The extended organization must therefore develop the capacity to re-think itself and quickly recompose itself in response to its environment and these new links.

We argue that one of the characteristics of the extended organization is that every action centre or mini-business forming the network has the potential to further extend the boundaries of the initial contractor, and to initiate new cooperation. Its potential extension, in terms of both skills and geography, is unlimited and can present risks. The strategic nature of the subcontractor cascade (shared responsibilities through a multiplication of subcontractors and contractors, the supply chain, value chain or overall logistics), which includes all of the actors and activities that enable the production of a final product (Sofiane, 2009) is specifically designed to offer organizational flexibility and geographic reach that the integrated model does not provide. Finally, there are at least two ways in which an organization becomes extended. The first is through a reduction in its direct production units, via market-driven decentralisation. Secondly, it can create new commercial and

[5]See Sauvy A., 1980. *La machine et le chômage*, DUNOD. The spillover theory argues that technical progress that improves productivity leads to a transfer (spillover) of jobs from one sector to another.

[6]The contract is seen as simply the act of giving consent and takes no account of authority and dependency relationships.

contractual relationships, and manage its resources through a network of partners.

While communication is one of the keys in the extended organization it enables them to manage their resources and partners—it can also represent a risk. In practice, the multitude of internal actors can also lead to the risk of leaked information about industrial processes or organizational strategies. The communication of information has strategic value as it makes it possible to gain power (Crozier & Friedberg, 1977). Individuals always have a degree of autonomy and pursue their own objectives, which are not necessarily compatible with those of the organization—especially when it consists of a fragmented constellation of partners (Vaughan, 2009). As much as it may try, the organization can never completely limit the autonomy of subcontractors. The opening up of extended organizations through market-oriented subcontracting networks can create a significant risk of information leak about resources and strategies in a given market, and lead to a loss of control with respect to its partners and competitors. For example, subcontractors from emerging countries can monopolize technical and organizational knowledge by copying processes before themselves developing high-tech industries that compete with those of industrialized countries. Faced with such a risk, the organization can take a strategic approach to the market, i.e. by subcontracting auxiliary functions while continuing to carry out core functions internally (Altersohn, 1997, p. 22). Otherwise, only the quality and strength of the links between the contractor and the subcontractor can reduce the risks associated with an organization's loss of confidential information.

4 THE EFFECTS OF THIS AMBIVALENT MODE OF ORGANIZATION ON THE RELIABILITY AND EFFICIENCY OF THE WORKFORCE

The motivations, forms of subcontracting and relations between contractors and service providers vary from one organization to another. In order to understand them better, it is useful to think of the subcontracting relationship as a form of employment relationship. Baudry (1992) argues that the two types of relationship are comparable. In both cases there is "quality economy", i.e. there is uncertainty about the work of the subcontractor, like that of the employee, in terms of productivity and results. The author shows that there is a plurality of mechanisms that govern inter-firm relations. Production is based not only on the contract and authority but also (and above all) on trust. Jounin (2006) also sees working relationships as going beyond purely mechanical aspects. Contracts "provide the framework, but within this framework actors build trust and informal loyalties [...]. Personality comes back into the game, loyalty is re-injected, tacit alliances are established that go beyond employment contracts and compensate for their fragility."

However, unlike the employment relationship, subcontractors are in a different, intermediate position. Paid work is very often a subordinate position, although being this position does not necessarily mean oppression and servitude. It can be a situation where work-related skills are made available to a third party or a contractor. The particular characteristic of subcontracting is that the company is no longer in a direct employer-employee relationship, but in an indirect relationship (Tinel *et al*. 2007). In practice, the commercial contract replaces the employment contract. The company continues to mobilise its productive effort remotely through subcontractors.

4.1 *Transformation of the workforce and risk management*

Subcontracting may affect teamwork. As it becomes commonplace the workforce is restructured into those who are directly and those who are indirectly mobilised. Jounin (2007) used a case study of a building site to demonstrate the importance of subcontracting in the construction industry. Out of 120 workers working on a large construction project, 80 were temporary workers employed by three subcontractors. Among the 40 who worked for the lead company, only 15 were direct hires. Therefore organizations need to create and cooperate with a fragmented workforce with different statuses, schedules and functions, united by a single goal. The SUMER 2003 survey (Hamont-Cholet & Sandret 2007) showed that the support of the workforce and the hierarchy protects against the risk of accident: the accident risk increases by 20% when workers cannot discuss with their bosses their concerns about how to do the job.

Similarly, Puech's analysis (2004) of a hotel's housekeeping staff identified two categories of workers, a fixed staff and subcontracted personnel, which highlighted the divided nature of the workforce. His case study showed that entire management of the workforce was tailored to meet the hotel's production requirements as closely as possible. The author noted significant differences in terms of employment conditions and wages in the two groups of staff (one employed by the hotel and the other employed by the subcontractor).

The first group worked full time, had a fixed number of rooms to clean and a fixed salary. The second group worked part time at a fixed pace: a certain number of rooms to be cleaned each hour. Their salaries were not fixed because their schedules varied between 20–30 hours per week.

The author observed a significant difference in salary conditions within the same occupational group. According to Peuch, "the use of subcontracting allows the group to compensate for variations in activity levels, a particular feature of the hospitality industry. The subcontractor's employment contracts are therefore established in order to respond to the needs of the company as far as possible, i.e. almost exclusively part time." The consequence was that around thirty subcontractors members of the housekeeping staff took strike action as a result of a collective sense of injustice. While working hours were their main motivation, above all, the subcontractor's staff demanded equal status with the hotel's staff. This study shows that the use of subcontractors is not without consequences and that the internal organization of a company can be a source of threat. The organization itself contains the necessary elements for both its growth and its death.

According to a 2006–2007 survey on organizational change and computerization (Algava & Amira, 2011, Table 1) subcontracting is widespread in the public construction and hospitality industries. However, most subcontractors are found in industry; both subcontractors who carry out the work themselves and those who in turn subcontract others (intermediate subcontractors).

4.2 *Subcontracting at the origin of both vulnerability and reliability*

In this section we focus on industrial organizations as a source of both risk (Perrow 1999) and reliability (La Porte & Consolini, 1991). These approaches are two sides of the same coin and we present them here as ways to understand the origins of reliability or risk within at-risk industrial organizations. Issues of reliability and unreliability are played out in the workforce (Bourrier 1999), and are particularly seen in strategies that locate actors depending on the constraints they are subject to. It is therefore important to understand the effect of the changes that organizations go through.

When subcontractors are used there is a multiplication of dual-source employment statuses (CEE 2008 pp. 57–68, p. 60 Table 1, p. 61 Table 2). In the 1980s, 63% of businesses used short-term contracts and 59.8% used subcontractors. In 2000, 70% of companies used short-term contracts and 85.3% used subcontractors.

Triangular subordination situations have spatially and temporally reshaped organizations. This is particularly seen in the widespread use of temporary employment contracts, flexible working hours and polyvalent/multi-skilled jobs. Alongside these changes in personnel management modes, power and the exercise of authority is changing. The need for results and constraints related to the pace, flexibility, objectives and the assessment of work are more visible in the subcontracting relationship.

According to a 2006–2007 survey on organizational change and computerization (Algava & Amira 2011), the employees of subcontractors were, on average, subject to greater constraints in terms of scheduling, pace, flexibility and objectives than those of prime contractors, and their working conditions were poorer. On the other hand employees of subcontractors had greater autonomy over their work than their colleagues with respect to initiatives taken to improve their workplace. The survey showed that non-intermediate subcontractors (those who carried out the work themselves and did not subcontract) received more direct instructions, but had fewer specific task-related targets to meet than both intermediate subcontractors and employees of the contractor. However, this formalisation of working practices does not seem to have reduced the autonomy of subcontractor's employees.

The increase in work carried out under constraints and the scope for autonomy has at least two consequences. First, the widespread use of management practices where individuals are closely monitored means that staff are motivated by the fact that their results are regularly evaluated. Secondly, they know that if their results are unsatisfactory there will

Table 1. The various forms of subcontracting.

Variable	Weight		
Duration of the activity of the subcontractor	Short	Moderate	Long
Place where the subcontractor carries out work	External	Intermediate	Internal
Share of the activity in the organization	Small	Average	Significant
Nature of the subcontracting activity	Simple and substitutable	Average	Complex, non-substitutable
Place of the subcontractor in the production process	Supply—intermediate production—final production		

be negative consequences. The client may not renew the contract; a decision which would have negative consequence for many of the subcontractor's employees. Results-based performance means that employees are subject to significant constraints. The hierarchy requires increased professionalism in order to be the best. The situation is one in which the hierarchy issues objectives that must be met without fail.

In an at-risk organization (for example in the nuclear sector), working under such constraints can be beneficial in terms of both efficiency and reliability. The work of Bourrier (1999, pp. 205–251) highlights the benefits of subcontracting. Although it may be normal to expect that subcontracting reduces transparency and leads to an increase in incidents, the author noted total transparency regarding outsourced activities at the Nogent nuclear power. Subcontractors did not hesitate to declare the slightest production deviation in order to protect themselves against certain incidents. The author explained this behaviour in terms of the significant economic and qualitative constraints subcontractors are subject to. Consequently, in order to secure the renewal of their contract they seek to guard against any incidents that may occur at the client's site and demonstrate their usefulness.

However, if these constraints on objectives and the pace of work can lead to more effective organizations, they are also likely to increase the risk of accidents. An analysis by the French Department for Research, Clinical Trials and Statistical Analysis (*Direction de l'animation de la recherche, des études et des statistiques analysis*, Dares) (Hamont-Cholet & Sandret 2007) confirmed that employees who report "always having to rush" increase their risk of an accident by 26%. A high workrate may also limit its effectiveness and quality. According to Vaughan (2009) the space shuttle Challenger accident occurred following a sequence of deviations from technical procedures in order to meet set deadlines. The technical culture of the aerospace industry is very sensitive to safety issues. According to the author, the politico-bureaucratic imperatives associated with a cost and time culture went against this technical culture.

5 CONCLUSION

This paper forms the first part of a sociological study. The different forms of subcontracting shown in these studies enable us to reflect on the impact of an increasingly widespread mode of governance that is having an effect on the workforce. The diversity of statuses present in productive organizations tends to change the organization of work. The use of subcontractors leads to both restructuring and tensions within the workforce. A better understanding of the composition of this workforce, and its reactions means that it becomes possible to anticipate events and shield productive organizations from certain risks associated with staff management. Sociological qualitative research methods are likely to provide us with a better insight into this scenario and help us to assess the associated risks.

ACKNOWLEDGEMENTS

We would particularly like to thank TOTAL, GDF SUEZ, SNCF and AFNOR, who are the partners of the Mines ParisTech Resilience Engineering Chair. These companies sponsored this research and thereby contributed to the creation of knowledge in the field of industrial risks.

REFERENCES

Abdul-Nour G., Jacob R., Julien P.-A. & L. Raymond, 2003. L'entreprise-réseau, dix ans d'expérience de la Chaire Bombardier Produits récréatifs, Presses de l'université du Québec.

Algava E., & Amira S., 2011. Sous-traitance: des conditions de travail plus difficiles chez les preneurs d'ordres, Dares Analyses n°011.

Altersohn C., 1997, La sous-traitance à l'aube du XXIè siècle, L'harmattan.

Askenazy P. 2004. Les désordres du travail. Enquête sur le nouveau productivisme, Seuil.

Barthélemy J., Donada C. 2007. Décision et gestion de l'externalisation: une approche intégrée. Revue Française de Gestion, vol. 33, n°77, pp. 101–111.

Barthélemy J., 2007. Stratégies d'externalisation: Préparer, décider et mettre en oeuvre l'externalisation d'activités stratégiques, Collection: Stratégies et Management, Dunod-3ème edition.

Barrand J., Gumb B., Badot O., Benameur K., & Blum V., et al. 2010. L'entreprise agile: Agir pour une performance durable, Collection: Stratégies et Management, Dunod.

Baudry B., 1992. Contrat, autorité et confiance. La relation de sous-traitance est-elle assimilable à la relation d'emploi ? In: Revue économique. Volume 43, n°5, pp. 871–894.

Baudry B., 2013. Quasi-intégration et relation de sous-traitance industrielle: une évaluation des travaux de Jacques Houssiaux, Revue de l'économie industrielle, N°142.

Benchimol G., 1993. L'entreprise étendue, Hermès, Coll. Systèmes d'information.

Berger S., 2005. How We Compete: What Companies Around the World Are Doing to Make It in the Global Economy. New York: Doubleday.

Bourrier, M., 1999. Le nucléaire à l'épreuve de l'organisation. Presses universitaires de France.

Capraro M., & Baglin G., 2002. L'entreprise étendue et le développement des fournisseurs. Presses Universitaires Lyon. P.19.
CEE (Centre d'études de l'emploi), 2008. Le contrat de travail, Paris, La Découverte « Repères », 128 pages.
Chaillou B., 1977. Définition et typologie de la sous-traitance. In: Revue économique. Volume 28, n°2.
Coase, R.H., 1937. The nature of the firm. Revue Economica. Vol 16, Page 23.
Crozier & Freidberg, 1977, L'acteur et le système; Points Essais, Paris.
Defelix C. & Picq T., 2013. De l'entreprise étendue à la « gestion des compétences étendue »: enjeux et pratiques en pôles de compétitivité, @GRH, Vol. 2 n° 7, pp. 41–66.
Demmou L., 2011. Le recul de l'emploi industriel en France entre 1980 et 2007—Ampleur et principaux déterminants: un état des lieux. Economie et statisitque, n° 438–440.
Geyer D., 2007. L'externalisation offshore de système d'information, Revue française de gestion, n°177, pp. 129–139.
Ghertman M., 2003. Oliver Williamson et la théorie des coûts de transaction. Revue française de gestion, N° 142, pp. 43–63.
Hamont-Cholet S. & Sandret N., 2007. Accidents et conditions de travail in Premières synthèses informations, Dares Analyses, N°31.2.
Hatzfeld, N., 2000. Organiser, produire, éprouver: histoire et présent de l'usine de carrosserie de Peugeot à Sochaux, 1948–1996. Thèse de doctorat. EHESS.
Houssiaux J., 1957. Le concept de « quasi-intégration » et le rôle des sous-traitants dans l'industrie. In: Revue économique. Volume 8, n°2, pp. 221–247.
Jounin N., 2007. L'illégalité sous-traitée ? Les conséquences du recours à des employeurs intermédiaires dans le secteur du bâtiment. Droit social, n°1, pp. 38–45.
Jounin, N., 2006. Loyautés incertaines, les travailleurs du bâtiment entre discrimination et précarité. Thèse de doctorat en sociologie, université Paris VII-Urmis, sous la direction d'Alain Morice. P.47.
La Porte & Consolini, 1991.Working in practice but not in theory: theoretical challenges of high reliability organisations, Journal of Public Administration Research and Theory, 1 (1) (1991), pp. 19–47.
Magaud J. & Sugita K., 1993. Le retour des réseaux une comparaison Franco-Japonnaise, Annale des mines gérer et comprendre.
Mazaud, F., 2006. De la firme sous-traitante de premier rang à la firme pivot: une mutation de l'organisation du système productif Airbus, Revue d'Economie Industrielle, N°113, 1er Trimestre, pp. 45–60.
Mazaud F. & Lagasse M., 2009. « 7. Externalisation et coordination stratégique des relations de sous-traitance: le cas d'Airbus », in Bernard Baudry et Benjamin Dubrion, Analyses et transformations de la firme.
Moreau F., 2003. L'entreprise élargie: de nouvelles formes d'organisation », Insep Consulting Ed. Moreau Defarges P., 2003. La gouvernance, PUF, Que sais-je? 127 pages.
Morley, C., 2005. Processus métiers et SI. Dunod.
Niang N., 2013. Internationalisation des services et normes internationales Une perspective d'économie politique postcoloniale, in Jean-Christophe Graz et Nafi Niang, Services sans frontières, Presses de Sciences Po Académique, pp. 337–380.
Nogatchewsky G. & Donada C., 2005. Dépendance asymétrique dans les alliances verticales: comment un client vassal contrôle-t-il ses fournisseurs ? Management International Review 10, 1 pp. 63–74.
Perez, Y.A., 2007. Conseil, innovation et dynamiques organisationnelles de « l'entreprise étendue » in n°281, Humanisme et Entreprise.
Perrow, C., 1999. Normal accidents: Living with high risk technologies. Princeton University Press. P. 88.
Pesqueux Y., 2008. L'organisation en réseau comme forme « indéterminée », Université virtuels et collaboration, Evry.
Ponnet M., 2011. Les relations de sous-traitance et leurs effets sur la sûreté et la sécurité dans deux entreprises: SNCF et GrDF, Thesis supervised by Benoit Journé and de Charles Suaud. University of Nantes.
Puech I., 2004. Le temps du remue-ménage. Conditions d'emploi et de travail de femmes de chambre, Revue Sociologie du travail, vol. 46, no 2.
Quélin B., 2007. L'externalisation: de l'opérationnel au stratégique, Revue française de gestion, n°177, p. 113–128.
Quélin B. & Duhamel F., 2002. Externalisation: logique financière et logique de compétence sont liées, Enquête du Groupe HEC.
Rorive B., 2005. L'entreprise réseau revisitée: une tentative d'ordonnancement des nouvelles formes d'organisation, Revue Gérer et comprendre, n°79, pp. 63–75.
Roy M. & Audet M., 2002. La transformation vers de nouvelles formes d'organisation plus flexibles: un cadre de référence, Gestion (Vol. 27), pp. 43–49.
Samaganova A. 2008. L'efficience collective du cluster du logiciel de Saint-Pétersbourg, Revue d'Économie Régionale & Urbaine, vol. 2, pp. 225–235.
Simon, H.A. 1983. Administration et processus de décision. Economica.
Sofiane A., 2009. Externalisation et création de valeur au sein de la « Supply Chain »: l'entreprise étendue, La Revue des Sciences de Gestion, n°236, pp. 85–93.
Thébaud-Mony A., 2000. L'industrie nucléaire: sous-traitance et servitude. Inserm, Coll. Questions en santé publique.
Tinel B. et al., 2007. La sous-traitance comme moyen de subordination réelle de la force de travail, Actuel Marx, n°41, pp. 153–164.
Vaughan, D., 2009. The Challenger launch decision: Risky technology, culture, and deviance at NASA. University of Chicago Press.
Veltz P., 2000. Le nouveau monde industriel, Gallimard.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Human error analysis: Review of past accidents and implications for improving robustness of system design

R. Moura*, M. Beer, E. Patelli & J. Lewis
Institute for Risk and Uncertainty, University of Liverpool, UK

F. Knoll
NCK Inc., Montreal, Canada

ABSTRACT: Since the establishment of the high-technology industry and industrial systems, developments of new materials and fabrication techniques, associated with cutting-edge structural and engineering assessments, are contributing to more reliable and consistent systems, thus reducing the likelihood of losses. However, recent accidents are acknowledged to be linked to human factors which led to catastrophic consequences. Therefore, the understanding of human behavioural characteristics interlaced with the actual technology aspects and organisational context is of paramount importance for the safety & reliability field. This study first approaches this multidisciplinary problem by classifying and reviewing 200 major accident data from insurance companies and regulatory authorities under the Cognitive Reliability and Error Analysis framework. Then, specific attention is dedicated to discuss the implications for improving robustness of system design and tackling the surrounding factors and tendencies that could lead to the manifestation of human errors.

1 INTRODUCTION

1.1 *The need for human reliability analysis*

Despite the evolution of engineering methods and fabrication techniques, recent accidents involving complex industrial systems within high-technology industries such as oil & gas, nuclear and aerospace were acknowledged to be consistently interrelated to human factors which led to tragic consequences (e.g. Rio-Paris Flight 447, Macondo and Fukushima). No one can deny the impact of human actions and decisions on the performance of engineering systems, hence justifying the need for evaluating the interaction between humans and systems through a suitable Human Reliability Analysis (HRA).

HRA is mainly a predictive tool, intended to estimate the probability of human errors and assess the human factors contribution to the overall risk through the use of qualitative and/or quantitative methods. Essentially, traditional HRA tools consist of (i) the identification of potential human erroneous actions, followed by (ii) the consideration of internal and external factors that could influence the human performance, finally resulting in (iii) the estimation of human error probabilities. The key step in this approach is defining possible tasks to be performed by a human operator, considered to be an element or component subjected to failure due to inborn characteristics, thus having an "inbuilt probability of failure". Modifiers known as performance shaping factors, error-forcing conditions, scaling factors or performance influencing factors, depending on the methodology, are then applied to adjust the likelihood of human failure when performing the assessed task.

On the other hand, some contemporary approaches to HRA such as "A Technique for Human Error Analysis"—ATHEANA (Barriere et al. 2000), the Connectionism Assessment of Human Reliability (CAHR) based on Sträter (2000) and the Cognitive Reliability and Error Analysis Method (CREAM) by Hollnagel (1998) were developed around the principle that the fundamental element is, in fact, the context in which the task is performed, reducing previous emphasis on the task characteristics *per se* and on a hypothetical inherent human error probability.

Several HRA methods comprising both "task-centred" and "context-centred" approaches are currently in use. Bell & Holroyd (2009) reported 72 different techniques to estimate human reliability and considered 35 as potentially relevant. Further analysis highlighted 17 of these HRA

*National Agency for Petroleum, Natural Gas and Biofuels (ANP), Brazil.

tools to be of potential use for major hazard directorates. For additional details on some of the existing methods, a summary of five commonly used HRA techniques in the offshore industry and other high-hazard facilities has been presented by Moura (2012), where the main features of the Human Error Assessment and Reduction Technique (HEART), the Technique for Human Error Rate Prediction (THERP), the Standardized Plant Analysis Risk (SPAR-HRA), the Justification of Human Error Data Information (JHEDI) and the Systematic Human Actions Reliability Procedure (SHARP-1) were reviewed.

Regardless of the variety of HRA methods available to enable practitioners to assess the risks associated with human error by estimating its probability, the substantially high uncertainties related to the human behavioural characteristics, interlaced with actual technology aspects and organisational context, turn this kind of evaluation into a very complicated matter, raising reasonable concern about the accuracy and practicality of such probabilities.

1.2 *The data collection problem*

Swain (1990) argues that the most serious problem for HRA is the unavailability of meaningful data (or less-than-adequate data) on human performance that could assist quantitative predictions of human behaviour in complex systems. Posing similar reservations, The International Atomic Energy Agency (1990) report on human error classification and data collection stressed this matter, claiming that a global data collection scheme would be *extremely difficult, if not impossible, to create*, justifying this unenthusiastic view by the amount of data related to each human error that should need to be generated in order to satisfy a wide range of objectives required by applications dependent on human performance databanks.

Indeed, in spite of some recent efforts to gather human performance data and overcome this issue, such as Gibson & Megaw (1999) CORE-DATA, the accessibility and usage of data is still very limited, due to four main reasons. Initially, human performance data collection usually begins within a specific domain, making the classification scheme or taxonomies closely associated with the industry where the issue was first raised. Trying to transpose terms and nomenclatures from one industry to another is challenging, thus human error information are likely to be captured under different frameworks.

Secondly, the insertion of the human performance data in a HRA, which would have to be subsequently combined with an equipment/system reliability analysis to finally reach a meaningful result in the probabilistic safety assessment, is complex and time consuming. Consequently, practitioners tend to use expert elicitation (or a qualitative approach) as a shortcut to include human error data in probabilistic risk/safety assessments, leaving the commitment to collect quantitative data behind.

In addition, the data collection and interpretation process could lead to significantly different results, depending on the data source and the acquisition method (field data, simulator data, HRA modelling, expert elicitation, operation observation, reporting methods, near misses, performance indicators, accident investigation reports etc.).

Lastly, despite the increasing complexity of engineering systems and safeguards reduced the possibility of accidents caused from a single failure, the exact interactions between human behaviour, technology and organisation currently required to produce the specific chain reaction leading to a disaster are very difficult to predict and highly associated with a specific work situation, thus unlikely to be repeatable.

2 CLASSIFICATION METHOD

2.1 *The Cognitive Reliability and Error Analysis Method (CREAM) taxonomy as a common framework to classify accidents*

An innovative use of the CREAM taxonomy was conceived as a common framework to classify accidents from different industries. Other classification methods such as The Human Factors Analysis and Classification System—HFACS (Shappell et al. 2007) and the Error Promoting Conditions (EPCs) from the Human Error Assessment and Reduction Technique (HEART) presented by Williams (1989) revealed good potential to be used as a classification scheme (in fact, it is one of the central functions of HFACS) and were also reviewed. However, the former taxonomy has deep associations with aviation accidents (e.g. crew resource management and personal readiness), and the latter does not differentiate between human, technological and organisation EPCs among the 39 nomenclatures available. In addition, HEART is designed to be used prospectively, i.e. to estimate human error probability, while HFACS main application is in retrospective analysis of accidents in the aviation field. Therefore, the use of both would have implied adjustments to the original taxonomies.

Conversely, the CREAM taxonomy (Figs. 1, 2 and 3) offers a very effective and clear division between human erroneous actions (phenotypes) and their possible causes or contributing factors

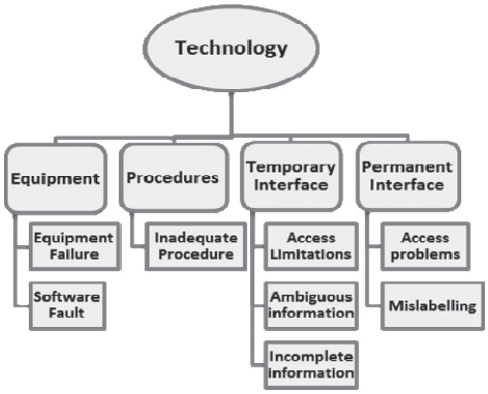


Figure 1. "Technology" taxonomy, adapted from Hollnagel (1998).

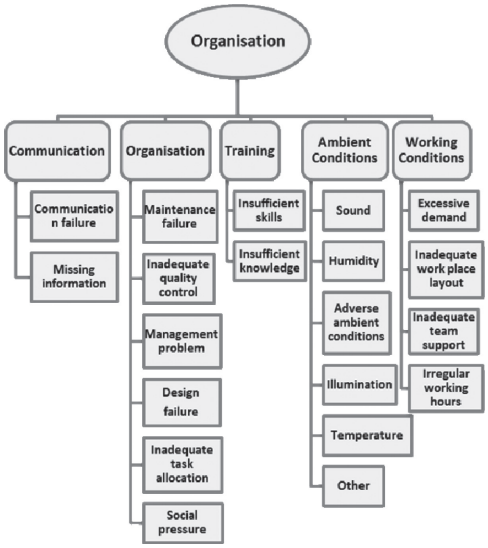


Figure 2. "Organisation" taxonomy, adapted from Hollnagel (1998).

(genotypes), grouped by three expressive categories: man, technology and organisation. Furthermore, the terminologies are generic and easily associated with most industrial sectors.

A noteworthy feature of CREAM's original application as a Human Reliability Analysis approach is the fact that the method was designed for both prospective and retrospective evaluations, whether supporting accident investigations aiming at the search for causes, or predicting events that are likely to occur. This flexibility enables the use of the CREAM HRA method as a data input to the chosen classification scheme, whether

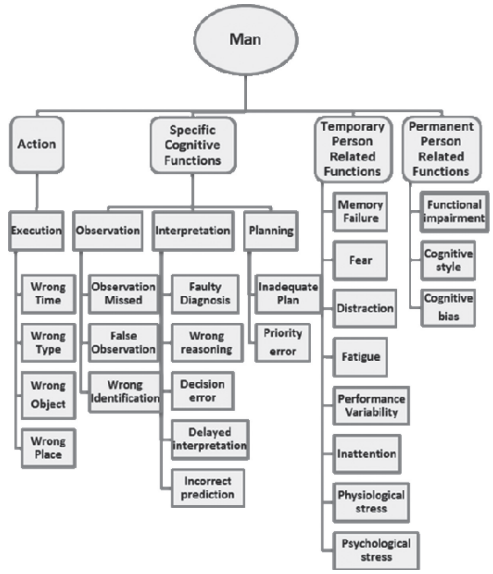


Figure 3. "Man" taxonomy, adapted from Hollnagel (1998).

prospectively, via simulation, or retrospectively, through the execution of accident analysis.

It is worth to notice that this work applies a "retrospective method" for data collection based on CREAM taxonomy, but certainly not following the procedures developed by Hollnagel to perform accident analysis. It means that the CREAM retrospective technique is not used whatsoever, considering that the accidents collected were submitted to extensive investigation and the causes and contributing factors are already exposed in the reports, being the current gap the need for interpretation and classification of the data under a common framework.

3 REVIEW OF 200 MAJOR ACCIDENTS DATA

3.1 *Data collection*

To deal with uncertainties related to data collection and overcome the "less-than-adequate" data problem in this research, factual data from accident investigation reports and case studies were interpreted and then organised to fit the scheme presented in Figures 1, 2 and 3. These accident reports were collected from insurance companies, regulatory bodies, commissions of inquiry, investigation boards and industry experts, such as MARSH Inc., the Australian Department of Industry and Resources (DoIR), the Australian National Petroleum Safety Authority (NOPSA), the Brazilian National

Petroleum Agency (ANP), the European Agency for Safety and Health at Work (EU-OSHA), the National Aeronautics and Space Administration (NASA), the Norwegian Foundation for Scientific and Industrial Research (SINTEF), the Petroleum Safety Authority Norway (PSA), the UK Department of Employment, the UK Health and Safety Executive, the US Bureau of Safety and Environmental Enforcement (BSEE), the US Chemical Safety and Hazard Investigation Board (CSB), the US Department of Energy (DoE), the US Environmental Protection Agency (EPA), the US Fire Administration (USFA), the US Minerals Management Service (MMS), the US National Transportation Safety Board and the US Occupational Safety and Health Agency (OSHA).

These events are listed in Table 1 by industrial activity.

3.2 *Relevance of the data sample*

The UK Control of Major Accident Hazards Regulations (1999) define "major accident" as *an occurrence (including in particular, a major emission, fire or explosion) resulting from uncontrolled developments in the course of the operation of any establishment and leading to serious danger to human health or the environment, immediate or delayed, inside or outside the establishment, and involving one or more dangerous substances. Most of the 200 accidents reviewed fit the United Kingdom's legal definition for major accident.*

Table 1. Accidents distribution by industry.

	Accidents	
Industry	#	%
Aviation	09	4.50
Chemicals factory	29	14.50
Chemicals storage	01	0.50
Construction	12	6.00
Crystal factory	01	0.50
Education	01	0.50
Fiberglass factory	01	0.50
Fireworks storage	01	0.50
Food industry	03	1.50
Gas processing	09	4.50
Gas station	01	0.50
Hydroelectric plant	01	0.50
Ink & paint factory	01	0.50
Metal signs factory	01	0.50
Metallurgical industry	06	3.00
Oilfield waste disposal plant	01	0.50
Petrochemicals	25	12.50
Pharmaceutical industry	01	0.50
Polymers factory	01	0.50
Power plant	01	0.50
Refinery	38	19.00
Sterilisation services	01	0.50
Sugar factory	01	0.50
Terminals and distribution	12	6.00
Tyre & rubber factory	01	0.50
Upstream (oil & gas)	36	18.00
Waste treatment plant	03	1.50
Waste water plant	01	0.50
Water supply	01	0.50

Forty four of the studied accidents accounted for 1,075 fatalities.

Of the events analysed, 91 reports included some cost information, thus it was possible to calculate a gross estimate (using cumulative inflation rate to update to 2013 values) of £20.25 billion in material losses. Furthermore, it is acknowledged that costs related to environmental recovery, litigation etc. would dramatically increase these figures. For example, in a Wall Street Journal article about the Macondo Oil Spill, which occurred in the Gulf of Mexico in April 2010, Fowler (2013) reported that BP had already paid around US$ 14 billion in spill clean-up; US$ 10 billion to individuals, businesses and governments; US$ 4 billion in a criminal settlement; and US$ 2 billion in environmental restoration and research. Not to mention the impact on the company's reputation/brand, reflected in the stock market: Bell (2012) reported a 35.00% drop of BP's stock price from 2010 to 2012.

Hence, these numbers highlight the significance of this research's data sample.

3.3 *Data collection and classification demonstration method*

To demonstrate exactly how the interpretation and classification of the data was performed, a heat exchanger rupture followed by an ammonia release, which occurred in a Tyre & Rubber Factory, will be scrutinised on Table 2. This is based on the study case publication from the US Chemical Safety and Hazard Investigation Board (2011).

Basically, on 11 June 2008, a heat exchanger containing ammonia has ruptured due to an overpressure, triggered by a failure during the maintenance process. One worker was killed and seven others were injured during this event.

Therefore, in the above example, the operator failed to perform the maintenance job sequence, skipping the reopening manoeuvre of a closed isolation valve after replacing a rupture disk. The investigation report did not provide further information about any person related function (memory failure, distraction, fatigue, inattention, stress etc.) that could have led to this specific phenotype (erroneous action). In the following day, another operator overlooked the status of the isolation valve (here we have a clear cogni-

Table 2. Tyre & Rubber factory classification example.

Group	Sub-group	Factor	Justification*
Man	Execution	Wrong place	Sequence, jump forward. One operator closed an isolation valve between the heat exchanger shell (ammonia cooling side) and a relief valve, to undertake a maintenance job, specifically a burst rupture disk replacement. However, after replacing the rupture disk, the reopening of the closed isolation valve was skipped, due to unknown reasons. On the following day, another operator closed a block valve to clean the pipe, isolating the ammonia pressure control valve from the heat exchange.
Man	Cognitive function (observation)	Observation missed	Second operator did not observe closed status of isolation valve and closed block valve, isolating the ammonia pressure control valve from the heat exchange. Afterwards, he started to steam the process line to clean the pipeline. The closed isolation and block valves prevented the increasing ammonia pressure from safely venting through either the ammonia pressure control valve or the rupture disk and relief valve.
Technology	Equipment	Software fault	Information delay. During the emergency, a malfunction in the computerized electronic badge-in/badge-out system delayed supervisors from immediately retrieving the list of personnel in their area.
Technology	Procedures	Inadequate procedures	Incomplete text/missing instructions. i) ASME Code requirement to have a competent person, capable of releasing the pressure, continuously monitoring pressure vessels with relief devices blocked or when there is a possibility of pressurisation above design limit, was not reflected in operating procedures. ii) Supervisors were to account for their employees using a master list generated from the computerized electronic badge-in/badge-out system, but there were no further instructions on how to compensate the expected absence of some members of the emergency response team. Therefore, the supervisors were unable to detect if there was a missing worker designed as a member of the emergency response team.
Organisation	Communication	Communication failure	Message not received. Turnover documents and sign-off procedures that should have alerted whether maintenance was completed or not, as well as the current status of the process, were not effective communication channels.
Organisation	Organisation	Maintenance failure	The relief system was not available due to a maintenance failure. Although maintenance workers had replaced the rupture disk, the valve isolating the rupture disk was not reopened thus the relief valve was not available.
Organisation	Organisation	Inadequate quality control	Inadequate quality control procedures. The information that the isolation valve on the safety relief vent remained in the closed position and locked-out was limited to a handwritten note. Although quality control measures (lockout/tag-out procedures to manage the work on the heat exchanger rupture disk were applied), the progress and current state of the maintenance job was not clearly documented. Moreover, there was not a post-maintenance quality check to verify if the service was properly concluded.
Organisation	Organisation	Design failure	Inadequate emergency system design, poor location of instruments and alarms. Alarm system was not fit for purpose due to a design failure. During emergency, operators were supposed to sound a location-specific alarm using pull-boxes located throughout the production unit. However, the water spray from the automatic water deluge system and the ammonia vapour prevented responders from reaching the alarm pull-box in the affected process unit.
Organisation	Organisation	Inadequate task allocation	Inadequate managerial rule (deficient organisation of work due to the lack of safety principles). After the conclusion of the maintenance job (rupture disk replacement), the work order system required the process operator to sign-off upon the completion of service. However, there was no evidence that this occurred (no signal of a signed copy of the work order was found).

(*Continued*)

Table 2. (*Continued*)

Group	Sub-group	Factor	Justification*
Organisation	Organisation	Social pressure	Group thinking. Although operating procedures required maintenance personnel to obtain production operators' signatures in work orders and keep these documents at production control stations, this was not regularly followed. Therefore, the blatant institutional disregard for procedures shows that the risk perception/understanding of the maintenance worker was clearly guided by the working practice among maintenance personnel.
Organisation	Training	Insufficient skills	Performance failure. Supervisors failed to perform workers headcount during emergency measures. Some employees had not been fully trained on partial and plant-wide evacuations procedures. Procedures established that plant-wide evacuation and shelter-in-place drills should be conducted at least four times a year, but such drills had not been conducted in the four years prior to the incident. Drills could have indicated problems with the worker headcount procedure.

*Inferred from evidences and descriptions from the US Chemical Safety and Hazard Investigation Board (2011) Study Case.

tive function failure—observation) and started to clean the process line. After classifying two man-related factors, one action error (wrong place, sequence, jump forward) and another specific cognitive function (observation missed), further two technology genotypes (equipment and procedures, linked to the escalation of the accident) and six organisation genotypes (communication, maintenance, quality control, design, task allocation, social pressure and training) were identified. The genotypes are the identified factors that caused or contributed to the accident or contributed to its escalation.

3.4 *Data classification results*

The examination of the 200 major accidents was similarly performed, and the following tables summarise the outcomes from these interpretations as well as the resulting categorisation.

Tables 3, 4 and 5 specify the number of appearances of the man-related, machine and organisations phenotypes and genotypes in the major accidents examined. Percentages relate to the total of events (200).

At least one human element was identified in 52.50% of the cases, with 50.00% of direct erroneous actions (phenotypes). Cognitive functions accounted for 45.50%, with the interpretation genotype appearing as the most relevant (31.50%). At least one technology genotype was recognised in 85.00% of the accidents, highlighting equipment failure (61.50%) and inadequate procedures (43.00%) as the foremost factors related to this group. Organisational issues appeared in 94.50% of the accidents, emphasising design failures (62.00%), inadequate quality control (57.00%) and inadequate task allocation (55.50%) as the most significant genotypes within the group.

A segregation analysis of the collected data shows that the prospect of a single group (man, machine or organisation) causing an accident is low. Of the examined events, only 1.00% show an erroneous action with a man-related genotype resulting in an accident. Technological factors were solely responsible for the undesirable outcome in

Table 3. Data classification results (main groups).

	Frequency*	
Group	#	%
Man	105	52.50
Technology	170	85.00
Organisation	189	94.50

*Number of events where groups appeared.

Table 4. Data classification results (factors & sub-groups).

	Frequency*			Freq.*
Factor	#	%	Sub-group	%
Wrong time	29	14.50	Execution	50.00
Wrong type	27	13.50		
Wrong object	06	3.00		
Wrong place	51	25.50		
Observation missed	29	14.50		
False observation	04	2.00	Cognitive functions**	45.50
Wrong identification	07	3.50		
Faulty diagnosis	25	12.50		
Wrong reasoning	23	11.50		
Decision error	17	8.50		
Delayed interpretation	06	3.00		
Incorrect prediction	07	3.50		
Inadequate plan	18	9.00		
Priority error	15	7.50		
Memory failure	02	1.00		
Fear	03	1.50		
Distraction	10	5.00	Temp person related functions	11.50
Fatigue	04	2.00		
Performance variability	02	1.00		
Inattention	01	0.50		
Physiological stress	02	1.00		
Psychological stress	05	2.50		
Functional impairment	00	0.00		
Cognitive style	00	0.00		
Cognitive bias	12	6.00	Perm. person related functions	6.00
Equipment failure	123	61.50	Equipment	62.50
Software fault	03	1.50		
Inadequate procedure	86	43.00	Procedures	43.00
Access limitations	01	0.50		
Ambiguous information	06	3.00	Temporary interface	13.00
Incomplete information	23	11.50		
Access problems	03	1.50		
Mislabelling	03	1.50	Permanent interface	3.00
Communication failure	22	11.00	Communication	27.50
Missing information	36	18.00		
Maintenance failure	70	35.00	Organisation	93.00
Inadequate quality control	114	57.00		
Management problem	20	10.00		
Design failure	124	62.00		
Inadequate task allocation	111	55.50		
Social pressure	15	7.50		
Insufficient skills	73	36.50	Training	52.50
Insufficient knowledge	66	33.00		
Temperature	03	1.50		
Sound	00	0.00	Ambient conditions	10.00
Humidity	00	0.00		
Illumination	01	0.50		
Other	00	0.00		
Adverse ambient condition	17	8.50		
Excessive demand	10	5.00		
Poor work place layout	06	3.00	Working conditions	11.50
Inadequate team support	05	2.50		
Irregular working hours	07	3.50		

*Number of events where factors or sub-groups appeared.
**Cognitive functions detailed on Table 5.

Table 5. Data classification results (cognitive functions).

Cognitive function	Frequency*	
	#	%
Observation	37	18.50
Interpretation	63	31.50
Planning	31	15.50

*Number of events where cognitive functions appeared.

Table 6. Segregation analysis (main groups).

Group/combination	Frequency*	
	#	%
Only man	02	1.00
Only technology	09	4.50
Only organisation	16	8.00
Man-technology	91	45.50
Man-organisation	103	51.50
Technology-organisation	161	80.50
Man-technology-organisation	91	45.50

*Events where a single group or combinations appeared.

only 4.50% of the cases, while 8.00% of the accidents were due to exclusively organisational factors. Conversely, all combinations involving at least two groups featured significantly in the dataset. A Man-Technology arrangement appeared in 45.50% of the cases, while a Man-Organisation combination performed in 51.50%. The Technology-Organisation pair figured together in 80.50% of the events. In 45.50% of the cases, the three groups appeared together. Table 6 summarises these results.

It is important to notice that the design failure is the most significant single genotype from all three groups, appearing with an incidence of 62.00%, closely followed by equipment failure (61.50%).

There is also a close relationship between the design failure genotype and the man group: 69.00% of the erroneous actions (execution errors) were accompanied by a design failure. In addition, 58.62% of temporary and permanent person related functions and 71.43% of cognitive functions were also connected to design failures. Another interesting feature can be extracted from a tendency analysis along the years, considering the design failure genotype and the man group. Figure 4 suggests an increase on the percentage of the man group contribution along the years, while a stable behaviour of the design failure genotype is observed.

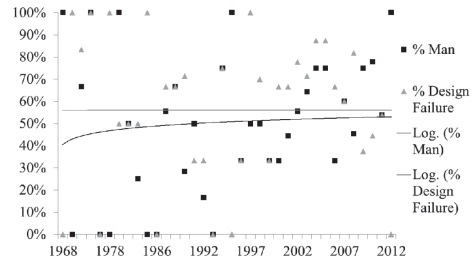


Figure 4. Man and design failure contribution along time.

4 DISCUSSION AND CONCLUSIONS

4.1 *Improving robustness of system design*

Even with the notable evolution of standards and regulations, the amount of design failures contributing to accidents does not appear to be reducing through time. The absence of a well-developed data source related to human performance in complex systems in addition to the diversity of human behavioural characteristics might be preventing reference documents and guidelines from containing unambiguous and direct design rules to deal with human interaction. This may, in turn, lead to this apparent inertia resisting a decrease in design failure. It could be explained by the fact that accidents are rare events, thus it is not an easy task to accumulate sufficient data to ascertain tendencies and improve robustness of system design. Therefore, data collection must be a long-term effort and needs to gather substantial evidence for it to be objectively converted into guidelines to be applied by designers.

This paper indicates that the use of taxonomies from a bi-dimensional approach such as CREAM to classify data is a potential solution to produce meaningful information from three different types of source using the same framework: (i) historical data, as demonstrated in this research, plus: (ii) incident investigations and (ii) prospective analysis, as in the original application of CREAM HRA. The common framework to conduct human reliability predictions as well as retrospective analysis of events during Human Reliability Analysis in a specific facility or industry is perfectly able to interface with the proposed classification scheme for past accidents, considering that they basically share the same taxonomy.

The increasing complexity of systems expanded the number of defences or barriers that needs to be breached in order to result in a major accident, explaining why accidents related to a single CREAM group are uncommon. During this study, the peripheral figures of one exact group

appearance (1.00%, 4.50% and 8.00% for man, technology and organisation, respectively), contrasting with the statistics of at least two groups (45.50% for man-technology, 51.50% for man-organisation and 80.50% for technology-organisation), showed that the presence of two or more CREAM groups is generally necessary to produce an accident. However, this complexity makes it almost impossible for one individual to anticipate all design nuances and connections with human and/or technological factors that could lead to undesirable outcomes. In addition, the relationship between design failures and the man group, explicitly the connection with cognitive functions (71.43% were associated to design failures) and execution errors (69.00% linked to design failures), shows that design failure and damage tolerance criteria must include (and be tested against) specific human related features highlighted by this study. This seems to be especially important with a failure in human interpretation of system status (wrong reasoning and faulty diagnosis), a potential observation missed and some execution errors (sequence, timing and type).

Therefore, the figures above indicate that reliability analyses should anticipate that cues, measurements or information originally intended to lead to a human action have a significant probability of being missed. Similarly, if system design allows situations in which some system analysis/diagnosis, interpretation or hypothesis formulation are required before taking an action, it is likely that specific cognitive functions (inferences, generalisations or deductions) will lead to undesirable outcomes. The design should also be tested against direct human execution errors, primarily focusing on: omissions; jumping forward a required action; performing a premature, delayed or wrong action; and performing a movement in the wrong direction, with inadequate speed or magnitude.

4.2 *Future developments*

The significance of the design failure genotype indicates a well-defined path for future investigation regarding the genesis and perpetuation of human errors.

Further research could also approach other data collection relevant features, due to the significant numbers observed in inadequate quality control (57.00%), equipment failure and maintenance failure (61.50% and 35.00%, respectively), inadequate task allocation (55.50%) and training (52.50%). Quality control guidelines could possibly join a comprehensive design robustness strategy as a failure identification and exclusion tool, while design failure prevention schemes might address both equipment reliability and maintenance efficiency. In addition, effective operational strategies appear to be connected to improved organisation of work by clear rules and principles and individual performance enhancement through workforce skills and knowledge improvements (to handle equipment/perform tasks and increase situation awareness).

Additional effort to expand the data sample is also desirable, whether to confirm or increase the robustness of the results.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support and insights of Christopher Price-Kuehne (MARSH Global Energy Risk Engineering Team), Gary Munley (Office for Nuclear Regulation), Steve Walker (HSE Energy Division—Offshore) and Nicola Stacey (Health and Safety Laboratory) during the development of this work. This study was partially funded by CAPES (Proc. nº 5959/13-6).

REFERENCES

Barriere, M., et al. 2000. NUREG-1624 *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*. Washington, DC: US Nuclear Regulatory Commission.

Bell, J. 2012. The Gulf Spill: BP Still Doesn't Get It. In Allen, F.E. (ed), *Forbes, 20 April 2012*. http://www.forbes.com/sites/frederickallen/2012/04/20/the-gulf-spill-bp-still-doesnt-get-it/.

Bell J. & Holroyd J. 2009. *Review of human reliability assessment methods*. Suffolk: HSE Books.

Fowler, T. 2013. BP Faces New Bout of Spill Liability. *The Wall Street Journal, 18 February 2013*. New York: Dow Jones & Company, Inc.

Gibson W.H. & Megaw T.D. 1999. *The implementation of CORE-DATA, a computerised human error probability database.* Suffolk: HSE Books.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method*. Oxford: Elsevier Science Ltd.

International Atomic Energy Agency. 1990. Human Error Classification and Data Collection. *Report of a technical committee meeting organised by the IAEA, Vienna, 20–24 February 1989*. Vienna: INIS Clearinghouse.

Moura, R. 2012. *Improving risk perception during the lifecycle of an offshore oil & gas production facility: the influence of human and organisational surrounding factors in the major-hazard assessment outcomes.* Cranfield: Cranfield University.

Shappell, S., et al. 2007. Human Error and Commercial Aviation Accidents: An Analysis Using the Human Factors Analysis and Classification System. *Human Factors* 49(2): 227–242.

Sträter, O. 2000. *Evaluation of Human Reliability on the Basis of Operational Experience*. Cologne: GRS. (English translation of the Report GRS-138: Beurteilung der menschlichen Zuverlassigkeit auf Basis von Betriebserfahrung.)

Swain, A.D. 1990. Human Reliability Analysis—Need, Status, Trends and Limitations. *Reliability Engineering and System Safety* 29: 301–313.

The Control of Major Accident Hazards Regulations. 1999. http://www.legislation.gov.uk/uksi/1999/743/contents/made. Surrey: National Archives.

US Chemical Safety and Hazard Investigation Board 2011. *Case Study 2008-06-I-TX Heat exchanger rupture and ammonia release in Houston, Texas*. Washington, DC: CSB Publications.

Williams, J.C. 1986. HEART—A Proposed Method for Assessing and Reducing Human Error. *Proceedings of the 9th Advances in Reliability Technology Symposium, Bradford, 2–4 April 1986.* Warrington: National Centre of Systems Reliability.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Operational and organizational barriers as means of enhancing safety and learning

T.J. Steiro, E. Hansson Blix, J. Seljelid, T.S. Johansen, R.J. Bye & H.N. Hansen
Safetec Nordic AS, Norway

A. Doumit
Saipem Norway AS, Norway

ABSTRACT: The Norwegian Petroleum Safety Authority (PSA) has put a strong demand on barrier management in order to avoid major accidents. Barriers can be seen as technical, operational or organizational aspects which by themselves or together are to prevent a defined sequence of events from occurring, or influence the sequence in a way that damages/losses are mitigated. Safety barriers are thus physical and/or non-physical means. Barrier management is the coordinated activities needed in order to establish and uphold barriers so they are maintained, monitored and functional at all times. In this article we will present findings demonstrating how the barrier management system is working. The focus is on the role of the individuals/operators and the learning aspects involved. Empirical data is based on ongoing barrier projects for drilling rig companies.

1 INTRODUCTION

In the aftermath of the Deepwater Horizon accident in 2010, the Norwegian Petroleum Safety Authority (PSA) and the industry have focused on barriers against major accidents. In their guideline, PSA states that:

The main purpose of barrier management is to establish and maintain barriers so that the risk faced at any given time can be handled by preventing an undesirable incident from occurring or by limiting the consequences given that such an incident has occurred. Barrier management includes the processes, systems, solutions and measures which must be in place to ensure the necessary risk reduction through the implementation and follow-up of barriers (PSA, 2013).

Safetec is currently developing barrier management systems for offshore rig companies operating on the Norwegian Continental Shelf. Promising models and concepts have been developed in close collaboration with rig companies and our aspiration is to have an integrated follow up system that helps the operators to maintain the integrity of their operations. The system will be related to various risk analysis and risk management studies.

2 BARRIER MANAGEMENT

2.1 *Introduction to barrier management*

The first step in implementation of barrier management for a facility as a rig company is to establish the barrier management system. The risk picture for offshore facilities is well defined and the regulations require risk analysis to be performed and updated from early design phases and throughout the lifetime of the operation.

The overall objective of the barrier management system is to protect the facility against the defined risk, either by preventing or limiting each of the specified major accident hazards. The barrier management system will be area specific or system specific, as the risk picture is differentiated throughout the areas of the facility. Major risk hazards such as blowout, gas leaks, fire and explosions, loss of stability and collisions are more or less generic. The handling of risk and the barrier systems may however be facility specific, especially when it comes to the barrier elements, representing the lower level of a barrier system.

There are different possibilities for the representation of barrier functions, but the usual way is to break down the barrier functions into barrier systems, sub-systems/sub-functions and barrier elements. As an example, the below diagram is an illustration of the barrier function "prevent blowout". Xue et al. (2013) points out that offshore drilling is a high-risk and high-cost operation, and blowout is one of the most serious accidents that a drilling rig and its crew might face. The Macondo blowout warns operators that the vigilance to blowouts should never be reduced.

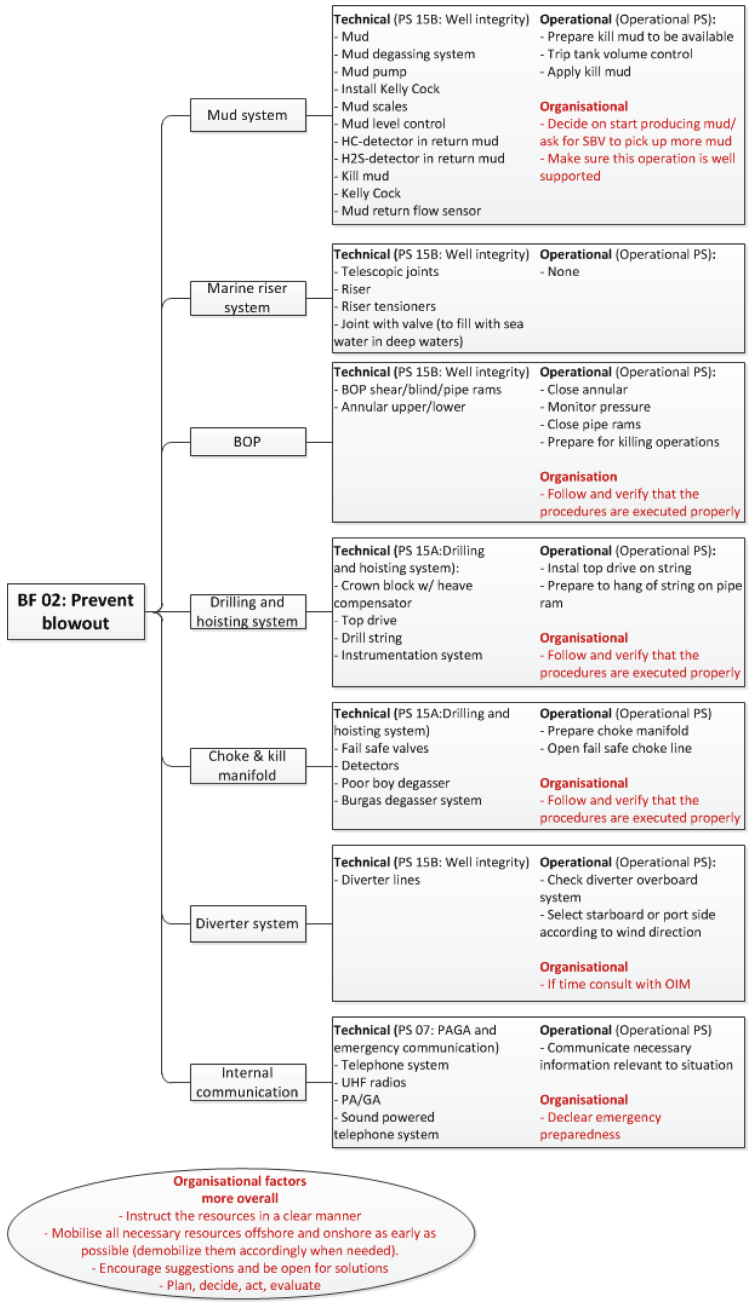


Figure 1. Barrier function with safety critical systems and barrier elements.

2.2 *Barrier management as an integrated part of the safety management*

For the barrier management system to play a role in the safety management of the company; work processes, integration in the operation routines and systematic approaches for following up the barrier status will be required. This will demand knowledge and training for both the onshore and offshore organization. Most companies operating in the oil and gas industry on the Norwegian

Continental Shelf are in the process of establishing and implementing barrier management systems, but we will claim that only a few have reached the final goal of having an integrated barrier management system where the status of the barriers is continuously monitored, maintained and controlled.

2.3 *Barriers—a theoretical foundation*

Sklet (2006 a) claims that the concept of safety barriers is related to the energy model developed by Gibson (1961). Haddon (1980) developed the model further as he provided ten strategies to prevent accidents. Barriers also play an important role in the Management Oversight and Risk Tree (MORT) concept (Johnson, 1980). Rosness et al. (2002) describe energy and barriers as one of the main overall perspectives on safety management. Reason (1997) articulated the barrier perspectives in the famous "Swiss cheese model" and opens up for the more human and organizational side of the barrier perspectives. However, Kjellén (2000) limits barriers to physical countermeasures to stopping or limiting an energy release. Hollnagel (2004) claims on the other hand that barriers are not restricted to the physical nature, but combine types of barriers from protecting against the release of energy to event report and safety policies.

Bolman and Deal (1989) claim there are four main perspectives in understanding organizations. These are the structural perspective, the human relation perspective, the political perspective and the symbolic perspective. The authors further state that the perspectives can be seen as complementary highlighting different aspects of the organization. Barrier management system can so far be seen as part of the structural framework. We will argue that in order to succeed, human relational aspects need to be included such as competence, learning and participation. In 2003, the operators on the Norwegian Continental Shelf were challenged by the PSA to set a target for reducing the frequency of hydrocarbon releases and to identify improvement measures (Sklet, 2006 b).

Several initiatives were conducted both with respect to hydrocarbon releases and barriers in process plants Sklet, Vinnem & Aven (2006) and safety barriers introduced to prevent hydrocarbon releases during wireline operations (Sklet, Steiro & Tjelta, 2005). Duijm (2009) states that the use of safety barriers diagram improves the quality of the risk analysis and the understanding of the role of safety barriers by identifying demand and failure condition for each safety barrier. This forces the analyst to consider the correct sequence, causal relationships in the diagram and further ensure that all safety barriers or safety functions are complete (Duijm, 2009). Rausand (2011) divides safety barrier functions into proactive and reactive functions regarding if they function before or after an undesired event. Hollnagel (2008) argue that barriers are necessary, but may represent a reactive approach which is insufficient by itself to guarantee safety. He further stresses the need for safety to be proactive and looking into the future (Hollnagel, 2008). This calls for more dynamic approaches to barrier management by linking barrier management to organizational learning. Organizational learning is part of the human relation perspective Bolman and Deal (1989).

2.4 *Operational and organizational aspects of barrier management*

The concept of barrier management and the approaches to it has been under constant debates and development both by the industry and by regulatory authorities such as the PSA. The understanding of the technical barriers has been comprehensive and unchanged. The understanding of operational barriers as the tasks to be performed by humans/operators to maintain, monitor and activate the technical barriers is well established while the concept of the organizational barriers is more challenging and difficult to grasp.

Hence, the PSA has reached an understanding of the organizational barriers as the roles that perform the operational barrier elements. This has been described in several presentations given by the PSA since the issuing of the latest version of barrier guideline in January 2013 (PSA, 2013). One example given by PSA (Ersdal, 2014) is the barrier function "detect and rebut" related to the major accident "ship collision".

Other actors have included in the definition of the organizational barriers aspects such as leadership, cooperation and competence. These are aspects that will influence the technical and opera-

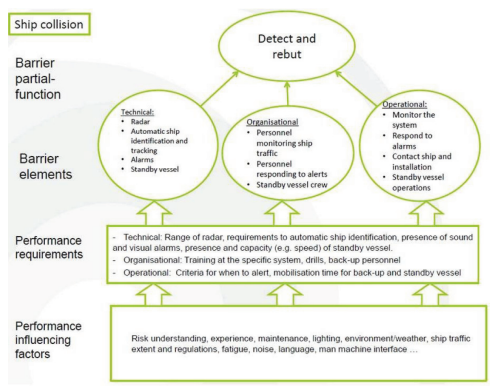


Figure 2 Barrier function for prevention of Ship Collision (Ersdal, 2014).

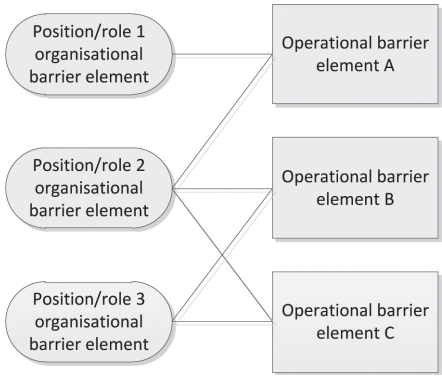


Figure 3. Illustration of some possible relations between position/roles and operational barrier elements.

tional barrier elements. In the PSA interpretation those are seen as performance influencing factors. The conceptualizations of respectively operational and organizational barrier elements as the human actions and the roles that perform the actions have however, some limitation in terms of providing a holistic overview for managing the barrier systems, because it may give an impression of a 1:1 relationship between operational (i.e. actions) and organizational (i.e. personnel/roles) barrier elements.

Operational barrier elements, i.e. *"Planned human actions or interventions that can actively stop an undesired sequence of events, or directly reduce the consequences of an undesired event"*, may consist of several sub-task that are carried out by several different persons in an organization (see Fig. 3). Further, some persons may perform tasks in their daily work that represent sub-tasks of several operational barrier elements.

The implication of this is that some personnel groups may be considered as more critical than others in terms of performing tasks that are necessary to maintain operational barrier elements. A mapping of the relationship between position and tasks related to operational barriers, denoted as *safety critical tasks*, are therefore considered to be important in order to ensure that the personnel in different positions are aware of their responsibility in relation to operational barrier elements, and actually receive the necessary resources (e.g. skills and knowledge, communication, workload/time pressure etc.) to perform their tasks.

3 CONCEPT FOR IDENTIFYING OPERATIONAL AND ORGANIZATIONAL BARRIERS

Safetec has developed a concept for identifying the relationship between operational and organizational barrier elements called "Safety Critical Tasks and Positions". In this section we will give an introduction to the concept and describe the use and result from a specific case.

3.1 *Safety critical tasks and positions—the concept*

The concept is based on examining all types of documentations such as; Quantitative Risk Analysis (QRA), job descriptions, operational duties and responsibilities, operational manuals and governing procedures and reviewing scenarios through workshops etc. In addition operational personnel are interviewed to examine and identify tasks and responsibilities connected to handling of the major accident risk identified for the installation. As a part of the interviews, the status of the performance influencing factors, i.e. skills and knowledge, communication, workload/time pressure etc. are explored as well. The next step is to link the safety critical tasks and personnel associated to them, and rating the position in terms of criticality. The concepts link safety critical tasks to the Major Accident Hazards.

The concept is illustrated in Figure 4.

In this concept we use the following defined Performance Influencing Factors:

1. Skills and knowledge (generic)
2. Site specific knowledge
3. Training
4. Procedures
5. Communication (with other actors relevant for the performance of the task)
6. Degree of redundancy (personnel)
7. Workload/time pressure
8. Supervision (offshore)
9. Onshore support provided for the offshore drilling operations.

Safety critical tasks are defined as:

"Specific action and tasks that must be performed to realize a certain technical or operational barrier function".

Safety critical personnel are defined as:

"Personnel with roles that involve the performance of safety-critical tasks. Safety critical personnel

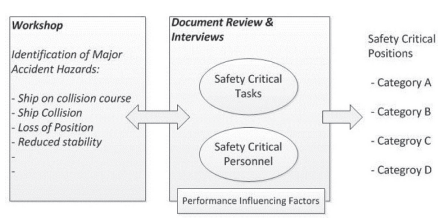


Figure 4. Safety critical tasks and positions.

represent organizational barrier elements which are necessary to realize certain barrier functions. The personnel are classified according to how they are critical for the maintenance of one or more operational barrier elements". Safety critical personnel represent organizational barrier elements.

Based on the definitions of safety critical tasks and safety critical positions, different positions will perform different types of safety critical tasks and thereby representing different influences on the functioning of the operational and/or technical barrier elements. Therefore we have classified four main categories of safety critical personnel (positions with associated safety critical tasks) and categorized roles according to this.

The positions are classified as A, B, C and D.

The classification of safety critical positions is illustrating the relationships between tasks, personnel and an undesired event. By having control of the relation between barrier elements and safety critical positions, barriers can be managed through the focus on safety critical tasks. Based on this, actions can be made to ensure that these positions comply with the necessary requirements for a certain safety critical position. Performance influencing factors are defined as conditions that are of importance for barriers functions and barriers elements ability to function as intended (PSA 2013).

A tool for identifying safety critical tasks and key operating personnel is a mean for both making the organization more conscious on principles regarding barrier management, to create a framework for the offshore drilling company to work continuously on barrier management linked to competence and to be able to better assess the competence. Consequently, it means that competence is better linked to the barrier management system and can function more proactively as stressed by Hollnagel (2008).

Table 1. Category A, B, C and D personnel.

Cat.	Description
A	Positions that imply main responsibility of performance of tasks that represents operational barrier elements, which may *directly* result into an escalation towards one or several hazard if carried out in an incorrect manner.
B	Positions that implies main responsibility of planning, coordinate, advise and control the performance of tasks related to *operational barrier elements* that may directly result into an escalation towards one or several hazards if carried out in an incorrect manner (tasks performed by category A).
C	Positions that implies main responsibility of planning, coordinate, advise and control of tasks related to *maintenance of technical barrier elements* that prevent escalation towards one or several hazards (tasks performed by category D).
D	Positions that imply main responsibility of performance of tasks related to *maintenance of technical barrier elements, and/or performance of other tasks that supports safety critical personnel of category A, B and C.*

3.2 *Case description*

The concept "Safety Critical Tasks and Positions" was applied on a drilling rig operating on the Norwegian continental shelf. The work started out by developing a barrier philosophy for the company and a barrier strategy for each of the drilling rigs. In parallel, the maintenance program for one of the rigs was updated performing criticality analysis. For the technical barriers the main source of testing and verification is covered by the maintenance program and an effort was made to link tests and other maintenance activities to the barrier system. The barrier diagram for "Prevent

Table 2. Category A, B, C and D positions.

Cat.	Positions
A	Dynamic Positioning Operator
	Maritime Section Leader/chief mate
	Crane Operator
	Engine Room Operators
	Rig administrator
	Senior Driller
	Driller-Aux
	Derrickman
	Subsea engineer
B	Drilling Section Leader
	Toolpusher
	Offshore Installation Manager
	Safety Supervisor
	Medic
C	Technical Section Leader/Chief Engineer
	Electrical Section Leader
D	Derrickman Assistant
	Driller Assistant
	Roughneck
	Roughneck Trn
	Subsea Engineer Trn
	Able Seaman
	Crane Operator Assistant
	Boatswain
	Maintenance Operator
	Motorman
	Storekeeper
	Electrician
	Hydraulic Engineer
	Rig Mechanic
	Technical Assistant
	Welder

Blowout" in Figure 2 is a part of the barrier system for this specific rig. This work was carried out mainly in 2013.

While the technical barriers may be more concrete and tangible, the organizational barriers and the role of the personnel are foreseen as more unclear. To overcome this challenge we aimed to identify a means to link tasks/positions to barrier management using the concept "Safety Critical Task and Positions". After a workshop with the onshore organization, two consultants spent four days onboard the rig interviewing personnel to examine the tasks and responsibilities they were handling. A total of 16 interviews were carried out. The table below presents the results from the study and categories of the positions onboard the rig during normal operation. The picture for an emergency preparedness situation will be different.

The aim is to link the positions onboard the drilling rig to their safety critical tasks and the impact on the hazard situations. Below are some examples.

The DPO (Dynamic Positioning Operator) performs the following tasks; control of the rig (heel/trim), ballast, monitor radar, cargo handling, fire- and gas detection, logging, tension on line (anchor draw work). For the DP- operator, the following major accident hazards are relevant to the failure in performing his tasks as intended:

- Ship on Collision Course
- Ship Collision
- Loss of Position (DP)
- Reduced Buoyancy/Stability

The failure of the DPO in performing his safety critical tasks, for instance dynamic positioning and stability calculation as needed, can lead to reduced buoyancy and stability or total loss of stability. If the DPO does not perform the required navigational tasks or communicate with vessels on collision course and relevant personnel onboard the rig, this may cause a ship collision. Mishandling of the DP-system may cause the rig to lose position on DP, and this may escalate to other hazards (kick or blow out caused by the rig moving out of position and the riser may be damaged or well is not shut in when the rig is starting to move out of position). Consequently, the DPO is defined to be in category A.

The Offshore Installation Manager (OIM) plays an important role of any offshore installation. In this setting the OIM is only categorized as B during normal operations; main responsibility of planning, coordinate, advise and control the performance of tasks related to operational barrier elements that may directly result into an escalation towards one or several hazards. In an emergency and preparedness situation the role of the OIM is different. The OIM also plays an important role in fostering a safe culture that is a reporting, just, flexible and learning culture (Reason, 1997). Kjellén (2000) points to the importance of top management commitment to safety.

4 DISCUSSION

4.1 *Humans as organizational barrier elements*

In this paper we have given an introduction to barrier management and different approaches to the organizational aspects. The presented concept "Safety Critical Tasks and Positions" has illustrated how operational positions can be classified as safety critical in relation to major accident hazards. It can be argued that defining operational personnel as organizational barriers may enhance the respect and understanding of importance of their roles, and hence their competence. On the other hand, it should be emphasised that this should not as a consequence put all responsibility for preventing accidents on the sharp end of the organization, the overall responsibilities lies within the management offshore and onshore.

We see that the approach presented in this paper is in line with the approach from PSA when it comes to defining organizational barrier elements as the roles or personnel onboard. We will however claim that our concept of safety critical functions has one major advantage when it comes to implementation of barrier management. The actual relationship between positions/roles (organizational barrier elements) and operational barrier elements has to be represented and understood in order to conduct a more holistic barrier management. Identifying safety critical tasks and positions and the relationship to operational and technical barrier elements makes it possible to:

- Control and monitor whether the positions in the organizations are able to handle their entire task portfolio related to operational barriers
- Identifying the degree of redundancy of personnel necessary to perform safety critical tasks
- Identify and monitor resources and conditions necessary for performing the tasks in a correct manner (e.g. skills and knowledge, communication, workload/ time pressure etc.)

PSA (2013) guideline as shown in Figure 5 illustrates the integration of the barrier management with the safety management. It can be argued that if the barrier management system is defined with all barriers being in the "sharp end", it is not sufficient to monitor and control the barriers to control major accident risk. Major accident risk will also be highly related to safety critical decisions, planning and communication, not only in the offshore



Figure 5. Integration of the barrier management with safety management (PSA, 2013).

organization and in the "sharp end" but in the entire organization. The illustration in Figure 5 may be misleading as it may indicate that risk is under control by barrier management alone.

Defining and describing a barrier management system is not sufficient for having a positive safety effect. The system needs to be implemented as part of the risk management system. The concept presented in this paper can be described as participatory and the advantage of a participatory approach is that the personnel themselves has defined and constructed the system. This ensures verification against real life and ownership and understanding. Employee participation and involvement in safety barrier analysis can serve as a vehicle for the development and maintenance of safety barriers (Kongsvik et al. 2014).

The way we have classified personnel may give surprising results, but will contribute to empowerment of the operational personnel.

4.2 *The learning perspective*

By mapping and representing the relationship between operational and organizational barrier elements by the concept "Safety Critical Tasks and Positions" one may identify organizational vulnerability or even organizational dysfunctional aspects, related to the organization of the personnel, tasks and manning (e.g. responsibilities, task portfolios, work load, lack of redundancy of personnel etc.). This information may be used to improve the organizational design in order to improve the barrier functions.

Further, the status of the performance influencing factors may be continuously followed up through assessments or when major organizational changes are implemented. This demonstrates that barrier management is not only a separate tool but also an important factor integrated to the management of the organization.

We believe that the following elements are central in barrier management as fundament for learning. That is competence, communication and workload, physical working environment and leadership.

4.2.1 *Competence*

It can be argued that competence (knowledge, skills, experience and attitudes) play a crucial role in upholding the barriers both in maintaining the system and to execute the tasks in a safe manner. The procedures and documentations are the structures that support and enable the operators to perform the tasks in accordance with best practice.

4.2.2 *Communication*

The quality of communication, i.e. asking and feeling comfortable with asking for a Safe Job Analysis to be performed, play an immediate effect on the performance of the operations. Open and clear communication is always important in high risk organizations. Open and direct communication has been identified as a key factor within High Reliability Organization thinking (Weick & Sutcliffe, 2007). Providing a language and a vocabulary for barriers are important in order for personnel to be aware and work proactively with barriers.

4.2.3 *Workload, physical working environment and leadership*

Reporting on the working environment should lead to improvements in the organization and therefore aligned to the work of barriers. It could in turn lead to management of change. The function of management of change is to contribute to the management of all technical, operational and organizational changes in order to avoid major accidents. Leadership is seen as more indirect, but playing a significant role in order to create and establish commitment to the barrier management philosophy and strategy. It covers both the onshore and offshore execution of leadership. It is also about establishing and environment to act safe and put safety before production (Reason, 1997). The rig focuses on the operational side and more on day-to-day activities. The onshore organization is more on to the long-term planning and monitoring of activities. Workload and the physical environment will typically play an important, but more indirect role, on the performances. Perceived not so good work environment has a negative impact on

performances. However, a perceived positive working environment do not necessary lead to higher performance. Psychosocial questionnaire should therefore be indicators for performances.

4.2.4 *Learning perspective from an offshore management viewpoint*

The implementation part is where the concept of barrier management succeeds or fails. The study presented in this paper identified the key safety critical positions, the challenge for the onshore management is for these positions to be made aware of what exactly is required of them in a barrier management terms and through the management system of the company.

In general, where there is found reluctance offshore to embrace new soft safety skills, it can be stated that this is often due to the concept and practical applications not being fully explained to, and hence understood, by the personnel in these positions. Hopefully this approach will make them see their clear contribution both directly and indirectly. In addition we see the interplay and interaction between different personnel better illustrated with this concept.

If, we can convince these key safety critical positions and call them 'barrier keepers', of the need for, and a good understanding of a more modern approach to operational barriers i.e. placing less reliance on the use Observation/ STOP Card type systems and greater emphasis on the maintenance of barriers, then this will be carried over to other crew members.

We believe that this concept can contribute to more learning to assess what the organization has learned and also identify gaps. It is also an opportunity to assess if there is need for adjustment and critical look into existing practice and executing double loop learning (Argyris & Schön, 1978). This should be done regularly and if changes are introduced. Other studies such as psychosocial evaluations covering important topics as demand, resources, expectations, stress, management and bullying will give valuable input and make the system dynamic.

5 CONCLUDING REMARKS

As we have discussed in this paper, establishing a barrier management system does not in itself improve the safety level. It may however be an excellent "tool" for understanding and controlling risks. How the concept is defined, for instance how and what we define as organizational barrier elements, is of less importance giving that the barrier systems is constructed for the specific risk of the asset. This requires a good understanding of risk and the frame conditions influencing it. In this paper we have emphasized the importance of identifying and representing the relationship between operational personnel and barrier elements. Including operational personnel in the development of the barrier system, as we have described in this paper, is important for a successful implementation of barrier management.

The concept "safety critical tasks and positions" needs further development and need to be strengthened by more input for the work to be properly aligned. The work on barrier management provide valuable input and in particular to the assessment of the different safety critical tasks.

We believe that the work presented in this paper will meet the PSA (2013) expectations in terms of barrier management. However, this is development work and improvements need to be done. Several rigs will be employed on the Norwegian Continental Shelf and it is believed that the next industry battle will be a "battle for competence", therefore focusing on barrier management is not only a tool to control risk but might also be a tool to demonstrate the importance of different categories and for people to see that *"I have an important role in this organization and I too contribute with regards to barrier management"*. This could help personnel to see their role and responsibilities in the organization and create a more holistic meaning for them and thereby also include more symbolic aspects of the barrier management to further elaborate on Bolman and Deal's (1989) taxonomy. In this article we have looked into structural and human resource (learning, participation) aspects and touched upon symbolic aspect (seeing your positions as part of a holistic system. However, following the thinking of Bolman and Deal (1989) further work and development should also address the issue of power. Kongsvik et al. (2014) has given some suggestions focusing on participation.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all people in the rig company. We would also like to thank Synne-Emilie Bergersen & Lars-Erik Alstad Aas and two anonymous reviewers for providing us valuable and constructive comments on an earlier version of this paper.

REFERENCES

Argyris, C. & Schön, D. 1978. *Organizational learning: a theory of action perspective*. Reading, Massachusetts. Addison-Wesley.

Bolman, L.G. & Deal, T.E. 1989. *Reframing Organizations: Artistry, Choice, and Leadership.* Jossey Bass.

Duijm, N.A. 2009. Safety-barrier diagrams as a safety management tool. *Reliability Engineering and System Safety 94 (2)*: 332–341.

Ersdal, G. 2014. The Norwegian barrier regulation. Barrier management principles and application to marine system safety. Offshore Risk and Safety seminar, 2014.

Gibson, J. 1961. The contribution of experimental psychology to the formulation for the problem of safety. *Behavioral approaches to accident research*, 77–89.

Haddon, W. 1980. The Basic Strategies for Reducing Damage from Hazards of All Kinds. *Hazard Prevention.* Sept./Oct. 1980.

Hollnagel, E. 2008. Risk + barriers = safety? *Safety Science 46 (2)*: 221–229.

Hollnagel, E. 2004. *Barrier and accident prevention. Hampshire.* UK: Ashgate.

Johnson, W.G. 1980. *MORT safety assurance systems.* New York: Marcel Dekker.

Kjellén, U. 2000. Prevention of Accidents Through Experience Feedback. CRC Press.

Kongsvik, T., Haavik, T. & Gjøsund, G. 2014. Participatory safety barrier analysis; a case from the offshore maritime industry. *Journal of Risk Research, 17 (2):* 161–175, DOI: 10.1080/13669877.2012.761275.

PSA 2013. Principles for barrier management in the petroleum industry, 2013.

Rausand, M. 2011. *Risk assessment: theory, methods, and application.* Hoboken, NJ: Wiley.

Reason, J. 1997. *Managing risks of Organizational Accidents.* Ashgate.

Rosness, R., Guttormsen, G., Steiro, T. & Tinmannsvik, R.K. 2002. Organizational Accidents and Resilient Organizations: Five Perspectives.

SINTEF Industrial Management, STF38 A02413.

Sklet, S. 2006 a. Safety barriers: definition, classification, and performance. *Journal of Loss Prevention in the Process Industries 19 (5):* 494–506.

Sklet, S. 2006 b. Hydrocarbon releases on oil and gas platforms: Release scenarios and safety barriers. *Journal of Loss Prevention in the Process Industries 19 (5):* 481–493.

Sklet, S. Vinnem, J.E. & Aven, T. 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release); Part II Results from a case study. *Journal of Hazardous Materials*, *137 (2)*: 692–708.

Sklet, S., Steiro, T. & Tjelta, O. 2005. Qualitative analysis of human, technical and operational barrier elements during well interventions. ESREL 2005, Tri City, Poland. Balkema.

Weick, K.E. & Sutcliffe, K.M. 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* San Fransisco: Jossey-Bass.

Xue, L., Fan, J., Rausand, M. & Zhang, L. 2013. A safety barrier based accident model for offshore drilling blowouts. *Journal of Loss Prevention in the Process Industries, 26 (1)*: 164–171.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Presumptions of culture: Applications and safety implications

F. Størseth
Safety Research, SINTEF Technology and Society, Norway

ABSTRACT: Contemporary safety thinking is saturated with cultural ideas. Culture is presumed important—for safety. Culture has become part of the convention, the normal scientific approach to understand and improve safety. It is part of the standard toolbox in terms of explanatory and interpretive repertoire. But, what is the nature of the culture conceptions? How is culture "applied" in terms of interpretations and explanations? Pursuing such questions, this paper identifies conceptions of culture by conferring source material pertaining to the Norwegian petroleum industry (official documents and an incident investigation reports). The analysis was performed by establishing a set of analytical dimensions or thematic axes: *The What, The How, The Where, and The Who* of safety culture. The results of these analyses are discussed. The core thesis of this paper is that the premises, presumptions, and implications of a given concept need active consideration. And, in a mode of efficient application, there is a danger of merely pointing towards "culture", and omitting the necessary "detour" of specifying suppositions and implications involved in the given cultural concept. This underscores the need to actively "apply" theory (Størseth and Grøtan, 2011). By addressing issues of theoretical underpinnings and presumptions concerning association, function and causality—a needed, additional layer of analysis and learning as application (Baumard, 1999; Størseth and Tinmannsvik, 2013) is forced into consideration, bringing awareness to the "directions" that silently influence interpretive and explanatory efforts to understand and improve safety.

1 INTRODUCTION

The text should fit exactly into the type area of 187 × Culture is part of the explanatory and interpretive repertoire. Culture is presumed important—for safety. But, what is the nature of the culture conceptions? How is culture "applied" in terms of interpretations and explanations? What are the implications of the chosen path? Inspired by such questions, this paper aims to identify theoretical underpinnings and conceptual building blocks of culture as it is described, defined and applied within the context of Norwegian Petroleum industry. This aim was specified by formulating a set of analytical dimensions or thematic axes. These are loosely formed themes and elements with the intention of creating an analytical platform, a defined approach for searching for ideas related to culture. The principal idea that is pursued here is the value of creating an angle, a reference point for thinking and analysis. The formulated analytical dimensions were:

Concept features: What are the presumed key features, dimensions and elements? This involves searching for definitions, operationalizations, characterizations, theories and philosophies. In short: What?

Concept model supposition: How is the concept interpreted, construed and explained? This involves looking for explanatory dynamics. How are core issues related to the concept explained? What are the advocated associations? In short: How?

Concept placement: Where is the concept (e.g. 'safety culture') placed? This involves looking for where—in given systems/organizations dimensions and dynamics of culture are thought located. In short: Where?

Concept actors defined: Who are defined and identified as concept actors and agents? This involves who is argued as the 'cultural creators' and/or 'cultural bearers'; i.e. who are pinpointed and argued as being responsible for acting out given cultural features. In short: Who?

2 METHOD

According to Bem and deJong, researchers and scientists must move beyond inspection, enumeration and description of the observed (Bem and deJong, 1997). The author concurs and derives from this that the scientific effort must involve elements of construction, in the sense of using our imagination, or pre-understandings, or theories with the intention of moving beyond the observable. The following reports how these efforts were pursued methodologically.

2.1 *Reflection as method*

The defined aim of the study was to explore and identify 'premises of culture'. The founding idea was to explore the workings of culture concepts and conceptions; how they develop, take form, move and have implications. To approach these issues, a set of documents were selected as analytical basis:

- An official Petroleum Safety Authority (PSA) investigation report (PSA, 2012)
- A PSA booklet on HSE and culture (PSA, 2002)
- A PSA article on principles of barrier management (PSA, 2013)

In a classical scientific sense, these documents served as the source material, the *empirical data*. However, my analytical approach, i.e. the way I made use of these data sources can be said to involve a blurring of the lines between data (observations) and going beyond the observables (theory). This is an old challenge for philosophers of science (Bem and de Jong, 1997). A variation of this "dilemma" has been addressed specifically by advocating the premise that "theory *is* method" (see Størseth and Grøtan, 2011).

My methodological approach can be denoted as *reflexive*. Specifically this involved a continuous oscillation between (document) analysis and collaborative reflection and discussion of findings with my research colleagues. To elaborate on this: We were four researchers involved in the research task that this study is part of; four different researchers each representing different scientific traditions and "denominations". My deliberate choice was to make use of this variety. Thus, I decided to approach the work in the following manner:

1. Individual analysis of selected material. A report/article/investigation report was selected for individual analysis. These individual analyses served as input/context for a reflection meeting reserved for discussing the findings.
2. Reflection meetings to test and develop hypotheses, conjectures and findings from my individual analyses. Through these reflection sessions, my working models, assumptions, as well as findings were tried, refuted, and—and developed. In turn, serving as the next step forward in terms of analytical efforts.
3. Application of the reflection meeting discoveries in subsequent individual document analysis. Here, my analytical effort shows its (hermeneutical) circular shape.

In this way, I deliberately opened up for a research approach that placed me (the researcher) as part of the process. This is close to what Alvesson and Sköldberg (2009) denote the principle of abduction.

2.2 *The principle of abduction*

Abduction denotes a process that blurs the lines between induction and deduction. Like induction, the abductive process begins with an empirical basis. But importantly, theoretical preconceptions are never rejected. They are accepted, and allowed to influence and "color" the analysis. In this sense, abduction is closer to deduction.

Analyzing empirical "facts" may here be both combined with, and preceded by various sets of theory and conjecture. This suggests an approach where theory may serve as an inspiration for how to observe, as well as vice versa; i.e. that the "facts" (the observables) may represent sources of inspiration for theory. *"Facts" "serve to occasion the theory, while continually plying the role of critical tuning instrument and fount of new ideas for the theory"* (Alvesson and Sköldberg, 2009, page 4). As noted by Alvesson and Sköldberg, the acknowledgement and application of pre-understanding is a similarity to hermeneutical method (e.g. Eco, 1990).

The principle of abduction illuminates the reflection process throughout my study. In other words, it shows how I (the researcher) applied and made use of the "facts" (documents). It also emphasizes the intentional alternation between data analysis, application of theory, and reflection processes that tested and developed conjectures along the line of the study.

My methodological approach is more about reflection than procedure. But, as shown above, the analytical process has been systematically pursued—by an intentionally designed work process, continually alternating between individual analysis, collaborative reflection and development of our results and conjectures.

3 RESULTS

3.1 *PSAs HSE culture booklet*

PSA defines culture as: "the knowledge, values, norms, ideas and attitudes which characterize a group of people" (PSA, 2002, page 5–6). This definition lists cultural components or dimensions and can thus be seen as the formal framing of 'The What'. According to PSA, culture is about technology, economics, law and regulation. This also resonates with 'The What'. It may be read to suggest the various spheres that (HSE) culture may be part of; or it may suggest various contexts of which it (HSE culture) is associated with. In any case, the context(s) that are suggested are vast and indefinite.

Norwegian regulations (from 2002) demands that companies possess what is described as a "sound HSE culture". However, as emphasized by PSA, these regulations offer no clear definition of culture. Consequently, PSA's intention (via the HSE culture booklet) is to provide approaches to understand culture, so that to enable "such a culture to be created" (PSA, 2002, page 3–4).

This aim is interesting in that it explicitly states that culture can be designed and shaped. In a very generic sense then, this relates to 'The How'; the HSE culture concept is possible by effort. It is presumed formable and shapeable. Furthermore, emphasis is put on the necessary connection between words and actions, a clear message underscoring the notion that culture is more than a dormant set of values. Culture is reflected in action, in what is done, and how. A similar point is made by underscoring that culture is more than some compound of knowledge, values and attitudes (PSA, 2002).

PSA states that a sound HSE culture is a reporting, just, flexible, and learning culture. For our purposes, the focus on learning is of particular interest, as it carries suggestions for both 'The Where' (i.e. concept placement in the form of where culture thought to be placed or positioned), as well as 'The Who' (i.e. the designated ambassadors of culture). PSA draw attention to issues regarding learning and conflicting objectives. They list a specific set of checkpoints in these regards, see Table 1.

The checkpoints (above) contain *a sense of direction*, a direction which also conveys information about 'The Where' and 'The Who'. There is a sense of u*ni-directionality* at play here, from somewhere (management?) to the operational. Do they (operational) have the sufficient criteria to realize or "live by" the culture? It is here to be argued that the checkpoint has a certain "flavor" of uni-direction that subtly suggests (1) where culture is "designed", and (2) who are thought to be the designated ambassadors of such culture. Although this conveys presumptions concerning a possible cultural design process, PSA put emphasis to the fact that cultural change is related to a range of factors. In fact, they present a model that encompasses a wide context for culture and cultural change.

PSA emphasize that *"Many factors can cause cultural change in an enterprise, as in the wider community. Some of these factors are listed in the cultural model (…). They represent the frame conditions for petroleum activities and offshore work. At the same time, we influence these frame conditions through our knowledge, values and norms"* (PSA, 2002, page 23–24). A rendition of the model as referred to in the quote is presented in Figure 1.

The figure illustrates forces of mutual interplay and influence. Discussing the cultural model, PSA point towards several challenges that needs careful consideration:

- Cultural variation and culture in plural form: sub-cultures, counter-cultures etc.
- The potential individual influence
- Power
- The danger of superficial culture diagnosis (no quick fix, neither with disciplining or bureaucratization/procedures)

PSA states clearly that there are no short-cuts. Building culture is demanding. But, who are the builders? Who are the creators of culture? Although the cultural model (Fig. 1) establishes reciprocity, there is a tone here that seems to further suggest that norms and values are to be adequately

Table 1. PSA checkpoints regarding conflicting objectives.

1	Are conflicting objectives discussed in a specific and constructive manner?
2	Have clear, realistic and accepted criteria been established for the way operational personnel should deal with normal conflicts between objectives?
3	Are procedures and job descriptions adjusted to ensure a balance between safety and efficient performance of the work?
4	Who decides the procedures? Do operational personnel participate in maintaining procedures and job descriptions?
5	Who decides the procedures? Do operational personnel participate in maintaining procedures and job descriptions?

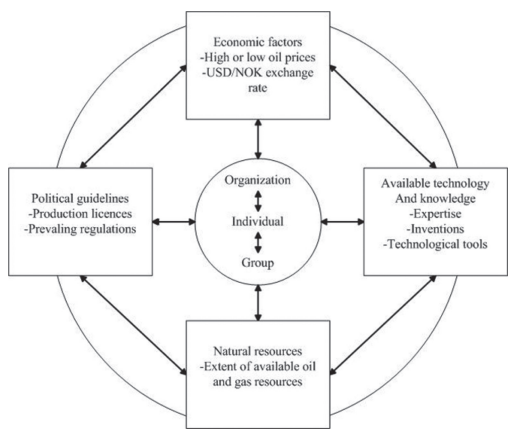


Figure 1. PSAs cultural model (PSA HSE culture thematic brochure, 2002, page 24).

established, and then released into the system for correct adherence and administration. Personnel must be trained, instructed or "prepared". The implication of the latter is that it is the personnel that are the designated "bearers" of culture—the actors defined as to adhere to the given culture.

This impression is strengthened considering the final section in the thematic brochure. The section is entitled "Section 6 Management and culture". Starting with a reference to an official publication on Norwegian framework regulations (Section 11; Report 7 2001–2002 to the Storting, specifying that what is given attention and priority by management becomes culture). It is stated that: *"The management plays a key role as the provider of the company's values and visions in the HSE area"* (PSA, 2002, page 31–32). The section holds several tips for how the manager/management, closing with the following: *"Managers who can take the pulse of their own organization and who pick up small but important nuances in the working climate have everything it takes to be a good culture-builder"* (ibid).

3.2 *PSAs principles for barrier management*

Barrier management refers to a systematic, ongoing effort to ensure that safety barriers are relevant, effective and robust. The main purpose is to establish risk handling barriers, aiming to prevent undesirable events or limiting their consequences, should they occur. Barrier management denotes the processes, systems, solutions and measures that are needed in order to ensure necessary risk reduction (PSA, 2013). These definitions provide insight into how barriers are managed (PSA, 2013, page 3):

Barrier: Technical, operational and organizational elements which are intended individually or collectively to reduce possibility for a specific error, hazard or accident to occur, or which limit its harm/disadvantages.

Barrier element: Technical, operational or organizational measures or solutions which play a part in realizing a barrier function. *Barrier function:* The task or role of a barrier. Examples include preventing leaks or ignition, reducing fire loads, ensuring acceptable evacuation and preventing hearing damage.

Performance influencing factors: Conditions which are significant for the ability of barrier functions and elements to perform as intended.

The following passage illustrates how these concepts are related: *"Personnel, equipment and systems are referred to or described not as barriers, but as barrier elements. Performance requirements must be set for the technical, operational or organisation elements required for the individual barrier to be effective (in other words, to realise its barrier function)" (PSA, 2013, page 5).*

Where do conceptions of culture fit into this? Although culture is referred to repeatedly, the purpose is not to include it into the barrier management as such. 'The Where' is defined as outside of the barrier management control scope; but—culture is still appointed as an important potential contributor. This suggests influence without further specification.

Is 'The How' left open? This is a question for the discussion section.

Attention is now turned to the Heimdal incident, as an example of where culture conceptions are put into application.

3.3 *The Heimdal incident*

The incident. On the 25th of May 2012 a hydro carbon leak occurred on the Heimdal installation (Statoil) during a testing of two emergency shutdown valves. The testing of the emergency valves was prepared by pressure releasing a pipeline towards the torch. In this pipeline, a ball valve is the final barrier against the torch. This valve was exposed to a pressure far beyond design, and it failed. A gas leak was a fact. The leak was estimated as 3500 kg with a leak rate on 16, 9 kg/s. Gas was detected in a wide area of the installation. PSA concludes that the event led to a very serious situation and that a major accident could have been the result with marginally changed circumstances (PSA, 2012).

Investigation report. PSA identified the immediate cause as a ball valve (final barrier towards torch) that was exposed to a pressure that far exceeded its design pressure. The valve failed.

Underlying causes. PSA identify weakened performance shaping factors are the most important underlying causes contributing to the incident (PSA, 2012, page 20). The most important incident causes were identified as inadequate design combined with inadequate risk assessments and procedures for valve opening/shutting (ibid, page 21). PSA build explanatory momentum in their investigation report by emphasizing connections between deficient leadership involvement and lack of experience transfer and learning:

Deficient leadership involvement. PSA argue for a discrepancy between the company's defined 'A-standard[1]' and the way that the work was performed. PSA also draws attention to the fact that in addition to the A-standard, the Statoil-book

[1]A "common performance pattern" defined by the company; meant to identify risk related to the activity and demands connected with the activity (formal demands, work method).

emphasizes the importance of compliance and leadership. This explicitly denotes leader responsibility as communicator, role model, instructor and guide/advisor in an A-standard. Also, continuous risk assessment en route in the work operations is to be performed. PSA states that they cannot see the leaders in the Heimdal organization, neither on—or offshore has functioned as role model, trainer or advisor for an execution of the A-standard performance pattern with accompanying risk assessments.

PSA point towards a range of factors that the associate with inadequate risk assessments concerning the task at hand:

- Lack of leadership involvement
- Lack of personnel involvement in planning the work
- Deficient communication to personnel (that were to execute the operation)
- Inadequate labeling of valves
- Unclear specification of how to perform the task in hard to read procedures

Lack of experience transfer and learning. PSA identifies a lack of using previous incidents for learning. Information from previous incidents are not processed, communicated and applied for learning purposes in the Heimdal organization. PSA provide several reasons for this. For instance, by reviewing the company's own incident reports, they find that several of the incidents has its background in a combination of technical failure, weak design and the operation of the installation/facility. It is also pointed out in several of these reports that there previously has been repeating similar incidents.

Still, this has according to PSA not lead to any measures to prevent repetition. PSA draws attention to PSAs yearly report "Risk level on the Norwegian shelf" (RNNP) which contains a major risk indicator for hydro carbon leaks. PSAs point is that it is the companies themselves that provide data from their own incidents here. In other words, the incidents should be known to Statoil and the parts of the organization they are relevant for. PSA also refer to a study concerning hydro carbon leakage causes on the Norwegian shelf that was performed by the RNNP in 2010. The study identified a range of hydro carbon leaks on due to human intervention in technical solutions with unfortunate design. The study identified a need to redesign these solutions to reduce risk. The study has been sent and communicated to Statoil. Still, there is according to PSA no trace of this knowledge been applied.

PSA identifies weaknesses in terms of necessary competence and risk understanding. PSA states that Statoil has not ensured that personnel (both land—and offshore) had the necessary competence and risk understanding for handling the work in a safe manner. PSA argues that the incident showed a deficiency on a wide range of levels (barrier elements and performance influencing factors. The culture reference is indirect here; via the emphasis on performance influencing factors.

But what discriminates the one from the other? Where is the line to be drawn, between performance influencing background factor and barrier element? With this we re-visit the challenges of barrier management. That is, the challenges concerning categories and classifications. Is culture by definition outside of the control scope? Or, is it "allowed" to appear and potentially affect barrier elements?

4 DISCUSSION

4.1 *The HSE culture booklet*

The operationalization and contextualization of the concept is theoretically thorough and has what can be denoted as "scholarly appeal" in terms of both depth and width. Further thoroughness is added considering how PSA acknowledges the complexity and challenges related to how the petroleum industry is organized (operators vs. contractors, sub-contracting). Still, the complexity and broad scope that is established serves as a strong reminder: How is this to be controlled? Shaped? Regulated?

Design by management? Is culture a management project? Is culture design a designated task for management? The culture booklet conjures up a kind of one-sided force of influence. In the checkpoints, both criteria and procedures are emphasized as important, to provide the operationals' with tools and judgment aids for safe and efficient operation. Although there is nothing inherently wrong with this, there is a unidirectional "flavor" to this that is strengthened by the fact that no emphasis is put on any complementing criteria or procedures in more distant corners (further away from operation).

Although not stated, it could be speculated that "operational" applies all over the system. However, as this is not stated explicitly, attention is somewhat drawn towards operational in the closer proximities to hazard. It must be noted however, that this unidirectional hint is moderated when PSA discuss factors that may affect HSE culture (page 23–30). But still, the management orchestration responsibilities are emphasized. Of course, pointing towards management responsibility can be said to be nothing but natural. But, given the potential role of such a document, there may be a risk of consolidating a view that establishes management as 'The Who' in terms of cultural shaping or design.

If so, an unfortunate effect could be that the mutual dynamics and reciprocity of cultural building is lost. In other words, that mutual responsibilities and possibilities of cultural development and performance are pushed out of scope.

4.2 *Barriers and the cultural backdrop*

Although the importance of culture is emphasized, the argumentation is that culture is outside of the barrier management scope. This is not to say that it is unimportant. Rather, culture is referred to as one of several more or less abstract background "conditions". Culture is placed within the category "performance influencing factors" group. These are factors held as potentially important. But, they are argued as not within range of being established as barrier elements accompanied by performance requirements. On page 26, PSA explicitly presents a reason for not bringing culture in as a barrier element: *"One of the stipulations for a barrier element is that performance requirements must be set for it, and that this performance must be verifiable. Investigations and surveys can be conducted into the culture in an enterprise, for example,* ***but it will be difficult to establish verifiable performance requirements for that culture****. So culture cannot be regarded as a barrier element" (emphasis added).*

Is culture omitted because it is impossible to control (performance requirements)? Or is it because culture, by default represents "something" too far from barrier realizing actions and decisions? No answer will be provided here. Still, it is interesting to note the distinction between what is presumed in the culture booklet in terms of a shapeable culture, and what is noted regarding barrier management: that culture is beyond the control scope.

It is here to be argued that by defining culture as outside the range of barrier element control; 'The How' of cultural influence may be at risk of being downplayed, if not ignored.

It is hard to disagree with a model that places culture in "the background"; as part of the context—something "back there". At the same time, features of culture may exert its influence in specific ways, in specific situations. Effects or (unwanted) side effects of a culture may indeed exert its specific influence. By categorically placing culture as "outside" there is a danger of letting cultural aspects pass unattended. Cultural aspects that potentially would be of critical importance in terms of realizing a barrier function.

Hopkins' (2012) analysis of the Macondo blowout is a strong example here (see National Commission report, 2011a, 2011b). Hopkins put emphasis to the fact that dynamics of e.g. consensus-mode, normalization of warnings (Vaughan, 2005), and groupthink were part of how signals were "effectively" ignored in the run-up to the blowout.

4.3 *The Heimdal incident*

Culture is not referred to by name here; that is, the concept is not explicitly referred to. Still, ideas permeated with culture are part of PSAs interpretation and suggested explanation. Culture dynamics are *applied* to build the thesis of the investigation.

PSA emphasize weakened performance influencing factors as the most important underlying causes. PSA defines performance influencing factors as "Conditions which are significant for the ability of barrier functions and elements to perform as intended" (PSA, 2012, page 3). As noted above (section on principles for barrier management), performance influencing factors are classified as outside of any specific barrier element.

Although the causes are defined as underlying, it is here to be suggested that they may quickly become linked to the three barrier elements. This is by "methodological default", as it is the barrier elements that are defined as within the control scope. In fact, the investigation can be said to implicitly build its case by showing how background cultural aspects (performance influencing factors) do exert active influence *within* the triad of barrier elements. If so, this stands in opposition to what PSA states regarding barrier management.

This underscores the challenges concerning "the cultural influence". If nothing else, it shows the importance of staying wary of the premises that concepts, methods and approaches are rested upon.

4.4 *Conclusions*

Before concluding, it must be emphasized that this study is no PSA witch-hunt. The heavy focus on PSA documents is however justified in light of their importance within the Norwegian context. PSAs role in the Norwegian petroleum industry is very active, not only in terms of their control mandate, but also in terms of setting the safety agenda. This is reflected in their communication and collaboration with various research organizations in Norway, but also with their focus on dialogue and communication with the industry.

The starting point for this study was to examine concepts and conceptions of culture in the Norwegian petroleum industry context. By analyzing a selected set of texts and documents, the study has put the foundational premises and assumptions to the fore front.

By focusing on presumptions and applications of the culture concept, the analysis has identified theoretical principles and ideas of association that

rests somewhat hidden within the culture concept; but that potentially influence interpretation and explanation.

Specifically, the study has identified:

- How theoretical premises contain ideas of unidirectional influence in terms of 'The What', 'The How', 'The Where', and 'The Who' of how culture is being designed and constructed.
- How culture in one sense is being defined by default as being outside the control scope; but that in terms of interpretation and explanation of an incident reveals ideas of how culture stretches into, and affects the barrier functions "up front". This demonstrates the challenges of applying static categories and classes that are kept controllable for methodological purposes.

The focus in this study was "locked on" the culture concept. However, the main message here is of concern for safety work and management in a generic sense.

The generic conclusion that should be derived from this is that theoretical and conceptual "building blocks" deserve constant attention as they exert influence in terms of interpretation and explanation of safety.

The Norwegian petroleum industry is efficient and professional, with highly skilled professionals involved: safety authorities, the industry themselves, researchers and consultants. But, it is precisely this efficient and professional work mode that creates a danger in that various concepts (like "culture") are eagerly taken aboard and efficiently installed as part of the prevailing, often tacit world views.

In this mode of efficient application, there is a danger of merely pointing towards "culture", and omitting the necessary "detour" of specifying suppositions and implications involved in the given concept (in this case: cultural concept). This underscores the need for a more active application of theory (Størseth and Grøtan, 2011). By addressing issues of theoretical underpinnings and presumptions concerning association, function and causality, a needed, additional layer of analysis and learning as application (Baumard, 1999; Størseth and Tinmannsvik, 2013) is forced into consideration, bringing awareness to the "directions" that silently influence interpretive and explanatory efforts to understand and improve safety.

ACKNOWLEDGEMENTS

This work has been carried out as part of the project entitled Translating HSE culture within the petroleum industry ('TRACULT'), led by Studio Apertura at NTNU Samfunnsforskning AS and funded by The Research Council of Norway. The paper represents the opinions of the author and does not necessarily reflect the opinions or policies of the above mentioned organizations.

REFERENCES

Alvesson, M. and Sköldberg, K. 2009. *Reflexive Methodology. New Vistas for Qualitative Research,* Sage Publications.

Baumard, P., 1999. *Tacit Knowledge in Organizations*. Sage Publications, London.

Bem, S. de Jong, H.L. 1997. *Theoretical issues in psychology—An introduction.* Sage Publications.

Eco, U. 1990. *The Limits of Interpretation.* Bloomington: Indiana University Press.

Hopkins, A. 2012. *Disastrous Decisions. The Human and Organisational Causes of the Gulf of Mexico Blowout.* CCH Australia Limited.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011a. *Deepwater—The Gulf Oil Disaster and the Future of Offshore Drilling*. Report to the President.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011b. *The Chief Councel's Report. Macondo—The Gulf Oil Disaster. A supplement to the report to the President.*

PSA, 2002. *HSE and culture*, Petroleum Safety Authority Norway.

PSA, 2012. *Report after investigation of hydro carbon leakage on Heimdal 26.05.2012,* Petroleum Safety Authority Norway.

PSA, 2013. *Principles for barrier management in the petroleum industry,* Petroleum Safety Authority Norway.

Størseth, F. and Grøtan, T.O. 2011. Safety theoretical issues: scientific please, but keep it brief. *The 20th European Safety and Reliability Conference (ESREL 2011)*, Troyes, France, 18–22 Sept. 2011.

Størseth, F., Tinmannsvik, R.K. 2013. The critical re-action: learning from accidents, *Safety Science*, 50 (10), 1977–1982.

Vaughan, D., 2005. System effects: on slippery slopes, repeating negative patterns, and learning from mistake? In: Starbuck, W.H., Farjoun, M. (Eds.), *Organization at the limit. Lessons from the Columbia Disaster*. Blackwell Publishing, pp. 41–59.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Coding scheme to measure the operator's workload in advanced Main Control Room

S. Kim, Y. Kim & W. Jung
Korea Atomic Energy Research Institute, Daejeon, R.O. Korea

ABSTRACT: In an advanced main control room, the system operation is possible since the power plant facilities are controlled using the soft control embodied into the computerized procedures and distributed computers completely equipped with digital functions. Accordingly, though the task of the operators has been changed a great deal, due to a lack of appropriate guidelines on the role allocation or communication method of the operators, operators should follow the operating strategies of conventional MCR and the problem of an unbalanced workload for each operator can be raised. Thus, it is necessary to enhance the operation capability and improve the plant safety by developing guidelines on the role definition and communication of operators in an advanced MCR. In this research, to resolve this problem, we propose a COgnitive, Communicative and Operational Activities measurement approach (COCOA) to measure and evaluate the workload of operators in an advanced MCR. To check the applicability of COCOA, we evaluated the operator workload of an advanced MCR of a reference power plant through simulation training experiments. As a result, the amount of high workload of the Shift Supervisor (SS) was observed in relation to the computerized procedure system newly introduced into the environment of an advanced MCR. On the basis of these observations, it is necessary to reestablish the role and communication method of MCR operators suitable to the new operational environment and changed work and develop the appropriate operating guidelines.

1 INTRODUCTION

In a conventional Main Control Room (MCR) of a nuclear power plant, to operate the system facilities, the operators of each system operate various devices of the power plants by actuating the control switches on the board classified into each section. In an advanced main control room, however, the system operation is possible since the power plant facilities are controlled using the soft control embodied into the computerized procedures and distributed computers completely equipped with digital functions. Thus, for the operation of power plant facilities, while the operators of a conventional MCR can complete the work with the primary operation of the facilities, the operators under the environment of an advanced MCR need to additionally conduct such secondary operations as a GUI screen operation, which is not observed in a conventional MCR.

In addition, another feature of an advanced MCR is the use of computerized procedures [O'hara, 2002]. While the operators refer to the operating procedures written on a piece of paper in conventional power plants, the operators of an advanced MCR refer to the contents of relevant computerized operating procedures using computers. The execution of the computerized procedures of the advanced MCR includes logging of the step execution results of the procedures on computers in addition to the screen operation. As the feature of the computerized procedures of the advanced MCR, this requires the operators to conduct a new type of task.

Thus, the MMIS environment of the advanced MCR developed to improve the convenience of operation demands the operators to conduct more tasks on security of the exactness and convenience. Accordingly, though the work of operators has been changed a great deal, due to a lack of appropriate guidelines on the role allocation or communication method of operators, the problem of an unbalanced workload for each operator has been raised. Thus, it is necessary to enhance the operation capability by developing the guidelines on the role definition and communication of operators in an advanced MCR of NPPs. In order to resolve this problem, however, a method of measuring the workload according to the work execution of the operators is necessary, but the applicable method is not available at this time. In other words, due to the operational activities of operators characterized by the digital MMI environment of the advanced MCR, it is necessary to develop a framework

suitable to a measurement of the workload of the advanced MCR.

The objective of this research is to reestablish the role and communication method of MCR operators suitable to the new operational environment and changed work by developing an analytical system to evaluate the workload according to the work execution of the power plant operators in order to resolve the matters mentioned above and to contribute to a stable operation of NPPs by developing relevant operation guidelines and enhancing the operation capability in the new MMI operational environment.

In this research, we propose a COgnitive, Communicative and Operational Activities measurement approach (COCOA) to measure and evaluate the workload of operators in an advanced MCR.

2 BACKGROUND

2.1 *The necessity of workload measurement in the advanced MCR*

The basic requisite of the advanced MCR in nuclear power plants is to provide operators with the convenient factors for accurate and fast operations by equipping them with a variety of digital MMIS functions. The major functions that the advanced MCR should have are said to be Advanced Alarm System, Group-View Display on which operators can share the same screen and information, Soft Control in which electronic control is feasible by using computer GUI screens, Computer-based Procedure System to execute procedures using computer screens, and Computerized Operator Support System/Advanced Communication System to assist in situational awareness and decision making of operators [O'hara, 2002].

In other words, an advanced MCR is the design to which the state-of-the-art MMIS technology is introduced to display all the operations on monitors, showing a lot of differences from the board type of a conventional MCR in not only the work environment but also the task procedures and execution methods of the operators.

In particular, due to the use of Computer Based Procedures (CBPs), abnormal and emergency operations show large differences in the areas of information acquisition, operational control, role allocation of each assignment, and communication of operators in comparison with the task conducted with paper procedures under the environment of the conventional MCR. For example, in the board type of the conventional MCR, the operators actuate switches by moving, to operate the facilities of power plants, to the board on which the switches of relevant facilities are arranged, but in an advanced MCR, the operators can operate relevant facilities without locational shift using the Soft Controls of computers.

Thus, the work processing method of an advanced control room makes big differences in two aspects from that of conventional nuclear power plants.

First, there is a big difference in the information acquisition method on the conditions of the power plants and physical operation variables. Though in conventional MCR the Shift Supervisor (SS) in total charge of the operation can confirm the system conditions and operation variables of the power plants through communication with the Board Operator (BO) as Reactor Operator (RO), Turbine Operator (TO), and Electrical Operator (EO), in the advanced control room the entire operators including the SS can acquire and confirm the entire operation information through the Large Display Panel (LDP) and each operator's monitor.

Second, the advanced control room uses CBPs instead of paper document procedures. In the conventional MCR, SS conducts procedures while providing order and confirmation to BO with Paper Based Procedures (PBPs). On the other hand, in the advanced MCR, SS can confirm the necessary operation information through the LDP and his own monitor while conducting CBPs. Of course, SS instructs relevant operators to operate the instruments and equipment. It is a big difference that SS must operate for a conduction of procedures the system called CBPs in the advanced control room.

Table 1 shows the major differences in the operational environment of operators between the advanced main control room and the main control room of conventional nuclear power plants.

In this way, the environmental change of the MCR has caused the operation principles and roles of operators.

First of all, SS can confirm/check the conduction of procedures and the execution actions of RO/TO/EO while confirming directly operation variables without relying on RO/TO/EO. Second, the entire operators added to their work the use of a new system called CBPs and Soft Controls, increasing the procedural workload. Third, direct confirmation of operation information enabled the contents and methods of communication between operators can be changed.

Such changes in the control room environment affect the information acquisition and operation method of operators and eventually cannot but have an influence on the role and communication method of operators. According to what was observed at the time of verifying human engineering conducted during the design process of an

Table 1. Major differences in the operational environment of operators between conventional MCR and advanced MCR.

	Conventional MCR		Advanced MCR	
	SS	BO	SS	BO
Direct plant information gathering	X (SS can't get the plant operational variables without relying on board operators)	O	O	O
Using emergency operating procedure	O	X (BO performs the countermeasures according to SS's order without EOP)	O	O

advanced main control room, however, various types of operation methods were observed due to a lack of sufficient operational guidelines in such field.

Even though CBPs include such a support function as a supply of operational information, the workload of SS and BOs tend to increase since they have to use the new system called CBPs in order to execute the procedures.

Therefore, it is necessary to evaluate the effect of an advanced control room environment on the role and communication of operators, reestablish the role of each assignment in case of using CBPs and Soft Controls in comparison with the operational task of conventional standard nuclear power plants, and develop the guidelines on communication methods.

2.2 *Related work*

Since the operators in the Main Control Room (MCR) of NPPs or chemical plants may severely decrease their work performance in case they have a severe cognitive workload, methods to measure cognitive workload have been studied for a long time. The cognitive workload is in general defined from the difference between the capability of operators and the required resource for conduction of their tasks [Eggemeier et al., 1991][Gopher et al., 1986]. Basically, the method to calculate the cognitive workload is classified into four approaches of work performance-based measures, subjective workload method, task load analysis method and physiological monitoring method [Embrey et al., 2006].

The work performance-based measures analyze the workloads from the speed, accuracy, or error rate of the demanded tasks. In some cases, one or two additional tasks are required to the subjects for deeply understanding the availability of the cognitive resources [Cain, 2007].

The subjective workload measures evaluate the workloads on the basis of subjective experience for the demanded tasks. It primarily uses self-reporting questionnaires which ask the beliefs, values, preferences, and attitudes of the respondents. MCH (Modified Cooper-Harper), NASA TLX (Task Load Index) and SWAT (Subjective Workload Assessment Technique) are developed for evaluation of subjective cognitive workload measurement method [Wierwille and Casali, 1983][Hart and Staveland, 1988][Reid and Nygren, 1988].

The task load analysis approach calculates the requirements of target tasks as they are which may provide the psychological influence of the operators. This approach measures the workload by estimating the resources used for tasks [Mitchell, 2000a].

The physiological measures record the physiological signals that are strongly associated with the subjective experience of the operators. Electroencephalogram (EEG) is a record of voltage difference between various points on the head surface[Humphrey and Kramer, 1994]. Electrocardiography (ECG) is the most widely used method to measure the electrical activity within the heart. [Meshkati, 1988]. Electrodermal Activity (EDA) is a technique to measure electrical phenomena on the skin, and is used to understand the psychological state including the mental load. In addition, Electrooculography (EOG) is a technique to measure the movement of the eyeballs. High workload requirements cause a response delay in eyeball flickering and show a response to decrease the closed time of the eyes [Kramer, 1991].

Finally, the task load analysis approach calculates the requirements of target tasks as they are which may provide the psychological influence of the operators. This approach measures the workload by estimating the resources used for tasks [Mitchell, 2000a][Mitchell, 2000b]. It also evaluates the psychological and environmental factors that may affect the performance of the operators.

3 A PROPOSAL ON METHODOLOGIES FOR EVALUATION OF WORKLOAD OF OPERATORS

3.1 *Framework for evaluation of workload*

As explained in the previous section, in order to determine the workload of operators in the advanced MCR, both the communicative behavior between operators and the operational behavior for operation of MMIS-based control equipment should be considered in addition to a measurement of the cognitive workload. In order to resolve this problem, this research is based on the workload measurement method used in various existing fields, and it was realized in the way of integration with the workload analysis method required additionally.

The framework for operator workload measurement presented in this research is Cognitive, Communicative and Operational Activities Measurement Approach (COCOA), the method judged on the basis of the three-dimensional classification of cognitive task, communicative task and operational task.

First of all, the cognitive task represents the cognitive activities of operators conducted for operation and situation handling of the power plants. For classification of the cognitive task, we used the task classification scheme proposed by Hollnagel. [Hollnagel, 1996].

The communicative task represents the communicative activities of operators conducted for operation and situation handling of the power plants, such as information exchange between operators and instructions. The communicative classification table presented in the Extended Speech Act Coding Scheme developed by Kim was used for classification of the communicative task. [Kim et al., 2010]. Finally, the operational task represents the behavior which operators take to conduct the cognitive activities and it was newly defined in this research depending on the necessity.

Figure 1 shows the framework for 3 activities-based COCOA workload measurement used in this analysis.

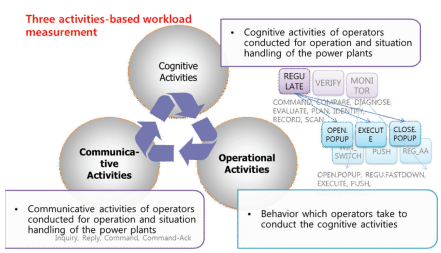


Figure 1. COCOA workload measurement framework.

As shown in Figure 1, it may be found that the task conducted by operators in the MCR of NPPs consists of cognitive activities, communicative activities, and operational activities. This is the area applied to the situations of not only normal operation but also abnormal/emergency operations of the power plants. In other words, though the 3 major task behaviors are the task behaviors classified independently depending on the task characteristic behavior, it may be considered that each individual task behavior itself does not represent the entire task but shows the task characteristics of operators most appropriately when the task behaviors are integrated.

Table 2 shows the taxonomy of three dimensions of operator activities (COCOA): cognition, communication, and operative activities.

3.2 *Workload evaluation process*

The data for an analysis of task load should be acquired to evaluate the workload. In general, the evaluation data are obtained by video-recording for the simulation experiments of operators. The acquired data are first classified into the procedures and procedural numbers, and the analysis was conducted. At the task analysis step for each procedural number, the kind of task is first selected from cognitive activities (diagnosis/decision-making), communicative activities, and operational activities. For each classified task, the relevant task behavior is judged and arranged, and the relevant tasks are then integrated to complete the workload evaluation. The workload evaluation results with the completed analysis show the execution results for the cognitive task, communicative task, and operational task of each operator. When an adjustment is needed to balance the workload from the results analyzed in this way, the workload of each operator is adjusted and averaged to raise the task conduction efficiency and satisfaction of each operator. Figure 2 is a block diagram of the workload evaluation process of operators in an advanced MCR.

3.3 *Workload evaluation example*

If it is assumed that the emergency operation procedures to be conducted by operators in an advanced MCR are the same as shown in Figure 3, the logic for an execution of the workload evaluation may be composed of the following. First, after procedural steps 1 through 4 are completed, the case where the conditions of detailed step 4.1 are satisfied and the case where they are not satisfied may be investigated. When the conditions are satisfied, detailed step 4.1 is skipped, and detailed step 4.3 is executed. When they are not

Table 2. Taxonomy of COCOA classification.

Dimension	Activity	Description
Cognitive activity	COMPARE	Comparing two or more entities of system states.
	DIAGNOSE	Recognizing or determining the cause of the system states by signals or parameters.
	EVALUATE	Checking a system state with consideration of other system parameters or states.
	EXECUTE	Performing a single prescribed action (ex. open, close, turn on, etc.)
	MAINTAIN	Sustaining a specific system state by executing or regulating systems.
	MONITOR	Continuously observing the system states or parameter.
	RECORD	Writing down or logging the system states or events.
	REGULATE	Changing the quantity, speed, or direction of the system parameters or states.
	VERIFY	Checking an entity of system states.
	SCAN	Briefly reviewing specific system states by displays or other information.
	PLAN	Formulating a path to achieve specific goals.
	IDENTIFY	Recognizing the overall state of a specific system.
Communicative activity*	COMMAND	Ordering an operator to execute or regulate a system or component.
	COMMAND-ACK	Informing whether a listener understood a command.
	INQUIRY	Asking about system states or parameters.
	REPLY	Answering a question.
Operational activity	SWITCH_SCR	Altering a display screen to read or operate specific parameters or states.
	OPEN_CTRLPNL	Opening a control panel to operate a specific system.
	CLOSE_CTRLPNL	Closing a control panel that has been opened.
	CLICK_EXECUTE	Pushing a button to operate a single entity (ex. opening a valve).
	CLICK_REGU_ UPDN	Pushing a direction button to regulate a system parameter or state (ex. opening a valve).
	CLICK_REGU_ FASTUPDN	Pushing a double-direction button to regulate a system parameter or state (ex. opening a valve).
	CLICK_ENABLED	Pushing a button to enable a control panel to be usable.
	CLICK_MANNUAL	Pushing a button to manually operate a single entity.
	CONF_STEP	Clicking a button confirming that all instructions of a step have been completed.
	CONF_SUBSTEP	Clicking a button confirming that an instruction of a step has been completed.
	ACK_ALARM	Checking and silencing a notifying alarm.
	CONF_CHANN	Pushing a button to verify the channel of an entity to be operated.

* The most frequently used communicative activities quoted in the table.

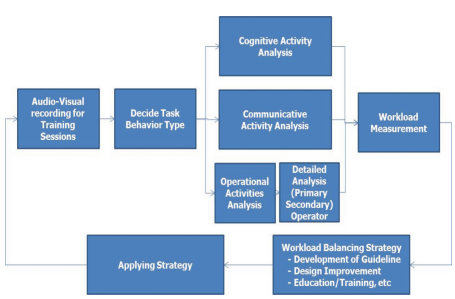


Figure 2. Workload evaluation process.

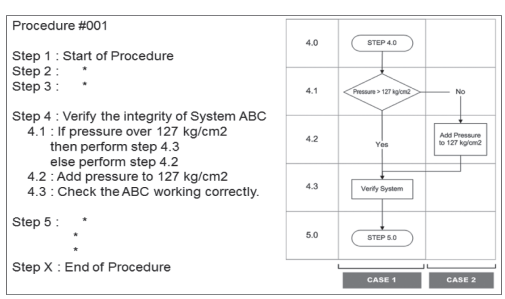


Figure 3. Emergency operation procedure (assumed).

Table 3. Workload analysis (dissatisfied condition).

Task ID	Step	Type of activity	Task activity	Operator (SS)	Operator (RO)
1	4.1	COMMUNICATION	INQUIRY	"Is the pressure of the pressurizer 127 kg/cm²?"	
2	4.1	COGNITION	COMPARE		Compare the pressure of the pressurizer.
3	4.1	COMMUNICATION	REPLY		"The pressure of the pressurizer is below 127 kg/cm²."
4	4.1	COGNITION	VERIFY	Confirm that the pressure of the pressurize is below 127 kg/cm².	
5	4.1	OPERATION	CONF_SUBSTE P	Confirm steps and check dissatisfaction.	
6	4.2	COMMUNICATION	COMMAND	"Maintain the pressure of the pressurizer above 127 kg/cm² by controlling valve AA."	
7	4.2	COMMUNICATION	COMMAND-ACK		"OK"
8	4.2	OPERATION	OPEN_CTRLPNL		Open the window for control of valve AA.
9	4.2	OPERATION	CLICK_REGU_UPDN		Control the opening of valve AA.
10	4.2	OPERATION	CLOSE_CTRLP NL		Close the window for control of valve AA.
11	4.2	COMMUNICATION	OBSERVATION		"I've completed the valve control."
12	4.2	COMMUNICATION	OBSERVATION_ACK	"OK"	
13	4.3	COGNITION	SCAN	Check if all the relevant steps are executed	
14	4	OPERATION	CONF_STEP	Check for move to the next step	

Number of activities: 14 (Cognition: 3, Communication: 6, Operation: 5).

satisfied, detailed step 4.2 is executed to control the pressure of the pressurizer, and the procedure execution then moves to the next step (detailed step 4.3).

When the conditions of detailed step 4.1 are not satisfied, the task behavior analysis results for procedural step 4.1 are the task activities between an SS and RO, and they are composed of 14 steps, as shown in Table 3. As the conditions of step 4.1 are not satisfied, an SS orders an RO to control the valve opening through the execution of step 4.2 (Task Id #6), and RO opens the control window for a valve opening to execute procedural step 4.2 and maintains the pressure by controlling the valve opening (Task Id #7—Task Id #12). The steps after this consist of the RO's report for control completion, and SS's confirmation of the system conditions.

As shown in the table, the results of the workload analysis for step 4 of the procedures indicate that step 4 consists of 3 cognitive tasks (two for SS, one for RO), 6 communicative tasks (three for SS, three for RO), and 5 operational tasks (two for SS, three for RO).

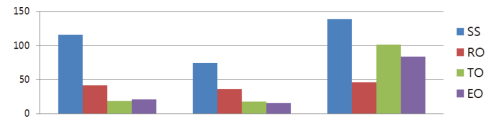
4 WORKLOAD EVALUATION USING COCOA ANALYSIS

To verify the validity for the workload evaluation framework of operators proposed in this research, the workload evaluation was conducted on the basis of the operator practice data used in the simulator of the training center of the reference plant, which was installed in the advanced MCR under an MMIS environment. The environment for acquisition of the task load evaluation data is given in Table 4.

The analysis results for the workload of operators in the advanced MCR of a reference plant are shown in Figure 4. The graph shows the total frequency of cognitive activities, communicative activities, and operational activities used during the process of executing a Standard Post Trip

Table 4. Environment for acquisition of workload evaluation data.

Items	Detailed contents
Scenario	LOCA(SPTAP + DP + ORP(LOCA)) SGTR(SPTAP + DP + ORP(SGTR))
Team	3 Training teams (advanced MCR operation teams)
Acquisition method	Video recording individual recording for each operator (SS, RO, TO, EO)



Procedure		Cognitive Activities				Communicative Activities				Operational Activities			
		SS	RO	TO	EO	SS	RO	TO	EO	SS	RO	TO	EO
1	SPTAP	38.6	14.1	4.4	12	25.6	12	5	7.6	52.6	12.3	16.6	36.3
2	DP	19.6	4.3	2.9	3.4	10.4	2.6	2.8	3.4	23.4	3.9	4	15.4
3	ORP	57.8	22.7	11.3	5.1	38.4	21.5	10	4.8	62.4	30.1	80.3	32
Sum		116	41.1	18.6	20.5	74.4	36.1	17.8	15.8	138.4	46.3	100.9	83.7

Figure 4. Workload analysis results.

Action Procedure (SPTAP), Diagnosis Procedure (DP), and correspondence procedures (Optimal Recovery Procedure (ORP) for Loss of Coolant Accident (LOCA) and Steam Generator Tube Rupture (SGTR)). Figure 4 shows the average total number of activities that appear when the LOCA and SGTR scenarios are executed, and the table at the bottom of Figure 4 shows the frequency of cognitive tasks conducted by operators for each procedure and each activity.

The results for the workload analysis indicate that the cognitive activities of SS are far more than those of other operators. It was found that as the communicative activities of SS are also the most, SS leads the entire MCR. Not only that, but SS is also found to conduct more operational activities than other operators. This shows that SS increases the frequency of operational activities by executing diagnostic procedures (SPTAP + DP) and Optimum Operation Procedures (ORP), using the CBPs, under the operation environment of an advanced MCR.

5 GENERAL CONCULSTION

In this research, we proposed a framework to measure and evaluate the workload of operators in an advanced MCR and the workload was measured through the simulator training experiment of the advanced MCR of a reference plant to verify the validity of the framework.

The workload analysis results of operators in the advanced MCR of the reference plant show that the cognitive and communicative activities of SS are more than those of other operators. This is because SS is responsible for confirming the accuracy of the procedural execution in the case of an emergency and should continue to conduct the operational guidance and surveillance activities. Though the CBPs and personal information processing system basically provide a variety of information on the status of the power plants, SS has a high amount of cognitive activities and also has a high amount of communicative activities for understanding of the operators' behavior and plant status since SS should judge and decide whether all the instructions are executed or not in the CBPs.

Not only that, but these analysis results also show that the workload for operational activities of the SS is heavier than that of other operators. Whenever the SS, who operates the CBPs, executes each instruction and step, the SS should mark in the CBPs whether they are executed and whether they are satisfactory. Thus, many operational activities are required for the execution. It is easy to understand that SS, who has to conduct a high amount of cognitive and communicative activities due to the workload caused by such operational activities, is more overloaded. It may be predicted that SS will be given an additional workload due to the operational activities increased in comparison with the workload under the environment of a conventional MCR.

The COCOA developed in this research presents the framework suitable to a workload analysis of the operators in an advanced MCR. This also presents the taxonomy for additional operation activities of operators to use the computerized procedures and soft control added to the advanced MCR, and it enables an integrated measurement of the operator workload in various dimensions of cognition, communication, and operation. Of course, even though it is impossible to get an arithmetic average of the load values measured in each dimension, additional research is needed to present a comprehensive measure in consideration of the weighed values between factors (dimensions). In addition, the measurement method presented in COCOA is regarded as a calculation method to enable a comparison between operators.

On the basis of these observations, it is necessary to reestablish the role and communication method of MCR operators suitable to the new operational environment and changed work and develop the appropriate operating guidelines.

As additional research, it is judged that the evaluation of operator workload through more experiments is needed to prove the validity of COCOA,

and in-depth research on an equalization plan for the workload unbalance of operators analyzed through COCOA is also needed.

ACKNOWLEDGEMENT

This work was supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) grant, funded by the Korean government, Ministry of Science, Ict & future Planning (MSIP). (Grant Code: 2012M2A8A4025991)

REFERENCES

Cain, B., 2007. A Review of the Mental Workload Literature, *Technical Report, RTO-TR-HFM-121-Part-II*.

Eggemeier, F.T., Wilson, G.F., et al., 1991. Workload assessment in multi-task environments. Multiple task performance, D.L. Damos. London, GB, Taylor & Francis, Ltd.:, pp. 207–216.

Embrey, D., Blackett, C., Marsden, P., Peachey, J., 2006. Development of a Human Cognitive Workload Assessment Tool, Human Reliability Associates.

Gopher, D. and Donchin, E., 1986. Workload—An examination of the concept. *Handbook of Perception and Human Performance*. Volume 2. Cognitive Processes and Performance. K.R. Boff, L. Kaufman and J.P. Thomas, John Wiley and Sons, Inc:, pp. 41–49.

Hart, S.G. and Staveland, L.E., 1988. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. *Human Mental Workload*. P.A.M. Hancock, N. Amsterdam, North-Holland, pp. 139–183.

Hollnagel, E., 1996. A Cognitive task analysis of the SGTR scenario. Technical report, NKSRAK-1(96) R3.

Humphrey, D.G. & Kramer, A.F., 1994. Toward a psychophysiological assessment of dynamic changes in mental workload. Human Factors, Vol 36, pp. 3–26.

Kim, S., Park, J., Han, S., & Kim, H., 2010. Development of extended speech act coding scheme to observe communication characteristics of human operators of nuclear power plants under abnormal conditions. *Journal of Loss Prevention in the Process Industries*, Vol 23, pp. 539–548.

Kramer, A.F., 1991. Physiological metrics of mental workload: A review of recent progress. *Multiple task performance.* D.L. Damos. London, UK, Taylor & Francis, Ltd., pp. 279–328.

Meshkati, N., 1988. Heart rate variability and mental workload assessment. *Human Mental Workload.* P.A. Hancock and N. Meshkati. Amsterdam, NL, Elsevier Science Publishers B.V. (North-Holland), pp. 101–115.

Mitchell, D.K., 2000. Mental Workload and ARL Workload Modeling Tools. Army Research Laboratory, Report No ARL-TN-161.

O'Hara, J., Brown, W.S., Lewis, P.M., & Persensky, J.J., 2002. Human-System Interface Design Review Guidelines. *NUREG-0700* Rev.2. U.S.NRC, Washington. DC.

Reid, G.B. and Nygren, T.E., 1988. The subjective workload assessment technique: A scaling procedure for measuring mental workload. *Human Mental Workload.* P.A.M. Hancock, N. Amsterdam, Elsevier Science Publishers B.V. (North-Holland), pp. 185–218.

Wierwille, W.W. and Casali, J.G., 1983. A validated rating scale for global mental workload measurement applications. *Proceedings of the Human Factors Society*—27th Annual Meeting, pp. 129–133.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A survey of Bayesian Belief Network Applications in Human Reliability Analysis

L. Mkrtchyan, L. Podofillini & V.N. Dang
Paul Scherrer Institute, Switzerland

ABSTRACT: Applications of Bayesian Belief Networks (BBNs) to Human Reliability Analysis (HRA) are receiving increasing attention. This paper surveys these applications, aiming at identifying the areas of HRA for which BBNs can be attractive. The survey is based on an extensive search of the literature (2006–2013). The literature is divided into groups depending on the HRA aspect primarily addressed with the use of BBNs. Five groups are identified and analysed: modelling of organizational factors, analysis of the relationships among Performance Shaping Factors (PSFs), extensions of existing HRA methods (in practice, SPAR-H and CREAM), HRA dependence assessment, and the assessment of situation awareness. Each application emphasizes a different BBN feature: e.g. ability to deal with scarce data, to incorporate diverse information, to model complex multi-layer relationships. This survey focusses on how the BBN framework is used to capture the different HRA aspects. An important aspect outside the scope of the present paper is how the BBNs are built, i.e. the incorporation of available data and/or expert judgment in the construction of the models and the determination of their parameters—this aspect will be addressed in future work.

1 INTRODUCTION

Human Reliability Analysis (HRA) is the area of risk analysis aimed at analysing the human contribution to system reliability and safety. A number of HRA methods have been developed, different in their scope, approaches for analysing the human performance conditions, and human error quantification approaches. An overview of methods can be found in Kirwan (1994).

An important class of HRA methods is based on models, which typically represent and quantify the relationships among the factors influencing the human failure probability. Examples of these models are those underlying SPAR-H (Gertman et al. 2005), CREAM (Hollnagel, 1998) and the recently developed causal models such as in Groth & Mosleh (2012). Generally, the relationships between influencing factors and human failure probabilities are challenging to capture. The influencing factors can be many and interdependent (correlated and with dependent effects on the failure probability); the data available to inform these relationship is limited and, if present, it is challenging to use.

In this context, modelling frameworks able to represent complex, non-deterministic relationships with limited information are attractive for HRA. In particular, recently, Bayesian Belief Networks (BBNs) (Jensen & Nielsen, 2007) are increasingly being explored, developed and applied for HRA. Use of BBNs in risk and reliability analysis is relatively established, while their use for HRA is quite recent (mostly from the last five years). In addition to the features already mentioned, BBNs are especially suitable for HRA for the following reasons. First, BBNs handle both causal and evidential reasoning: this allows not only the estimation of Human Error Probabilities (HEPs) given the contributing factors but also the analysis of the most dominant factors given a human failure. Second, BBNs can incorporate information of different nature from different types of evidence sources—a key feature in case comprehensive data is not available. Third, because of their straightforward graphical representation of cause-effect relationships, BBNs are easy to use for both domain experts and analysts, and the results are easy to interpret for non-experts. Finally, the probabilistic nature of BBNs allows them to be integrated with other mathematical models such as fault trees and event trees; therefore the results can be used in Probabilistic Safety Assessment (PSA).

The present paper systematically surveys HRA applications of BBNs. The review is based on an extensive search of the academic literature (2006–2013). The literature is divided into

five groups depending on the HRA aspect primarily addressed. Each application emphasizes a different BBN feature: e.g. ability to deal with scarce data, to incorporate diverse information, to model complex multi-layer relationships. After a brief introduction of BBNs (Section 2), Section 3 gives the overview of the surveyed papers and of their grouping. The studies are discussed in detail by group in Sections 4–7; a brief overview of the individual studies is provided in the Appendix. The conclusions from the survey are given at closure.

2 BAYESIAN BELIEF NETWORKS

BBNs model probabilistic relationships among variables, with variables and relationships represented as nodes and links of the network (Jensen & Nielsen, 2007). Graphically, BBNs are represented as directed acyclic graphs (therefore, the feedback cycles cannot be modelled) connecting nodes with links. The quantitative relationships among the connected nodes are represented as conditional probability distributions for each variable (node) in the network.

For BBNs with discrete nodes, the conditional probability distributions are stored in Conditional Probability Tables (CPTs). The CPTs are obtained either from data, expert judgment or both. The automatic quantification of CPTs from data typically requires large data samples. This is the case of some data-rich applications, e.g. in molecular biology, medical diagnostics, or financial economics. In these applications, typically, both the BBN structure and relationships are learnt from data: in these, BBNs are used to identify the important factors, their relationships (correlations and causal relationships) and their quantitative influence on the variables of interest.

In the risk analysis domain, BBNs are used to represent uncertain knowledge about factors and relationships. With few exceptions, data is scarce (if at all available), so that the CPTs are obtained by expert elicitation. For these applications, the development of processes to avoid biases and efficiently elicit large number of probabilities is an important area of research and a key element for successful application of BBNs (Jensen & Nielsen, 2007).

Once the BBNs are built, they can be used both for diagnostic and predictive applications by making inference about the variables in the network. Inference in BBNs is based on the concept of belief propagation which refers to computing posterior marginal probability distributions of a set of variables of interest, after obtaining some observations of variables in the model.

3 BAYESIAN BELIEF NETWORKS IN HRA: OVERVIEW OF THE SURVEYED STUDIES

The surveyed studies of HRA-related BBNs were grouped according to the HRA aspect they address (Table 1). Namely, these are studies using BBNs: 1) to represent the possible impact of Management and Organizational Factors (MOFs) on HEPs; 2) to analyze the relationships between interdependent Performance Shaping/Influencing Factors (PSFs/PIFs); 3) to extend existing HRA models to capture additional features allowed by the BBN modelling framework; 4) to model HRA dependence; 5) to assess situation awareness. These HRA aspects are strongly inter-related. For example, representing the impact of organizational factors would also explicitly capture the dependence across multiple human failure events introduced by MOFs. In the compilation of in Table 1, whenever a study fits into multiple groups, the study was classified according to the most representative HRA aspect treated.

The subsequent sections discuss each of these groups of contributions in detail. A short description and summary of the individual contributions is presented in the Appendix. The contributions related to situation assessment are inspired by the application of BBNs as diagnostic tools; their aim is to identify opportunities for misdiagnosis and predict their probabilities in the frame of simulation-based risk assessment. Due to this specificity and space limitations, further discussion of this group is omitted.

4 BBNS TO MODEL ORGANIZATIONAL FACTORS

There are significant challenges to the incorporation of MOFs in quantitative risk assessment.

Table 1. HRA aspects addressed by the reviewed works.

HRA aspect	Contributions
Organizational factors impact assessment	(Martins & Maturana, 2013), (Cai et al. 2013), (Vinnem, et al. 2012), (Gran et al. 2012), (Trucco et al. 2008)
PSF/PIF relationship assessment	(Sundarmurthi & Smidts, 2013), (Stempfel & Dang, 2011), (Dang & Stempfel, 2012), (Podofillini et al. 2013), (Musharraf et al. 2013), (Groth & Mosleh, 2012)
Situation assessment	(Lee & Seong, 2009), (Kim & Seong, 2006a), (Kim & Seong, 2006b)
HRA method extensions	(Groth and Swiler, 2013), (Kim et al. 2006)
Dependence assessment	(Baraldi et al. 2009), (Ekanem & Mosleh, 2013), (Mosleh et al. 2012)

MOFs by their nature are difficult to define and classify; the link between MOFs and their impact on safety can be subtle and long-term; data is hard to obtain because of the difficulty to establish appropriate taxonomies. The lack of an established set of MOFs and corresponding definitions hinders comparisons and benchmarking analyses across different studies. The reader can refer to (Mohaghegh et al. 2009), (Mohaghegh & Mosleh, 2009) for a comprehensive discussion on the issue.

Generally, the use of BBNs to model the impact of MOFs aims to explicitly model their multi-level and hierarchical influences on the HEPs, as discussed in Li et al. (2012), Cai et al. (2013) and Martins & Maturana (2013). Many of the influencing factors typically considered by HRA methods can be thought of having direct influence on the HEP, e.g. the quality of the human machine interface and the time available for the personnel to carry out their tasks. In contrast, many of those referred to as MOFs have indirect effects: for example the management's commitment to safety influences the quality of personnel training, which then directly influences the HEP. The BBN ability to represent multi-level relations helps to model these types of hierarchies. Figure 1 shows an example of the hierarchical influences.

Trucco et al. (2008) use BBNs to model the dependence among multiple failure events introduced by organizational factors. The effect of the organizational factors is to modify the probability of each basic event through the corresponding organizational variable; in this way, the same organizational factor may impact multiple basic events. The study combines two frameworks; namely fault trees and BBNs. As advocated by Mohaghegh et al. (2009) this combination appears to be the most promising approach for integrating organizational influences in risk assessment. Figure 2, taken from Mohaghegh et al. (2009) shows the concept for the integration of the BBN, event tree, and fault tree modelling techniques.

In general, the surveyed studies focus on the potential advantages of BBNs to model the subjective, hierarchical, and "soft" relationships characterizing MOFs. A key element for the development of these models is the assessment of the quantitative relationships underlying them. The assessment is based on expert judgment, given the absence of empirical data: the process for the elicitation of the judgments becomes a fundamental component of the model development and of its acceptance. Therefore, approaches to effectively elicit expert judgment, while avoiding biases, are generally sought in the surveyed studies. A survey of these approaches is outside the scope of the present paper.

A concern related with the surveyed studies is their limited emphasis on the operationalization of the factors. For the quantitative incorporation in safety analysis, MOFs require clear definitions, operationalizations and measuring techniques. As mentioned, an important contribution in this sense comes from the modelling principles in Mohaghegh & Mosleh (2009). Also, Vinnem et al. (2012) discusses how the measuring of influencing factors was approached: the scoring of each factor (a six-point scale is used, from A to F, see Table 2) is assessed via questionnaires and interviews. However, in most of the references, MOFs are presented as BBN nodes with their states (typically, binary), with no guidance on how to assess the states (i.e., how an analyst should decide between "Organizational Culture" being "Appropriate" or "Non Appropriate" taking one example from Table 2).

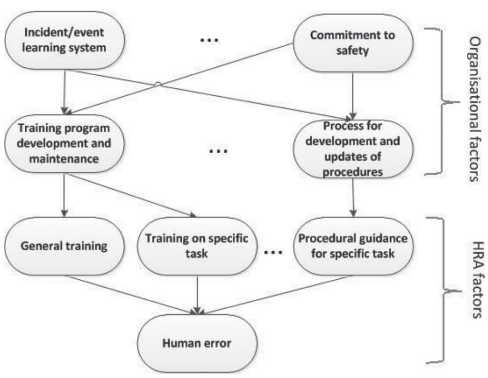


Figure 1. Example of multi-level influences typically modelled by BBNs: direct and indirect influences of the error probability.

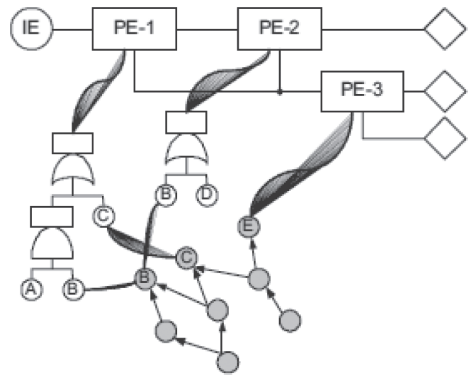


Figure 2. Concept for the integration of MOFs in probabilistic safety assessment, combining the BBN, the event trees, and fault tree frameworks (Mohaghegh et al. 2009).

Table 2. Some of MOFs and states used in BBNs.

Reference	Nodes (states)
Martins & Maturana (2013)	Coordination of work (Poor, Good) Training (Appropriate, Inadequate) Organizational culture (Appropriate, Inappropriate) Turnover (Low, High) Company programs (Absent, Present)
Cai et al. (2013)	Poor safety plan (Yes, No) Poor safety culture (Yes, No) High commercial pressure (Yes, No) Poor standards development (Yes, No) Poor training standards (Yes, No) Inadequate reference material (Yes, No)
Li et al. (2012)	Organizational goals and strategies (NA)* Organizational structure (NA) Organizational resources (NA) Communication (NA) Organizational management (NA) Organizational culture (NA)
Trucco et al. (2008)	Training of personnel (NA) Operation plan (NA) Maintenance plan (NA) Compliance with regulations (NA)
Vinnem et al. (2012)	Management competence (A, B, C, D, E, F)*
Gran et al. (2012)	Management information (A, B, C, D, E, F) General management (A, B, C, D, E, F) Supervision (A, B, C, D, E, F) Governing documents (A, B, C, D, E, F)

*NA indicates no information available from the reference.
**Six-point scale used to determine the factor state (A to F). "A" corresponds to best industry practice; "F" corresponds to an unacceptable condition.

5 BBNS TO MODEL THE RELATIONSHIPS AMONG PSFS

Most HRA methods use PSFs to support the analysis of the contextual conditions under which human failure may occur. In the qualitative HRA, PSFs help analysts to systematically address all factors believed to be important to human performance. In the quantitative HRA, PFSs are frequently used to modify a generic error probability to capture the effect of the context in which the task of interest is carried out.

Typically, when multiple PSFs are assumed to influence the HEP, HRA methods model the PSF joint influence by cumulating the effect of each factor, as if each of them would act independently on the HEP. However, PSFs can have interacting effects: good performance conditions (e.g. support from the procedural guidance or highly experienced personnel) can compensate for the difficulty of a highly complex task; on the other hand, a complex task carried out under limited procedural guidance support, by unexperienced personnel would be characterized by a very high failure probability, much higher than if these three factors would be present alone.

BBNs are naturally suited to model the effects of interacting PSFs. Indeed, the key practical problems are to identify the interacting factors and quantify their joint effects. This is the common issue addressed by the studies included in this category in the survey (Sundarmurthi & Smidts, 2013), (Stempfel & Dang, 2011), (Dang & Stempfel, 2012), (Podofillini et al. 2013), (Groth & Mosleh, 2012). All papers address identification and quantification of the interactions as these emerge from data (see Fig. 3 for a typical view of the BBN structure for these applications): empirical data in Groth & Mosleh (2012) and Sundarmurthi & Smidts (2013); artificial data in Stempfel & Dang, (2011), Dang & Stempfel (2012), Podofillini et al. (2013).

A unique feature of the work in Groth and Mosleh (2012) is the use of empirical data to inform the BBN development, both for the graphical and quantitative parts: data analysis (correlation and factor analysis) allows identifying the causal relationships among the PSF, their interaction to produce errors and some of the BBN conditional probabilities. The uniqueness relates to the fact that, as mentioned in the introduction, the typical approach for BBN applications in field with poor data availability is to use expert judgment for building the structure of the networks and then the available data for quantifying the relationships.

A primary aspect of the work by Groth & Mosleh (2012) is the exploration of the Error Contexts (ECs), which are certain combinations of PSFs (Fig. 3) which are more likely to produce a human error (Groth & Mosleh, 2012). ECs

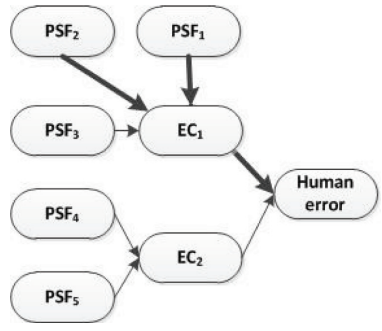


Figure 3. An example of PSFs hierarchical structure and influence on human error (the line style depends on the importance and strength of the link).

are identified from the data patterns, via Factor Analysis. For example, one of the ECs emerging from the data is the combination of inadequate teamwork and training to respond to a complex, dynamic situation (involving three PSF, "Team", "Training" and "Complexity"). The probability of an error occurring when this combination occurs is much larger than when these factors act alone. This suggests the importance of teamwork and training to cope with complex tasks (good teamwork and training can compensate the challenges of complex situations so that the probability of error can significantly decrease).

The main aim of Sundarmurthi & Smidts (2013) is to develop an HRA model suitable for the dynamic PSA simulation environment integrating plant physical models and operating crew models into stochastic simulation engines. The relationship among PSFs is first represented with causal graphs as an initial structure of BBNs. The relationship between two elements/nodes in causal graphs is expressed in terms of statistical correlation calculated from data or with expert judgment. In the causal graphs the importance of each PSF is explored in terms of its influence by other factors.

The main aim of the work presented in Stempfel & Dang (2011), Dang & Stempfel (2012), Podofillini et al. (2013), is to examine the BBNs as a modelling tool to capture the relationships among the PSF as these emerge from data. The artificial data (generated, with known properties) is used to evaluate the capability of the BBN models to reproduce the known properties. A key assumption of the artificial data was that in addition to their individual effects on performance, some PSFs interacted producing an additional contribution to the HEP. In other words, their joint effect was more than the sum of their individual effects. The formalism of the BBN clearly supports the modelling of such interactions. Stempfel & Dang (2011) investigated how the BBN model compared to a model where this interaction term is neglected: a multiplicative model was fitted to the data. As expected, it performed poorly on all configurations where more than one PSF was present. The references analyse the BBN performance under different modelling conditions: reduced data sets (Stempfel & Dang, 2011), missing and/or incorrect data values (Dang & Stempfel, 2012), different BBN structures (Stempfel & Dang, 2011 and Dang & Stempfel, 2012), uncertainty in the BBN parameters (Podofillini et al. 2013). As expected, the BBN performance degrades as the size and quality of the data set decreases. Combination with expert judgment can be sought to improve the BBN performance in these cases.

6 BBN-BASED EXTENSIONS OF HRA METHODS

Among the reviewed studies two contributions present BBN versions of the HRA methods SPAR-H and CREAM. In Groth & Swiler (2013) the authors state that the reason for using the BBN version of a known and widely used HRA method is to demonstrate the benefits of using BBNs on a method with which practitioners are familiar. This is believed to help in "bridging the gap" between the development of HRA methods by researchers and its adoption by the practitioners.

The study in Groth & Swiler (2013) presents a BBN version of the SPAR-H method. The network structure consists of the eight PSFs of SPAR-H and the human error (all PSF nodes directed into the human error node). Being a BBN replica of SPAR-H, the CPTs are given by the SPAR-H relationships between PSFs and error probabilities. Building on the BBN version of a familiar method, the study shows how the BBN framework can accommodate analyses with perfect, partial or no information on the PSF states as well as evidential reasoning (i.e. about the PSFs states given error occurrence). Finally, possible modifications to the model are discussed by adding additional PSFs and discussing the interdependency among PSFs.

The study in Kim et al. (2006) is based on the HRA CREAM method. BBNs are used for the probabilistic assessment of the control mode, different from the original CREAM formulation in which the control mode is deterministically determined. The control mode represents the degree of control that the personnel has over a situational context. The situational context is captured by the state of nine Common Performance Conditions (CPCs), each having three or four possible ratings. Depending on the ratings, CREAM suggests a basic diagram to decide the control modes. The BBN developed in Kim et al. (2006) study is used to extend the described deterministic approach in CREAM and it calculates the probability distribution of control modes given the probability distributions of nine CPC nodes.

7 BBNS FOR DEPENDENCE ASSESSMENT

In HRA, dependence analysis refers to assessing the influence of the failure of the operators to perform one task on the failure probabilities of subsequent tasks (Swain, 1983).

The THERP handbook (Swain, 1983) suggests general rules to determine the dependence, qualified in terms of levels (from zero to complete) providing a formula for computing the dependent, conditional probability for each dependence level.

In current HRA practice, dependence assessment is generally supported by decision trees that guide analysts through the assessment of the different factors influencing dependence (e.g. closeness in time between two successive tasks, similarity of the cues related to the two tasks).

Two lines of research have addressed the use of BBNs for dependence assessment in HRA. The first one investigates the use of BBNs (Baraldi et al. 2009) as expert models, to increase the repeatability and the transparency of the dependence assessment. The BBN nodes in this study are based on the dependence factors described in THERP (Fig. 4). The lack of traceability in the development of the decision trees used for dependence analysis is one of the main motivations behind the work by Baraldi et al. (2009). The consequence is that the fundamental assumptions behind the influence of factors (e.g. which factors are important and how much each influences the model output) are not directly linkable to the developed model. The work in Baraldi et al. (2009) generally is included in the larger activity of the authors of the present paper to improve traceability and transparency of model development in HRA via systematic expert elicitation approaches (cf. Podofillini and Dang, 2010).

The second line of research aims at using BBNs to more explicitly capture the causal dependencies between different human failure events (Ekanem & Mosleh, 2013), (Mosleh et al. 2012). The causal dependencies are originated by the fact that the same PSFs influence multiple HFEs: BBNs are used to explicitly model these influences. In terms of structure, BBNs developed for these applications would have multiple HFE nodes and different factors influencing the different HFE nodes as necessary. Note that this line of research for capturing HFE dependences has a strong connection with the uses of BBNs for incorporating organizational factors in the PSA framework: organizational factors constitute fundamental, common causes of human failures.

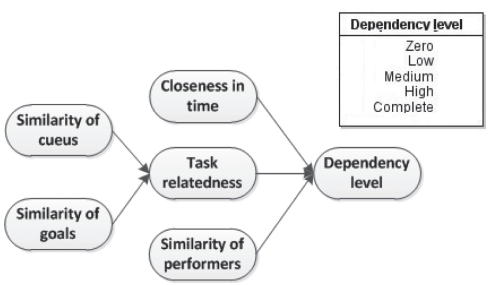


Figure 4. HRA dependence modelling with BBNs (Baraldi et al. 2009).

8 CONCLUSIONS

This paper has surveyed recent applications of BBNs for HRA application—a recently increasing trend for HRA. The applications have been grouped into five categories, four of which are discussed in this review.

BBNs have been used for incorporating MOFs in probabilistic safety assessment. The BBN attractiveness for this aim is in their ability to capture "soft" relationships, typical of the influences of these factors. In addition, their graphical interface largely facilitates the discussion on the identification and definition of the influencing factors behind the model development phase. This feature appears particularly interesting for the modelling of MOFs because the procedures for their identification and definition are relatively unestablished so that any tool able to improve the process transparency is beneficial. BBNs are embedded in the classical fault tree and event tree frameworks to capture the overarching effect of MOFs over multiple failure events (possibly explicitly modeling the dependence effect introduced by the MOFs).

The second group of applications addressed BBNs to model the relationships among PSFs, intended as how PSFs interact to determine the human failure probability. These applications demonstrate the superiority of BBNs to reproduce these relationships compared to the simplified models more typically used in HRA, i.e. in which the factors independently influence the HEP. Ideally, the relationships should be captured by the BBNs as these emerge from empirical data. However, the amount of data available still does not allow the construction of BBNs solely on empirical grounds, so that elements of expert judgment are always present.

The third group of applications applies BBN to modify existing HRA methods, to provide additional modelling capabilities that the methods would not support. For example, these relate to introduction of interdependencies in the PSF and/or multiple layers. As pointed out by Groth and Swiler (2013), the introduction of BBNs into existing HRA models can foster the acceptability of BBNs by the HRA community. Indeed, practitioners would be more willing to accept a new model when this is embedded in a familiar framework (such as SPAR-H or CREAM as in the surveyed works). Also, the possibility offered by BBNs to incorporate new information would allow enhancing existing HRA methods with new data, via the BBN learning mechanism.

The fourth group of applications dealt with dependence assessment. Dependence assessment is an area of HRA characterized, in practice, by the absence of quantitative empirical data. In this

framework, BBNs have been used as a modelling tool to improve the traceability of the models supporting the assessment. This necessarily implies the adoption of a systematic framework for eliciting expert judgement and converting it into a quantitative model. Indeed, the need for systematic treatment of expert judgments to develop BBNs is not specific to dependence assessment and not to HRA. Still within the domain of dependence assessment, BBNs have been used to explicitly model the impact of common factors among multiple human failure events. This has been done exploit the possibility to incorporate the BBN framework with fault and event trees, similarly to how the MOFs in PSA is envisioned.

This paper has surveyed how BBNs model each aspect of HRA. However, an important element for BBN applications has been left out: the process for BBN development. The analysis of the process of model development is key for the acceptability of the BBN framework in HRA where the transparency of the adopted models is very important: models need to be understood, reviewed, and accepted. This requires a systematic process to utilize available data and expert judgment in the model development phase. The next phase of this survey will be to analyse how these elements are incorporated in the BBN development.

ACKNOWLEDGEMENT

This work was funded by the Swiss Federal Nuclear Safety Inspectorate (ENSI), under DIS-Vertrag Nr. 82610. The views expressed in this article are solely those of the authors.

REFERENCES

Baraldi, P., Conti, M., Librizzi, M., Zio, E., Podofillini, L. & Dang, V.N. 2009. A Bayesian Network Model for Dependence Assessment in Human Reliability Analysis. *Proceedings of the European Safety and Reliability Conference (ESREL)*, *September 7–10, Prague*, 223–230.

Cai, B., Liu, Y., Zhang, Y., Fan, Q., Liu, Z. & Tian, X. 2013. A dynamic Bayesian networks modelling of human factors on offshore blowouts. *Journal of Loss Prevention in the Process Industries*: 639–649.

Dang, V.N. & Stempfel, Y. 2012. Evaluating the Bayesian Belief Network as a Human Reliability Model—the effect of unreliable data. *Proceedings of the PSAM 11*.

Ekanem, N.J. & Mosleh, A. 2013. Human failure event dependency modelling and quantification: A Bayesian network approach. *Proceedings of the European Safety and Reliability Conference* 537–543.

Gertman, D., Blackman, H., Byers, J., Haney, L., Smith, C. & Marble, J. 2005. *The SPAR-H Method.* NUREG/CR-6883. Washington, DC: US Nuclear Regulatory Commission.

Gran, B.A., Bye, R., Nyheim, O.M., Okstad, E.H., Seljelid, J., Sklet, S., Vatn, J. & Vinnem, J.E. 2012. Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. *Journal of Loss Prevention in the Process Industries* 25(3): 582–593.

Groth, K.M. & Mosleh, A. 2012. Deriving causal Bayesian networks from human reliability analysis data: A methodology and example mode. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 226(4): 361–379.

Groth, K.M. & Swiler, L.P. 2013. Bridging the gap between HRA research and HRA practice: A Bayesian network version of SPAR-H. *Reliability Engineering and System Safety* 115: 33–42.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method: CREAM*. New York, Elsevier.

Jensen, F.V. & Nielsen, T.D. 2007. *Bayesian Network and Decision Graphs*. New York, NY, USA, Springer science.

Kirwan, B. 1994. *A Guide To Practical Human Reliability Assessment.* CRC press.

Kim, M.C. & Seong, P.H. 2006a. A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety* 91: 580–593.

Kim, M.C. & Seong, P.H. 2006b. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. *Reliability Engineering and System Safety* 91: 270–282.

Kim, M.C., Seong, P.H. & Hollnagel, E. 2006. A probabilistic approach for determining the control mode in CREAM. *Reliability Engineering and System Safety* 91(2): 191–199.

Lee, H.C. & Seong, P.H. 2009. A computational model for evaluating the effects of attention, memory, and mental models on situation assessment of nuclear power plant operators. *Reliability Engineering and System Safety* 94(11): 1796–1805.

Martins, M.R. & Maturana, M.C. 2013. Application of Bayesian Belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents. *Reliability Engineering and System Safety* 110: 89–109.

Mohaghegh, Z. & Mosleh, A. 2009. Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations. *Safety Science* 47(8): 1139–1158.

Mohaghegh, Z, Kazemi, R. & Mosleh, A. 2009. Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. *Reliability engineering and System safety* 94(5): 1000–1018.

Mosleh, A., Shen, S.H., Kelly, D.L., Oxstrand, J. & Groth, K.M. 2012. A Model-Based Human Reliability Analysis Methodology. *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 11)*, *Helsinki, Finland*.

Musharraf, M., Hassan, J., Khan, F., Veitch, B., MacKinnon, S. & Imtiaz, D. 2013. Human reliability assessment during offshore emergency conditions. *Safety Science* 59: 19–27.

Podofillini, L., Dang, V.N., Zio, E., Baraldi, P. & Librizzi, M. 2010. Using Models To Incorporate Expert Knowledge In Human Reliability Analysis—A Dependence Assessment Method. *Risk Analysis* 30(8): 1277–1297.

Podofillini, L., Pandya, D. & Dang, V.N. 2013. Representation of parameter uncertainty in Bayesian Belief Networks for Human Reliability Analysis. *Proceedings of the European Safety and Reliability Conference* 585–593.

Stempfel, Y. & Dang, V.N. 2011. Developing and Evaluating the Bayesian Belief Network as a Human Reliability Model Using Artificial Data. *Proceedings of the European Safety and Reliability Conference*.

Sundarmurthi, R. & Smidts, C. 2013. Human reliability modelling for Next Generation System Code. *Annals of Nuclear Energy* 137–156.

Swain, A. & Guttmann, H.E. 1983. *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* NUREG/CR-1278, US NRC, USA.

Trucco, P., Cagno, E., Ruggeri, F. & Grande, O. 2008. A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation. *Reliability Engineering and System Safety* 93(6): 845–856.

Vinnem, J.E., Bye, R., Gran, B.A., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J. & Vatn, J. 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries* 25(2): 274–292.

APPENDIX

Table. The reviewed contributions of BBNs use in HRA.

Reference	Description	HRA aspect
Groth and Swiler, 2013	Develops a BBN replicating the HRA model underlying SPAR-H; demonstrate possible model extensions, eg. hierarchical, multi-level relationships, incorporation of additional data, interdependent PSFs.	ME
Martins & Maturana, 2013	Discusses both evidential and causal reasoning (probability of failure given specific MOF states probability of MOF states given failures have occurred). The BBN structure is derived from event trees and fault trees developed by the authors.	MOFA
Ekanem & Mosleh, 2013	Dynamic BBNs to model dependency among HFEs in an accident sequence. Every time an HFE occurs, Bayesian updates are conducted to incorporate the new evidence (in the form of observation of the previous failure and/or of the state of the influencing factor).	DA
Sundarmurthi & Smidts, 2013	Data-driven BBNs for incorporation into dynamic PSA models. BBN used also as diagnostic tool for identifying the PSF combinations that most prominently occur in accidents involving human error.	PSFA
Cai et al. 2013	Assesses HEPs by dynamic BBNs accounting for the effects of repair actions (eg. repaired alarms or communication systems) on some nodes (eg. modelling clarity of indications or quality of communication). The BBN structure is derived from fault trees developed by the authors.	MOFA
Musharraf et al. 2013	Application of BBNs as HRA model for offshore emergency conditions. For the assessment of selected probabilities, multiple expert aggregation done with the combination rule of Dempster-Shafer Theory.	ME
Groth & Mosleh, 2012	Presents a framework for developing causal models incorporating diverse sources: empirical data, expert judgment, cognition models. BBNs are able to capture the relationships among PSFs, and between PSFs and Error Contexts as these relationships emerge from data.	PSFA
Vinnem et al. 2012, Gran et al. 2012	Uses BBNs to estimate the impact of MOFs on three types of human error: mistakes, violations and slips. Fault Trees and Event Trees are integrated into BBNs mode. Discusses a procedure to define and measure MOFs.	MOFA
Dang & Stempfel, 2012, Stempfel & Dang, 2011, Podofillini et al. 2013	Approach based on artificial data (generated, with known properties) for evaluating BBNs performance to estimate HEPs and to capture the relationships among PSFs. Representation of uncertainty in BBN parameters.	PSFA
Baraldi et al. 2009	Uses BBN-based expert system to assess dependency among HFEs in an accident sequence. BBN structure is derived from THERP guideline on dependence. The BBN output is the confidence in the level of dependence.	DA
Trucco et al. 2008	Uses BBNs to model the influence of MOFs on error events (both technical and human) BBN relationships via expert judgement, elicitation with recursive (e.g. Delphi) method.	MOFA
Kim & Seong, 2006a, Kim & Seong, 2006b, Lee & Seong, 2009	BBNs as computational models for situation assessment of nuclear power plant operators. Used to assess probability of mis-diagnosis of plant accidents. Approach inspired by BBN applications as diagnostic/decision aid.	SA
Kim et al. 2006	BBN-version of HRA CREAM method; the BBN is used to introduce probabilistic relationships between the state of performance conditions and the control mode in CREAM, extending the deterministic relationships from the original method formulation.	ME

ME—HRA method extension; DA—HRA dependence assessment; MOFA—Assessment of MOF impact; PSFA—PSFs relationship assessment; SA—Situation assessment.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Aggregating expert-elicited error probabilities to build HRA models

L. Podofillini, L. Mkrtchyan & V.N. Dang
Paul Scherrer Institute, Villigen PSI, Switzerland

ABSTRACT: Models for Human Reliability Analysis (HRA) applications are characterized by a strong component of expert judgment. With the increasing attention to the empirical basis of HRA, it becomes important that, whenever expert judgment is used as a source for the method development, this is done rigorously. The present paper represents one step further in that direction, dealing with the development of Bayesian Belief Networks (BBNs) models for HRA. Expert assessments of selected error probabilities are formally aggregated and converted into BBN relationships. An approach is then proposed to fill in the missing relationships. This overcomes the need to elicit all model relationships, which in many cases is impractical. The approach is demonstrated on a very simple HRA model, which suits well the illustration purposes. Given the importance of this issue for HRA (and several other applications), it seems worthwhile to systematically investigate the attractiveness of alternative approaches to develop BBN models based on elicitation of partial information.

1 INTRODUCTION

The increasing use of Probabilistic Safety Assessment (PSA) to support regulatory and operational decisions requires that methods be developed to the extent possible on an empirically sound basis. For Human Reliability Analysis (HRA), this means that methods should be based on data from operational experience, studies in simulator environments, as well as theoretical cognitive models. A significant step in this direction has been achieved with the International and US HRA Empirical Studies, which aimed at an empirically-based understanding of the strengths and weaknesses of a number of HRA methods (Forester et al. 2013).

Bayesian Belief Networks (BBN) have demonstrated promising features for HRA application (Groth & Mosleh 2012, Mkrtchyan et al. 2014). BBNs are models representing and quantifying probabilistic relationships among factors. Their primary use is the representation of knowledge and decision support under uncertainty; their application is established in diverse areas such as medical diagnosis and prognosis, engineering, finance, information technology, natural sciences (Jensen and Nielsen 2007). In HRA, BBN applications have addressed the incorporation of management and organizational factors, investigation of the relationships among the performance shaping factors, dependence analysis, situation assessment and diverse extensions of existing HRA methods (See Mkrtchyan et al. 2014 for a survey of these applications).

Ideally, the increased attention to the empirical basis of HRA methods should be seen in BBN applications as well. Examples are Groth & Mosleh (2012) and Sundarmurthi & Smidts (2013): these references propose methodologies to develop BBNs based on the combination of data, expert judgment and cognitive models. Expert judgment is required because of the difficulty of collecting data covering the entire scope and situations addressed by HRA models. Indeed, despite important efforts in the collection of HRA data, the challenges underlying the collection and the use of this type of data are such that statistically significant data to fully construct HRA models is currently not available. A rigorous integration of data, theoretical models and expert knowledge is seen as the way ahead for enhancing HRA models (Groth & Mosleh 2012).

The present paper focuses on the use of expert knowledge to construct HRA models. Rigorous treatment of expert judgment is seen as necessary before tackling the integration of the three main sources for HRA (data, theoretical models, judgment). The first aspect addressed by the present paper is the aggregation of expert estimates to inform the quantitative relationships of a BBN (the Conditional Probability Distributions, CPDs). In particular, the Bayesian approach recently presented in Podofillini & Dang (2013) is adopted, which allows formally and transparently aggregating expert estimates, so that both the inherent variability of the human error probability and the experts' variability are represented and distinguished in the final probability distribution.

The second aspect relates to the difficulty to directly elicit all CPDs from one or more experts.

When many assessments need to be made, possible biases in the elicitation of probabilities and inconsistencies arise. For a comprehensive discussion of possible biases and inconsistencies, see (Cooke, 1991). An attractive alternative, the subject of the present paper, is to elicit selected model relationships or, more generally, partial model information, and then complete the rest of the relationships with algorithms. This approach is attractive for HRA because of the large number of relationships to be assessed (a medium-size HRA model is characterized by probability distributions numbering on the order of 20–50 to fully characterize the model). Some approaches for developing a complete set of BBN relationships from a limited number of elicitations have been proposed and applied in the literature (Fenton et al. 2007) but their application to HRA has been limited. Some examples are (Martins & Maturana 2013, Cai et al. 2013); however, these required the assumption of independence in the factor influences. This assumption can be problematic for HRA applications because of the factor interactions: these are indeed a motivation for the application of BBNs in HRA. Recently, Podofillini et al. (2014) have applied the approach developed by Fenton et al. (2007), which allows capturing some degree of dependence among the factors. With the developed BBN, it was possible to represent different levels of error forcing impact (therefore, of associated error probability). The study by Podofillini et al. (2014) underscores the attractiveness of combining limited information with algorithms to complete the model relationships. A difficulty in the application of the algorithm by Fenton et al. (2007) is that the choice of the functions and their parameters needed for the development of the BBN can be quite subjective (no hard rules connecting the elicited information and these functions exist).

This paper presents a new concept to fill in the missing CPDs in a BBN by interpolating among the available ones (i.e. those elicited from the experts). In particular, the available CPDs are approximated by parametrized functions. The parameters of the missing CPDs are obtained by interpolating those corresponding to the available ones. The idea behind the approach is to decrease the subjectivity in the development of the model: the parameters of the approximating functions are calculated from those of the available ones, as opposed to being determined by the model developer.

The paper is organized as follows. The next section briefly introduces BBNs in general and, specifically, the BBN used to demonstrate the approaches. A two-input, one output BBN is used: this is certainly a strongly simplified model, but it well-suited for illustration because the behaviors of the algorithms and outputs are easy to interpret. Section 3 briefly presents the approach from Podofillini & Dang (2013) to inform CPDs by Bayesian aggregation of expert estimates and applies it to determine the selected relationships on the simple example. The interpolation approach to fill in the rest of the relationships is then presented and applied in Section 4. The conclusion section will underscore some elements for discussion.

2 BAYESIAN BELIEF NETWORK (BBN)

2.1 *Introduction*

BBNs model probabilistic relationships among variables, with variables and relationships represented as nodes and links of the network (Jensen & Nielsen, 2007). Graphically, BBNs are represented as directed acyclic graphs connecting nodes with links (consequently, feedback cycles cannot be modeled). The quantitative relationships among the connected nodes are represented as Conditional Probability Distributions (CPDs) for each variable (node) in the network. The CPDs are determined either from data or by expert judgment, or both. In the risk analysis domain, BBNs are used to represent uncertain knowledge about factors and relationships. In many cases, data are scarce (if at all available), so that the CPDs are obtained by expert elicitation. For these applications, the development of processes to avoid biases and efficiently elicit large number of probabilities is an important area of research and a key element for successful application of BBNs (Jensen & Nielsen, 2007).

2.2 *A BBN for a simplified HRA model*

As mentioned, for illustration purposes, a very simple BBN is used (Fig. 1). The BBN has two input nodes, representing the factors Human-Machine Interface (HMI) and task complexity. The output node models the Human Error Probability (HEP). The states of the nodes are given in Tables 1 and 2. Note that the definition of the output node (Table 2), modeling the HEP, is rather different than in typical HRA applications of BBNs. In these, the output

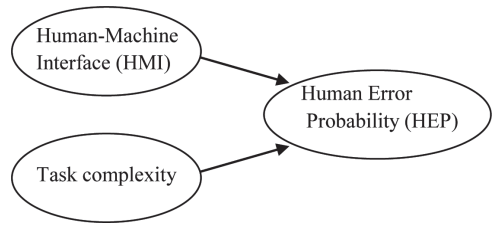


Figure 1. The BBN of the simplified HRA model.

Table 1. Definition of the BBN input nodes and states.

Node	States
Human-Machine Interface (HMI)	Strongly Success Forcing (SSF) Nominal (N) Less Than Adequate (LTA) Error Forcing (EF)
Task complexity	Very Low (VL) Nominal (N) Very High (VH)

Table 2. Definition of the BBN output state (HEP).

State #	State label	Reference probability value	Probability range
1	Very high	1	>3.2e-1
2	High	1e-1	(3.2e-2, 3.2e-1)
3	Moderate	1e-2	(3.2e-3, 3.2e-2)
4	Low	1e-3	(3.2e-4, 3.2e-3)
5	Very low	1e-4	<3.2e-4

node generally models whether the Human Failure Event (HFE) occurs: therefore the node is binary and the probability of the failed state is the HEP. In the present application, a multi-state node is used, with the states modeling different levels of error probability (from very low to very high, Table 2). This allows modeling the uncertainty in the HEP assessment, by assigning different probabilities to each HEP state. Indeed, the precision of the assessment is related to the probability interval covered by each state. The present application basically considers the case in which the BBN is used to predict the order of magnitude of the HEP (each state covers a factor of 10 in the HEP range from 1 to 1e-4). As reported in Table 2 each state is assigned a qualitative label as well as a reference probability value and range. The values determining the probability range associated to each reference value are the geometric mean of the reference HEPs of two successive intervals. The combination of qualitative labels and numerical values is often used in the elicitation of probabilities (e.g. Forester et al. 2007). The association of probability ranges to each state will be used in the application of the approach to aggregate the expert estimates (Section 3.2).

3 ELICITING SELECTED CPDS: A BAYESIAN APPROACH

3.1 *Bayesian aggregation of expert estimates*

The Bayesian approach to aggregate expert estimates entails that the estimates concerning an unknown quantity (e.g. a probability value) are used to update a prior belief concerning that quantity.

The basic assumption for the approach used in the present paper is that the quantity of interest (e.g. the HEP in the HRA case) is distributed according to a known distribution family (e.g. a normal, lognormal, beta), with unknown parameters (Mosleh, 1994). The expert opinion is then used to update the knowledge on the values of these parameters. Following the model presented by Mosleh (1994), the expert opinion comes as estimates of specific realizations of the quantity of interest.

As noted by Podofillini & Dang (2013), an element that challenges the direct elicitation of CPDs for HRA applications follows from the fact that these CPDs generally correspond to HEPs for combinations of factor states. For example, in the simple case considered in the present paper (Tables 1 and 2), one would need to elicit the applicable HEP in case the HMI is "nominal" and the task complexity is "very high" (indeed, more realistic HRA models would involve more factors and intermediate nodes). Generally, the factor labels and operationalizations may be felt as too generic and abstract: it may be difficult for experts to contextualize these factors and provide HEPs. To address this issue, Podofillini & Dang (2013) proposed an approach in which experts would be provided specific performance conditions, corresponding for example to PSA actions. These performance conditions are represented by the pattern of factor ratings under investigation. Continuing the example above, this may be in the form of a specific PSA Human Failure Event (HFE), in which the human-machine interface is "nominal" and the task complexity is "very high". Once the experts have analyzed the HFEs and provided their estimates, the output of the approach in Podofillini & Dang (2013) is the probability distribution (continuous or discrete, depending on the cases) of the HEP for the specific factor configuration under analysis.

The situation of interest for BBNs with discrete nodes is the one presented by Podofillini & Dang (2013), in which experts provide their estimate on a discrete scale, say on an n-point scale, $x_1, x_2, \ldots, x_n$. The scale can be expressed with numerical values (e.g. $x_1 = 1, x_2 = 0.1, x_3 = 0.01, x_4 = 0.001$ and the like), or representing reference values (e.g. the mean, the median or just an indication of the expected order of magnitude) for the human error probability. As shown in Table 2, each point of the scale can be also expressed with qualitative judgments (e.g. x_1 = "very likely", x_2 = "likely", x_3 = "possible", x_4 = "very unlikely"). When dealing with discrete

probability distributions, the Bayesian model can be written as:

$$\pi_j = k^{-1} L(\boldsymbol{E}/j)\pi_j^0 \quad j = 1,2,...,n \tag{1}$$

where π_j is the j-th element of the posterior probability distribution, $\boldsymbol{\pi} \equiv \{\pi_1, \pi_2, \ldots, \pi_n\}$, of the variable of interest, x (e.g. the HEP); $\boldsymbol{\pi^0} \equiv \{\pi_1^0, \pi_2^0, \ldots, \pi_n^0\}$ is the prior distribution, updated in light of the evidence $\boldsymbol{E} \equiv \{i_1^*, i_2^*, \ldots, i_N^*\}$, where N is the number of experts. Each element of the evidence i_h^* represents the expert assessment that the i_h^*-th point in the scale applies to the HFE under consideration. Factor k normalizes (over j) the expression to a probability distribution.

The likelihood term $L(\boldsymbol{E}/j)$ is interpreted as the probability of evidence $\boldsymbol{E}$, given that the actual value of x is x_j. This is a function of two elements.

- Matrix F, representing the inherent variability of the HEP.
- Matrix G, representing the confidence that the expert provides the correct HEP value.

In particular, element f_{ij} is the probability that the realization of the HEP of the specific HFE considered by the expert is within the interval represented by x_i, when the applicable (or reference value or reference judgment, depending on how the variable x is expressed) probability is represented by x_j (x_j being for example the mean, the median, or just an indication of the order of magnitude).

Element g_{ij} is the probability that the expert assesses $X = x_i$, when attempting to estimate x_j (i.e. when attempting to quantify the HEP of an HFE with HEP represented by x_j). G represents the confidence in the expert assessing the true value for X. For example, a "perfect" expert would asses the real value of the HEP: the G matrix would be the unity matrix. An unbiased expert would be modeled by a probability distribution centered on the correct value: the narrower the distribution, the higher the confidence on the expert. The next Section 3.2 provides an example of how to determine the values of the f_{ij}'s and the g_{ij}'s. Podofillini & Dang (2013) derive expressions of the likelihood term in (1), in the cases of dependent and independent expert assessments. The expressions are omitted here for brevity.

3.2 *Application to the simple HRA model*

As mentioned, for the analyses of this paper, we assume that the experts analyze specific HFEs with factor combinations corresponding to selected BBN relationships. The judgments are provided on the scale presented in Table 2. The expert assessments are then converted into corresponding CPDs. Then, these CPDs are used as interpolation anchors to fill in the rest of the CPDs.

The elements of the matrices F and G are calculated as follows. Each reference value x_i i = 1, 2, …, 5, of Table 2 is interpreted as the median of an HEP uncertainty distribution. Therefore, the HEP assessment problem becomes that of assessing which of the five x_i's best represents the median, based on the expert estimates. The error factor (square root of the 95th and 5th percentiles) of the uncertainty distribution is assumed to be known and equal to 5; this significantly simplifies the assessment procedures, because only one parameter has to be assessed (the median). Indeed, the value of 5 for the error factor represents a commonly accepted confidence range for HEPs (Podofillini & Dang 2013).

Under the above assumptions, the elements of the F matrix (Table 3) are interpreted as: f_{ij} = probability that the realization of the HEP is within interval i, given the median HEP is x_j. For example, element f_{12} is the probability that the HEP would realize within interval 1 (> 3.2e-1) given its median is x_2 (1e-2).

For the G matrix, a lognormal distribution with an error factor of 10 is assumed the confidence in the expert providing the correct value of the HEP. This corresponds to being 90% confident that the expert estimate would deviate within less than a factor of 10 above and below the correct value. The elements of the G matrix (Table 4) are therefore interpreted as follows: g_{ij} = probability that the expert assessment of the HEP is x_i, when the realization is x_j. For example, element g_{12} is the probability that the expert would assess the HEP as x_1 (>3.2e-1), when its realization is x_2 (1e-2). For use in the calculation, the elements of the matrix G are then modified to avoid too low probabilities (i.e. below ~ 1e-2) of expert estimates deviating

Table 3. Elements of matrix F, f_{ij} = probability that the realization of the HEP is within interval i, given the median HEP is x_j.

	j				
i	1	2	3	4	5
1	8.8E-1	1.2E-1	2.1E-4	2.0E-9	8.8E-17
2	1.2E-1	7.6E-1	1.2E-1	2.1E-4	2.0E-9
3	2.1E-4	1.2E-1	7.6E-1	1.2E-1	2.1E-4
4	2.0E-9	2.1E-4	1.2E-1	7.6E-1	1.2E-1
5	8.8E-17	2.0E-9	2.1E-4	1.2E-1	8.8E-1
Sum	1	1	1	1	1

*Elements at the matrix top border (e.g. $f_{11}, f_{12}, \ldots$) are obtained by integrating the lognormal pdf from +∞. Similarly, elements at the matrix bottom border (e.g. $f_{51}, f_{52} \ldots$) are obtained by integrating the lognormal pdf from 0.

Table 4. Elements of matrix G, g_{ij} = probability that the expert's assessment is x_i when attempting to estimate x_j – modified distribution tails with 1e-2 residuals.

	j				
i	1	2	3	4	5
1	7.7E-1	2.1E-1	1.0E-2	1.0E-2	1.0E-2
2	2.0E-1	5.8E-1	2.0E-1	1.0E-2	1.0E-2
3	1.0E-2	2.0E-1	5.8E-1	2.0E-1	1.0E-2
4	1.0E-2	1.0E-2	2.0E-1	5.8E-1	2.0E-1
5	1.0E-2	1.0E-2	1.0E-2	2.1E-1	7.7E-1
Sum	1	1	1	1	1

*See note to Table 3 for how border elements (different from the residuals) are calculated.

Table 5. Position of the anchors relative to the HMI-task complexity state combinations.

	Human-machine interface			
	SSF	N	LTA	Error forcing
Task complexity				
VL	Anchor 1			Anchor 2
N				
VH	Anchor 3			Anchor 4

by more than two intervals from the appropriate one, as suggested in Podofillini & Dang (2013). Therefore, elements with values below 1e-2 are set to 1e-2 as reported in Table 4.

The assumptions made in the present paper on the distributions underlying the F and G matrices, although reasonable, may be subject to further investigation in future work.

3.3 *Cases of expert assessment*

Two (hypothetical) cases are assumed: assessments from a single expert and from multiple (four) experts. The anchor assessments are provided on the four factor combinations corresponding to the extremes of the ranges for HMI and task complexity (Table 5). The anchor combinations and corresponding expert assessments are provided in Table 6.

Note that, in the single expert case, the assessments reported in Table 6 would represent the expert belief that the two factors HMI and Task complexity influence the HEP to different degrees. Indeed, an error-forcing HMI leads to very high error probability, independently of the task complexity (anchors 2 and 4 in Table 6); on the other hand, very high task complexity does not necessarily results in very high error probability (see anchors 3 and 4 in Table 6). This different importance is reflected as well in the assessments by the four experts. However, these are characterized by different levels of agreement (for example, the assessments for anchor 4 show a high degree of consistency among the experts compared to those for anchor 3). The different importance of the two factors and the different levels of agreement have implications of the final CPDs, as discussed in Section 4.

Table 6. Anchor combinations and corresponding expert assessment (hypothetical).

		Assessment of HEP	
Anchor	Factor combination HMI/task complexity	Single expert	Multiple experts *
1	Strongly success forcing/ very easy	VL	Ex1: VL ** Ex2: VL Ex3: VL Ex4: L
2	Error-forcing/ very easy	VH	Ex1: VH Ex2: H Ex3: VH Ex4: VH
3	Strongly success forcing/ very high	H	Ex1: L Ex2: H Ex3: VH Ex4: M
4	Error-forcing/ very high	VH	Ex1: VH Ex2: VH Ex3: VH Ex4: VH

* The four experts are indicated as Ex1, …, Ex4.
** VL: Very Low; L: Low; M: Moderate; H: High; VH: Very High.

By using the approach from Podofillini & Dang (2013), the judgments are converted into probability distributions of the different probability ranges, (Figs. 2 and 3). In the single expert case, the probability distributions have their maxima on the value assessed by the expert (Fig. 2 vs. Table 6). As presented in detail in Podofillini & Dang (2013), the uncertainty on the distributions combines the level of confidence in the expert estimates and the intrinsic variability of the HEP.

In the multiple expert case, the probability distributions reflect the aggregated assessments: e.g. the pronounced maximum in case of expert agreement and larger uncertainty as the level of disagreement increases. For example, comparing the distribution for anchor 4 in the single and multiple expert cases (bottom right plots in Figs. 2 and 3), the more pronounced maximum on Very High ($i = 5$) is the result of the agreement among the four experts that the applicable HEP range is $i = 5$ (Table 6); in the

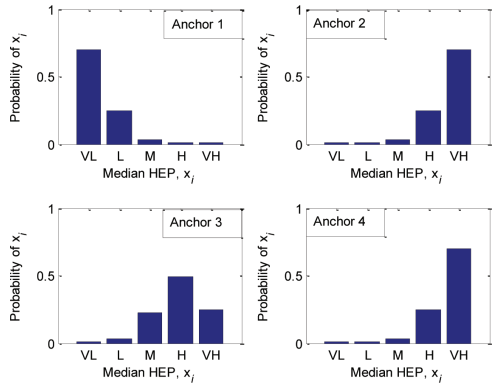


Figure 2. Conversion of the expert assessments (Table 6) in probability distributions—single expert.

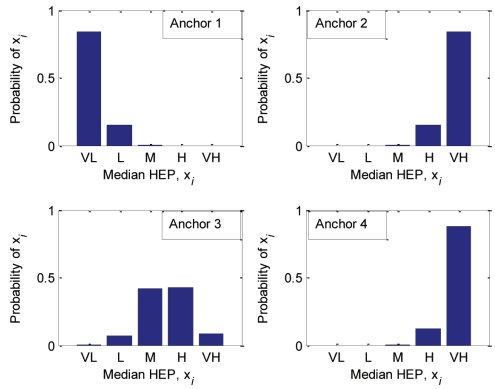


Figure 3. Conversion of the expert assessments (Table 6) in probability distributions—four experts.

single expert case shown in Figure 2, the less pronounced maximum for anchor 4 reflects the lower confidence that $i = 5$, given that it is based only on a single assessment. In contrast, the disagreement among the experts on the applicable value for Anchor 3 (Table 5) translates into two HEP values with practically equal likelihood (Moderate, $i = 3$ and High, $i = 4$).

4 THE CONCEPT FOR DERIVING THE MISSING RELATIONSHIPS: APPROXIMATE & INTERPOLATE

The expert assessments cover a selected subset of the BBN relationships. The rest have to be determined based on the properties emerging from the available judgments.

The concept presented in this paper is to fill in the missing CPDs by interpolating among the available ones. In other words, referring to Figures 3 and 4, the CPD from anchor 1 would gradually move to that for anchor 3 as task complexity changes from very easy to very difficult and to that for anchor 2 as HMI becomes error-forcing; likewise for the other factor combinations. The approach has two main elements:

– The available CPDs are approximated by functions, described by parameters
– The parameters of the missing CPDs are obtained by interpolating among the available ones CPDs

Of course, two key assumptions are required: on the approximating functions and on the interpolation rule. In the present paper, Normal functions are used (therefore the parameters would be the mean and the standard deviation) and the interpolation is linear on the factor states.

4.1 *Approximating the anchor distributions*

Assuming normal functions for the approximation, the first step is to determine the parameters of the functions approximating the probability distributions obtained from the elicitation (e.g. Figs. 2 and 3). This was done by minimizing the sum of the squared difference between each value of the distributions assessed for the anchors and the corresponding value of the Normal function (appropriately normalized so that the values sum to 1). As example, Figure 4 shows the result for the single expert assessment, anchor 3. In Figure 4, the bars replicate the anchor 3 distribution of Figure 2. The dotted line shows the Normal function that best approximate the distribution; the circles show the values of the Normal function in correspondence of each value of the distribution. Note that the Normal function should not be interpreted as a probability density: it is just used to approximate the discrete probability distribution in its five values

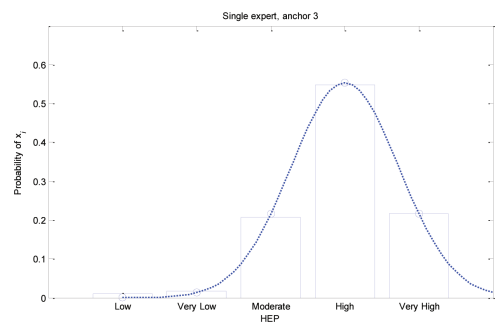


Figure 4. Example of approximation of anchor distributions by a Normal function—single expert, anchor 3.

(as shown in Fig. 4). Generally, the Normal distribution was found to approximate well all anchor distributions. This is not surprising because of the assumption made in Section 3.2 of lognormal uncertainty distributions for the HEP realizations and for the expert deviation from the correct value: these distributions become normal in the log-scale of the probability introduced by Table 2. However, the Normal distributions fail to represent the tails introduced by the residuals of 1e-2 introduced to modify the elements of the G matrix (see in Fig. 4 the underestimation of the probability of the Low and Very Low probability intervals). Indeed, studying alternative approximating functions can be expected to represent an important subject of future work.

Indeed, in order to evaluate the Normal function, the states of the output node HEP are assigned a numerical scale (the Normal function is truncated within the scale). The scale 1 to 5 was used (1: for "very low" to 5 "very high"). Note the choice of the scale has no influence on the resulting approximating function because of the normalization. The values of the resulting parameters of the approximating function are reported in Table 7.

4.2 *Obtaining the missing CPDs by interpolation*

Once the anchor parameters are obtained (Table 7), it becomes easy to obtain the missing values by linear interpolation (Tables 8 to 10).

The tables show that the interpolation approach gradually changes the parameter values across the anchors. For example, the parameter μ in the single expert assessment case (Table 8) is interpolated across the values corresponding to the anchor statements. The latter values are exactly matching the expert assessments of Table 6. This is indeed expected because the anchor distributions have maxima on the expert assessments as discussed with reference to Figure 2. For the multiple expert case, the anchor values of μ represent "in-between" assessment (e.g. 3.5 for anchor 3, HMI being "Strongly Success Forcing" and Complexity "Very High", Table 6), resulting from the aggregation of the different expert evaluations.

Table 7. Parameters of the normal functions approximating the anchor distributions from expert assessments (Table 6).

	Single expert		Multiple experts	
Anchor	μ	σ	μ	σ
1	1	0.72	1.2	0.42
2	5	0.72	4.8	0.42
3	4	0.84	3.5	0.77
4	5	0.72	4.7	0.32

Note that μ and σ are to be intended as descriptive parameters for the approximating Normal function. They are not related to the mean and standard deviation of the corresponding discretized function.

Table 8. Values of the parameter μ (single expert). Shaded cells: anchor values; white cells: interpolated values.

	HMI			
	SSF	Nominal	LTA	EF
Complexity				
Very low	1.0	2.3	3.7	5.0
Nominal	2.5	3.3	4.2	5.0
Very high	4.0	4.3	4.7	5.0

Table 9. Values of the parameter σ (single expert). Shaded cells: anchor values; white cells: interpolated values.

	HMI			
	SSF	Nominal	LTA	EF
Complexity				
Very low	0.72	0.72	0.72	0.72
Nominal	0.78	0.76	0.74	0.72
Very high	0.84	0.80	0.76	0.72

Table 10. Values of the parameter μ (multiple experts). Shaded cells: anchor values; white cells: interpolated values.

	HMI			
	SSF	Nominal	LTA	EF
Complexity				
Very low	1.2	2.4	3.6	4.8
Nominal	2.4	3.2	4.0	4.8
Very high	3.5	3.9	4.3	4.7

Table 11. Values of the parameter σ (multiple experts). Shaded cells: anchor values; white cells: interpolated values.

	HMI			
	SSF	Nominal	LTA	EF
Complexity				
Very low	0.42	0.42	0.42	0.42
Nominal	0.60	0.52	0.45	0.37
Very high	0.77	0.62	0.47	0.32

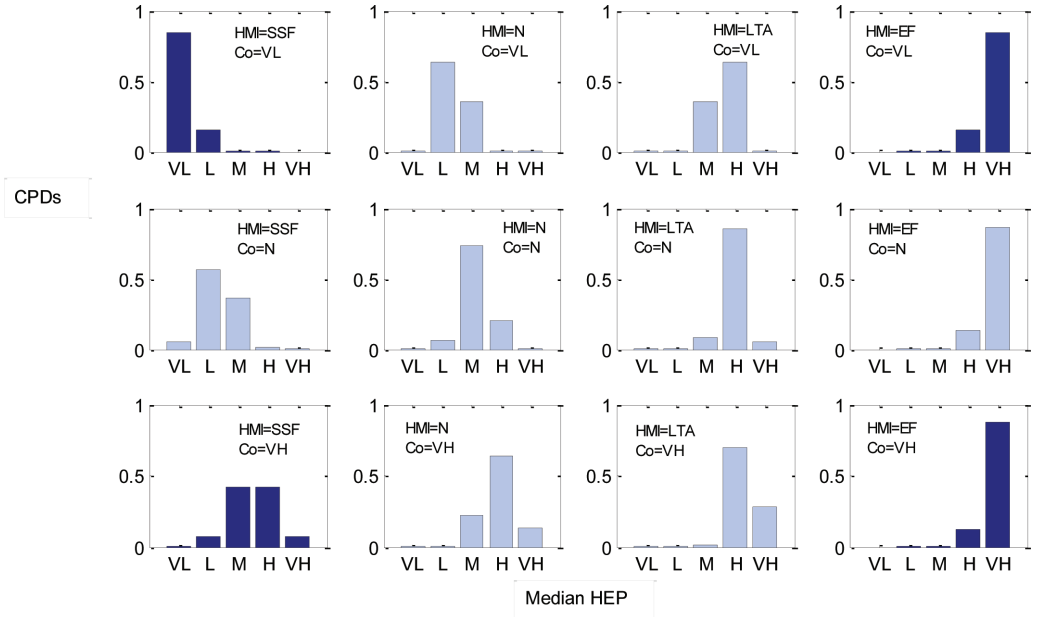


Figure 5. CPDs for the simple BBN model (multiple expert elicitation): dark blue: anchors CPDs; light blue: derived from interpolation approach.

Concerning σ, it is interesting to note how the different levels of uncertainty are reflected in the multiple expert case. The smallest value of σ corresponds to anchor 4 in which all experts agree that the HEP should be "very high", ie. $i = 5$. The largest value corresponds to anchor 3, where the largest disagreement is seen (Table 6).

Finally, Figure 5 shows all the CPDs obtained by applying the proposed approach: as desired, in the approach development, the CPDs gradually shift across the anchors.

5 DISCUSSION AND CONCLUSIONS

The present paper has dealt with the development of BBN models for HRA. Expert assessments on HEPs are formally aggregated and converted into CPDs for selected BBN relationships. An approach is proposed to fill-in the missing relationships. This allows overcoming the elicitation of all model relationships, which in many cases can be impractical.

The aim of the fill-in approach is to limit the level of judgment required to determine the rest of the model relationships. The parameters defining the missing relationships are calculated from those elicited from the expert. The approach assumes that the CPDs are discretizations of underlying Normal distributions (as it is the case, for example in the literature approach by Fenton et al. 2007). The linear interpolation of the CPD parameters allows to automatically build the missing relationships without additional subjectivity injected in the model. This contrasts with the approach in Fenton et al. (2007) in which the parameters of the missing relationships need to be determined by the model developer.

Indeed, one element of subjectivity in the presented approach is the choice of the Normal functions as well as of the interpolation function (linear). However, the applicability to HRA of these or possibly alternative choices can be tested in different applications. Once (if) a best choice is identified, this element of subjectivity would be removed.

An important feature of the combination of the aggregation and fill-in approaches is the treatment of uncertainties. The aggregation approach allows to formally and transparently consider the possibly different confidence in the assessed CPDs. Then, the fill-in approach maintains this information and, by interpolation, the CPDs gradually move across the areas of the model with different levels.

It is worth finally noting that different alternative approaches exist to develop BBNs based on limited elicited information. Given the importance of this issue for HRA (and several other applications), it seems worthwhile to systematically investigate the attractiveness of these alternatives for their application to HRA, addressing different aspects such

as the type and amount of information required from the expert, handling of uncertainties, possible limitations on the number of node states, and the like.

ACKNOWLEDGEMENTS

This work was funded by the Swiss Federal Nuclear Safety Inspectorate (ENSI), under DIS-Vertrag Nr. 82610. The views expressed in this article are solely those of the authors.

REFERENCES

Cai, B., Liu, Y., Zhang, Y., Fan, Q., Liu, Z., Tian, X. 2013. A dynamic Bayesian networks modelling of human factors on offshore blowouts. *Journal of Loss Prevention in the Process Industries*, 26: 639–649.

Cooke, R.M. 1991. Experts in uncertainty. New York: Oxford university press.

Fenton, N.E., Neil, M., Caballero, J.G. 2007, Using ranked nodes to model qualitative judgments in Bayesian networks. *IEEE Transactions on Knowledge and Data Engineering,* 19(10): 1420–1432.

Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., Lois, E. 2007. *ATHEANA User's Guide*, NUREG-1880, U.S. Nuclear Regulatory Commission, Washington, DC.

Forester, J.A. et al. 2013. The International HRA Empirical Study—Final Report—Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data, OECD Halden Reactor Project, HPR-373, March 2013, Halden, Norway (An edited version will be published by the U.S. Nuclear Regulatory Commission as NUREG-2127).

Groth, K.M. & Mosleh, A. 2012. Deriving causal Bayesian networks from human reliability analysis data: A methodology and example mode. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 226(4): 361–379.

Jensen, F.V. & Nielsen, T.D. 2007. *Bayesian Network and Decision Graphs*. Springer science, New York, NY, USA.

Martins, M.R. &. Maturana, M.C. 2013. Application of Bayesian Belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents. *Reliability Engineering and System Safety*, 110: 89–109.

Mkrtchyan, L., Podofillini, L., Dang, V.N. 2014. A survey of Bayesian Belief Network applications in Human Reliability Analysis. *Proceedings of ESREL 2014, European Safety and Reliability Conference*, Wroclaw, Poland, 14–18 Sept. 2014.

Mosleh, A. 1992. Bayesian Modeling of expert-to-expert variability and dependence in estimating rare event frequencies. *Reliability Engineering and System Safety*, 38: 47–57.

Podofillini, L. & Dang, V.N. 2013. A Bayesian Approach to Treat Expert-Elicited Probabilities in Human Reliability Analysis Model Construction. *Reliability Engineering & System Safety*, 117: 52–64.

Podofillini, L., Mkrtchyan., L., Dang, V.N. 2014. Quantification of Bayesian Belief Net Relationships for HRA from Operational Event Analyses. *Probabilistic Safety Assessment and Management PSAM 12*, June 2014, Honolulu, Hawaii.

Sundarmurthi, R. & Smidts C. 2013. Human reliability modelling for Next Generation System Code. *Annals of Nuclear Energy*, 52: 137–156.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Organizational factor inclusion in Human Reliability Analysis (HRA) tools

N. Balfe & S. Cromie
Centre for Innovative Human Systems, Trinity College Dublin, Dublin, Ireland

ABSTRACT: There is an increasing recognition of the role played by organizational factors in major accidents and incidents, but many of the tools available for human factors analysis focus on the specific factors related to the task. This study used the STAMINA model to assess the scope of the Performance Shaping Factors (PSF) in five HRA tools. The goal was to understand the extent to which team and organizational factors are accounted for in different HRA tools as compared to the more traditionally recognized task and individual factors. The analysis highlights the mismatch between the increasing understanding of the importance of organizational factors and the relative lack of account of these factors in traditional HRA methods.

1 INTRODUCTION

The causes of accidents have moved from predominantly mechanical faults or failures in past decades to a current situation where human and organizational factors are recognized as root causes of major accidents. Taking aviation for example, the Comet disasters in the 1940s were due to a lack of understanding of metal fatigue in pressurized aircraft hulls. More recent aviation accidents, such as the Air France Flight 447 which crashed in the Atlantic following incorrect pilot reactions to inconsistent air speed indications, and even the Tenerife air accident in 1977 have listed human error as a contributing factor or leading cause. Outside of aviation, human error has also been associated with major accidents in the oil and gas (e.g. Piper Alpha in 1988, Deepwater Horizon in 2010), rail (e.g. Clapham in 1988, Eschede in 1998), and maritime (e.g. Herald of Free Enterprise in 1987, Costa Concordia in 2012) industries.

Human error is a term subject to increasing debate with the main argument against its use pointing towards the negative connotations it holds for the individual who had the misfortune to commit an error in the chain of events leading to an accident. This is especially true considering that the same action may have been appropriate and even applauded under a different set of circumstances. Dekker (2006) points out that systems are not intrinsically safe and individuals are often required to make trade-offs between safety goals and the other goals of the organization. As well as placing inappropriate blame on an individual, who may have acted in an entirely understandable manner, the term serves to deflect attention from more fundamental socio-technical issues and the ability to seek out and appropriately control variability in human performance (Hollnagel and Amalberti, 2001).

The recent train derailment in Santiago de Compostela is a case study in this—media reports firmly established human error as the accident cause early on in the investigation (e.g. Topham, 2013; Dowsett & Larraz, 2013), and this was followed by reports of previous reckless behaviors by the driver involved. Later accounts of his reputation for cautious behavior were not as widely reported. But the debate in the media over the possible culpability of the driver distracted from the more serious issues involved: the poor design of the track at that location and the consequent need for a serious reduction in speed combined with the lack of supervisory automation systems for monitoring speed—a system which was in place for the rest of the line (Burgen, 2013). These design flaws created a situation in which human error was far more likely, and the right set of circumstances occurred when the driver was distracted by a work related call. The organizational factors that allowed these to take place have not yet been fully investigated and/or reported to the authors' knowledge, however the rail infrastructure manager has already moved to install speed controls on the section of track, as well as reviewing protocols governing communications between drivers, control center staff and train crews in light of the accident.

Other examples of organization contributions to accidents include the degradation of the safety management system in the Bhopal chemical accident in 1984 (Gupta, 2002), poor equipment and job design in the Herald of Free Enterprise

maritime accident in 1987 (Sheen, 1987), poor signal design and lack of safety controls in the Ladbroke Grove rail accident in 1999 (Cullen, 2001). These, and other accidents, serve to illustrate that while the immediate cause of an accident may lie in an individual's actions, the control of these factors often lies with the organization in the design of the system and the implementation of controls that support human performance.

The motivation behind this research is the idea that organizational factors are not well accounted for and there are limited methods and tools available to assess how well an organization is working to control risks relating to human performance. The Human Factors discipline provides trained professionals and a range of methods and techniques to assess systems for human performance, but it is still a minority discipline and human factors assessments can sometimes be regarded as a tick-box exercise rather than a critical part of the engineering design and company operations.

The IEA defines human factors as "the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance." (IEA, 2000). The discipline has developed tools to assess operator workload, the design of human-machine interfaces, the design of the working environment, including thermal, lighting, and noise factors, etc. However, some industries still focus on controlling individual behaviors through training, and rewarding safety behaviors. These are both valid approaches, but without any recognition of the role of the organization and the potential improvements at the design level, it is unlikely to be optimal.

1.1 *STAMINA model*

The STAMINA Model of human performance was developed to underpin human factors training, primarily in the aircraft maintenance industry, but it has also been applied in the pharmaceutical sector (Konstantinos et al., 2011). It adopts the EASA definition of human factors as 'anything that affects an individual's performance" (EHFAG, 2012). The model is composed of four elements:

- Task—characteristics of the task itself that can promote or reduce error;
- Individual—the strengths and limitations of humans performing the task;
- Team—effectiveness of team interaction, e.g. communication, peer pressure, etc.;
- Organization—factors that can limit or promote the effectiveness of the organization as a whole, e.g. design of roles, management of resources, etc.

This model has proved to be a useful tool, both in structuring human factors training and in analyzing the requirements of legislation and the current status of organizations (Konstantinos et al., 2011). The model is used in this research to structure the analysis of the factors considered in Human Reliability Analysis tools.

2 HUMAN RELIABILITY ANALYSIS

Techniques for the identification and evaluation of human error are typically labeled Human Reliability Assessments (HRA). A complete HRA starts with a definition of the problem and development of a task analysis to support the HRA (Kirwan, 2005). The core of HRA is the Human Error Identification (HEI) and Human Error Quantification (HEQ) stages, and several methods have been developed to specifically focus on these two areas. From these, control measures can be identified to reduce the overall system risk.

The task analysis is the human factors equivalent of the functional analysis in systems engineering. Functional analysis is a description of system functions achieved by arranging functions in logical sequences. Decomposition of higher-level functions adds more detail and allows system objectives to be allocated to lower-level functions. Similarly, task analysis identifies and examines the tasks performed by human operators when interacting with the system (Kirwan & Ainsworth, 1992). Without these representations of the tasks and activities it would not be possible to correctly analyze the task, identify and evaluate all the relevant risks. Common task analysis representations include Hierarchical Task Analysis (HTA; Annett & Duncan, 1967), Link Analysis (Chapanis, 1996), Operational Sequence Diagrams (Kirwan & Ainsworth, 1992), Cognitive Task Analysis (CTA; Stanton et al., 2005) as well as more general process and flow-chart techniques. The data for these representations are usually captured through observations, analysis of documentation, and/or interviews.

Specific methods have been developed to support human factors analysis with regard to HEI or HEQ. HEI tools include TRACER (Shorrock and Kirwan, 1998), SHERPA (Embrey, 1986), and GEMS (Reason, 1990) while HEQ tools include SLIM (Embrey et al., 1984), APJ (Seaver and Stillwell, 1983), and TESEO (Bello and Colombari, 1980). HEI techniques consider what errors are possible (the External Error Mode; EEM), why that error might occur (the Performance Shaping Factors; PSFs), and the psychological mechanism responsible for the error. Despite the number of HEI techniques developed, Kirwan (1992),

in a comparison of techniques, found that HEI is more of an art than a science, and relies to a large extent upon the expertise of the human factors professional.

HEQ techniques focus on calculating the Human Error Probability using a basic formula of the number of errors occurring divided by the number of opportunities for error (Kirwan, 1996). All HEQ techniques share the same difficulty—access to reliable data on human error rates. Typically, a base error rate is identified for a particular type of task and this is modified according to the circumstances to account for factors in a particular environment that may increase the probability of error. The base error rates can be based on task observation or recording, incident data, simulator data or expert judgement. Many HEQ tools include base error rates, which have been collected either from specific domains (e.g. nuclear simulation data used in THERP) or generic domains (e.g. generic tasks in HEART) but it is usually recommended, where possible, to use task specific information. This information can be extremely difficult to collect. Even where detailed accident and incident data is available, the number of opportunities for that error to occur may not be available, the number of opportunities for that error to occur may not be available and so it is not possible to calculate an accurate error rate.

The final step of the HRA process, control measure identification, largely relies upon the human factors practitioner's general knowledge and skill, supported by applicable standards and validated methods where possible. Where possible, control measures should make the design inherently safer, but in some cases the best available mitigation may be to generate new procedures or provide operator training.

Complete HRA methods cover both HEI and HEQ and these are the methods analyzed in this research. The tools covered are THERP, HEART, SPAR-H, CREAM, and ATHEANA.

2.1 *THERP*

The Technique for Human Error Rate Prediction (THERP) was developed by Swain and Guttman (1983) to evaluate the probability of human error within specific tasks. THERP uses a fault tree approach to model Human Error Probabilities (HEP), but also attempts to account for other factors in the environment that may influence these probabilities. These factors are referred to as Performance Shaping Factors (PSF). The probabilities used in THERP can either be generated by the analyst, usually from simulator data, or can be taken from tables generated by Swain and Guttman from available data and expert judgement.

Kirwan (1996) lists the key elements of the THERP process as:

- Decomposition of tasks into elements;
- Assignment of nominal HEPs to each element;
- Determination of effects of PSF on each element;
- Calculation of effects of dependence between tasks;
- Modelling in a HRA Event Tree;
- Quantification of total task HEP.

THERP is a complete methodology, from generation of task analyses, through error identification and representation, to quantification of human error probability. The documentation associated with the technique contains methods, models and tables of estimated human error probability to inform the analysis.

2.2 *HEART*

The Human Error Assessment and Reduction Technique (HEART) structures PSF considerations for the analyst who uses these to modify basic error probabilities. It assumes that human reliability is dependent on the generic nature of the task and that the level of reliability will be consistent (given a likelihood within probabilistic limits) under 'perfect' conditions. The reliability can be varied for non-perfect conditions using Error Producing Conditions (EPCs).

Kirwan (1996) lists the key elements of the HEART process as:

- Classify a task into one of the generic categories;
- Assign a nominal HEP to the task;
- Determine which Error Producing Conditions (EPCs: effectively PSFs) may affect task reliability;
- Determine the Assessed Proportion Of Affect (APOA) for each EPC;
- Calculate the task HEP.

Eight generic categories are provided within HEART and are related to the level of familiarity an operator has with the task as well as the task complexity/difficulty. Each generic category has a nominal human unreliability score associated with it. EPCs are listed within the tool, each with an associated multiplier to be applied to the unreliability score; however, the analyst must use their judgment to decide how much of a negative effect each EPC has on the task and calculate appropriately.

2.3 *SPAR-H*

The Simplified Plant Analysis Risk Human Reliability Assessment (SPAR-H) was developed in 1999 from a previous method (ASP/SPAR). This

method classifies tasks as either action tasks or diagnosis tasks and assigns a generic error rate based on this. Potential benefit or detriment is included through eight PSFs:

- Available time;
- Stress and stressors;
- Experience and training;
- Complexity;
- Ergonomics (and HMI);
- Procedures;
- Fitness for duty;
- Work process.

2.4 *ATHEANA*

A Technique for Human Event ANAlysis (ATHEANA) was developed by the nuclear industry due to a perceived need for a human error analysis tool that more closely modeled actual operational events and which put a stronger focus on contextual factors. The quantification is based around three calculations. First, calculating the probability of an 'Error Forcing Condition' (EFC; i.e. the probability that the plant will be in a state which may induce an error). This is determined by a combination of plant conditions and PSFs. Second, the probability of an Unsafe Action (UA). And third, the probability of not recovering from the initial UA. This third area incorporates the possibility of alarms and/or feedback to the operator allowing them to correct the UA.

Key steps in the process are:

- Integration of the issues of concern into the ATHEANA HRA/PRA perspective;
- Identification of human failure events and unsafe actions that are relevant to the issue of concern;
- For each human failure event or unsafe action, identification of (through a structured and controlled approach) the reasons why such events occur (i.e. elements of an EFC—plant conditions and performance shaping factors);
- Quantification of the EFCs and the probability of each unsafe action, given its context;
- Evaluation of the results of the analysis in terms of the issue for which the analysis was performed.

EPCs are identified using structured search schemes regarding plant conditions and rules and error types.

2.5 *CREAM*

The Cognitive Reliability Error Analysis Method (CREAM) is a second-generation error analysis method developed by Hollnagel (1998) which can be used both predictively and retrospectively. The technique involves identifying the importance of human performance in a given context and application of a cognitive model. In contrast to other techniques, CREAM focuses the analysis on the context of the task rather than the task itself.

Four basic control modes are represented within the cognitive model taken from Hollnagel's Contextual Control Model (COCOM), and the reliability is generated from these:

- Scrambled control: the choice of the forthcoming action is unpredictable or haphazard. The situation in question may be portraying rapid alterations in unexpected ways thus eliminating the operator's ability or opportunity to make deductions about the next action required;
- Opportunistic control: the next action is determined by superficial characteristics of the situation, possibly through habit or similarity matching. The situation is characterised by lack of planning and this may possibly be due to the lack of available time;
- Tactical control: performance typically follows planned procedures while some ad hoc deviations are still possible;
- Strategic control: plentiful time is available to consider actions to be taken in the light of wider objectives to be fulfilled and within the given context.

The assessment should commence with the generation of a task analysis to facilitate further analysis. Common Performance Conditions (CPCs) are then used to determine which mode the system is operating under. A count of positive CPCs (improving reliability) against negative CPCs (reducing reliability) for the system under analysis allows the control mode to be determined. If the potential for error is sufficiently low, the analysis may stop at this point, or it may be necessary to continue with a more detailed analysis.

3 ORGANIZATIONAL FACTORS

Direct human factors contributions to accidents and incidents tend to be described as human errors (Reason, 1990). Various factors including biological factors (e.g. age, gender, size, handicaps), physical condition, mental condition, competence, and personality may all contribute to human performance. All of these can be managed to some degree by the organization, and the failure to do so can be regarded as an organizational contribution to an accident.

Organizational factors are those areas under the control of the company management that can contribute to a safer working environment. Organizational factors may not be as readily identified during an accident investigation, as they tend

to require a deeper level of analysis than is always performed following an accident/incident. Leveson (2011) suggests that organizational factors are frequently not identified because traditional accident investigation models stop once an immediate causal event has been identified. Therefore, the factors leading an operator towards an error are not analyzed. Similarly, organizational factors may not be well accounted for in risk assessments where the focus has been on identifying possible human errors. Organizational factors can include management commitment to safety, training, communications, stability of the workforce, supervison and teamwork, among others (Gordon, 1998).

The organizational element of human performance management has often been measured in terms of its safety culture, which Reason (1997) describes as an engine driving an organization towards increasing safety and is composed of

- an informed culture, in which managers have the information needed to manage safety;
- a reporting culture, in which people are prepared to report their errors and near misses;
- a just culture, in which people are encouraged to provide information on genuine errors but willful violations are punished;
- a flexible culture, one which can adapt to meet changing circumstances;
- a learning culture, one which has the ability to analyze and draw the correct conclusions from safety data and act upon it.

The research into safety culture has led to the use of safety climate measurement tools as a Safety Performance Indicator (Guldenmund, 2000) but the results are largely intangible and may not help organizations identify where they need to focus attention in order to improve safety (Sorenson, 2002). The lack of a generally accepted definition for safety culture or safety climate also limits their usefulness as concepts since they do not support a systemic methodology for their measurement (Zhang et al., 2002).

In contrast, organizational factors cover more tangible areas, such as the provision of appropriate training and development of procedures, human factors input to the design of HMI, and appropriate design of job roles. These are often included in HRA techniques as performance shaping factors or error producing conditions. However, there is no comprehensive framework defining organizational factors and their measurement, despite their recognized importance in managing safety.

4 METHOD

This study used the STAMINA model to categorize the performance shaping factors in five HRA tools: HEART, THERP, SPAR-H, CREAM, and ATHEANA. The performance shaping factors were taken from available literature on the five methods (Swain & Guttman, 1983; Gertman et al., 2005; Hollnagel, 1998; Cooper et al., 1996), and in the case of HEART, the railway adaptation by Gibson (2012) was used.

The STAMINA model was supplemented by an 'Environment' category to capture factors relating specifically to the physical environment in which the task is performed. There were therefore five categories for the analysis: Task, Environment, Individual, Team, and Organization. Each PSF (or equivalent) was assessed to determine to which category it should be assigned.

The aim of the study was to understand how the factors influencing human performance within available HRA methods are spread across the five different areas. A review of the literature in the area did not identify any similar studies, and although some studies have highlighted the lack of a standard set of PSFs (e.g. Groth & Mosleh, 2012), the choice of PSFs within HRA tools has largely been unchallenged. This study was designed to give an insight in to possible gaps in the tools available for the analysis of human performance, particularly in terms of recognition of the possible impact of the organization on individuals' safety performance.

5 RESULTS

5.1 *Performance shaping factors*

THERP had the largest set of PSFs across the five tools analyzed, and contained 69 PSFs across three categories of External PSFs, Stressors, and Internal PSFs. Within the external PSFs, situational characteristics such as the environment in which the task is conducted, the work hours and organizational structure were covered. External PSFs also included job and task instructions, and equipment and task characteristics. Stressors were both psychological (e.g. task speed, distractions) and physiological (e.g. fatigue, hunger, radiation). The final category of internal PSFs included training and experience, motivation, and sex differences. SPAR-H contained eight PSFs, including available time, stress/stressors, complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes. HEART contained 27 Error Producing Conditions (EPCs) across six categories of task design, interface, competence management, procedures, person, and environment. CREAM contained nine Common Performance Conditions (CPCs) including adequacy of organization, working conditions, adequacy of MMI and operational support, availability of procedures/plans, number of simultaneous goals, available

time, time of day, adequacy of training and experience, and crew collaboration quality. CREAM also contains a set of antecedents under the broad categories of person-related, technology-related, and organization-related. However, these are not included in the application of the HRA tool and have not been included in the analysis. Finally, ATHEANA contained nine PSFs of procedures, training, communications, supervision, staffing, human-system interface, organizational factors, stress, and environmental conditions.

5.2 *Analysis*

Figure 1 describes the results of the analysis. In total, 47% of the factors in the five HRA tools related to the specific task being analyzed, 11% to the environment, 17% to the individual, 8% to the team, and 18% to the organization.

There was considerable variation in the tools in terms of the extent to which they addressed different areas of the STAMINA model; however, all tools had a primary focus on the task, with the exception of ATHEANA which had a majority of elements focused on the organization. Environmental factors were also not widely accounted for, despite being a key influencer on task performance, and often under the control of the organization. Team factors also failed to play a major role in many of the tools.

HEART and CREAM featured the largest number of task-related PSFs as a proportion of the total number of PSFs in each tool (59% and 56% respectively). The most common task-related PSFs were procedures and HMI, which appeared in all five HRA tools, and available time appeared in four tools. THERP and HEART had the highest number of PSFs related to the task, as they also had the highest overall number of PSFs. THERP included a number of PSFs related to the requirements of the task, such as memory requirements and decision-making, while HEART featured PSFs relating to conflicting goals.

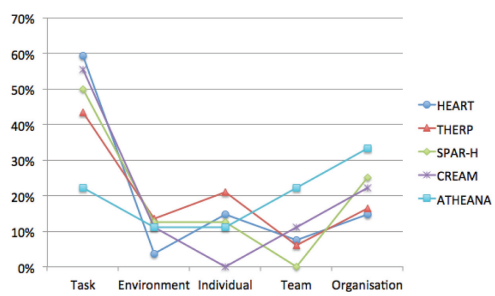


Figure 1. Analysis of the PSF according to the STAMINA model.

All five tools included environmental stressors but apart from THERP, none went in to any detail, i.e. the four remaining HRA tools simply listed environmental conditions as a PSF. THERP provided more specific PSFs including temperature extremes, radiation, oxygen insufficiency, and vibration. However, THERP did not cover less extreme environmental conditions such as lighting levels, glare, and noise.

HEART and THERP featured a higher number of individual related factors as compared to the other tools. SPAR-H simply included a broad 'fitness for duty' PSF while ATHEANA listed 'Stress'; CREAM did not feature any individual related factors. HEART and THERP both covered factors relating to individual experience and previous training, emotional stress, and physical condition. THERP was the most comprehensive, also including factors relating to fatigue, pain, motivation, attitudes, and sex differences.

Team related factors was the smallest group, with only nine PSFs appearing across all five tools and SPAR-H did not contain any team factors. Quality of communications was the most common team factor, featuring in three of the tools. There was no agreement between the tools across the remaining six factors classified as team related. These covered actions by others, team structure, group identifications (THERP), crew collaboration (HEART), and supervision (ATHEANA).

The proportion of organizational factors represented in the five tools ranged from 15% (HEART) to 33% (ATHEANA). There was considerable variation in the factors covered within the organizational category. Experience and training provided by the organization appeared in three tools, organizational structure/role design, fatigue management, staffing, and work processes/policies all appeared in two tools. Both CREAM and ATHEANA had a generic PSF of 'Organization' while THERP included a number of more specific factors related to reinforcement of behaviors.

6 DISCUSSION

The analysis of the results found that, as expected, there is a stronger focus on task and individual factors than on team and organizational. The strong focus on the task element within all five HRA tools is to be expected, since HRA is typically used to analyze the probability of failure of a particular task. However, the focus of the HRA tools is not compatible with the acknowledged role of organizational factors in major accidents.

The role of human error in safety analysis is increasingly considered outdated and unhelpful in creating a cooperative socio-technical system.

New methods for assessing events, such as the Event Risk Classification (ERC) element of the ARMS methodology (ARMS, 2010) have moved towards a focus on effectiveness of the preventative and recovery barriers in relation to an undesirable event. This helps focus the organization on the positive measures it can take to promote safety. A similar concept is needed to support human performance through the identification, measurement and management of the relevant organizational factors.

Existing safety culture surveys provide organizations with information on how mature they are in terms of safety, but the elements measured are largely intangible and provide organizations with the knowledge that they need to improve, but not necessarily what and how they should improve. A tool developed to allow an organization to analyze its strengths and weaknesses in terms of supporting human performance could help the organization focus on tangible areas for improvement. This could be achieved either through the strengthening of the role of organizational factors within the existing HRA paradigm, or through the creation of a new approach with a stronger focus on the organization. The development of a tool in this area would also serve to provide more support for the critical task of control measure identification within existing HRA approaches.

Task factors, are by nature, very variable and can be difficult to identify and quantify, particularly early on in the design of a new system. In contrast, organizational factors are more stable and are by definition, within the control of the organization. Our suggestion is that more can be achieved by focusing efforts on improving organizational factors to support human performance. To achieve this, the set of organizational factors will need to be expanded to include those that will directly influence the task, environment, individual and team factors. Examples of this might be the existence of a standard within the organization for an ergonomic review of the environment and equipment, explicit role design and function allocation, selection and recruitment activities explicitly related to the job requirements, and an assessment of the quality of procedures design rather than the quality of the individual procedures related to a particular task.

7 CONCLUSION

Hollnagel et al. (2013) in a white paper for the air traffic control industry suggest that the focus should be moved from viewing human activities in a system as a liability or hazard to recognizing that human activity is an intrinsic part of the system and is subject to variability. Supporting human performance enables a system to become more flexible and resilient, and development of better tools and measures for managing and controlling organizational factors will be critical for supporting human performance.

The study reported here has shown that the traditional HRA factors do take account of some organizational factors, but these are relatively limited in comparison to the task factors. The next steps for this research will be to draw together a coherent framework of tangible organizational factors that will help organizations assess their strengths and weaknesses in terms of supporting human performance. A tool based on this framework could facilitate organizations in continuously improving safety.

ACKNOWLEDGEMENTS

This research was financed under EU FP7 Marie Curie Actions Initial Training Networks as part of the Innovation in Risk Assessment through Human Factors project (InnHF; www.innhf.eu)—FP7-PEOPLE-2011-ITN: Project ID 289837.

REFERENCES

Annett, J. & Duncan, K.D. 1967. Task analysis and training design. *Occupational Psychology*, 41, 211–221.

ARMS. 2010. *The methodology for Operational Risk Assessment in Aviation Organisations.* Retrieved 30 March from www.skybrary.aero.

Bello C.G. & Colombari V. 1980. The human factors in risk analyses of process plants: The control room operator model 'TESEO'. *Reliability Engineering* 1(1), pp. 3–14.

Burgen, S. 2013. Spanish railway safety under review after Galicia crash, say bosses. *The Guardian*, August 8. Retrieved 16 May 2014.

Chapanis, A. 1996. *Human Factors in Systems Engineering*. New York: John Wiley & Sons.

Cooper, S.E., Ramey-Smith, A.M., Wreathall, J., Parry, G.W., Bley, D.C. Luckas, W.J., Taylor, J.H., Barriere, M.T. 1996. *A Technique for Human Event Analysis (ATHEANA)—Technical Basis and Methodological Description.* Washington DC: US Nuclear Regulatory Commission (USNRC).

Cullen, W. 2001. *The Ladbroke Grove Rail Inquiry: Part 2 Report*. London: HSE Books.

Dekker, S. 2006. *The Field Guide to Understanding Human Error.* Hampshire: Ashgate.

Dowsett, S. & Larraz, T. 2013. Spanish train wreck driver got warnings before crash. *Reuters*, August 2. Retrieved 16 May 2014.

EHFAG (2012). 2012 European Strategy for Human Factors in Aviation. Cologne: EASA.

Embrey, D.E. 1986. SHERPA: a systematic human error reduction and prediction approach. Paper presented at the *International Topical Meeting on Advances in Human Factors in Nuclear Power Systems,* Knoxville: Tennessee.

Embrey, D.E., Humphreys, P., Rosa, E.A., Kirwan, B., & Rea, K. 1984. *SLIM-MAUD: An approach to assessing human error probabilities using structured expert-judgement*. USNRC Report NUREG/CR-3518. Washington, DC: USNRC.

Gibson, H. 2012. *Railway Action Reliability Assessment User Manual: A technique for the quantification of human error in the rail industry.* London: RSSB.

Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. 2005. *The SPAR-H Human Reliability Analysis method.* NUREG/CR-6883. Washington, DC: US Nuclear Regulatory Commission.

Gordon, R.P.E. 1998. The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering & System Safety* 61(1): 95–108.

Groth, K.M., & Mosleh, A. 2012. A data-informed PIF hierarchy for model-based Human Reliability Analysis. *Reliability Engineering and System Safety, 108*, 154–174.

Guldenmund, F.W. 2000. The nature of safety culture: A review of theory and research. *Safety Science*, 34(1): 215–257.

Gupta, J.P. 2002. The Bhopal gas tragedy: Could it have happened in a developed country? *Journal of Loss Prevention in the Process Industries*, 15: 1–4.

Hollnagel, E. 1998. Cognitive Reliability and Error Analysis Method. Oxford: Elsevier.

Hollnagel, E. and Amalberti, R. 2001. The Emporer's New Clothes, or whatever happened to "human error"? Keynote presentation at the *4th International Workshop on Human Error, Safety and System Development, Linköping, June 11–12, 2001.*

Hollnagel, E., Leonhardt, J., Licu, T., and Shorrock, S. 2013. *From Safety-I to Safety-II: A White Paper*. Brussels: Eurocontrol.

International Ergonomics Association. 2000. *What is Ergonomics?* Retrieved March 30, 2014 from www.iea.cc.

Kirwan, B. 1992. Human error identification in human reliability assessment. Part 2: Detailed comparison of techniques. *Applied Ergonomics*, 23(6): 371–381.

Kirwan, B. 1996. The validation of three human reliability quantification techniques, THERP, HEART and JHEDI: Part 1 technique descriptions and validation issues. *Applied Ergonomics,* 27(6): 359–373.

Kirwan, B. 2005. Human reliability assessment. In J.R. Wilson & N. Corlett (Eds) *Evaluation of Human Work*, 3rd edition: 833–875. Boca Raton, FL: CRC Press.

Kirwan, B. & Ainsworth, L.K. 1992. *A Guide to Task Analysis.* London: Taylor & Francis.

Konstantinos, K., Marinos, T., Byrne, P.., Ross, D., Cromie, S., & Corrigan, S., 2011. Investigating human factors in biotechnology and pharmaceutical manufacturing industries. *European, Mediterranean & Middle Eastern Conference on Information Systems 2011, May 30–31, Athens, Greece.*

Leveson, N.G. 2011. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

Reason, J.T. 1990. *Human Error.* Cambridge: Cambridge University Press.

Reason, J. 1997. *Managing the risks of organisational accidents.* Aldershot, UK: Ashgate.

Seaver, D.A. and Stillwell, W.G. 1983. Procedures for using expert judgement to estimate human error probabilities in nuclear power plant operations. NUREG/CR-2743. Washington, DC: USNRC.

Sheen, M.J. 1987. *MV Herald of Free Enterprise Report of Court No. 8074 Formal Investigation*. London: Department of Transport.

Shorrock, S.T. and Kirwan, B. 1998. TRACEr—a technique for the retrospective analysis of cognitive errors in Air Traffic Management. In D. Harris (Ed) *Engineering Psychology and Cognitive Ergonomics,* Vol. 3, pp. 163–171. Aldershot, UK: Ashgate.

Stanton, N.A., Salmon, P.M., Walker, G.H., Baber, C., & Jenkins, D.P. 2005. *Human Factors Methods: A Practical Guide to Engineering and Design.* Aldershot, UK: Ashgate.

Sorenson, J.N. 2002. Safety culture: A survey of the state-of-the-art. *Reliability Engineering and System Safety*, 76(2): 189–204.

Swain A.D. and Guttmann H.E. 1983. *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. NUREG/CR-1278. Washington, DC: US Nuclear Regulatory Commission.

Topham, G. 2013. 'Railway accidents happen because someone makes a mistake'. *The Guardian*, July 25. Retrieved 16 May 2014.

Zhang, H., Wiegmann, D.A., von Thaden, T.L., Sharma, G., & Mitchell, A.A. 2002. Safety Culture: A concept in chaos? Proceedings of the *46th Annual Meeting of the Human Factors and Ergonomics Society.* Santa Monica: Human Factors and Ergonomics Society.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Design methods of reducing human error in practice

M. Butlewski, M. Jasiulewicz-Kaczmarek, A. Misztal & M. Sławińska
Chair of Ergonomics and Quality Management, Poznan University of Technology, Poznań, Poland

ABSTRACT: Optimization of reliability in work systems and the often complex, technical objects contained within them, results in a large elimination of technical faults. But due to the significant role played by the human in causing damage, enforcing limitations to manage only the technical components of the system will not bring about the desired effect. Depending on the type of industry, the human factor is recognized as the cause of up to 80% of failures. This means that the human more or less directly contributes to a significant part of the failures. In order to reduce this problem there are many different methods and approaches that are used for obtaining the fallibility of the human—technical system operator at a sufficiently low level. The following article analyzes the construction methods for assessing and reducing human error and analyzes their scope of application, together with some practical examples. As a method to solve the problem, comparison of methods was done together with an analysis of their applicability and event models. As a result of the work it was found that in practical applications the best results in terms of reduction in the number of undesirable events were achieved with the application of selected methods. A comparison of the causes of undesired actions allowed to determine the most common problems for example: rule violations and mistakes, a lack of knowledge, and omission. The most common remedial measure for human error in the field of simple production situations was workers' awareness. The proposed method consists of the measurement of the relationship between symptoms, phase of the human error, and means of preventing that error under specified organizational and technical conditions.

1 INTRODUCTION

The issue of human error has for many years constituted the subject of scientific research and practical activities. In view of the improvement of production methods and a general increase in quality, naturally human error became the object of an even greater interest, since it has an impact in a greater degree than ever before on the efficiency of production systems and safety during use of machinery and equipment.

The research on the problem of human error can be differentiated based on the approach to the problem of error, and more specifically its elementary character. For researchers related to ergonomics, human error is in first order the result of a specific sequence of events and not the cause. This assumption allows on the one hand to disclose the diversity of the character of human error, while on the other hand allows for its increased elimination. Applying ergonomic design properly oriented to human error, one can obtain much more reliable anthropometric systems (Hankiewicz 2012).

2 SPECIFICS OF THE HUMAN ERROR PHENOMENON

Human error is a concept so well-known worldwide that it is often cited but not actually defined. It should be noted that this term is understood as an action that is not intended; not desired by a set of rules or an external observer; or that led the task or system outside its acceptable limits (Senders & Moray 1991). Human error is not connected with the accident, and thus the result, because it is independent (the same error in other circumstances may lead to different results) and can be simultaneously the result of other circumstances causing the error. However, very often it is considered from the point of view of an accident, due to the fact that it is only after the accident that an analysis is performed which reveals the existence of a specific human error. Another limitation of the category of human error is to specify that human error is understood as only such action, which was not purposely intended by the human (and therefore an action done in good faith, not a deliberate violation of the established rules) (Reason 1990).

For this reason, under the category of human error should fall activities such as: failure to perform an action, or a modified performance as a result of inattention, forgetfulness, or misunderstanding the instruction (Wrzesińska 2012).

Most common classification of types of human error is presented in Figure 1.

The classification presented in Figure 1 does not reveal, however, a number of specific causes of human error which have their source in a large part in psychological factors in decision-making (Więcek-Janka 2011) that will eventually take the form of the following causes:

– lack or inadequate procedure
– poor hazard identification
– poor or lack of training
– poor design and lack of ergonomic assessment
– overload, workload
– fatigue, lack of rest, stress at work
– vague or unclear roles and responsibilities
– different distortion

Human error is always one element in a whole sequence of events, the outcome of which determines whether it will be considered serious, and if it will ultimately be classified as an error on the part of the human.

Human error can occur at any of the three basic stages of the operator's work (receiving information, its processing and adequate performance—Fig. 2), and it can always be seen as a lack of balance between the demands of work and human capabilities in the specified function of time. This allows the conclusion that the prevention of human error can be associated with the appropriate control of the above-mentioned balance by adapting it to the level of the expected interference (Fig. 3).

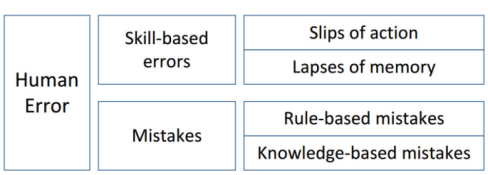


Figure 1. Human error classification (HSG48).

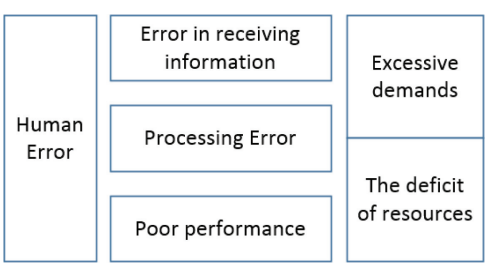


Figure 2. Human error root cause (own preparation).

The scheme of the formation of human error arising from external causes is presented (Fig. 3). Based on the presented scheme, one can conclude that reducing error can be achieved by reducing the impact of distractions from the material environment as well as the technical and organizational factors of distraction. Among the factors of the material environment can be mentioned such factors as noise, vibration, lighting, and microclimate. In contrast, technical and organizational distractions include factors such as the pace of work, organization, supervision, etc. The use of the cybernetic scheme human-technical object thus provides significant opportunities to reduce human error by identifying the different categories of distracters. Moreover, based on the presented model (Fig. 3) it can be seen that the last step (performance) is critical in the absence of security for unintentional action, because there are no following steps in which to correct the error. This also raises another solution for methods of reducing human error—reserving, which despite its costliness brings about the best results. Considering the chain of events would indicate the diverse possibility of solutions identifying the error in an specified phase. It would therefore be more indicative of determinants its creation and based on them determine its probability. The specified level of probability should activate further levels of precautions. Finally, it should also be noted that an important function in controlling the possibility of human error is the magnitude of the impact in the event of its occurrence, which is a stimulus whose effect depends again on the balance between individual ability and the strength of the stressor.

The next and very important group of factors includes the psychological basis of committing errors such as: long-term ability to comply with the rules, the perception of risk, resistance to stress, locus of control, and social patterns. At the macro-social level, determinants of psychological error will also be factors such as the ability

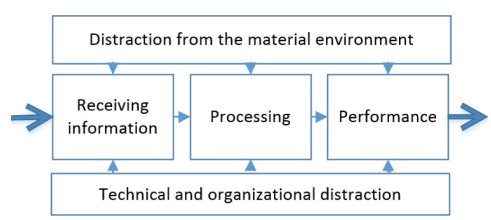


Figure 3. External human error scheme (based on Tytyk 2001).

to work in groups, taking on a specific role, and competitiveness.

To sum up, it should be noted that only some of the issues cited in the field of human error indicate the applicability of ergonomic models to know its character. Due to the limited capacity of this publication as well as the fairly extensive literature on this topic, and also the fairly obvious relationships between variables, the issue will not be considered to a greater extent when describing the practical methods of reducing human error, except for design proceedings targeted to human infallibility.

3 METHODS, FACTORS, AND INDICATORS OF PREDICTION OF HUMAN ERROR

Connected with the concept of human error are mainly those situations where there is a large responsibility for the committed error. This increased responsibility is particularly true in the case of operating work (operators of vehicles and machines) (Butlewski & Sławińska 2014). To the most commonly used in calculations indicators of reliability of the human-operator are included the following four quantitative indicators: infallibility, preparedness, restitution and timeliness. Indicator of infallibility is the probability of flawless operation of the operator, which can be determined with respect to the distinguished operation and the entire algorithm of actions. This ratio is expressed by the following formula (Sławińska 2011)

$$P_j = (N_j - n_j)/N_j, \tag{1}$$

where:

P_j—probability of flawless execution of operations;

N_j—total number of operations performed;

n_j—number of errors.

Indicator of preparedness of the operator is the probability that the operator will join operations at any time (Sławińska 2011).

$$K = 1 - (T_0/T), \tag{2}$$

where:

K—preparedness indicator;

T_0—operator's "time off," operator's absence in a given period at a given workstation;

T—total work time of the operator.

Indicator of restitution relates to the possibility of self-assessment by the operator and making adjustments in own actions. This indicator expresses the probability of correcting errors committed by the operator (Sławińska 2011).

$$P_{pop} = P_k \cdot P_{wyk} \cdot P_p, \tag{3}$$

where:

P_{pop}—probability the operator will act after the appearance of an error with the aim of correction;

P_k—probability of sending a signal from the control device;

P_p—probability of correcting erroneous operations during repeated performance of the task;

P_{wyk}—probability of correctly performing the task.

Indicator of timeliness (time adequacy of the operator's actions) is introduced due to the fact that actions that are correct but taken at the wrong time, do not lead to the goal. It expresses the probability of execution of the tasks in time (Sławińska 2011).

$$P_a = P\{\tau < t_1\} = \int_0^{t_1} f(\tau) d\tau \tag{4}$$

where:

P_a—probability of timeliness;

$f(\tau)$—function of time distribution of execution

t_1 constant value

In summary, human reliability indicators are based on the creation of a particular probability of leaving the operator and the factors which influence him/her in terms of a function of time. It can therefore be noted that for this reason they are based on the theory of homeostasis, which contains both the appropriate conditions and the appropriate resistance to interference.

4 DESIGN METHODS DIRECTED AT LIMITING HUMAN ERROR

The nature of the problem of human error caused a broad interest from scientists from different disciplines, which allowed the development of a range of methodological approaches. Here should be distinguished the trend of cognitive psychology which allows the identification of factors responsible for specific human activity (Fedota & Parasuraman 2010). In this framework, examined are the circumstances of making wrong decisions and the factors that encourage this, for which is used for example the Stroop test (Stroop 1935). These studies have a cognitive character and contribute to the development of guidelines for anthropotechnical systems that limit errors. Another group of methods of a cognitive character are methods of investigating both errors and failures (McBride et al. 2013). These methods are used to determine the causes of accidents in real operating conditions, after their occurrence. In turn, simulations are used to model the circumstances of human error

and to determine the scale of the consequences. All of these methods are the basis for the development of management methods to allow for the reduction of human error, from which a particular interest is put on ergonomic methods. They have a meta-method character, which form a combination of methods of action in terms of a number of factors. Due to the methodical difficulty of disconnecting them from the others they have been reported in the next chapter of this publication. It must therefore be noted that ergonomic predictors of human error lead to the conclusion that all efforts to improve the ergonomic quality of work lead to the reduction of exposure to man-made errors in the humanocentric system (Jasiulewicz-Kaczmarek 2009). This statement is, however, despite its accuracy unsuitable because of its excessive generality. It is therefore necessary to define that for ergonomic methods of reducing human error we will consider these approaches, which will be directed at reducing the vulnerability of the human-operator to make mistakes, by identification and limitation of the factor responsible to the greatest extent for the mistake.

More precise measures and calculations of ways to reduce human error arise when one points to five basic ways of reducing error (Kariuki & Lowe 2007):

- Training—48%
- Procedures—20%
- Supervision—13%
- Displays—13%
- Skills and knowledge—6%

Percentages given indicate the involvement of a particular method in preventing human errors.

However, there is concern that the prediction error of the method that is burdened with an error in the classification of the cause. Relative weights of factors affecting a human error event may also vary depending on the conditions in which the error is considered.

Human fallibility may be limited, but these are costly actions that must be justified as a specific economic result. These approaches can be divided into specialized, taking into account only the specific situation, and universal, which are methodologies that relatively quickly are used in the following areas of human functioning such as poka yoke, which as a design approach has been adapted to management activities (Pakdil et al. 2009). Methods of design are also developed that cause manufactured items to be more resistant to interference, including by limiting the human impact on the efficiency of the manufacturing system (Mrugalska 2013). Design methods can also be divided due to the site of action in the event of an error sequence. With the growth of computer technology there is a clear shift of techniques from the limiting of the effects of error to detection and limiting of the causes. An example of such an approach can be found in the automobile industry which after implementing systems limiting the effects of error (safety belts, airbags) began to increasingly develop driver anomalous behavior detection systems. Examples of such systems are: Driver Alert Control (DAC), which prevents drivers from falling asleep while driving, Lane Departure Warning (LDW) which oversees that the vehicle stays on an adequate track, and Collision Warning system, which consists of a set of radars registering the appearance of obstacles in the vehicle's path, warning of a possible collision, and in critical cases capable of activating the automobile's brakes (Menes 2011).

In the case of the more general situation, when there is no known mechanism of error, one should follow the procedure of specifying the circumstances of error and allowing to implement mitigation methodologies. We can mention here such methods as:

- HAZOP—human error hazard and operability study (Swann & Preston 1995)
- HEART—human error assessment and reduction technique (Kirwan 1996)
- HEIST—human error identification in systems tool (Kirwan 1994)
- HET—human error template (Stanton et al. 2006)
- HERCA—human error root cause analyses (Ławniczak et al. 2014)
- HRA—human reliability assessment
- THEA—technique for human error assessment early in design (Pocock et al. 2000)
- THERP—technique for human error rate prediction (Swain & Guttmann 1983)
- SHERPA—systematic human error reduction and prediction (Baber & Stanton 1996)

Many methods of reducing human error are also based on the determination of whether human error actually occurred. Therefore, among these methods are included fault tree analysis and MORT event analysis.

An analysis of methods allows one to focus the method of action to the following activities (modules):

- human error identification (determination of what can go wrong?, taxonomy of errors)
- human error quantification (an estimate of how often a human error will occur?)
- human error or its impact reduction (determination of how human error can be pre-vented from reoccurring or its impact on the system be reduced?).

Many methods are an improvement over the previous ones taking into account certain factors or extending the scope of the analyzed reality. For this reason, the use of only one method does not allow for a complete picture, and the selection of methods should be preceded by an in-depth analysis.

5 CASE STUDIES—SOME PRACTICAL EXAMPLES

As a basis for the analysis of human error, utilized are illustrative examples of accidents at work, in which the direct or indirect cause was human error. The cause was adopted from the findings of the post-accident teams which determine the cause of the accidents. As part of the identification of the causes of human error, used were SHERPA and HERCA classification methods.

As the examples show, every human error is the result of at least several factors, the combination of which results in an adverse effect. All cases point to an additional factor—failure to follow instructions and the accepted principles of operation.

On the basis of event analysis using a variety of methods it is indicated that the classification offered by them can be used for both analytical and design goals. Although one can point to direct evidence for errors in design when looking at the operator's error, a significant part of the responsibility is on the side of the operator, his/her training and the attitude to compliance with the rules.

Human error is therefore not the reason, but the effect of specific circumstances under which is an user. Still the deficit of specified human resources is a factor of the error. This deficit can be attention, ability to make decisions under stress or performance, regardless of the degree to assess whether he was the reason the chain of events.

The use of different methods for the study of human error, not used for the purpose of design, can bring a benefit in the form of a greater visibility of the range of possible preventive measures. Still, a big problem are situations arising from multiple causes, especially in non-standard cases—such as emergencies (Bajda et al. 2011), which are the biggest source of accidents caused by human error.

In the presence of insufficient resources describing human error, it seems advisable to apply a combination of factors not only describing the categories of human error but also the way of its limitation (Fig. 4). Such an approach would allow for the development of groups of symptoms that would describe the probability of the occurrence of a specific human error. The model structure allows to determine the strength with which a particular factor affects the other categories (spatial arrangement of cube), at the same time not pointing at single factor dependencies, which in reality de facto do not exist. Identification of human error in the proposed system could be based on the estimation of the relationship between deficits in the field of cube walls in combination with deficits of the environment—the ambient of the cube. This combination may in the future allow the prediction of human errors before they occur.

Table 1. Human error causes comparison (own elaboration on the basis of www.poznan.oip.pl).

No.	Cause according to national labor inspectorate	SHERPA behavior taxonomy	HERCA cause
1	Improper work methods applied by the victim, involving the improper hand position during machining of the object, at the level of the knife shaft, and omitting checking the device	Action: omitted	Forgetfulness and inattention
2	Operator used the wrong equipment for the particular part of the depot	Action: right action, wrong object	Attitude and behavior
3	Operator was not careful while driving under the roof of the depot with a raised load	Action: omitted	Behavior: error caused by lack of attention
4	Improper application of equipment, lack of coordination	Action: wrong action, right object	Forgetfulness and inattention

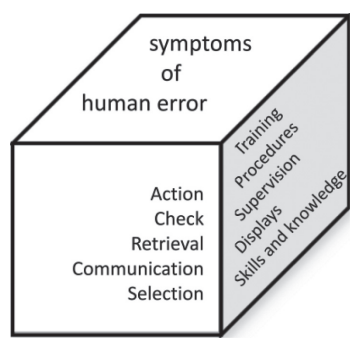


Figure 4. Human error cube.

6 CONCLUSION

Design with an increased resistance to human error will increasingly translate to the success of manufacturing complicated technical objects. It is enough to imagine a car incapable of having an accident or a completely safe machine. Achieving this goal requires a transition to the next level ergonomic quality, which will have a dynamic character and be responsive to the currently existing methods of prevention and thus static methods. Dynamic methods allow for the anticipation of an error made by a human, which will allow avoiding the substantial consequences in accordance with the principle that prevention is better than treatment.

REFERENCES

Baber, C. and Stanton, N.A. 1996. Human error identification techniques applied to public technology: predictions compared with observed use, Appl. Ergonomics, 27, 119–131.

Bajda A., Wrażeń M. Laskowski D. 2011. Diagnostics the quality of data transfer in the management of crisis situation, Electrical Review 87(9A), pp. 72–78, Sigma-Not, Poland.

Butlewski, M., Sławińska, M.,. 2014. Ergonomic method for the implementation of occupational safety systems, Occupational Safety and Hygiene II—Selected Extended and Revised Contributions from the International Symposium Occupational Safety and Hygiene, SHO 2014, pp. 621–626.

Fedota J. & Parasuraman R. 2010. Neuroergonomics and human error, Theoretical Issues in Ergonomics Science, 11:5, 402421.

Hankiewicz K. 2012. Ergonomic Characteristic of Software for Enterprise Management Systems, in: P.Vink (ed.), Advances in Social and Organizational Factors, CRS Press, Boca Raton, pp. 279–287, ISBN: 9781439870198 http://www.poznan.oip.pl/ accesed 20140221.

Jasiulewicz-Kaczmarek M. 2009. Participatory Ergonomics as a Method of Quality Improvement in Maintenance B.T. Karsh (Ed.): Ergonomics and Health Aspects, HCII 2009, SpringerVerlag Berlin Heidelberg, LNCS 5624, pp. 153–161.

Kariuki S.G., Lowe K. 2007. Integrating human factors into process hazard analysis, Reliability Engineering and System Safety, 92(16):1764–1773.

Kirwan, B. 1994. A guide to practical human reliability assessment, Taylor and Francis.

Kirwan, B. 1996. The validation of three human reliability quantification techniques THERP, HEART, JHEDI: Part I technique descriptions and validation issues. Applied Ergonomics. 27(6) 35937.

Ławniczak I., Iwanowicz A., Mazurek P., Butlewski M. 2014. Praktyczne Zastosowanie Metody Herca W Zarządzaniu Wiedzą O Przyczynach Wypadków Przy Pracy (In Press).

McBride S., Rogers W., Fisk A.D. 2013. Understanding human management of automation errors, Theoretical Issues in Ergonomics Science, DOI: 10.1080/1463922X.2013.817625.

Menes M. 2011. Współczesne kierunki rozwoju techniki samochodowej, Transport Samochodowy, nr 4, s.1936.

Mrugalska, B. 2013. Environmental Disturbances in Robust Machinery Design In: Arezes, P. et al. (eds.) Occupational Safety and Hygiene. pp. 229–233. Taylor and Francis Group, London.

Pakdil F., Özkök O., Dengiz B., Kara I., Selvi N. Kargı A. 2009. A systematic approach to reduce human and systemrelated errors causing customer dissatisfaction in a production environment, Total Quality Management & Business Excellence, 20:1, 129137, DOI: 10.1080/14783360802351728.

Pocock, S., P. Wright, and M. Harrison. 2000. THEA—a technique for human error assessment early in design. InRTO-NATO (HFM) Working Group 30. http://www.cs.york.ac.uk/˜stevep/.

Reason J. 1990. Human error. New York: Cambridge University Press.

Reducing error and influencing behaviour. 1999. ISBN: 9780717624522; Series code: HSG48.

Senders, J.W., Moray, N.P. 1991. Human Error: Cause, Prediction, and Reduction. Lawrence Erlbaum Associates, p.25. ISBN 0898595983.

Sławińska M., 2011, Reengineering ergonomiczny procesów eksploatacji zautomatyzowanych urządzeń technologicznych (ZUT), Wydawnictwo Politechniki Poznańskiej, Poznań.

Stanton N., Harris D., Salmon P., Demagalski J., Marshall A., Young M., Dekker S., Waldmann T. 2006. Predicting design induced pilot error using HET (human error template) A new formal human error identification method for flight decks, Royal Aeronautical Society, 2006/2/1.

Stroop, J.R. 1935. Studies of interference in serial verbal reactions. Journal of Experimental Psychology, 18, 643–662.

Swain A., Guttmann H. 1983. NUREG/CR 1278. SAND800200. RX, AN. Handbook of Human Reliability Analysis with Emphasis on. Nuclear Power Plant Applications.

Swann, C.D., Preston, M.L. 1995. Twenty five years of HAZOPs. J loss prevention in the Process Industries. 1995, 8, pp. 349353.

Tytyk E. 2001. Projektowanie ergonomiczne. Wyd. Naukowe PWN, Warszawa-Poznań.

Więcek-Janka E. 2011. Decisions and games, wydawnictwo Politechniki Poznańskiej, Poznan.

Wrzesińska J. 2012. Czynnik ludzki jako determinanta występowania wypadków przy pracy w: Bezpieczeństwo zdrowia publicznego w zagrożeniach środowiskowych. Postępy metodologii badań, pod red.: Konieczny J., Garmond Oficyna Wydawnicza, Poznań.

Maintenance modelling and optimisation

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A hierarchical framework for the measurement of maintenance efficacy and efficiency using performance indicators

G.M. Galante, R. Inghilleri & C.M. La Fata
Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica (DICGIM), Università degli Studi di Palermo, Palermo, Italy

ABSTRACT: Maintenance plays an important role in achieving the organizational goals so that the measurement of its effectiveness and efficiency has become an essential element of industrial strategy. In literature several Maintenance Key Performance Indicators (MKPIs) are proposed but none structured approach is suggested to select the best set of MKPIs able to synthetically describe a specific maintenance context. The paper proposes a structured methodology for the maintenance performance measurement by means of MKPIs. Firstly, a multi-level hierarchical framework able to synthesize the most meaningful perspectives affecting the performance of the maintenance process is designed. Successively, some MKPIs proposed in the literature are assigned to the hierarchical framework and ranked by an Analytic Hierarchy Process-based approach. A procedure to deal with incomplete and inconsistent pair-wise comparison matrices is proposed. Finally, a mathematical model is formulated to select the set of MKPIs representing the best compromise between the completeness and the conciseness of the returned information.

1 INTRODUCTION

Nowadays, maintenance is more and more considered as an important support function in business with significant investments in physical assets and plays an important role in achieving the organizational goals (Tsang 2002). As a consequence, the measurement of the maintenance performance has become an essential element of strategic thinking of asset owners and managers to be utilized for identifying business processes, areas and departments that need to be improved to achieve the organizational goals (Parida 2006). Over the last two decades, a large number of performance measurement frameworks has been suggested as regards the evaluation of the overall organizational performance. To the contrary, the area of maintenance performance and management is still in need of more future systematic research efforts (Simões et al. 2011). Nowadays, literature on Maintenance Performance Measurement (MPM) models and Maintenance Key Performance Indicators (MKPIs) principally lacks on two aspects. Firstly, proposed MPM frameworks are generic, without considering the business specific environment of the company where these tools should be applied in. Secondly, the available literature mainly proposes a huge list of MKPIs but lacks an agreed-upon methodological approach for selecting specific MKPIs from the listed indicators. With this recognition, the present paper aims at proposing a structured methodology for the maintenance performance measurement by means of a restricted and comprehensive list of MKPIs. The organizational context which the present paper is focused on is that of a high risk process plant where the way maintenance is managed and performed is fundamental to prevent the occurrence of hazardous events. The whole methodology has been designed and implemented in cooperation with the maintenance staff of a refinery plant in order to allow to the maintenance manager to measure, check and communicate the maintenance process performance on the base of different perspectives. The methodology consists of several steps. Firstly, a *customized hierarchical framework* capable of synthesizing the most meaningful aspects affecting the effectiveness and the efficiency of the maintenance process is designed. The stakeholder of the hierarchical framework is the company's maintenance manager that needs to communicate the maintenance process results to both the top management and the maintenance technicians. As a consequence, the hierarchical framework is thought in such a way to incorporate all those perspectives that the maintenance manager deems to be fundamental in order to *vertically* communicate and eventually improve the maintenance performance. It consists of multiple levels so that information returned by each level provide a greater detail on a particular aspect of the immediately higher one. Successively, MKPIs already proposed in the technical and scientific literature are

collected in order to obtain a comprehensive list of MKPIs. Among them, indicators deemed to be the most appropriate to describe the specific maintenance process are selected and then assigned to the hierarchical framework. Then, an Analytic Hierarchy Process (AHP)-based approach (Saaty 1994) is proposed to rank the assigned MKPIs. In particular, the decision maker is asked to supply just pair-wise comparison judgments on which he/she is confident. Namely, incomplete pair-wise comparison matrices could be supplied and then need to be opportunely handled. Finally, a mathematical programming model is formulated and solved in order to select the *optimal set* of MKPIs by means of which measuring the maintenance performance. Actually, managing a large number of MKPIs can be counterproductive in terms of lack of conciseness of the returned information. In addition, calculating a large number of MKPIs requires a considerable effort in terms of input data to be recorded. As a consequence, MKPIs to be used need to be carefully selected among those assigned so that if on the one hand they synthesize the needed information in the best possible way, on the other hand their number is not too large.

The paper is organized as follows. The literature review is supplied in Section 2. The whole methodology is synthesized in Section 3, the classical AHP method is presented in Section 4, whereas its application to the maintenance performance measurement problem is detailed in Section 5. The mathematical model is reported in Section 6. A case study is reported in Section 7 and conclusions finally drawn in Section 8.

2 LITERATURE REVIEW

The most widely used business performance model is the Balanced SCorecard (BSC) of Kaplan & Norton (1996). The classical BSC model has been also used for the maintenance performance measurement (Visser & Pretorius 2003) but the feasibility of its application for managing the performance of a specific function, as maintenance, is still an uncharted area which needs researching (Tsang et al. 1999). In fact, the classical BSC model is not able to capture all facets of the maintenance function because of the several interrelationships between the maintenance and the other organizational functions. As a consequence, several contributions have been proposed aiming at adapting the BSC to the maintenance performance measurement problem (Mather 2005, Alsyouf 2006, Bakhtiar et al. 2009, Wireman 1998). Nevertheless, to the authors opinion the BSC model is not easily understandable by the maintenance staff. Furthermore, each organization is unique in its structure, function and business position so that a performance measurement framework may be suitable for one organization and may not be suitable for another one. With this recognition, a maintenance performance measurement model should be focused on the specific organizational context so that critical (key) factors influencing the overall maintenance effectiveness and efficiency are identified.

The common way of measuring the performance of key factors is that of making use of indicators. As regards the maintenance function, numerous MKPIs have been already defined in the scientific and technical literature principally with relation to the manufacturing sector (EN:15341 2007). In addition, several contributions have been proposed over the last few years as regards the problem of ranking *a priori* defined set of KPIs in order to evaluate the overall organizational performance (Wua et al. 2009). To the contrary, few contributions exist with relation to the ranking of MKPIs. Amodeo (2005) starts from the BSC concept to define the fundamental aspects (pillars) upon which the overall maintenance operation rests. From these basic pillars, a hierarchical decomposition is proposed in order to arrive to the lowest measurable function, whereby obtaining the fundamental attributes to be used to manage the general goal. A conceptual framework that provides a guideline for choosing maintenance performance indicators is developed by Muchiri et al. (2011). Authors emphasize that further research work is recommended on the methodological approach of choosing the right MKPIs among the given indicators listed in literature. Van Horenbeek & Pintelon (2014) develop a generic hierarchical framework which is based on the corporate and maintenance strategy and incorporates all organizational levels (i.e. strategic, tactical and operational). Then, authors suggest an ANP-based method to customize the proposed framework.

3 PROPOSED METHODOLOGY

A structured methodology for the measurement of the maintenance process performance by means of a restricted number of MKPIs is here proposed. It comprises the following steps:

1. Definition of a *customized* hierarchical framework able to synthesize all those aspects that affect the maintenance performance of the specific organization.
2. Collection of MKPIs already proposed in the scientific and technical literature.
3. Selection of MKPIs deemed to be the most appropriate to be used in the specific organizational context.

4. Assignment of selected MKPIs to each aspect of the hierarchical framework.
5. Application of the AHP-based approach to rank the assigned MKPIs.
6. Formulation of a mathematical programming model to identify the optimal set of MKPIs among those assigned that represents the best compromise between the conciseness and the completeness of the returned information.

3.1 *Definition of the customized hierarchical framework*

The hereafter presented hierarchical framework (Fig. 1) takes into account the way maintenance process is performed within the organization and has been designed in cooperation with the subject company maintenance staff. It comprises more levels and *nodes*. Each node represents a particular aspect on the base of which measuring the maintenance performance and, whenever deemed to be necessary, it is further branched in order to detail the considered aspect. In such a way, the highest level nodes are representative of more generic aspects of maintenance and return information potentially of interest to the company's top management. To the contrary, the lower level nodes are more detailed and specific so that returned information are mainly addressed to maintenance technicians. The proposed hierarchical framework is explained in the following.

The first level (i.e. the level zero) represents the goal, namely the *measurement of the maintenance process performance*. The next level (i.e. the level 1) comprises all those aspects deemed to be critical in terms of their influence on maintenance effectiveness and efficiency. Particularly, the following five aspects are considered at the first level of the hierarchical framework:

1. Technical (node 1). It aims at highlighting the influence on plant reliability and availability of *how* maintenance actions are performed within the organization.
2. Economical (node 2). It aims at giving evidence to the economical aspects of maintenance (maintenance efficiency), from the budgeting to the expenditure phase.
3. Organizational (node 3). It regards the way maintenance activities are planned, scheduled and carried out. In addition, it includes all those issues related to the management and training of maintenance personnel.
4. Health, Safety and Environment (HSE) (node 4). It highlights the impact of maintenance actions on the health and safety of inner and outer maintenance personnel, as well as on the environment.
5. Warehousing (node 5). It aims at describing the efficacy and the efficiency of the maintenance spare parts management.

Successively, each one of the level-1 nodes is further branched in order to detail the expected information. Referring to the Technical node (node 1), it is branched into the Reliability (node 1.1) and the Availability (node 1.2) nodes. Actually, reliability and availability are two different and common measures relating to the maintenance process effectiveness. The node Availability (node 1.2) is further branched into the nodes Corrective Maintenance (node 1.2.1), Preventive Maintenance (node 1.2.2) and General (node 1.2.3). Namely, the attention is firstly focused on the two main maintenance policies performed in the plant in order to detail how the way they are carried out affects the plant's availability. The General node aims at including the measures describing general aspects that do not regard a particular maintenance policy. The Economical node (node 2) is branched into the Corrective Maintenance (node 2.1), Preventive Maintenance (node 2.2) and General (node 2.3) nodes. Nodes 2.1 and 2.2 aim at focusing the attention on the efficiency of corrective and preventive maintenance actions, whereas the node 2.3 returns information on the whole maintenance process efficiency disregarding the type of maintenance policy. The Organizational node (node 3) firstly includes an aspect (node 3.1) related to the maintenance actions planning, scheduling and execution in order to highlight if maintenance work is opportunely planned, scheduled and carried out on-time.

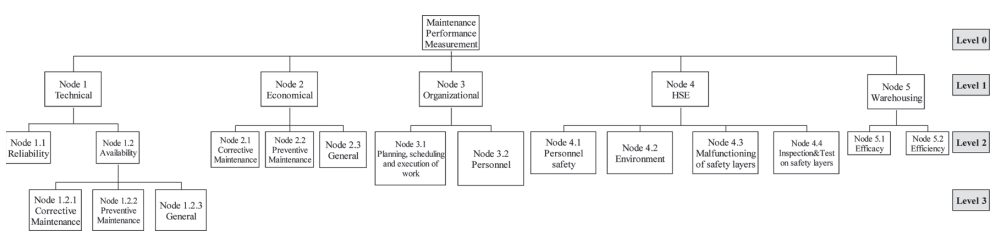


Figure 1. Hierarchical framework.

Secondly, the node Personnel (node 3.2) relates to *what* the organization makes for the maintenance personnel improvement by the training activities. The HSE node (node 4) involves an aspect related to the safety of inner and outer maintenance personnel (node 4.1), and a further node (node 4.2) that focuses the attention on the environmental impact of the maintenance process. In addition, taking into account the particular organizational context, two further aspects are detailed. The first one (node 4.3) concerns the failure due to a wrong maintenance on safety barriers installed to prevent the occurrence of hazardous situations or to mitigate the related consequences. The second one (node 4.4) aims at highlighting the correct execution of inspection activities on such safety barriers. Finally, the node Warehousing (node 5) concerns the management of maintenance spare parts both on the effectiveness and efficiency point of view.

3.2 *Maintenance Key Performance Indicators (MKPIs) collection and assignment*

A specific function as the maintenance one requires specific indicators to measure its performance. Scientific and technical contributions propose a huge number of MKPIs, even if the main part of them relates to manufacturing industries. Aiming at measuring the influence of each specific aspect of the designed hierarchical framework on the whole maintenance process performance, MKPIs already proposed in the literature have been collected and analyzed in cooperation with the subject company maintenance staff. Therefore, the significance of each MKPI has been evaluated in terms of its applicability to the particular organizational context as well as in terms of its easiness of comprehension and importance to describe a specific aspect. Among those collected, just those indicators deemed to be useful to describe the maintenance process have been selected and then opportunely assigned by a top-down procedure. A total number of 116 MKPIs has been collected from the existing literature. Among them, 58 MKPIs have been selected and assigned to the lowest level nodes of the hierarchical framework. The next step of the designed methodology consists in ranking such MKPIs on the basis of their capability in measuring the maintenance process performance. The AHP-based approach here proposed is detailed in Section 5, whereas the classical AHP method is synthesized in the following Section 4.

4 ANALYTIC HIERARCHY PROCESS (AHP)

Proposed by Saaty in the late of 70's, the AHP is a multi-criteria decision making method that supports the decision maker in the evaluation and selection of alternatives through the use of pair-wise comparison judgments. It comprises the following five steps:

1. Problem decomposition. It comprises the individuation of the goal (i.e. the decisional problem to be solved), of the criteria/sub-criteria on the base of which evaluating alternatives, and of the alternatives to be ranked in respect to the goal, eventually to select the best one.
2. Expression of pair-wise comparison judgments with relation to each pair of elements belonging to the same hierarchical level in respect to the immediately higher element. Evaluations are expressed through the use of appropriate semantic scales. The most used one is that proposed by Saaty (2008).
3. If n is the number of items (criteria, sub-criteria or alternatives) to be compared with relation to a specific element of the immediately higher level, the total number of judgments required to the decision maker is $[n \cdot (n - 1)/2]$. Each pair-wise comparison judgment constitutes the element a_{ij} of the so-called reciprocal pair-wise comparisons matrix.
4. Local priorities computation. The local priority (or relative importance) that each element of the hierarchical structure takes in respect to the immediately higher level is calculated by one of the techniques proposed in the literature. Among them, the most used one is the eigenvector method (Saaty 1977).
5. Consistency evaluation. As stated by Saaty, local priorities make sense only if arising from consistent or near consistent matrices. As a consequence, a consistency check on opinions expressed by the decision maker needs to be performed. Saaty proposed a Consistency Index (CI) calculated as follows (1):

$$\mathrm{CI} = \frac{\lambda_{max} - n}{n - 1} \tag{1}$$

where n is the size of the pair-wise comparison matrix and λ_{max} is the corresponding maximum eigenvalue. Then, the Consistency Ratio (CR) is given by the following expression (2):

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{2}$$

where RI is the random index calculated by Saaty (Saaty 1977) as the mean value of the CIs of 500 randomly filled matrices of the same size. If CR is less than 0.1, then the matrix can be considered as acceptably inconsistent. Otherwise, the decision maker is commonly asked to provide

again his/her own judgments until an acceptably inconsistent pair-wise matrix is obtained.
6. Global priority computation. It consists in synthesizing the local priorities across all criteria and sub-criteria in order to determine the global priority of alternatives in respect to the goal. The most used method is the distributive mode that is an additive aggregation with normalization of the sum of local priorities to the unity. Alternatively, the ideal method (Belton & Gear 1983) normalizes by dividing the score of each alternative by the score of the best alternative under each criteria.

5 AHP-BASED APPROACH TO RANK MKPIS

5.1 *Gathering pair-wise comparison judgments from the decision maker*

An AHP-based approach is here proposed to derive the weights of MKPIs assigned to nodes of the hierarchical framework. With relation to the specific organizational context, the decisional problem is the maintenance performance measurement (goal) that is hierarchically structured as previously described in Section 3.1. Alternatives to be evaluated and ranked are the assigned MKPIs. Commonly, the AHP hierarchical structure includes criteria and sub-criteria on the base of which ranking the available alternatives. Instead, the here proposed hierarchical framework comprises those perspectives on the base of which evaluating the maintenance process performance. The AHP can be used to determine their relative importance in respect to the immediately above hierarchical level. For instance, let suppose to compare the Technical aspect (i.e. Node 1) with the Economical one (i.e. Node 2) in respect to the immediately higher level, namely the goal. Then, expressing a pair-wise comparison judgment means answering the question "*how much more or less important the Technical aspect is than the Economical one of the same level in measuring the maintenance performance?*". It is obvious that such a relative importance strictly depends on stakeholders whom the information is addressed to.

In the classical AHP method, alternatives are pair-wise compared on the base of the selected criteria/sub-criteria. Generally, all alternatives can be evaluated on all criteria/sub-criteria. Referring to the specific application, alternatives to be compared are the MKPIs assigned to a specific aspect. Then, for each aspect, the assigned alternatives are pair-wise compared on the basis of their description capability. For instance, let KPI_1 and KPI_2 are two indicators assigned to a generic node not branched. Then, expressing a pair-wise comparison between the KPI_1 and the KPI_2 means answering the question "*how much do you believe the* KPI_1 *better or worst describes the aspect represented in the considered node than the* KPI_2?". However, the decision maker might not have a strong opinion on a comparison judgment so that he/she is not able to express any evaluation. That is particularly true with relation to pair-wise comparison judgments concerning the MKPIs because of a real difficulty of the decision maker to fully appreciate the different description capability. In such a situation, one could alternatively proceed as follows:

1. Forcing the decision maker to express all pair-wise comparisons required by the AHP method.
2. Allowing the decision maker to express only pair-wise comparisons on which he/she is confident and eventually force him/her so that judgments span all elements of the pair-wise comparison matrix.

To the author's opinion, referring to pair-wise comparison judgments among MKPIs, the best way to proceed in the light of the previous considerations is that described at point 2, namely allowing the decision maker to provide from $(n–1)$ to $[n\cdot(n–1)/2]$ judgments that span all elements of the pair-wise comparison matrix. Each evaluation represents the relative capability of MKPIs in describing the aspect they belong to. Whether a pair-wise comparison matrix includes less than $[n\cdot(n–1)/2]$ comparison judgments as here allowed, such a kind of matrix is commonly defined *incomplete*. As a consequence, missing judgments need to be determined in order to continue with the application of the classical steps of the AHP. Several approaches have been proposed in the literature to deal with incomplete pair-wise comparison matrices (Fedrizzi & Giove 2007, Gomez-Ruiz et al. 2010). Such methods determine the missing values so that the matrix inconsistency is minimized. Among them, the most mentioned and applied completion method is the Revised Geometric Mean of Harker (1987) synthesized in the following Section 5.2. As regards the pair-wise comparisons of the aspects needed by the classical AHP for the computation of their relative weights, one believes that the problem of the matrix incompleteness cannot occur. As a consequence, pair-wise comparison matrices concerning the relative importance of each aspect of level i in respect to the aspect of level $(i–1)$ are here assumed to be complete.

5.2 *Revised Geometric Mean (RGM) method*

Let assume the decision maker provides an incomplete pair-wise comparison matrix $\boldsymbol{C}$, which the generic element is c_{ij}. Then, Harker states that

computing the principal eigenvector $\boldsymbol{W}$ of the matrix $\boldsymbol{C}$ coincides with solving the same problem with relation to the quasi-reciprocal matrix $\boldsymbol{A}$ which elements a_{ij} are obtained as follows:

- $a_{ij} = 0$ if c_{ij} is a missing judgment, with $i \neq j$;
- $a_{ij} = c_{ij}$ if c_{ij} is not a missing judgment, with $i \neq j$;
- $a_{ij} = 1 + m_i$ if $i = j$;

where m_i is the number of missing judgments in the row i of the incomplete matrix $\boldsymbol{C}$. Namely, $\boldsymbol{C}$ and $\boldsymbol{A}$ have the same eigenvector $\boldsymbol{W}$, and the relation $\boldsymbol{A} \cdot \boldsymbol{W} = \boldsymbol{C} \cdot \boldsymbol{W}$ holds. Therefore, once decision maker pair-wise comparisons have been collected, all incomplete matrices are here completed by the Harker's method. Then, the methodology continues with the measurement of the inconsistency of all complete (or completed by Harker) matrices, namely the classical consistency check described in Section 4 needs to be performed. Therefore:

1. if the checked matrix is acceptably inconsistent, then local priorities of aspects and MKPIs can be calculated by means of the eigenvector method.
2. if the checked matrix is unacceptably inconsistent, then such an inconsistency needs to be reduced. The common way to proceed is to ask the decision maker to supply again his/her judgments and recalculate the CR of the new pair-wise comparison matrix. The procedure is reiterated aiming at reaching an acceptable consistency. Alternatively, different methods have been proposed in literature to reduce matrices inconsistency. The procedure here used is detailed in the following Section.

5.3 *Consistency improvement of complete matrices*

Several techniques have been proposed in literature to improve the matrix consistency (Obata et al. 1999, Hu et al. 2006). They firstly identify the comparison judgment that results in a greater inconsistency and then suggest a value to replace it. When changes are made, the CR is calculated again and the process is repeated until an acceptable CR is obtained. The method here used to improve the pair-wise comparison matrix consistency is that suggested by Saaty (2003). It uses the following relationship:

$$n \cdot \lambda_{max} - n = \sum_{\substack{i,j=1 \\ i \neq j}}^{n} (\varepsilon_{ij} + \varepsilon_{ij}^{-1}) \tag{3}$$

where λ_{max} is the maximum eigenvalue of the matrix $\boldsymbol{A} = [a_{ij}]$, and ε_{ij} is a generic element of the matrix $\boldsymbol{E}$ determined by the Hadamard product $\boldsymbol{A} = \boldsymbol{W} \cdot \boldsymbol{E}$, being $\boldsymbol{W} = [w_i/w_j]$ the vector of local priorities of the unacceptable inconsistent matrix $\boldsymbol{A}$. Therefore, the matrix $\boldsymbol{E} = [\varepsilon_{ij}]$ is obtained as $\boldsymbol{E} = \boldsymbol{W}^{-1} \cdot \boldsymbol{A}$. The ε_{ij} farthest from one implies the greatest inconsistency arising from a_{ij}. Then, the corresponding a_{ij} and a_{ji} are deleted from the matrix $\boldsymbol{A}$ that is completed by the Harker method. The new eigenvector is calculated and the previous a_{ij} is replaced by the Saaty scale value nearest to the w_i/w_j obtained by the new eigenvector.

If the decision maker has not been able to express all judgments, the procedure here proposed preliminary utilizes the Harker method to complete the pair-wise comparison matrix. Then, aiming at reducing the matrix inconsistency if necessary, the aforementioned ε-method to identify the most inconsistent judgment is employed. In order to replace it, the decision maker is one more time involved to reformulate such a judgment provided that it was originally supplied by the decision maker. To the contrary, namely the judgment found to be the most inconsistent one has not been previously expressed by the decision maker, then it arises from the application of the Harker method. Therefore, at the first iteration of the procedure, it cannot be the most inconsistent one. Instead, during next iterations, even a judgment obtained by Harker could be the most inconsistent one. In such a case, it is erased and the Harker's method applied again. The same procedure is used when the most inconsistent judgment coincides with one of those already reformulated by the decision maker. The described methodology is iterated until an acceptable matrix inconsistency is reached. Summing up, the proposed procedure tries to reduce the matrix inconsistency by involving again the decision maker just on that judgment that he/she was previously able to express if it results to be the most inconsistent one. However, even if reformulated, such a judgment could successively result to be the most inconsistent so that it could be erased. The flow-chart of the whole methodology is synthesized in Figure 2.

Once all pair-wise comparison matrices related to aspects and MKPIs are acceptably inconsistent, the final local priority vectors are obtained. The final step of the AHP-based approach is the computation of the MKPIs global priority vector in respect to the goal. The ideal method mentioned in Section 4 is here applied. The ideal mode is preferred to the distributive one because it avoids that the best MKPI belonging to a more numerous group is disadvantaged in respect to that assigned to a smaller group. Actually, referring to a generic node of the hierarchical framework, using the distributive mode leads to divide the corresponding weight to MKPIs assigned to it. Therefore, the more the number of assigned MKPIs is, the smaller the local

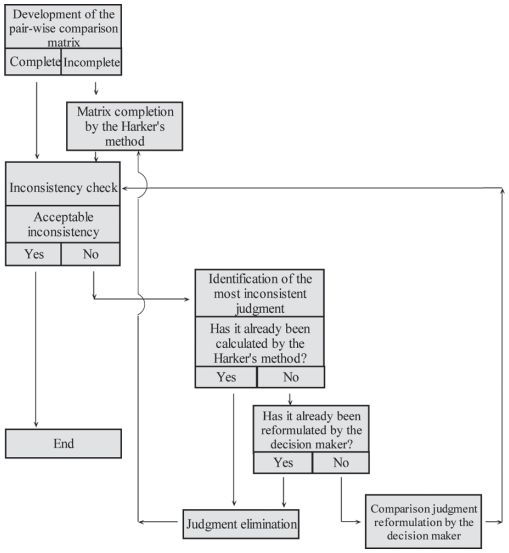


Figure 2. Iterative procedure for the improvement of the pair-wise comparison matrix inconsistency.

priority of each MKPI becomes. However, applying the ideal method leads to global priorities that do not sum to one. As a consequence, if deemed to be necessary, one can renormalize by using a normalization method among them already proposed in the literature.

6 MATHEMATICAL PROGRAMMING MODEL

Once global priorities of MKPIs in respect to the goal are calculated, the problem of choosing the optimal set of MKPIs still holds. Actually, calculating and monitoring over the time more and more MKPIs could result time-consuming in computational terms and amount of input data to be recorded. As a consequence, the optimal set of MKPIs needs to be selected among all those previously assigned to the hierarchical framework and ranked by the AHP-based method. Such a set is asked to be the best compromise between the information completeness and its conciseness. To this purpose, a mathematical model is formulated. The used nomenclature is reported below:

- i generic indicator of the list of MKPIs, with $i = 1, \ldots, N$.
- j generic node of the level 1 of the hierarchical framework, with $j = 1, \ldots, M$.
- g_i global priority of MKPI i arising from the application of AHP-based method.
- p_j local priority of the node j belonging to the level 1 of the hierarchical framework and calculated by the AHP.
- n_{min} minimum number of MKPIs to be selected for each node of level 1.
- α_{ij} numerical value that takes 1 if the MKPI i belongs to the node j, 0 otherwise.
- x_i Boolean variable that takes 1 if the MKPI i is selected, 0 otherwise.

The problem is formulated as follows.

$$max\ F(x) = max\left[k_1 \sum_{i=1}^{N} x_i \cdot g_i - k_2 \frac{\sum_{i=1}^{N} x_i}{N} \right] \tag{4}$$

Subject to:

$$(1 - p_j) \cdot \sum_{i=1}^{N} x_i \cdot \alpha_{ij} \geq n_{min} \qquad \forall j \tag{5}$$

$$k_1 + k_2 = 1 \tag{6}$$

The first term of the expression (4) aims at choosing those MKPIs having the highest global priority (i.e. a greater capability of description), whereas the second term represents the number of indicators to be selected. Both terms of the objective function range from 0 to 1. The parameters k_1 and k_2 are the weights representing the relative importance that the analyst attributes to each term of the objective function. Constraint (5) forces the model to choose at least a fixed number of MKPIs with relation to each level-1 node.

7 CASE STUDY

The proposed methodology has been implemented on a refinery plant. The subject company maintenance staff has been actively involved for the customization of the maintenance hierarchical framework, for the selection of the most meaningful MKPIs among those already proposed in the literature and for the expression of pair-wise comparison judgments needed by the designed methodology. Specifically, a total number of 116 MKPIs has been collected from the scientific and technical literature and supplied to the maintenance staff. Among them, 58 MKPIs have been selected on the base of their significance and applicability to the specific organizational context and assigned to each node of the designed maintenance framework.

The software Expert Choice has been used as a support tool to implement the AHP-based approach to rank the assigned MKPIs. The

mathematical programming model has been solved by means of Lingo fixing k_1 equal to 0.6 and k_2 equal to 0.4, whereas n_{min} has been set equal to 2 for each level-1 node. Twenty-nine MKPIs have been finally selected.

8 CONCLUSIONS

Nowadays, existing literature on Maintenance Performance Measurement (MPM) and Maintenance Key Performance Indicators (MKPIs) principally lacks on two aspects. Firstly, proposed MPM frameworks are generic and disregard the business specific environment of the company where these tools should be applied in. Secondly, the available literature mainly proposes a huge list of MKPIs but lacks a methodological approach for selecting specific MKPIs from the listed indicators. With this recognition, a structured methodology for the maintenance performance measurement by means of a restricted and comprehensive list of MKPIs has been proposed. The approach has been thought with relation to a high risk process plant where the way maintenance is managed and performed is fundamental to prevent the occurrence of hazardous events. The subject company maintenance staff has been involved in the definition and implementation of the whole methodology that actually arises from a real need of the maintenance manager to measure, check and communicate the maintenance performance on the base of different perspectives. Firstly, a *customized hierarchical framework* capable of synthesizing the most meaningful aspects affecting the effectiveness and the efficiency of the maintenance process has been designed. It comprises multiple levels and nodes so that information useful for all organizational levels are incorporated. Actually, each node represents a particular aspect on the base of which measuring the maintenance performance and, whenever deemed to be necessary, each node has been further branched in order to detail the considered aspect. Then, MKPIs already proposed in the literature have been collected and analyzed in cooperation with the subject company maintenance staff in order to select the most appropriate to describe the specific maintenance process. Then, an Analytic Hierarchy Process (AHP)-based approach has been implemented to rank MKPIs previously assigned to nodes of the hierarchical framework. MKPIs to be evaluated are not compared in respect to any criteria or sub-criteria but in respect to their relative capability in describing the specific aspect which they have been assigned to. In addition, the decision maker has been asked to supply just pair-wise comparison judgments on which he/she was confident so leading to *incomplete* pair-wise comparison matrices. The latter have been opportunely completed and checked in terms of resulting consistency. Then, an iterative procedure to improve the pair-wise comparison matrices consistency has been implemented. Finally, taking into account that calculating a large number of MKPIs requires a considerable effort in terms of input data to be recorded as well as leads to a lack of conciseness of the resulting information, a mathematical programming model has been formulated and solved to select the *optimal set* of MKPIs.

Even if designed with relation to a high risk process plant, the proposed methodology can be implemented in different contexts. Actually, it constitutes a structured approach that supports maintenance managers in measuring the maintenance process performance.

REFERENCES

Alsyouf, I. 2006. Measuring maintenance performance using a balanced scorecard approach. *Journal of Quality in Maintenance Engineering* 12(2): 133–149.

Amodeo, M.M. 2005. A structured methodology for identifying performance metrics and monitoring maintenance effectiveness. *Thesis submitted to the Faculty of the Graduate School of the University of Maryland, College Park, in partial fulfillment of the requirements for the degree of Master of Science.*

Bakhtiar, A., Purwanggono, B. & Metasari, N. 2009. Maintenance Function's Performance Evaluation Using Adapted Balanced Scorecard Model, *World Academy of Science, Engineering and Technology* 34: 541–545.

Belton, V. & Gear, A. 1983. On a shortcoming of Saaty's method of analytical hierarchies. *Omega* 11: 228–230.

EN: 15341, 2007. Maintenance Key Performance Indicators. *European Committee for Standardization (CEN).* Brussels, Belgium.

Fedrizzi M. & Giove, S. 2007. Incomplete pairwise comparison and consistency optimization. *European Journal of Operational Research* 183: 303–313.

Gomez-Ruiz, J.A., Karanik, M. & Peláez, J.I. 2010. Estimation of missing judgments in AHP pairwise matrices using a neural network-based model. *Applied Mathematics and Computation* 216: 2959–2975.

Harker, P.T. 1987. Alternative modes of questioning in the AHP. *Mathematical Modelling* 9: 353–360.

Hu, Y.-C. & Tsai, J.-F. (2006). Backpropagation multilayer perceptron for incomplete pairwise comparison matrices in analytic hierarchy process. *Applied Mathematics and Computation* 180: 53–62.

Kaplan, R. & Norton, D. 1996. The Balanced Scorecard: Translating Strategy Into Action. *Harvard Business School Press*. Boston, MA.

Mather, D. 2005. The Maintenance Scorecard: Creating Strategic Advantage. *Industrial Press*. New York.

Muchiri P., Pintelon, L., Gelders, L. & Martin, H. 2011. Development of maintenance function performance measurement framework and indicators. *International Journal of Production Economics* 131: 295–302.

Obata, T., Shiraishi, S., Daigo, M. & Nakajima, N. 1999. Assessment for an incomplete comparison matrix and improvement of an inconsistent comparison: computational experiments, *ISAHP*, *Kobe, Japan, August 1999*.

Parida, A. 2006. Development of a Multi-criteria Hierarchical Framework for Maintenance Performance Measurement Concepts, Issues and Challenges. *Doctoral Thesis, Division of Operation and Maintenance Engineering, Luleå University of Technology*.

Saaty, T.L. 1977. A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology* 15: 234–281.

Saaty T.L. (1994). The Analytic Hierarchy Process. *McGraw Hill Company*. New York.

Saaty, T.L. 2003. Decision-making with the AHP: Why is the principal eigenvector necessary. *European Journal of Operational Research* 145: 85–91.

Saaty, T.L. 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences* 1(1): 83–98.

Simões, J.M., Gomes, C.F. & Yasin M.M. 2011. A literature review of maintenance performance measurement. A conceptual framework and directions for future research. *Journal of Quality in Maintenance Engineering* 17(2): 116–137.

Tsang, A.H.C., Jardine A.K.S. & Kolodny, H. 1999. Measuring maintenance performance: a holistic approach. *International Journal of Operations & Production Management* 19(7): 691–715.

Tsang, A.H.C. 2002. Strategic dimensions of maintenance management. *Journal of Quality in Maintenance Engineering*. 8(1): 7–39.

VanHorenbeek, A. & Pintelon, L. 2014. Development of a maintenance performance measurement framework—using the analytic network process (ANP) for maintenance performance indicator selection. *Omega* 42: 33–46.

Visser, J.K. & Pretorius, M.W. 2003. The development of a performance measurement system for maintenance. *SA Journal of Industrial Engineering* 14(1): 83–97.

Wireman, T. 1998. Developing Performance Indicators for Managing Maintenance. *Industrial Press, Inc.* New York, NY.

Wua, H.-Y., Tzeng, G.-H. & Chen Y.-H. 2009. A fuzzy MCDM approach for evaluating banking performance based on Balanced Scorecard. *Expert Systems with Applications* 36: 10135–10147.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

State of the art in Operation and Maintenance planning of offshore wind farms

M. Asgarpour
Department of Civil Engineering, Aalborg University, Denmark
Energy Research Centre of the Netherlands (ECN), Unit Wind Energy, The Netherlands

J.D. Sørensen
Department of Civil Engineering, Aalborg University, Denmark

ABSTRACT: Operation and Maintenance (O&M) costs of offshore wind farms are large contributors to the cost of energy. During last decades, methods have been developed for assessing the corrective maintenance costs, and many studies have been published for planning of preventive maintenance, but yet maintenance is not planned using advanced methods by taking all available information into account in a consistent manner. In this paper first a short literature review in O&M models for cost calculation of corrective maintenance and planning of preventive maintenance is given. Furthermore, an O&M study for a reference offshore wind farm is presented to illustrate the average costs and downtime for a typical offshore wind farm and to justify the necessity and potential of further development of current O&M models. At the end, a discussion on optimal O&M planning of offshore wind farms is given.

1 INTRODUCTION

Offshore wind energy is rapidly growing, but it's not yet competitive with conventional power plants due to its high cost of energy. By the end of 2013, more than 2000 offshore wind turbines were installed in Europe, making a cumulative total of 6.5 GW in 69 offshore wind farms (Corbetta et al., 2014).

Operational costs are one the main cost drivers of offshore wind energy and contribute approximately to 25% of the levelized cost of energy (*Offshore Wind Cost Reduction—Pathways Study*, 2012).

In order to fully exploit the offshore wind energy it is essential to reduce the levelized cost of energy from 17 to 12 ¢€/kWh by 2020 that can be partially achieved by reducing operational expenses of offshore wind farms.

Operational expenses of offshore wind farms are mostly caused by failure of wind farm components. In general the following maintenance actions can be considered for an offshore wind farm:

- Calendar based maintenance, once or two times per year and scheduled by the wind turbine manufacturer;
- Preventive maintenance actions to prevent failure of wind farm components scheduled by wind farm operator using information obtained from inspections, SCADA and condition monitoring system;
- Corrective maintenance actions after a component fails, such as repair or replacement, performed by wind turbine manufacturer during the guaranty period and performed by wind farm operator afterwards.

The purpose of the calendar based maintenance and preventive maintenance is to prevent the high costs of corrective maintenance and preserve the system functionality.

During the past decades of offshore wind energy, several studies have been performed on the following subjects:

- Estimation of corrective maintenance costs;
- Planning of preventive maintenance actions.

In the following sections first a short literature review in O&M models of offshore wind farms is given and then, an O&M study for a reference wind farm is presented. Furthermore, a discussion on optimal operation and maintenance planning of offshore wind farms is given.

2 ESTIMATION OF CORRECTIVE MAINTENANCE COSTS

When a wind farm component fails, the functionality of one or several wind turbines will be affected and therefore, it should be repaired or replaced as soon as possible.

If a wind turbine component fails F times in elapsed time T, then the estimated failure frequency is:

$$\lambda = F/T \quad (1)$$

The estimated failure frequency determined from equation (1) is based on the historical data and can't be used to determine the actual damage state of the component.

In Figure 1 the state of a component is illustrated. The figure presents a simple state model of a component and demonstrates two failures. Assuming there is no redundancy in the design, after each failure the whole system, in this example the wind turbine, stops functioning and a suitable maintenance action should be performed to repair or replace the failed component.

The average functioning time of a component is known as 'availability' and the average downtime of a component is known as 'unavailability'.

In other words, availability is the probability that a component is functioning and unavailability is the probability that the component is not functioning.

From the Figure 1 the unavailability can be calculated as:

$$U = MDT/(MDT + MTTF) \approx MDT/MTTF = \lambda/\mu \quad (2)$$

where MDT is 'Mean DownTime' and MTTF is 'Mean Time To Failure'.

Equation (3) also describes the relation between λ, which is the failure rate and μ, which is the repair rate with MDT and MTTF.

$$\lambda = 1/MTTF$$
$$\mu = 1/MDT \quad (3)$$

Furthermore, it can be easily seen that the sum of availability (A) and unavailability (U) is equal to 1 or 100%, therefore availability can be calculated easily from unavailability equations.

$$A = 1 - U = 1 - MDT/MTTF = 1 - \lambda/\mu \quad (4)$$

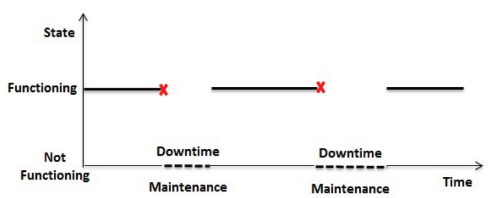


Figure 1. State of a component.

Estimation of corrective maintenance costs of a wind farm is essential, especially in the planning phase of the farm and can be derived from the equation (5):

annual corrective maintenance costs per component = annual failure frequency of the component × repair costs of the component (5)

In early operational years of a wind farm, accurate annual failure rate of the components is not available yet and therefore, data from a generic reliability database, like Reliawind database, will be used. After first years of operation, the annual failure rates of the components can be updated using the actual failure statistics in the farm.

Repair costs of the component include the costs of access vessels, spare parts and technicians to perform initial inspection, repair or replacement. Moreover, lost production and revenue losses due to the disturbed functionality of the wind turbine(s) are a part of the corrective maintenance costs.

In order to estimate the revenue losses, the total downtime of wind turbine(s) during the corrective maintenance should be estimated and to do so, expected waiting times for weather windows of given length are needed for each type of access vessel.

There are two methods to calculate the annual corrective maintenance costs of offshore wind farms:

- Mean value method used in ECN O&M Tool;
- Monte Carlo simulation in time domain used in ECN O&M Calculator, NOWIcob, O2M, MWCOST, and CONTOFAX.

2.1 *Mean value method*

The ECN O&M Tool developed by Energy Research Center of the Netherlands (ECN) is an Excel based tool to estimate overall expected costs of corrective maintenance actions based on the historical failure rates of wind farm components.

The ECN O&M Tool processes the time series of wind speed and significant wave height and then, calculates the mean wait time for a number of weather window lengths.

Furthermore, a polynomial is fitted to describe the mean waiting time as function of the needed weather window and then, these curves are used to calculate the lost production and revenue loss associated with each failure (Rademakers et al., 2008b).

2.2 *Monte Carlo simulation in time domain*

ECN O&M Calculator (Rademakers et al., 2008a) and NOWIcob (Norwegian offshore wind cost and benefit model) developed by NOWITECH

(Hofmann and Sperstad, 2013) both are simulation based tools to calculate the costs of inspections, preventive and corrective maintenance. Both tools take system effects into account and give also insight about required access vessels, technicians and spare parts for maintenance actions.

ECN O&M Calculator, NOWIcob, O2M developed by GarradHassan (Phillips et al.), MWCOST developed by BMT (Stratford) and CONTOFAX developed by Delft University of Technology (Van Bussel and Bierbooms, 2003) are similar in failure modeling and different in weather modeling. In all models failures can be simulated from a Poisson process with constant failure rate, which corresponds to random failures. In MWCOST it's also possible to define time dependent failure rates.

As discussed before, the models are different in processing the weather data. In ECN O&M Calculator and MWCOST historical time series of wind speed and significant wave height are used as input directly in the simulations.

In NOWIcob weather time series are generated by applying a Markov chain process and historical weather data are used to estimate transition matrices from one weather state to the next one (Hofmann and Sperstad, 2013).

The O2M model generates pseudo random time series of the significant wave height using FFT based on input time series, and then, inverse FFT to create artificial time series (Phillips et al.).

In CONTOFAX time series of accessible and inaccessible periods for each access vessel type are generated based on the Weibull distributions for accessible and inaccessible weather windows, which are found based on real time series. Therefore, in CONTOFAX only the availability is calculated because the wind speed is not included in the model and production loss cannot be calculated (Van Bussel and Bierbooms, 2003).

ECN has also developed ECN O&M Analyzer, which can be used to process operational data and study the components failure behavior. After first years of operation, failure rates defined in ECN O&M Calculator can be updated using the output of ECN O&M Analyzer to have an even more accurate estimation of corrective maintenance costs (van de Pieterman et al., 2014).

3 PLANNING OF PREVENTIVE MAINTENANCE ACTIONS

Preventive maintenance actions are performed to preserve system functionality and reduce the failure of components. There are several approaches for planning of preventive maintenance actions trough the life time of an offshore wind farm:

- Based on the predicted life time;
- Based on optimal preventive inspection intervals;
- Based on Reliability Centered Maintenance (RCM).

These approaches are described in the followings.

3.1 *Based on the predicted life time*

The simplest approach for preventive maintenance planning of offshore wind farms is based on only the predicted life time of components and not based on information obtained from inspections and condition monitoring.

The mentioned approach has been used in (Bharadwaj et al., 2007) which describes a simple probabilistic damage model for general corrosion of the tower structure. Assuming this to be the only damage mechanism causing failure of the structure, the remaining lifetime of the structure is calculated by the following model:

$$RL = (T_c - MAT)/C \tag{6}$$

where RL is the remaining lifetime in years, T_c is the current thickness of the structure in mm, MAT is the minimum allowable thickness in mm and CR is the corrosion rate in mm/year.

3.2 *Based on the optimal preventive inspection intervals*

Determining the optimal inspection intervals could be a challenge since long inspection intervals increases the corrective maintenance costs and short inspection intervals increases preventive maintenance costs and revenue losses due to the production lost.

This approach can be applied for the period when a defect in a component becomes detectable and failure occurs, known as delay time. In this approach optimal preventive inspection intervals are found to prevent the failure of components using rate of arising defects, delay time distribution, and cost and duration of preventive inspection.

In (Andrawus et al., 2008) a hybrid of Failure Modes and Effect Criticality Analysis (FMECA) and Delay-Time Maintenance Model (DTMM) is used to find optimal inspection intervals for selected critical components. The failure modes of the turbines are determined by FMECA approach and then mean delay time are derived by DTMM approach.

3.3 *Based on the reliability centered maintenance*

Reliability Centered Maintenance (RCM) is a systematic approach develop in aircraft industry that determines what to do to preserve system

functionality by balancing between corrective and preventive maintenance for critical components.

In (Andrawus et al., 2006) a hybrid of an RCM approach and Asset Life Cycle Analysis technique is used to find the optimal maintenance strategy for a wind turbine. In this paper possible failure modes and their causes and consequences are determined by RCM approach and it is concluded that condition based maintenance is the most cost effective option for the selected wind turbine.

In (Nilsson and Bertling, 2007) a reliability centered asset management approach is introduced to investigate how much decrease in amount of corrective maintenance actions justifies using a condition monitoring system for wind farms. In this paper it is concluded that a change from unplanned to planned maintenance of 47% is enough to make a condition monitoring system profitable.

In the followings first an O&M study will be presented and then, a discussion on optimal O&M planning of offshore wind farms is given.

4 O&M STUDY FOR A REFERENCE WIND FARM

In order to illustrate the average costs and downtime of a typical offshore wind farm and to justify the necessity of further development of current O&M models for offshore wind farms, an O&M study for a hypothetical offshore wind farm is performed. In the following sections, first the reference wind farm is discussed and then, the assumptions for the baseline O&M strategy are given. Furthermore, the results of O&M study for the reference wind farm are presented.

4.1 *Reference wind farm*

The reference wind farm used in this O&M study is a hypothetical 400 MW offshore wind farm. This wind farm consists of 80 NREL offshore 5 MW baseline wind turbines.

The wind farm is assumed to be located in vicinity of meteorological mast FINO3, approximately 80 km west of the German island of Sylt.

The water depth at the location of the wind farm is approximately 30 m. For the weather modeling the wind speed and significant wave height of FINO meteorological mast in the vicinity of the wind farm is used. The wind farm is illustrated in Figure 2.



Figure 2. Location of the reference wind farm in the vicinity of FINO3 meteorological mast [www.fino3.de].

4.2 *Theoretical wind turbine*

The 5 MW NREL offshore baseline wind turbine is a theoretical wind turbine representing the typical multi-megawatt offshore wind turbines used in the reference wind farm. The power curve of the turbine is illustrated in Figure 3.

The wind turbine is using a pitch control system with 90 m hub height and 126 m rotor diameter.

The NREL 5MW offshore baseline wind turbine is equipped with an internal crane with 2000 kg hoisting capacity, which can be used for hoisting of small components like pitch motors or yaw drives. For hoisting large components such as generator or nacelle a large external crane on a jack up vessel is required (Jonkman et al., 2009).

4.3 *Assumptions for baseline O&M strategy*

In order to calculate the annual maintenance costs and revenue losses ECN O&M Calculator developed by Energy Research of Netherlands (Rademakers et al., 2008a) is used. The baseline O&M strategy is defined based on default model available in ECN O&M Calculator.

In the baseline O&M strategy it is assumed that personnel will work only in one single shift during daylight periods for all possible maintenance to ensure a safe working environment. On average personnel work from 7:00 h to 19:00, which means the total workday length is set at 12 hours on average. Maintenance will only be initiated if the technicians can spend a minimum of 2 hours to the repair onsite.

In the baseline O&M strategy mostly main components are defined on a system level, except the rotor system and drive train, where the major subsystems are included in the breakdown. The failure

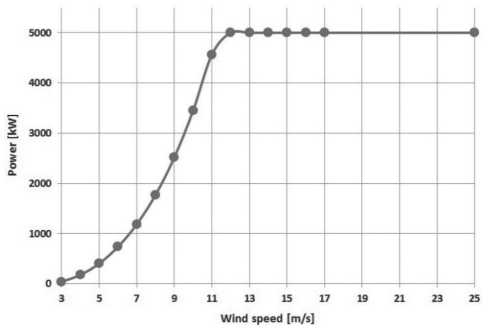


Figure 3. Power curve of theoretical wind turbine used in the NORCOWE reference wind farm.

frequencies of wind farm components are derived from the result of Reliawind project (Wilkinson and Hendriks, 2011).

For calendar based maintenance, all wind turbines in the wind farm will be maintained once per year with three technicians. Moreover, every five years a larger preventive maintenance campaign is carried out additional to the yearly maintenance.

A mother vessel is located in the proximity of the wind farm. This vessel offers accommodation for technicians to stay overnight. All year long, two crews of technicians are employed, who are exchanged from the mother vessel on a 2-weekly basis. Besides the mother vessel, the following vessels are used to transfer personnel and spare parts, and for hoisting of components: three workboats permanently leased of fixed contract, one chartered jack-up vessel when required, one chartered cable laying vessel when required, one chartered diving support vessel when required and one helicopter to transport technicians to the balance of plant structure when required.

Results of the O&M study.

As results of the simulation in the time domain, the following costs are calculated:

- Total maintenance costs M€ 66.5/year;
- Total revenue losses due to the lost production: M€ 28.7/year;
- Sum of total maintenance costs and revenue losses due to the lost production: M€ 95.2/year;
- Total maintenance costs per kWh produced: ¢€/kWh 3.92.

Form the summary of results it can be seen that the total cost of maintenance is about 23% of the price of energy, which demonstrates the necessity of an optimal model for O&M planning of offshore wind farms to contribute in cost of energy reduction.

From the breakdown of O&M costs and total down time per type of maintenance it can be seen that 89% of the total O&M costs and 95% of the total downtime is caused by unplanned corrective maintenance, which can be significantly reduced by using condition monitoring systems and an optimal preventive maintenance planning model to perform cost effective preventive maintenance actions.

In Figure 4 the breakdown of the total O&M costs is illustrated and it can be observed that most of the O&M costs are caused by equipment costs (43%) and revenue losses (30%) due to the lost production.

Furthermore, in Figure 5 the breakdown of the total downtime is illustrated. In Figure 5 it can be observed that about half (51%) of the total downtime is caused by weather delays that corresponds to long waiting time before a suitable weather window can be found.

It is of great interest to observe that only 15% of the total downtime is caused by the actual maintenance actions on wind farm components.

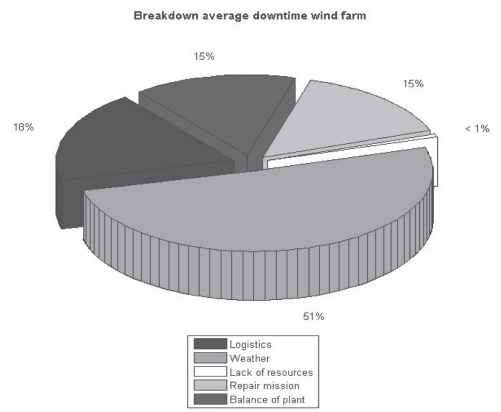


Figure 4. Breakdown of the total O&M costs.

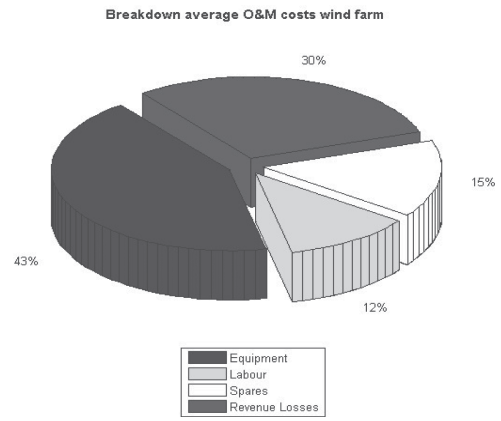


Figure 5. Break down of the total downtime.

5 DISCUSSION ON OPTIMAL PLANNING OF PREVENTIVE MAINTENANCE

As illustrated in the O&M study, corrective maintenance actions are the main contributors to operational expenses of offshore wind farms and they can be reduced significantly by using an optimal O&M model to support the wind farm operator in long term planning and short term decision making.

During the last decades several simulation based methods have been developed to estimate the maintenance costs, but they are mostly cost calculators and can't be used as an optimal short and long term planning tool.

In Figure 6 an optimal O&M planning model is illustrated which is consisting of the following parts:

- Inputs: inspection and maintenance results, SCADA, condition monitoring system and climate data;
- Processors: indicator model, deterioration model of critical components, risk based cost model and risk based decision model;
- Output: long term planning and short term decision support.

The model in Figure 6 includes the deterioration model of the critical components instead of the historical failure frequencies. The deterioration models should also continuously get updated by using an indicator model to determine the component failures more accurately.

The indicator model is obtaining direct and indirect information from inspection and maintenance results, condition monitoring systems and SCADA to update continuously the deterioration model of the components.

The model illustrated in Figure 6 also includes a decision model, which is consisting of risk based decision rules and decision criteria to process all input data and determine the optimal O&M planning.

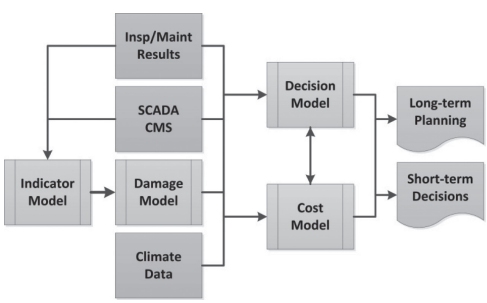


Figure 6. Model of an optimal risk and reliability based O&M planning tool.

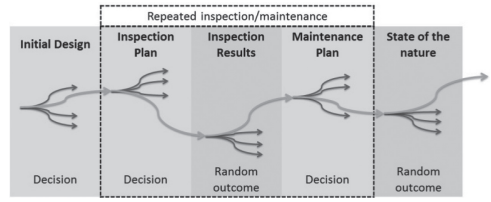


Figure 7. Decision tree for optimal O&M planning.

The developed decision rules and criteria should continuously get updated whenever new information is being available. Then, based on the feedback from the system all calculations are redone and the updated O&M plan is determined.

In (Sørensen, 2009) a risk based life cycle approach for optimal planning of preventive maintenance actions is described.

The approach is theoretically based on pre-posterior Bayesian decision theory and can be used when deterioration mechanisms such as fatigue, corrosion, wear and erosion are present and can be observed by inspection and monitoring before failure of the component occur. The decision tree described in this paper is illustrated in Figure 7.

The described risk and reliability based approach in Figure 6 can rationally take into account the uncertainty related to the deterioration and the future costs related to inspections and maintenance of offshore wind farms.

6 CONCLUSIONS AND FUTURE WORK

Through a case study for a reference offshore wind farm it was illustrated that O&M costs are about one quarter of the cost of energy. Furthermore, it was seen that a major part of the total costs and downtime of O&M actions are caused by unplanned corrective maintenance, which can be significantly reduced by using a risk and reliability based O&M model to support the wind farm operator in long term preventive maintenance planning and short term decision making.

As illustrated in Figure 6, in order to develop an optimal O&M model a risk based decision model and deterioration models of critical components should be developed.

Additionally, a short literature review in O&M models for cost calculation of corrective maintenance and planning of preventive maintenance was given. It is also of great interest to study the existing risk based O&M models for maintenance planning of offshore wind farms.

ACKNOWLEDGMENT

This work has been (partially) funded by Norwegian Centre for Offshore Wind Energy (NORCOWE) under grant 193821/S60 from Research Council of Norway (RCN). NORCOWE is a consortium with partners from industry and science, hosted by Christian Michelsen Research. The work presented in this paper has been made also possible by the Energy research Centre of the Netherlands (ECN).

REFERENCES

Andrawus, J.A., Watson, J., Kishk, M., Adam, A., 2006. The Selection of a Suitable Maintenance Strategy for Wind Turbines. Wind Engineering 30, 471–486. doi:10.1260/030952406779994141.

Andrawus, J.A., Watson, J., Kishk, M., Gordon, H., 2008. Optimisation of Wind Turbine Inspection Intervals. Wind Engineering 32, 477–490. doi:10.1260/030952408786411921.

Bharadwaj, U.R., Speck, J.B., Ablitt, C.J., 2007. A Practical Approach to Risk Based Assessment and Maintenance Optimisation of Offshore Wind Farms. ASME, pp. 483–492. doi:10.1115/OMAE2007-29260.

Corbetta, G., Pineda, I., Moccia, J., 2014. The European offshore wind industry—key trends and statistics 2013. EWEA, Brussels, Belgium.

Hofmann, M., Sperstad, I.B., 2013. NOWIcob—A Tool for Reducing the Maintenance Costs of Offshore Wind Farms. Energy Procedia 35, 177–186. doi:10.1016/j.egypro.2013.07.171.

Jonkman, J., Butterfield, S., Musial, W., Scott, G., 2009. Definition of a 5-MW Reference Wind Turbine for Offshore System Development (No. NREL/TP-500-38060, 947422).

Nilsson, J., Bertling, L., 2007. Maintenance management of wind power systems using Condition Monitoring Systems. IEEE, pp. 1–1. doi:10.1109/PES.2007.385616.

Offshore Wind Cost Reduction—Pathways Study, 2012.. The Crown Estate, London, UK.

Phillips, J.L., Morgan, C.A., Jacquemin, J., n.d. Evaluating O&M strategies for offshore wind farms through simulation—the impact of wave climatology. Garrad Hassan, Bristol, UK.

Rademakers, L.W.M.M., Braam, H., Obdam, T.S., 2008a. Estimating Costs Of Operation & Maintenance For Offshore Wind Farms. Presented at the EWEC 2008, ECN Wind Energy, Brussels, Belgium, p. 10.

Rademakers, L.W.M.M., Braam, H., Obdam, T.S., Frohböse, P., Kruse, N., 2008b. Tools For Estimating Operation And Maintenance Costs Of Offshore Wind Farms—State Of The Art. Presented at the EWEC 2008, ECN Wind Energy, Brussels, Belgium.

Sørensen, J.D., 2009. Framework for risk-based planning of operation and maintenance for offshore wind turbines. Wind Energy 12, 493–506. doi:10.1002/we.344.

Stratford, P., n.d. Assessing the Financial Viability of Offshore Wind Farms. Presented at the EWEC 2007, EWEA, Milan, Italy.

Van Bussel, G.J.W., Bierbooms, W.A.A.M., 2003. The DOWEC Offshore Reference Windfarm: analysis of transportation for operation and maintenance. Wind Engineering 27, 381–391. doi:10.1260/030952403322770986.

Van de Pieterman, R., Asgarpour, M., Rademakers, L.W.M.M., Braam, H., 2014. A structured approach for data collection and analysis Assess the offshore O&M strategy with OMCE. Presented at the EWEA Offshore 2013, ECN Wind Energy, Frankfurt, Germany, p. 10.

Wilkinson, M., Hendriks, B., 2011. Report on Wind Turbine Reliability Profiles—Work package WP1—Field Data Reliability Analysis—Deliverable D.1.3. Reliawind Project.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Maintenance of power systems considering time-dependent uncertainty

T. Iesmantas & R. Alzbutas
Lithuanian Energy Institute, Kaunas, Lithuania

ABSTRACT: There are a lot of different infrastructure maintenance approaches. One of it is Markov processes, which take into consideration changing states of the maintained object. However, the uncertainty of data is a forgotten matter when things turn to the maintenance modeling. The practice is to plug in points estimates and proceed with maintenance analysis. We take a Bayesian view on the power transformer maintenance modeling to take into account the uncertainties and to propagate it through the model. We will concentrate on theoretical models rather than applications to real data. Such a restriction is necessary as our foremost intention is to build a solid background, which will serve then as a framework for real world applications.

1 INTRODUCTION

Maintenance concept, especially when related to the context of power grid, is of great importance. As time is passing by the reliability requirements for systems are increasing, while the maintenance cost are not getting any cheaper (IEEE/PES Task Force, 1999). However, the common practice is to use time independent mathematical model for maintenance and parameter values are just point estimates obtained from the historical data—and it doesn't really matter what kind problem we might consider. Whether it is a power grid maintenance/inspection optimization task, or reliability predictions under the influence of maintenance/inspection rates, the "tradition" is the same—obtain point estimates and don't bother oneself by the data any more. In addition, uncertainty of data is almost never taken into consideration, or event when it is—not as the central part of the whole picture. We demonstrate in this paper that Bayesian framework is applicable to propagate data uncertainty through all the maintenance analysis aspects.

Surely, with Bayesian methods penetrating into every engineering problem, there is already some work in maintenance modelling field, like application of Bayesian networks (Khakzad, 2011). However, it is basically for modelling decision processes of maintenance under data uncertainty and the time-dependent maintenance specificity of power grid components was never (at least authors do not know of it) widely considered. On the other hand, mathematical modelling literature on maintenance of power grid components is not so vast in general.

In this paper we take a look at the problem of power transformers and as a reference model of their maintenance will be a Markov process (see Section 2). We provide complete picture on how transition rates between different states of transformer degradation can be estimated and present a view on how to do it sequentially, i.e. update parameters once new data arrives without recalculating everything starting with old data (Section 3). We also show how such updating makes life easier when taking into consideration optimization of the maintenance rates. In addition, Bayesian parameter updating abilities are applied to update the optimal maintenance policies sequentially (Section 4). All calculations are done with parameters not necessarily representing some specific set of transformers, as our intentions are to demonstrate theoretical analysis rather than some specific case calculations.

2 TIME-DEPENDENT MAINTENANCE OF POWER TRANSFORMERS

Since we do not seek some specific case investigation, we will start from general model of maintenance (without the cost consideration), which is a slight modification of the one considered in (Jirutitijaroen, 2004; Beehler, 1997). The general scheme of the Markov model is presented in Figure 1.

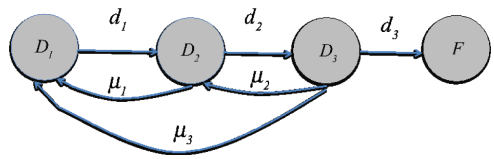


Figure 1. Markov model for maintenance.

For example, using it we may assume three states D_i, which approximate the deterioration of power transformer, while the last state F represents a complete failure and inability to carry through electricity. We consider the F state as an absorbing. The states after deterioration can be repaired at the rates μ_1, μ_2 and μ_3.

We assume that if the transformer fails (i.e. it is in state F), lines going through it cannot transmit electricity, i.e. failure of the transformer is equivalent to the outage of connected lines.

In this model the maintenance rates μ_i are assumed to be fixed. As we will investigate its effect on the reliability of the grid, so the estimation of these rates is out of the scope of this investigation.

A note about the deterioration is required here. Any transition rate d_i between the deterioration states does not reflect exactly the ageing process. Ageing during long time period generally weakens all system—components of power transformers fractures, cracks, etc. Thus, as time goes by, more often transitions between D_1, D_2, D_3 and F states will occur and transition rates may increase. In order to be able to model this effect age-dependent transition rates should be employed, i.e. time-inhomogeneous Markov processes should be considered. However, we will not use this kind of modelling here.

3 BAYESIAN INFERENCE AND SEQUANTIAL UPDATING

One of the purposes of this paper is to stress the importance of properly handling uncertainty in the maintenance-inspection modelling and the influence on overall network reliability. The prevailing practice in maintenance modelling is to plug-in point estimates of the parameters (in our case we have 6 unknown transition rates) and go along with it. However, estimates are uncertain, i.e. we do not have infinite amount of information in order to be able to have absolute certainty about their values. Thus, by blindly using point estimates without any consideration of uncertainty bounds we can make inspection or maintenance decisions, which are not very well informed. For example, there is a significant difference between the 95% confidence intervals [400; 700] and [200; 1300] of the MTTF (Mean Time To Failure), even though the expectations of MTTF may be equal in both cases. Quantified uncertainty allows to have a more informed insight on possible variations of parameters and their impact on considered result e.g. cost.

Bayesian framework is perfectly suited for such purposes and we will stick to it. In this section we'll briefly present Bayesian inference for Markov chain parameters. More in depth and more general considerations can be found in (Billingsley, 1961; Jacobsen, 1982; Bladt, 2005).

For the ease of general presentation we denote transition rate matrix by $Q=(q_{ij})$. Then the likelihood function can be expressed as follows (Bladt, 2005):

$$L_t(Q)=\prod_{i=1}^{n}\prod_{k=1} q_{ij}^{N_{ij}} \exp\{-q_{ij}R_i(t)\}, \tag{1}$$

where n is a number of states, N_{ij} is the number of transitions from state $\boldsymbol{i}$ to state $\boldsymbol{j}$ in the time interval [0,t], whereas $R_i(t)$ is the time that is spent in state i before time t.

As we seek to estimate the transition rates, according to Bayesian framework they have to have a prior distribution. For each unknown parameter we place a uniform distribution, so that the posterior distribution is proportional to the likelihood.

Since we do not assume any prior dependencies between the transition rates, we have a very nice simplification. Namely, the likelihood function (1) can be decomposed into likelihood functions for each separate transition rate q_{ij}, and the posterior distribution for each transition rate given data X is propotional to the following expression:

$$q_{ij}^{N_{ij}} \exp\{-q_{ij}R_i(t)\} \tag{2}$$

which is (after renormalization) a gamma distribution:

$$q_{ij} \mid X \sim Gamma(N_{ij}+1, R_i) \tag{3}$$

Having posterior distribution for the unknown transition rates, we can now perform inspection schedule analysis and its influence on the reliability. Suppose we decided on some optimal value of the inspection rates. As time goes by, additional data will become available and it would be reasonable to adjust our optimal inspection and maintenance plans. Fortunately, Bayesian approach allows performing such updating in a very natural way.

If the new data is X' and if we consider previous posterior distributions $\pi(q_{ij}\mid X)$ as our prior distribution, we obtain updated posterior distribution, which is expressed again as a gamma distribution:

$$q_{ij} \mid X \sim Gamma(N_{ij}+1+N'_{ij}, R_i+R''_i) \tag{4}$$

where N'_{ij} and R'' are calculated for the new data.

Since parameters might change considerably (especially in case of initially small samples), we can reconsider inspection rate and find another optimum. Thus, we propose, that Bayesian framework in addition to being the most natural way of propagating uncertainty in model parameters,

allows us a kind of sequential updating of not just parameters, but optimal inspection plans as well.

Since changes of parameters, as supported by the new data, are allowed, the sequential parameter updating has another useful feature—if due to ageing effect the transition rates do in fact change, this will partially be reflected in updated posterior distributions. Even though expectations of parameters might not change very much, uncertainty bounds will react to the additional information. Hence, this is another important reason for the uncertainty consideration.

4 POWER TRANSFORMER RELIABILITY UNDER UNCERTAINTY

Let's assume that we have observed some data sample over the time period of 10 years. The sample is such that data for posterior distributions of transition rates (except the maintenance intensity, as those will be assumed to be known) are as presented in Table 1.

Figure 2 represents 100 realisations of failure probability (unreliability) curves within 95% credibility belt. These curves represent the uncertainty level as is encoded in the gamma distributions of transition rates. Example clearly shows, how uncertain our decisions might be if we just use some point estimates.

The uncertainty directly can be transferred to other measures of interest, like the Mean Time To Failure (MTTF). For example using the collection of the parameters as above, the 95% credibility interval of MTTF is [47; 192] years. This interval is very wide and it is not encouraging that there is a 0.95 probability that the MTTF lies somewhere in that range. So, for better decision making, say in optimal maintenance scheduling, or in optimal cost analysis, we would suggest to take into account this uncertainty.

Table 1. Data for gamma distributions of uncertain parameters.

Parameter	N_{ij}	R_i	Expectation
d_1	83	177	0.47
d_2	6	20	0.30
d_3	1	3	0.33

Let's fix μ_1 and μ_2 parameters to the values to 0.5 and 0.7 accordingly and vary and μ_3 over the interval [0,20]. The MTTF and its upper/lower bound for 95% credibility interval changes as represented in Figure 3.

MTTF dependence on the maintenance rate can be used in the maintenance optimisation. However, the same problem with uncertainty as in unreliability case remains—uncertainty bounds shows that application of point estimates can be not the best choice.

And once again, uncertainty bounds can be used to make better informed decisions—maintenance cost evaluation when uncertainty is taken into account should serve as a better money allocation tool. From the plot we can see how wide MTTF uncertainty bounds can be and making decisions purely by means of expected values might lead to under or over estimation.

Let's assume in our further investigation, that maintenance optimization is equivalent to choosing maintenance rate μ_2 such that the upper bound of power transformer failure in the next 4 years probability (i.e. transition rate d_3) is not higher than 0.07, i.e. we want to choose such maintenance rate, so that in the next 4 years, the probability of transformer failure will not be higher that the value 0.07. The choice of time period and probability threshold is purely arbitrary and is only for the purposes of possible strategy demonstration rather than to imply some existing practice. Figure 4 illustrates the dependence on the maintenance μ_2 of 95% bound for the probability of failure in the next 4 years.

Now, let's assume, we want to update every 4 years our optimal maintenance (i.e. reflect changes of data in the adjustable maintenance rate μ_2). Due to the convenience of Bayesian updating procedure and the resulting gamma posterior

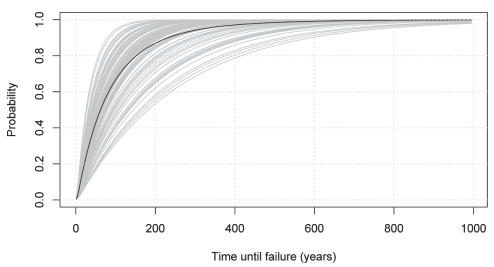


Figure 2. Uncertainty of unreliability function.

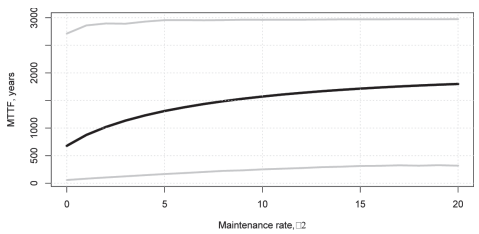


Figure 3. MTTF and its 95% confidence interval dependence on the maintenance rate.

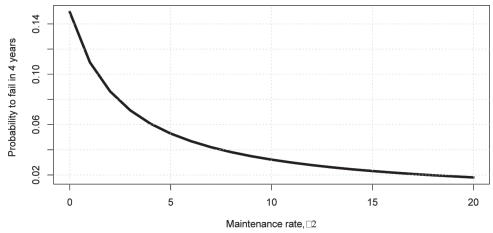


Figure 4. Upper 95% confidence bound of probability to fail in the next 4 years.

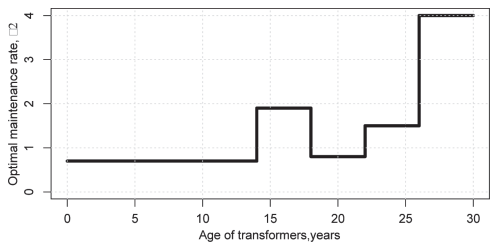


Figure 5. Change of optimal maintenance rate after updating every 4 years.

distribution, such maintenance corrections can be done without any recalculations of the previous analysis. All one needs to do is to update posterior gamma distribution with new data and then find another maintenance rate so that the probability in another 4 years is kept lower than 0.07.

Markov chains generate time-dependent probability distribution of transitions (even though it will eventually approach some steady state value) and we show optimal maintenance μ_2 or MTTF (Mean Time To Failure) to change each time we update transition rates as well. Figure 5 demonstrates, how this optimal maintenance rate changes when we update the model parameters (i.e. update deterioration rates) every 4 years.

The initial maintenance rate was 0.7. Since the upper bound of probability to fail in next 4 years was lower than the 0.07 value, there was no need to increase the maintenance rate. That is the reason for going 14 years with the same maintenance rate. Then, since the probability to fail increases with time, we have to update our maintenance with optimal schedules. As we update transition rates every 4 years, we update the optimal maintenance as well. However, after certain age the corrections of only one maintenance rate will not be enough, since to keep the upper bound of probability to fail in the next 4 years lower than 0.07 value, the maintenance rate will have to be extremely high (at the age of 30 years, it has to be approximately equal to 58 in order to keep the probability below 0.07).

If we would consider age-dependent transition rates (i.e. time inhomogeneous Markov chains), the easy transition rate updating procedure by gamma posterior distribution would not work, as the posterior distribution would be much more complicated and the analytical expression would not be known. Thus, in order to obtain posterior estimates one would have to employ numerical methods, like Markov Chain Monte Carlo methods (Gilks, 1996).

5 CONCLUSIONS AND FURTHER DISCUSSIONS

In this paper we have demonstrated how uncertainty in the data can be easily incorporated into the problem of maintenance optimization and how sequential updating of parameters using Bayesian approach can be applied when maintenance is adjusted according to the available information and possible uncertainty.

Bayesian updating of model parameters allows straightforwardly deal with uncertainty in data which is directly transferred to the decision about the optimal maintenance schedule. In addition sequential nature of the problem enables (at least at some degree) to deal with uncertainty in transition between transformer degradation states.

We have left the aspect of power transformer reliability influence on overall power grid reliability unexplored. It is very common approach to consider power grid nodes as perfectly reliable and just proceed further with failing electricity transmission lines. However, even thought the MTTF's are much longer for power transformers as compared to transmission lines, transformer have much more significant influence on the connectivity of the network and hence on the overall reliability. We showed, that reliability bounds for transformer can be very wide (especially when data sample is small).

Our previous work (Iešmantas, 2014) have provided some evidence that power lines do not follow identical distribution. Heterogeneity due to geographical locations, different weather conditions, etc. results to heterogeneity in failure rates of transmission lines. Since power transformers functions in different geographical areas as well, we can expect the same heterogeneity in their reliability to be present as well. This brings into picture additional level of uncertainty, so called between source uncertainty.

ACKNOWLEDGEMENT

This research was funded by the grant (No. ATE-04/2012) from the Research Council of Lithuania.

REFERENCES

Beehler, M.E., 1997. Reliability centered maintenance for transmission systems. IEEE Transactions on Power Delivery, 12(2):1023–1028.

Billingsley, P., 1961. Statistical inference for Markov Processes. Chicago: University of Chicago Press.

Bladt, M. and Sørensen, M., 2005. Statistical inference for discretely observed Markov jump processes. Journal of the Royal Statistical Society: Series B (Statistical Methodology), 67:395–410.

Gilks W.R., Richardson S. and Spiegelhalter D.J., 1996. Markov Chain Monte Carlo in Practice. Chapman & Hall/CRC.

IEEE/PES Task Force on Impact of Maintenance Strategy on Reliability, "Impact of maintenance strategy on reliability," Final Report, July 1999.

Iešmantas, T., Alzbutas, R., 2014. Bayesian assessment of electrical power transmission grid outage risk, International Journal of Electrical Power & Energy Systems 58:85–90.

Jacobsen, M., 1982. Statistical analysis of counting processes. Lecture notes in statistics, 12.

Jirutitijaroen, P., Singh, C., 2004. The effect of transformer maintenance parameters on reliability and cost: a probabilistic model. Electric Power Systems Research, 72(3):213–224.

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches, Reliability Engineering & System Safety, 96(8):925–932.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Decision-making support for maintenance optimisation of natural gas compressor stations

J. Blondel, L. Marle & O. Mozar
CRIGEN, GDF SUEZ, Saint-Denis La Plaine, France

A. Abdesselam
GRTgaz, Direction Technique, Bois-Colombes, France

F. Brissaud
DNV France, Paris, France

ABSTRACT: The purpose of this study is to help GRTgaz optimising the maintenance of its natural gas compressor stations. Availability stations modelling is therefore proposed, taking the probability of failure of Basic Functional Elements (BFE) and preventive and corrective maintenance actions into account. It also includes maintenance and system downtime costs. The system modelling was created in stochastic Petri nets with predicates.

1 INTRODUCTION

GRTgaz manages a gas transmission network in France and uses databases related to the technical features and operation data of its facilities.

CRIGEN, the GDF SUEZ Research and Technologies Division for Gas and New Energies, provides its methodological support to GRTgaz for the development of policies in the fields of asset and industrial safety management.

The present study deals with the asset management of Basic Functional Elements (BFE) at natural gas compressor stations, using feedback data. The purpose is to help GRTgaz optimising the frequency of its preventive maintenance. Consequently, a proposal was made to model BFE availability at compressor stations, taking the failure probabilities (with effect of ageing) and preventive and corrective maintenance into account. The modelling also incorporates the downtime costs of the system and the maintenance costs.

The modelling was carried out with stochastic Petri nets with predicates and the software used was the Petri net module of GRIF, developed by SATODEV. The results obtained in terms of frequency of failure, percentage of planned and unplanned downtime, and especially costs, make it possible to suggest areas where preventive maintenance frequencies can be optimised.

This study also provides an evaluation of the available data and a scientific approach combining feedback data and expert judgement.

2 DEFINITIONS AND HYPOTHESES

Only those components deemed to be critical in terms of downtime are taken into account in this study. Accordingly, the Basic Functional Elements (BFE) of natural gas compressor stations were broken down into nine parts, each of them having sub-components:

- Ultimate security system, comprising filters, instrumentation and valves;
- Process valves, comprising instrumentation, continuous valves, and on-demand valves;
- Filtration system, comprising filters;
- Natural Gas Compressor (NGC), comprising control systems and NGC with auxiliaries;
- Turbine, comprising a turbine with auxiliaries;
- Cooling tower;
- Safety valve;
- Air admissible circuit, comprising a filter;
- Oil circuit, comprising filters, a lubrication pump system, and aero oil.

Subsequently, the sub-components (note that there might be multiple instances of a given sub-component) will themselves be broken down into maintainable units. Note also that he input data, modelling, and results presented here pertain to one particular station (confidential).

2.1 *Series system*

BFE of natural gas compressor stations is considered as a series system (Procaccia et al. 2011)

with respect to its nine parts identified as critical, just like each of these parts with respect to its sub-components, and each of these sub-components with respect to its maintainable units. Accordingly, the downtime of any maintainable unit can itself cause BFE downtime.

2.2 *Two modes of operation*

Each maintainable unit has two modes of operation:

- "Continuous" mode, when the failure in the maintainable unit has an impact on the compressor station as soon as it appears;
- "On-demand" mode, when the failure in the maintainable unit only has an impact on the compressor station as of the moment when a demand is actually made upon the maintainable unit.

In the case of "on-demand" mode, it is considered that the (random) time between two demands made upon the maintainable unit follows an exponential distribution. The frequencies of demand are defined at the level of the sub-component and are therefore applicable to all its maintainable units.

When a demand is made upon a maintainable unit that is in operation, the duration of said demand is assumed to be negligible. On the other hand, when a demand is made upon a failing maintainable unit, the effect of said failure (which starts as of the moment of demand) lasts until the maintainable unit is put back into operation, regardless of the duration of said demand.

2.3 *Mean Time To Failure (MTTF)*

It is considered that the time between placing/replacing a maintainable unit "in operation" and its next failure follows a Weibull distribution of parameters η and β. The Mean Time To Failure (MTTF) without preventive maintenance of a maintainable unit is given by (Lannoy & Procaccia 2006):

$$MTTF = \eta \cdot \Gamma(1 + 1/\beta) \tag{1}$$

with the Gamma function defined by:

$$\Gamma(x) = \int_0^{-} u^{x-1} \cdot e^{-u} \cdot du \tag{2}$$

Parameter η is the scale parameter (in time units) and parameter β is the form parameter (without unit).

2.4 *Preventive maintenance*

For each maintainable unit, these two parameters define the preventive maintenance actions:

- Preventive maintenance period τ, with the preventive maintenance actions performed at times $t0+\tau$, $t0+2 \times \tau$, $t0+3 \times \tau$, etc. (provided the corresponding maintenance resources are available), defined by failure as of $t0 = 0$;
- Duration of preventive maintenance d (as of the moment when the corresponding maintenance resources are available), including supply times and inactivity times due, for instance, to the stopping of maintenance actions during nights and weekends.

These preventive maintenance action parameters are defined for each maintainable unit. Indeed, the maintainable units have been defined in such a way that each preventive maintenance action corresponds to a maintainable unit. Nevertheless, when the preventive maintenance actions do not cover the entire sub-component, the result is a "residual" maintainable unit which is not subject to preventive maintenance action.

Each preventive maintenance action on a maintainable unit has the effect of rendering that unit (and therefore the system) unavailable for a duration equal to the corresponding preventive maintenance duration to which is added any waiting time for the availability of the corresponding maintenance resources.

At the end of a preventive maintenance action, the maintainable unit in question is restored to a state that is "as good as new," i.e. any ageing effects of the maintainable unit are "reinitialised."

2.5 *Corrective maintenance*

The corrective maintenance actions start as soon as the failure in a maintainable unit is detected (provided the corresponding maintenance resources are available).

- When a maintainable unit is in "continuous" mode, the failure is detected as soon as it appears.
- When the maintainable unit is in "on-demand" mode, this happens as soon as a demand is placed upon the failing maintainable unit, or following a preventive maintenance action on it.

It is assumed that the (random) time between the start (as of the moment when the corresponding maintenance resources are available) and the end of the corrective maintenance action of a maintainable unit follows an exponential distribution. The Mean Times To Repair (MTTR) are defined at the level of the sub-component and are therefore applicable to all of the maintainable units that comprise it.

Each corrective maintenance action on a maintainable unit has the effect of rendering that unit, and therefore the system, unavailable for a duration equal to the corresponding corrective maintenance duration to which is added any waiting time for

the availability of the corresponding maintenance resources.

At the end of a corrective maintenance action, the maintainable unit in question is restored to a state that is "as good as new", i.e. any ageing effects of the maintainable unit are "reinitialised".

2.6 *Maintenance resources*

The maintenance resources used to perform preventive and corrective maintenance actions are limited in such a way that at any time, the number of resources used to perform any maintenance action may not exceed a certain value.

When the maintenance resources that are needed to perform a desired maintenance action are not available, the maintenance action in question is put on hold until the necessary maintenance resources are available. In the case of "conflict" (i.e. when multiple maintenance actions on hold could start at the same time), priority is given to corrective maintenance actions and, secondly, the choice is made in an equiprobable manner. All maintenance actions in progress must be terminated before releasing the corresponding maintenance resources.

The maintenance resources that are needed to perform corrective maintenance actions are defined at the level of the sub-component and are therefore applicable to all of the maintainable units that comprise it.

The maintenance resources that are needed to perform preventive maintenance actions are defined for each maintainable unit.

2.7 *Costs*

System downtime implies a cost per time unit. This cost is independent of the cause of the downtime (corrective maintenance or preventive maintenance).

Each corrective maintenance action implies a fixed cost. These costs are defined at the level of the sub-component and are therefore applicable to all of the maintainable units that comprise it.

Each preventive maintenance action implies a fixed cost. These costs are defined for each maintainable unit.

3 METHODOLOGY

3.1 *Reliability input data*

The first step consists of estimating the associated failure rates for each piece of equipment on the basis of feedback data.

According to Lannoy (1996), the Bayesian approach applies when:

– There is not much feedback data;
– Such data are "contaminated" by changes to the design, by changes to operation or by maintenance;
– It is desired to re-update previous estimates if new feedback observations become available.

In this case, there is not much feedback data, or even none at all for certain equipment families for which no failures were observed. This high level of reliability invalidates the frequency-based approach and does not make it possible to obtain an accurate estimate. The Bayesian approach is an alternative that makes it possible to take all of the available knowledge into account in order to attain the best and most accurate possible estimate.

The Bayesian approach (Procaccia 2008) was therefore applied for those equipment families with little feedback:

– Either by using offshore reliability data (OREDA);
– Or by consolidating local data (specific to a particular site) via national data (considered as prior in this case).

When OREDA data were used, Fisher Information weighting was performed in order to ensure a balance between prior and likelihood, with respect to information contribution.

In addition, it was necessary to ensure a correct match between the feedback and prior knowledge. It was sometimes necessary to weight the data according to the match level.

Expert data (Lannoy & Procaccia 2001) was also collected in order to compare the expert assessment to the results obtained. Accordingly, a questionnaire was used to collect two expert assessments: one from an expert in reliability and maintenance of the equipment studied, and the other from an expert in the operation of compressor stations.

As can be seen in Figure 1, for six equipment families, the result of the assessments is in line with the result of the feedback. Expert 1 was the more

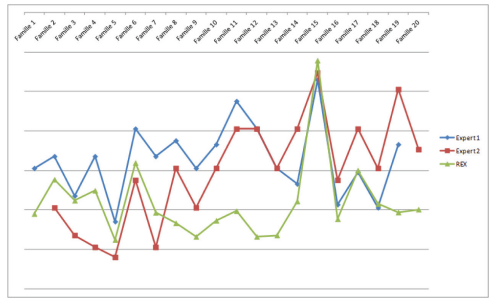


Figure 1. Failure rates provided by each expert compared to the GRTgaz feedback data (the values are masked for confidentiality reasons).

pessimistic in terms of reliability and expert 2 was more optimistic.

For the other families, the two experts were more pessimistic, giving higher failure rates than the feedback data.

The two expert assessments were incorporated using the Bayesian approach by giving equal weight to both experts.

All of the Bayesian calculations were performed using REXPERT software.

Organising the failure data into a hierarchy subsequently made it possible to identify critical equipment families according to their impact on the downtime of the facility (total for the site or partial for a workshop, for example).

The demand frequencies and the MTTF come from feedback data. (It should be noted that the MTTF were defined taking account of the current preventive maintenance periods and the formal parameters applicable to Weibull distributions.)

3.2 *Maintenance input data*

The periods (expressed in years) and the durations (expressed in hours) of preventive maintenance actions come from the current GRTgaz maintenance policy.

The average repair durations (expressed in hours), the costs of preventive maintenance actions and corrective maintenance actions, the maintenance resources needed to perform preventive maintenance actions and corrective maintenance actions, as well as the form parameters applicable to the Weibull distributions (β) come from expert judgement, based on GRTgaz's expertise.

The maximum number of maintenance resources that can be used at any given time is defined at four maintenance operatives, on the basis of GRTgaz's expertise.

The system downtime cost per time unit was estimated via GRTgaz's expertise.

3.3 *Modelling*

The modelling was carried out in stochastic Petri nets with predicates (Dutuit et al. 1997), using the Petri net module from GRIF software. This TOTAL software is developed by SATODEV (www.satodev.com).

Each maintainable unit was modelled separately. The architecture of the model presented in Figure 2 shows all the "groups" which each contain the model of a maintainable unit as presented in Figure 3.

Places 185 to 188 in Figure 3 make it possible to model the failure of the maintainable unit in question, the detection of said failure, and the associated corrective maintenance action.

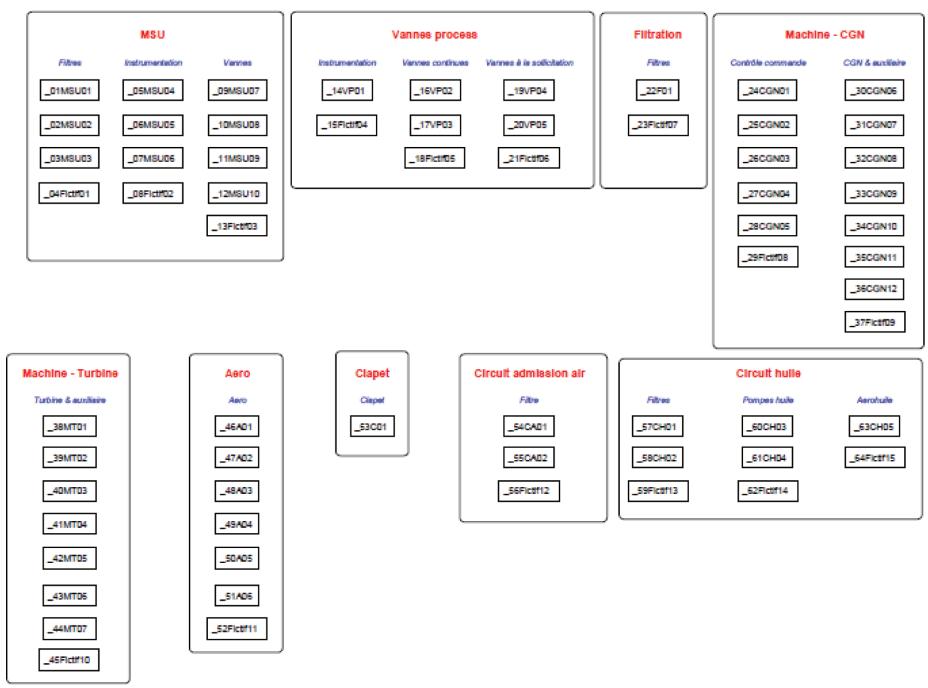


Figure 2. Architecture of the model.

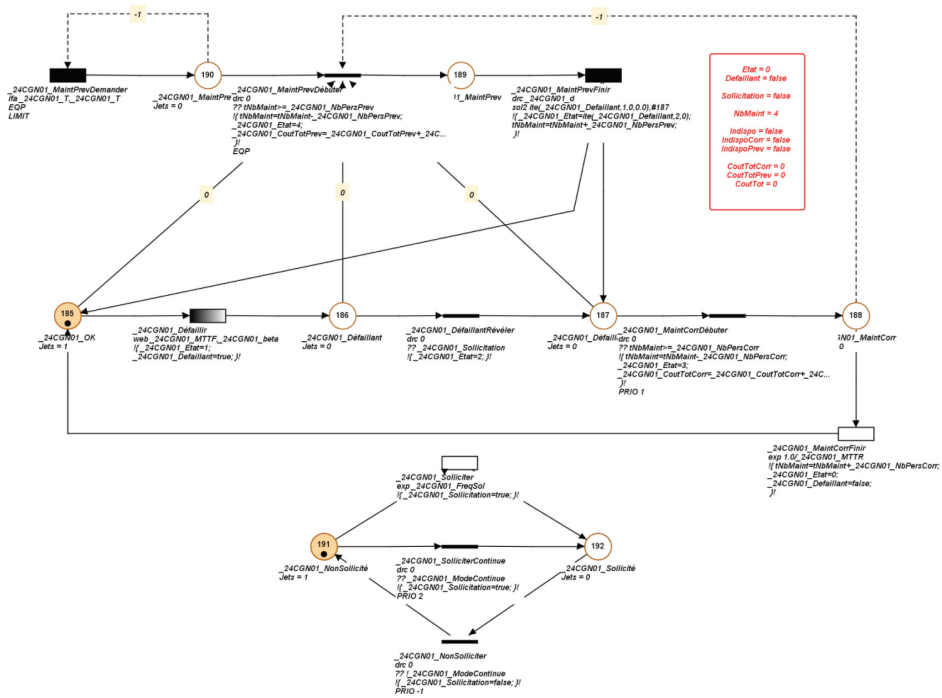


Figure 3. Model of a maintainable unit.

– The failure occurs according to the Weibull law defined in the hypotheses.
– The failure is detected as soon as a demand is placed upon the maintainable unit.
– Lastly, the corrective maintenance action begins as soon as the required maintenance resources are available, and ends according to the duration defined in the hypotheses. During the corrective maintenance action, the number of maintenance resources defined by the hypotheses is subtracted from the number of available resources, then added once the action is terminated. In addition, each time a corrective maintenance action starts, the total cost is increased by the cost defined by the hypotheses.

Places 189 to 190 in Figure 3 make it possible to model the preventive maintenance action of the maintainable unit in question.

– The request for such a maintenance action happens according to the period defined in the hypotheses.
– An "on demand" maintenance action then begins as soon as the required maintenance resources are available, and ends depending on the duration defined in the hypotheses.
– During the preventive maintenance action, the number of maintenance resources defined by the hypotheses is subtracted from the number of resources available, then added once the action is over. In addition, every time a preventive maintenance action begins, the total cost is increased by the cost defined by the hypotheses.

A variable state of the maintainable unit is defined with the following values:

– 0 when the maintainable unit is operational (initial state);
– 1 when the maintainable unit is failing and said failure has not been detected;
– 2 when the maintainable unit is failing and said failure has been detected;
– 3 when the maintainable unit is undergoing corrective maintenance;
– 4 when the maintainable unit is undergoing preventive maintenance;

Accordingly, the maintainable unit is failing when said status variable is not 0 and causes downtime of the sub-system to which it belongs when the status variable is equal to or greater than 2.

It should be noted that a preventive maintenance action may not begin while a corrective maintenance action is in progress. In addition, if a preventive maintenance action begins while the maintainable unit is failing and if said failure is not

detected, then said failure becomes detected once the preventive maintenance action is terminated.

Places 191 to 192 in Figure 3 make it possible to model the demand on the maintainable unit in question. Said demand is permanent in the event of "continuous" demand on the maintainable unit, or it is then defined according to the demand frequency stipulated in the hypotheses.

3.4 *Results*

The results were obtained from 10,000 simulations over an analysis period of 30 years. We can site the following types of results:

- The annual average failure frequency of the entire system;
- The main contributors to failure frequencies;
- The average unplanned downtime percentage of the entire system (due to failures);
- The main contributor to unplanned downtime;
- The average planned downtime percentage of the entire system (due to preventive maintenance actions);
- The main contributor to planned downtime;
- The average total downtime percentage of the system;
- The main contributor to total downtime.

Figure 4 shows the contribution of planned and unplanned downtime to total downtime.

3.5 *Modelling validation*

The simulations carried out on the basis of the Petri net models under the observed reliability and maintenance conditions make it possible to find the availability data observed in the system. This matching between the results of the simulations and the observed availability makes it possible to validate the proposed model.

Based on this model, changes to the preventive maintenance frequencies were made: +50%, +100%, +150%, +200% of the initial period.

In order to evaluate the effects of the maintenance policy modification, different simulations were realised with different values of the β parameter. In addition to the simulations based on the initial values of β, two others sets of simulations considered β+0.5 and β+1. These important values of the β parameter, corresponding to a more important materials ageing, leads to more failures. The different simulations allow the validation of the modelling as the given results confirm experts opinion.

Figure 5 below shows the change in total availability of the system, planned downtime (due to preventive maintenance) and unplanned downtime (due to corrective maintenance) as a function of these various frequencies.

In one hand, a drop in downtime due to preventive maintenance results of the increase in frequencies. In the other hand, the corrective maintenance, and thus the number of failures, increases. These two observations also make it possible to validate the model that restores the expected behaviour of the system.

In term of results, this figure shows also that total downtime remains stable, with the two abovementioned trends cancelling each other out. An increase was also observed in total downtime when preventive maintenance frequencies were doubled. This gives a limit that cannot be exceeded if we wish to maintain the same level of availability while reducing preventive maintenance.

Indeed, the initial results show that preventive maintenance frequencies can be doubled, thus reducing preventive maintenance costs by 50%, while maintaining the same level of system availability. However, a more refined analysis is needed in order to identify the optimum frequency for critical equipment in terms of availability and cost.

As presented here in a global approach, a similar analysis is carried out for each sub-system. The results show that for certain equipment the preventive maintenance reduction margin is less important. A more refined analysis is in progress

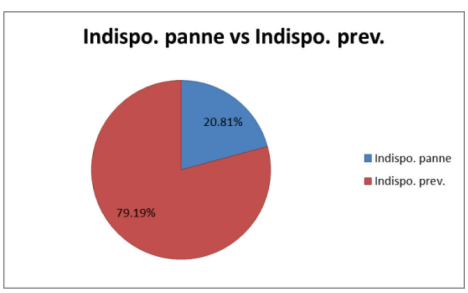


Figure 4. Contribution of planned and unplanned downtime to total downtime.

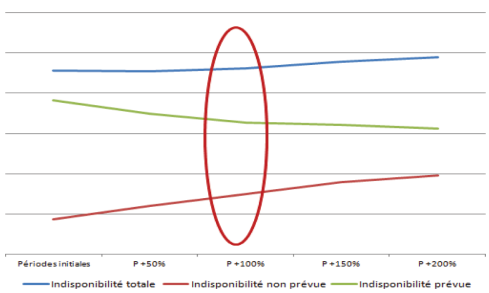


Figure 5. Change in downtime as a function of the frequency of preventive maintenance.

to identify the optimum maintenance frequency for critical equipment. This analysis incorporates the costs related to maintenance and downtime. It is important to note that the sub-systems concerned by safety challenges and for which there are statutory maintenance actions are taken into account in the model, but are not the subject of changes to maintenance policy.

4 CONCLUSIONS

This study made it possible to highly the value of using Petri nets to model an industrial facility. Taking into account the reliability and maintenance characteristics of the system (MTTF, MTTR, preventive maintenance actions, etc.) as well as the organisational constraints on maintenance (number of operators, work priorities, etc.) is essential.

The modelling is possible for a whole system (compressor station), but also for sub-systems (equipment), that makes it flexible.

The simulations based on this model make it possible to compare multiple scenarios on the basis of a group of performance and cost indicators. Consequently, they provide important and reliable decision-making support for maintenance optimisation.

This modelling, already implemented at one station, is being deployed at all GRTgaz stations. The possibility of reusing the model's building blocks and adapting them to the specific data and architecture of each station facilitate and optimise the study duration and cost.

To conclude, this study allowed the improvement of the maintenance approach and gives interesting gains perspectives.

REFERENCES

Dutuit Y., Chatelet E., Signoret J.P., and Thomas P. 1997, Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases, *Reliability Engineering System Safety* 55(2): 117–124.

Lannoy A. 1996, *Analyse quantitative et utilité du retour d'expérience pour la maintenance des matériels et la sécurité*. Paris: Eyrolles.

Lannoy A. & Procaccia H. 2001, *L'utilisation du jugement d'expert en sûreté de fonctionnement*. Cachan: Tec & Doc, Lavoisier.

Lannoy A. & Procaccia H. 2006, *Evaluation de la fiabilité prévisionnelle*. Cachan: Tec & Doc, Lavoisier.

Procaccia H. 2008, *Les fondements des approches fréquentielle et bayésienne*. Cachan: Tec & Doc, Lavoisier.

Procaccia H., Ferton E., Procaccia M. 2011, *Fiabilité et maintenance des matériels industriels réparables et non réparables*. Cachan: Tec & Doc, Lavoisier.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimization of maintenance and operational policies of an offshore wind farm subject to stochastic wind conditions

B. Castanier, C. Pehlivan & T.G. Yeung
École des Mines de Nantes—IRCCyN, Nantes, France

ABSTRACT: Offshore wind power has recently become a highly sought after source of sustainable energy. It consists of the generation of electricity through wind turbine farms located in bodies of water off the coast. While offshore wind farms have the advantage of greater wind availability and not taking up land space, they are also challenging to maintain do to their harsh environment and accessibility issues. We propose a Markov decision process to determine the optimal maintenance and operational policy of an offshore wind farm. The maintenance decision determines which subset of the wind turbines to maintain while the operation decision yields the optimal braking speed of the wind turbine in order to reduce deterioration on the system. Our model takes into account the stochastic wind and weather conditions through both the current conditions and a longer-term forecast in order to reduce the risk of taking wind turbines offline during high production periods. Furthermore, we model the accessibility and maintenance resource issues through a fixed maintenance duration period. The deterioration of the wind turbines is modeled via a stationary gamma process which eliminates the need for a complex physical model or a large amount of historical data. A numerical example is presented to highlight the effectiveness of our model.

1 INTRODUCTION

Offshore wind power has recently become a highly sought after source of sustainable energy. It consists of the generation of electricity through wind turbine farms located in bodies of water off the coast. Wind farms are increasingly proposed offshore as there are higher wind speeds available and they do not take up valuable land space.

In 2013 the wind energy sector in Europe had a production capacity of 117 GW and represented 8% of Europe's electricity consumption, doubling since 2008. This rapid rise is expected to increase even further with a more than tripling of production by 2030 to 25% of the European Union's consumption. Furthermore, all but six European countries generated at least some amount of electricity from wind (European Wind Technology Platform 2014).

In addition to increasing consumption, the key goal of the first ever Strategic Research Agenda and Market Deployment Strategy by TPWind was to significantly reduce the cost of wind energy (European Wind Technology Platform 2014). Given that operating and maintenance costs for wind farms comprise up to 30% of the cost of energy produced (Engels *et al.* 2009), the optimization of maintenance policies is a key factor in helping to realize this goal. Moreover, Van Bussel (1997) states that "a different approach to the maintenance strategy is needed that diverts from the existing practices and a technical re-design for the offshore wind turbines is essential to achieve a financially viable project for offshore wind farms."

Compared to land-based wind farms, offshore production presents several maintenance challenges. First, offshore wind turbines are significantly larger than their land counterparts are not as easily accessible. This creates the need for non-traditional maintenance resources such as cranes attached to vessels, helicopters and dedicated crews (Haddad *et al.* 2010) Furthermore, corrosion is a much greater risk due to the humidity and salinity of the sea or ocean. Secondly, the sea itself imposes constraints due to wave and wind conditions which can render the farm inaccessible for significant periods of time. For these reasons realistic, condition-based maintenance optimization models that take into account the unique features of offshore wind farms in order to help reduce cost and make this sustainable form of energy even more attractive. Therefore, in this paper we propose a new condition-based maintenance and operation optimization model for the entire offshore wind farm that takes into account the aforementioned challenges in order to give managers a clear and robust policy to implement.

2 LITERATURE REVIEW

A conceptual overview of operation and maintenance aspects of large offshore wind farms can be found in Bussel (1997, 2001), Bussel and Handerson (2001), and Bussel (2009).

In more focused work, there have been a few models which take a statistical approach to measure failure data to evaluate the reliability level of several critical components (Andrawus *et al*. 2007, Tavner *et al.* 2006, Guo *et al*. 2009). These models are primarily based on the Weibull distribution to model the failure rate.

Several simulation models also exist for analyzing the behavior of land-based single wind turbines (Tawner *et al*. 2006, Negra *et al*. 2007, Foley and Gutowski 2008) and McMillan and Ault (2008) use Monte Carlo simulation to quantify the cost effective ness of a condition-based maintenance strategy on a wind turbine. There have also been a few works using simulation to evaluate maintenance strategies for offshore wind farms. Rademakers *et al*. (2003) consider corrective maintenance strategies while Jacquemin *et al*. (2007) examined the interdependencies between key parameters of operating and maintenance practices such as transportation means, accessibility methods, and the number of maintenance personnel. Byon *et al*. (2011) investigated via simulation the effect of different maintenance strategies on the reliability of *onshore* wind farms using performance indices such as the number of failures, operating and maintenance costs, and availability. Karyotakis (2011) used variability in various input parameters to predict the performance of a planned intervention maintenance policy. These models do not address simultaneously condition based maintenance strategies for an offshore wind farm.

Finally, there are a few analytical models in the literature that deal with wind turbines. Byon *et al.* (2010) consider use a Markov Decision Process (MDP) to determine the optimal maintenance strategy under stochastic weather conditions. To our knowledge, this is the first mathematical model for wind turbine maintenance; however, it is in a land-based context. Haddand *et al.* (2010) use a MDP based on real options for the availability maximization of an offshore wind farm. This model takes a condition-based maintenance approach to identify the optimal combination of turbines to be maintained in the wind farm. Besnard *et al*. (2011) formulate a stochastic model for opportunistic maintenance planning of offshore wind farms. They use stochastic optimization to optimize the planning of service maintenance activities to take advantage of low wind periods in order to reduce production loss while the turbines are offline. Besnard *et al.* (2013) also consider the optimization for the maintenance support of offshore wind farms such as the location of maintenance accommodations, the number of technicians needed, the choice of transfer vessel, and the use of a helicopter. Finally, Byon (2013) extend their previous work to formulate a more tractable approximation of the dynamic decision making model. The approximation links external (e.g. weather) and internal (e.g., system health) conditions to linear decision rules. The advantages of the decision rules of the static condition-based model were used to derive a new set of decision rules. Improvements were then proposed to make the decision rules more adaptive to rapid changes in weather conditions.

In this paper, we propose a Markov decision process to optimize the optimal maintenance and operational decisions for an offshore wind farm subject to stochastic wind conditions. The maintenance decision consists of a form of selective maintenance to determine which subset of wind turbines, based on their degradation level, to maintain. The operational decision determines the optimal blade speed reduction or braking to use for the online wind turbines. Restricting or reducing the turbine speed will lead to less energy production, but also less deterioration on the system. Furthermore we consider an extended downtime period due to maintenance that takes into account the accessibility and resource issues related to offshore wind farms.

Our model further contributes to the existing literature in several key ways. First, rather than relying on a tremendous amount of historical data to derive a statistical model for the reliability or failure rate of the wind turbines, we present a stochastic process based approach utilizing the stationary gamma process to model the degradation of the wind turbines. This model has the advantage of needing only two parameters to model the degradation.

Byon *et al.* (2010) note that there are three stochastic factors that should be considered when modeling wind turbine maintenance: 1) weather conditions and wind speed, 2) repair interruption and delay, and 3) the long lead time for assembling maintenance crews and obtaining spare parts. Our model considers (1) by incorporating both the current wind speed and long-term wind speed forecast. This allows us to take into account the future weather conditions that will impact energy production should some wind turbines be taken offline for maintenance. We consider points (2) and (3) above through the implementation of a fixed maintenance duration during which the maintained turbines will be offline and unavailable for energy production. Moreover, our analytical MDP formulation considers the network or park of wind

turbines to optimize both condition based maintenance decisions for the farm as well as operational decisions. To our knowledge this is the first model to consider both types of decisions. The simultaneous optimization is valuable as the blade speed has a significant impact on wind turbine degradation as well as energy production output. We are then able to derive an optimal policy of which turbines to maintain and the blade speed of those in operation based on the current state of the wind farm and both current and expected future weather conditions.

3 MODEL FORMULATION

We consider an offshore wind farm comprised of N independent and identical wind turbines, each with a continuous deterioration index X_t. A deterioration index $X_t = 0$ represents a perfectly functioning wind turbine and $X_t \geq L$ represents the failed state (no production of energy). We assume that M different maintenances are available. We define an interval where the maintenance i is applicable by the degradation index interval (x_i, x_{i+1}). Hereafter, we refer to degradation state i such an interval. Let n_i represent the number of wind turbines in degradation state i. We also consider the current average wind speed w.

At each decision epoch we decide what selective maintenance actions to take as well as if any reduction in the wind turbine blade speed should be employed. Let i' be the selective maintenance threshold such that all wind turbines with a degradation state $\geq i'$ will be maintained. The operational decision of the wind turbine speed coefficient ρ denotes the reduction or braking of wind turbine blade speed for all wind turbines in operation where $0 \leq \rho \leq 1$. We assume that the maintenance duration is constant and always last δ time periods. Implicitly, this also assumes that all possible maintenance actions may be completed within δ time periods. δ is considered to be the amount of time necessary to assemble the necessary human and other resource, transport them to the farm, and perform all maintenance necessary. A maintenance cost c_i is incurred for each wind turbine under maintenance in state i as well as a fixed cost γ whenever maintenance is performed. We further assume that any wind turbine in maintenance is not functional during the maintenance period and therefore unable to produce energy. The maintenance action is considered to be "perfect," returning the wind turbine to a state "as good as new" i.e., $i = 0$. Once a maintenance period has begun no new maintenance may be initiated until the current maintenance period has been completed. The decision is given by the combination $D = (i', \rho)$.

In addition to the current average wind speed w, we also consider a wind forecast w_δ which is a long term wind forecast of the expected average wind speed over the next δ time periods. The incorporation of this parameter allows us to the take into account potential loss of energy production during periods of high wind while performing maintenance.

The degradation state space of the wind turbines can be expressed as

$$\bigcup_{i=1}^{M} n_i$$

And the complete system state space as

$$S = \left\{ \bigcup_{i=1}^{M} n_i, w, w_\delta, k \right\}$$

where $k = \{0, 1, \ldots, \delta\}$ is the number of periods remaining in the maintenance duration. $k = 0$ denotes that no maintenance is currently in progress, while $k = \delta$ indicates that maintenance has just begun.

We now present the complete Markov decision process formulation. Let $V(S)$ be the maximum expected discounted cost-to-go over the infinite horizon starting from this state. Then

$$V(S) = \max_{(i',\rho)} \left\{ -MX + PR - PL + \lambda \sum_{S'} p_{s'} V(S') \right\}$$

where

$$MX = \gamma + \sum_{i=i'}^{M} c_i n_i$$

$$PR = \sum_{i=0}^{i'-1} f(w, \rho) n_i$$

$$PL = \sum_{i=i'}^{M} g(w_\delta, \delta) n_i$$

λ is a discount factor, $0 \leq \lambda < 1$ and S' represents all possible future states of the system.

MX represents the maintenance cost. PR is the production reward. The energy production is a function of the wind turbine blade speed and the wind speed and given by the function $f(w, \rho)$ that we suppose is a linear function of the number of wind turbines that are operation. PL is the production loss due to wind turbines in maintenance and is given the function $g(w_\delta, \delta)$ and supposed as a linear function of the number of wind turbines currently offline due to maintenance.

A stationary gamma process is used to model the degradation index of each individual wind turbine. We use the gamma process as a general model of aggregate degradation due to its mathematical convenience and strictly increasing property (Van Noortwijk 2009). We have considered only a general deterioration metric rather than trying to model individual components or failure modes which would lead to an intractability for the complex network problem. By discretizing the process we are able to derive the transition probabilities of a wind turbine moving from state i to state a state $\geq i$. Then, using these individual transition probabilities we can then calculate the transition probabilities of the farm. The transition probabilities of the wind speed and wind forecast are assumed to be exogenous and known *a priori*.

4 NUMERICAL EXAMPLE

As a numerical example, we consider an offshore wind farm of size $N = 5$ and four failure mode levels, $i = \{0, 1, 2, 3\}$. We set the maintenance duration $\delta = 3$, so we therefore have $k = \{0, 1, 2, 3\}$. The maintenance decision is given as $i = \{1, 2, 3, 4\}$; $i = 4$ corresponds to no maintenance being performed. The results are displayed in Table 1. We consider three possible values for the braking factor of the turbines $\rho = \{0, 0.5, 1\}$. This corresponds to a complete stoppage of the turbines, half braking, and no braking, respectively. The maintenance costs used were $\gamma = 10$ and $c_i = \{8, 12, 30\}$. Note that this represents a nonlinear increase in the maintenance cost as the degradation level increases. The experiments were evaluated under three possible levels of current wind conditions $w = \{1, 2, 3\}$ and two wind forecasts $w_\delta = \{1, 2\}$.

For the energy production we choose a simple linear function

$$f(w, \rho) = 2w\rho$$

where 2 is an energy production coefficient. Similarly, the energy loss function is a simply a function of the wind forecast

$$g(w_\delta) = w_\delta.$$

We solve for the optimal policy using value iteration with $\lambda = 0.99$.

The transition probabilities were generated using a stationary gamma process with shape function parameters 2 and 1 and scale parameter equal to 10. The degradation indices were defined as $x_i = \{0, 2, 3, 5\}$. In order to simplify the evaluation of the stationary law, we assumed $\rho = 0.8$ as the average braking.

Table 1. Maintenance (Mx) decisions.

n_0	n_1	n_2	n_3	w	w_δ	Mx (i)	ρ
0	0	0	5	1	1	3	1
1	0	0	4	1	1	3	1
1	0	1	3	1	1	2	1
0	0	5	0	1	1	2	1
0	0	4	1	1	1	2	1
0	0	3	2	1	1	2	1
0	0	2	3	1	1	2	1
0	0	1	4	1	1	2	1
0	1	3	1	1	1	1	1
0	1	2	2	1	1	1	1
0	1	1	3	1	1	1	1
0	1	0	4	1	1	1	1
0	0	0	5	2	1	3	1
1	0	0	4	2	1	3	1
0	0	4	1	2	1	2	1
0	0	3	2	2	1	2	1
0	0	2	3	2	1	2	1
0	0	1	4	2	1	2	1
0	1	2	2	2	1	1	1
0	1	1	3	2	1	1	1
0	1	0	4	2	1	1	1
0	0	0	5	3	1	3	1
1	0	0	4	3	1	3	1
0	0	3	2	3	1	2	1
0	0	2	3	3	1	2	1
0	0	1	4	3	1	2	1
0	2	1	2	3	1	1	1
0	2	0	3	3	1	1	1
0	1	2	2	3	1	1	1
0	1	1	3	3	1	1	1
0	1	0	4	3	1	1	1

For the numerical results, we first analyze the maintenance decisions which are presented in Table 1. Note that Table 1 only shows those states and wind conditions in which maintenance (Mx) is prescribed. The complete policy is much too large to present in its entirety. We see from the table that both preventive ($i = 1, 2$) and corrective ($i = 3$) actions are taken by the model and that maintenance is only prescribed when the wind forecast is low. Generally, we find that maintenance is performed when there are only one or less wind turbines in perfect condition ($n_0 \leq 1$) or where $n_2 + n_3 \geq 4$. We also only see corrective maintenance performed when all or almost all of the wind turbines are failed.

The results also seem to indicate a threshold policy. We see that no maintenance is performed if $n_0 \geq 2$ or $n_1 \geq 2$. Interestingly, maintenance is still not prescribed at $n_1 \geq 2$ even when $n_0 = 0$.

Finally, we see that maintenance decisions are much more sensitive to the wind forecast than the current wind conditions. As noted we only

see maintenance when the wind forecast is low, however we do not see a significant change in the policy between different current wind conditions. The braking decisions, however, are sensitive to the current wind conditions.

We now analyze the braking decisions for the wind turbines. We see in Table 1 that at the beginning of the maintenance period, no braking is ever employed in the farm. This is intuitive as remaining wind turbines should be in sufficient condition such that braking is not warranted. Table 2 shows the portion of the policy where $\rho = 0.5$. Note that there is no maintenance prescribed here for any of these cases. This only occurs at the highest wind level ($w = 3$), but may be with either a high or low wind forecast.

Table 2. Turbine braking decisions.

n_0	n_1	n_2	n_3	w	w_δ	Mx (i)	ρ
5	0	0	0	3	1	4	0.5
4	1	0	0	3	1	4	0.5
4	0	0	1	3	1	4	0.5
3	2	0	0	3	1	4	0.5
3	1	0	1	3	1	4	0.5
3	0	0	2	3	1	4	0.5
2	3	0	0	3	1	4	0.5
2	2	1	0	3	1	4	0.5
2	2	0	1	3	1	4	0.5
2	1	0	2	3	1	4	0.5
1	4	0	0	3	1	4	0.5
1	3	1	0	3	1	4	0.5
1	3	0	1	3	1	4	0.5
1	2	0	2	3	1	4	0.5
0	5	0	0	3	1	4	0.5
0	4	1	0	3	1	4	0.5
0	4	0	1	3	1	4	0.5
0	3	0	2	3	1	4	0.5
5	0	0	0	3	2	4	0.5
4	1	0	0	3	2	4	0.5
4	0	0	1	3	2	4	0.5
3	2	0	0	3	2	4	0.5
3	1	0	1	3	2	4	0.5
3	0	0	2	3	2	4	0.5
2	3	0	0	3	2	4	0.5
2	2	1	0	3	2	4	0.5
2	2	0	1	3	2	4	0.5
2	1	0	2	3	2	4	0.5
1	4	0	0	3	2	4	0.5
1	3	1	0	3	2	4	0.5
1	3	0	1	3	2	4	0.5
1	2	0	2	3	2	4	0.5
1	1	0	3	3	2	4	0.5
0	5	0	0	3	2	4	0.5
0	4	1	0	3	2	4	0.5
0	4	0	1	3	2	4	0.5
0	3	1	1	3	2	4	0.5
0	3	0	2	3	2	4	0.5
0	2	0	3	3	2	4	0.5
0	1	0	4	3	2	4	0.5

There are many other possible states in which no maintenance is prescribed, and due to space limitations it is not possible to list them all. However, we can summarize our findings on the braking policy as a function of w and k. For low and medium wind levels ($w = 1, 2$) no braking is ever utilized by the model. Braking to half speed ($\rho = 0.5$) may be employed when $w = 3$ as noted in Table 2. The results do not show a strong sensitivity of the braking policy to the wind forecast.

In general, we find that the model proposes braking in states when there is a small number of functioning wind turbines in the farm, regardless of their degradation level, and also when the functioning wind turbines are highly degraded, regardless of the number of wind turbines in operation.

An interesting numerical result is the relationship between ρ and k. We find that as k decreases (i.e., as the maintenance duration becomes closer to completion), ρ also decreases. For example, when $k = 3, 2$, the model suggests half braking when $w = 3$ in order to keep the operating wind turbines functioning longer, however when $k = 1$ the model mostly proposes full braking (i.e., stopping the wind turbines). One would intuitively expect braking to decrease as the opportunity for maintenance becomes closer, but the model suggests otherwise. This could perhaps be due to the non-linear jump in maintenance cost for higher degradation levels. The model is choosing to stop the wind turbines rather than face a very high maintenance cost if they are further degraded.

5 SUMMARY AND CONCLUSIONS

We have formulated a Markov decision process model to jointly optimize the maintenance and operational decisions of an offshore wind turbine farm. We have incorporated many key aspects of this problem including extended maintenance durations and changing wind conditions.

Our model provides farm managers with an easy to implement policy based on the condition of the park while taking into account the evolution of degradation and both current and future wind conditions. Understanding the maintenance policy in relationship to the state of the farm can help managers to anticipate upcoming maintenance actions and therefore ensure that the necessary resources are in place. Furthermore, incorporating the breaking decisions allows extending the life of the turbine before maintenance is needed. Providing a tool to manage such a complex system of systems well help to reduce maintenance and

operating costs and allow offshore wind energy to become a more viable alternative in the future.

The optimal policy of our model seems to have appealing structure and it would be interesting to investigate this further to demonstrate the existence of various threshold or control-limit policies. We would also like to emphasize that this is a preliminary work to gain an initial understanding on the impact of various factors on the optimal policy. We have provided a small-scale numerical example and understand that, as always with dynamic programming, the curse of dimensionality comes into play as the size of the farm grows. The development of more efficient algorithms or heuristics, that perhaps take advantage of the policy structure, will be needed in evaluating real world offshore wind farms.

REFERENCES

Andrawus et al., 2007. Wind Turbine Maintenance Optimisation: principles of quantitative maintenance optimisation. *Wind Engineering*, Volume 31, Number 2, March 2007, pp. 101–110.

Besnard, F. Patriksson, M., Stromberg, A., Wojciechowksi, A, Fischer, K., Bertling L., 2011. A stochastic model for opportunistic planning of offshore wind farms. Proceedings of *2011 IEEE Trondheim PowerTech*.

Besnard, F.; Fischer, K.; Tjernberg, L.B., 2013. A Model for the Optimization of the Maintenance Support Organization for Offshore Wind Farms, Sustainable Energy, IEEE Transactions on, vol. 4, no. 2, pp. 443, 450, April 2013.

Byon, E., Ntaimo, L, Ding, Y., 2010. Optimal maintenance strategies for wind turbine systems under stochastic weather conditions. *IEEE Transactions on Reliability*, 59(2): 393–404.

Byon, E., 2013. Wind turbine operations and maintenance: a tractable approximation of dynamic decision making, *IIE Transactions*, 45:11, 1188–1201.

Engels, W., Obdam, T., and Savenije, F., 2009. ICurrent Developments in Wind, ECN Tech. Rep. ECN-E-09-96.

European Wind Technology Platform, 2014. Strategic Research Agenda/Market Deployment Strategy. http://www.windplatform.eu/.

Foley, J.T., Gutowski, T.G., 2008. TurbSim: Reliability-based wind turbine simulator. Electronics and the Environment, 2008. ISEE 2008. IEEE International Symposium on, vol., no., pp. 1, 5, 19–22 May.

Guo, H. et al., 2009. Reliability analysis for wind turbines with incomplete failure data collected from after the date of initial installation. *Reliability Engineering and System Safety*, version 94, pp. 1057–1063.

Haddand, G., Sandborn, P., Pecht, M., 2010. A real options optimization model to meet availability requirements for offshore wind turbines. http://www.prognostics.umd.edu/.

Jacquemin J. et al., 2007. Multi-dimensional optimisation of O&M provision for offshore wind projects. European Offshore wind conference. Operation and maintenance session. Berlin 2007.

Karyotakis, A., 2011. On the optimization of operation and maintenance strategies for offshore wind farms. Ph.D. Thesis.

McMillan and Ault, 2008. Specification of Reliability Benchmarks for Offshore Wind Farms. Proceedings of European Safety and Reliability, Valencia September 2008.

Negra N. et al., 2007. Aspects of relevance in offshore wind farm reliability assessment. IEEE transactions on energy conversion, vol. 22, no. 1, March 2007.

Rademakers et al., 2003. Assessment and optimisation of operation and maintenance of offshore wind turbines. Proceedings of the European Wind Energy Conference in Madrid. Report ECN WIND: ECN-RX--03-044.

Tavner, X. and Spinato, 2006. Reliability analysis of wind turbines. Wind Energy in press. DOI: 10.1002/we.204. Published online by Wiley Interscience, John Wiley and Sons 2006.

Van Bussel G., 1997. Operation and Maintenance Aspects of Large Offshore wind farms. Proceedings of the 1997 European Wind Energy Conference, Dublin, Ireland. pp. 272–279.

Van Bussel, G. and Zaaijer, M. 2001. Reliability, Availability and Maintenance aspects of large-scale offshore wind farms, a concepts study. Proceedings of MAREC (Marine Renewable Energy Conference). Newcastle, UK.

Van Bussel, G. and Henderson, A., 2001. State of the art and technology trends for offshore wind energy: Operation and Maintenance issues. Delft University of Technology, Part of the CA-OWEE project.

Van Noortwijk, J.M., 2009. A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety*, 94(1): 2–21.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An age-based preventive maintenance for offshore wind turbines

F.P. Santos, A.P. Teixeira & C. Guedes Soares
Centre for Marine Technology and Engineering (CENTEC), Instituto Superior Técnico, Universidade de Lisboa, Portugal

ABSTRACT: In this paper a strategy is presented for combining corrective maintenance replacements with age-based imperfect preventive maintenance repairs. Preventive maintenance actions are performed considering the components' age thresholds and an age reduction ratio, q. An offshore wind turbine consisting of several degraded components is considered. Failure models are based on onshore ones and derived through an empirical approach based on stress factors for mechanical systems. Generalized Stochastic Petri Nets with predicates and Monte Carlo simulation are used to model and simulate operation and maintenance activities considering logistic resources, times and costs, and weather constraints. A preventive maintenance repair cost function dependent on the age reduction effort, q, and on the age of the components is proposed and compared with an age independent cost function, in terms of their effect on the operation and maintenance costs and revenues.

1 INTRODUCTION

The Operation and Maintenance (O&M) of offshore wind farms faces more challenges than the onshore one given that the harsher offshore conditions limit, for example, the accessibility for routine servicing and maintenance. Even in favourable weather conditions, the O&M activities are still more costly than in onshore as they are influenced by the offshore distances, site exposure, wind farm size, wind turbine reliability and maintenance strategies. Moreover, offshore O&M tasks need special lifting equipment for the installation or change of major turbine components, which are not always available at short notice. Thus, for some European offshore wind farms the cost of energy is approximately 33% more than in onshore installations (Tavner 2012) and the O&M costs which are major contributors to the cost of energy can reach up to 30% of such cost (Nielsen & Sørensen 2011).

The Corrective Maintenance (CM) is widely used but as a reactive approach does not prevent costly repairs or replacements. This is a general problem (Guedes Soares et al. 2010) but in the offshore context failures often occur during seasons of the year when the accessibility to the turbine is limited due to the weather conditions leading to production losses (Nielsen & Sørensen 2011). In contrast, Preventive Maintenance (PM) can be planned in time so that the risk of major failures and downtimes is minimized and, the logistics and maintenance costs along with the system operability are optimized.

When modelling the maintenance and optimization of complex and real systems one is faced with the challenge of capturing the realistic aspects of a system's performance and the dynamics of the interactions among numerous subsystems or components (Guedes Soares et al. 2010, Zio et al. 2009). Simulation approaches are often essential for such purpose even when dealing with condition monitoring (Barata et al. 2002), which is being considered also for wind turbines (Van Horenbeek et al. 2013).

The offshore wind energy industry is quite recent not having reached the maturity of other industries such as the one of oil and gas production. Consequently, there has been a need to develop and adapt specific maintenance strategies for optimization, even though such strategies are broadly used in many fields.

In this paper a maintenance strategy combining CM replacements with age-based imperfect PM repairs is modelled and assessed. The PM is performed when the repair threshold age of the components is equalled or exceeded. A PM repair cost function having an age reduction ratio, q, and the age of the components as parameters is proposed. This is compared with an age independent cost function—already used in the literature (Ding & Tian 2012)—in terms of the effect on the O&M costs and revenues of an offshore wind turbine.

Four degraded components of the wind turbine are considered. The failure models are based on onshore ones and derived using an empirical approach based on stress factors for mechanical systems. Generalized Stochastic Petri Nets (GSPN)

and Monte Carlo Simulation (MCS) are used to model and simulate the O&M activities and the dynamics of the interactions between components considering the logistics, times and costs, and weather constraints.

2 LOGISTICS AND WEATHER CONSTRAINTS

A set of four components, rotor, gearbox, generator and pitch system of a 5 MW offshore wind turbine is considered for maintenance modelling and simulation. The turbine is located in a North Sea wind farm about 45 km from German shore. A capacitor factor of 50.8% has been reported by Lindoe (2011).

According to the International Energy Agency (2012), the German tariff for wind energy produced by offshore wind turbines is €0.15/kWh (€150/MWh) and is the reference value considered in the present study.

Three different maintenance categories based on Rademakers & Braam (2002) are used depending on the weight (BVG associates) of the component being replaced (CM) or repaired (PM), thus according to the vessel involved as is shown in Table 1.

The supply vessel is the only one docked at the harbour and used to perform PM actions. It transports a maintenance crew of 4 technicians and spares up to 1 ton [t] such as the pitch system. The maintenance crew has a 12 hour shift per day, 7 days a week, which includes the travelling times to and from the turbine when is to be maintained. Besides, it can start at any time of the day as long as all the logistics are available and there is a weather window allowing the performance of a full maintenance action.

At each maintenance, the sailing of the supply vessel with the maintenance crew is done every day up to its ending. This is valid for all maintenance categories. On the other hand, the jack-up and crane vessels stay at the turbine location. The supply vessel is set to arrive at the turbine at the same time as the jack-up or the crane vessel, so that the maintenance team can start working immediately.

Table 1. Maintenance categories.

	Turbine's components			
Categories (vessels)	Gearbox ≤ 65[t]	Generator ≤ 20[t]	Pitch syst. ≤ 1[t]	Rotor 90–150[t]
Supply	PM	PM	PM, CM	PM
Crane	CM	CM		
Jack-up				CM

The velocity values of each vessel and respective travelling times from the harbour to the turbine are shown in Table 2.

The times larger vessels take to arrive at the harbour and the delay for a spare pitch system to be available are presented in Table 3. The values of Table 2 and Table 3 are based on Rademakers & Braam (2002).

The costs of the turbine's components presented in Table 4 are approximate values retrieved from an offshore wind farm guide (BVG Associates) on 5 MW turbines. The cost of transporting a spare from the manufacturer to the harbour is assumed to be included in the components' unit cost.

The costs associated with the vessels and maintenance technicians are in Table 5, being approximate values based on Rademakers & Braam (2002).

Table 2. Velocity and traveling times of each vessel.

Vessel	Velocity [knots]/[kmh^{-1}]	Travelling time (one way) [h]/[day]
Supply	10.8/20	2.25/0.09
Crane	8.1/15	3.0/0.13
Jack-up	5.4/10	4.5/0.19

Table 3. Vessels' logistic times.

Maintenance category	Logistic time [h]/[day]
Supply	48/2
Crane	160/6.67
Jack-up	504/21

Table 4. Cost of components.

Component	Cost/unit [€]
Gearbox	863,000
Generator	247,000
Pitch system	123,300
Rotor	1,849,000

Table 5. Hourly rates and mobilization costs.

	Cost [€]
Supply vessel (hourly rate)	600
Crane vessel	
Hourly rate (0.04 days)	6250
Mobilization/demobilization	45,000
Jack-up vessel	
Hourly rate	6250
Mobilization/demobilization	57,000
Technician (hourly rate)	70

Table 6. Probabilities of weather windows and waiting times.

Season	Weather window probability	Waiting time for a weather window [day]
Winter	0.30	60
Autumn	0.50	30
Spring	0.60	10
Summer	0.80	3

The probabilities of occurrence of weather windows, i.e. of wind speed and significant wave heights within the O&M limits, and the waiting times for such windows (i.e. when weather conditions are over the O&M limits) to perform maintenance actions are given in Table 6 for each season of the year. These values are merely illustrative examples and do not represent real data statistics, which can be obtained only from real weather data when available.

3 STRESS FACTORS AND FAILURE MODELS

Offshore wind turbines endure higher stresses than onshore wind turbines such as environmental and power utilizations ones, due to being located in the marine environment. Thus, they experience higher failure rates (Karyotakis & Bucknall 2010) and for this reason onshore failure distributions are not adequate for modelling the behaviour and performance of an offshore wind turbine. However, there is a lack of available reliability data of offshore wind turbines (Karyotakis & Bucknall 2010), in fact only a few field data exists in the public domain (Tavner 2012). Consequently, power rating and environmental stress factors for mechanical systems (Davidson 1994) are considered in the present study as an empirical approach to derive failure distributions for the offshore wind turbine components from the typical onshore failure models (Ding & Tian 2012) of Table 7.

The "failure" in this context refers to the component's loss of function that leads to its replacement.

Failures rates of components of onshore wind turbines were used by Karyotakis & Bucknall (2010) in a reliability model based on stress factors for mechanical systems (Davidson 1994) to estimate a range of failure rates for offshore wind turbines. To do so, one has to assume that both onshore and offshore wind turbines are of the same type and also account for the higher environmental and power utilization stresses that offshore wind turbines are subject to (Karyotakis & Bucknall 2010).

Table 7. Failure parameters of onshore turbine components.

Component	Distribution	Scale parameter α [day]	Shape parameter β
Rotor	Weibull	3000	3
Gearbox		2400	3
Generator		3300	2
Pitch		1858*	3

*Parameter derived from Ribrant (2006) and Durstewitz (2005).

According to Davidson (1994) the reliability model is based on the linear Equation 1.

$$\lambda_{offshore} = \lambda_{onshore} \cdot (K_1 \cdot K_2) \cdot p(A) \quad (1)$$

where one has the following:

- $\lambda_{offshore}$ is the estimated offshore wind turbine failure rate for failure mode A;
- $\lambda_{onshore}$ is the failure rate of the system subjected to ideal conditions of minimal stresses (e.g. onshore);
- K_1 and K_2 are the environmental and power utilization stress factors, respectively. They represent the different conditions in which a system is used. In offshore conditions, they refer to the influence of weather and marine environment and, the effect of different operating power ranges on the reliability of the offshore wind turbine;
- $p(A)$ is a measure of the failure rate's proportion for failure mode A of the system. In this case, only a failure rate and failure mode is considered for each component and therefore $p(A) = 1$.

The empirical values of the environmental and power rating stress factors for mechanical systems (Davidson 1994) are shown in Tables 8 and 9, respectively.

The four components of the turbine are considered to be *marine, sheltered*, i.e. are within the nacelle but not exposed to the marine environment directly. Accordingly, $K_1 = 1.5$.

The values of Table 9 are graphically represented in Figure 1. The trend line shows that K_2 increases exponentially as a component rating is increased over its nominal rating.

The power rating stress factor represents the possible effect of different operation power ranges on the reliability of a wind turbine. Given that an offshore turbine is subjected to higher winds than an equivalent onshore one the percentage of power available relatively to the turbine's nominal rating is higher. Therefore, K_2 can be considered

Table 8. Environmental stress factors for mech. systems.

General environmental conditions	Environmental stress factor K_1
Ideal, static conditions	0.1
Vibration free, controlled conditions	0.5
General-purpose, ground-based	1
Marine, sheltered	1.5
Marine, exposed	2
Road	3
Rail	4
Air	10
Missile	100

Table 9. Power rating stress factors for mechanical systems.

Percentage of component nominal rating	Power rating stress factor K_2
140	4
120	2
100	1
80	0.6
60	0.3
40	0.2
20	0.1

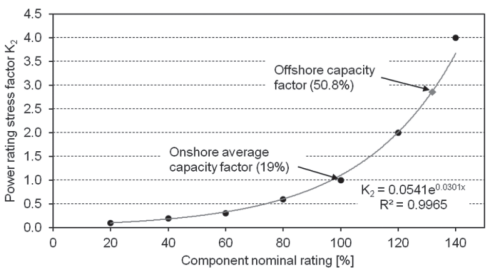


Figure 1. Power rating stress factor vs. component nominal rating [%].

as dependent on the capacity factor of a turbine. Consequently, the power rating stress factor of an offshore wind turbine can be calculated from the capacity factor of a specific installation. Moreover, K_2 when applied to failures rates accounts for the difference in the capacitor factors between offshore and onshore wind turbines (Karyotakis & Bucknall 2010; Karyotakis 2011).

By the end of 2011 the average capacity factor of wind turbines in Germany was 19% for a total of 29,075 MW of installed wind capacity of which 200 MW were offshore. The total number of turbines was 22,297 and of the 55 offshore wind turbines installed 33 were only connected to the grid in December of 2011 (International Energy Agency 2012). Therefore, it is reasonable to consider 19% as the onshore average capacity factor. Considering this value for onshore wind turbines and that it is assumed to represent 100% of component nominal rating, it can be seen in Figure 1 that $K_2 = 1$. Additionally, assuming 50.8% as the equivalent offshore wind turbine capacity factor, and inserting the value 50.8% – 19% + 100% = 131.8% in the exponential equation of Figure 1 one gets $K_2 = 2.86$.

Karyotakis & Bucknall (2010) consider constant failure rates in Equation 1 while in the present paper the failure rates of the components increase with time, following two-parameters Weibull distributions. Thus, substituting $\lambda_{onshore}$ in Equation 1 by the expression of a Weibull failure rate one obtains Equation 2.

$$\lambda_{offshore} = \frac{\beta_{onshore}}{\alpha_{onshore}}\left(\frac{t}{\alpha_{onshore}}\right)^{\beta_{onshore}-1} \cdot K_1 \cdot K_2 \qquad (2)$$

Having only one equation (i.e. Equation 2) for two parameters (α and β) it is assumed that one parameter has to be kept the same for onshore and offshore turbines. Consequently, taking as example the failure model of the rotor (see Table 7) for which the Mean Time To Failure (MTTF) is 7.34 years, a variation of –10% in the shape parameter, β, yields a MTTF of 7.31 years, whereas the same variation in the scale parameter, α, returns a MTTF of 6.61 years. In other words, the reliability distribution of a degraded component is more sensitive to variations in the values of α than to the variation of β. Therefore, considering the same β for onshore and offshore failure models, Equation 2 turns into Equation 3.

$$\frac{\beta \cdot t^{\beta-1}}{\alpha_{offshore}^{\beta}} = \frac{\beta \cdot t^{\beta-1}}{\alpha_{onshore}^{\beta}} \cdot K_1 \cdot K_2$$
$$\Leftrightarrow \frac{1}{\alpha_{offshore}^{\beta}} = \frac{K_1 \cdot K_2}{\alpha_{onshore}^{\beta}} \qquad (3)$$

Solving for $\alpha_{offshore}$ and substituting K_1 and K_2 by the previously obtained values one gets Equation 4.

$$\alpha_{offshore} = \frac{\alpha_{onshore}}{(K_1 \cdot K_2)^{\frac{1}{\beta}}} = \frac{\alpha_{onshore}}{4.29^{\frac{1}{\beta}}} = 4.29^{-\frac{1}{\beta}} \cdot \alpha_{onshore} \qquad (4)$$

Using Equation 4 with each of the components' failure models of Table 7 one obtains, according to the stress factors' approach, the failure distributions of the same components but for

Table 10. Failure parameters of the offshore turbine components.

Component	Distribution	Scale parameter α [day]	Shape parameter β
Rotor	Weibull	1847	3
Gearbox		1477	3
Generator		1594	2
Pitch		1144	3

the equivalent offshore wind turbine as shown in Table 10.

4 O&M STRATEGY

The O&M strategy consists of CM and PM actions. The CM tasks entail only unplanned replacements whereas PM activities are age-based and imperfect, being performed considering an age reduction ratio, q ($0 < q < 1$) when the age of a component is equal to or larger than some predefined time $p \times MTTF$, where $0 < p < 1$. The component after PM is therefore q younger, i.e. the age is reduced by q percent. The value, p, is a preventive repair threshold parameter which is the same for all components.

The age of a component after a maintenance action is given by Equation 5.

$$Age_i = \underbrace{\left[t_i - t_{i-1} + Age_{i-1}\right]}_{Age_i^{acc}} \cdot (1-q) \tag{5}$$

where Age_i and Age_{i-1} are the component's consecutive ages after the ith and $i-1$th maintenance tasks, respectively; Age_i^{acc} is the age at the beginning of the ith maintenance action, accumulated from the $i-1$th maintenance task; t_i and t_{i-1} are the calendar times at the beginning of the ith and at the end of the $i-1$th maintenance actions, respectively. The CM is always perfect since it replaces the component by a new one (as if $q = 1$), thus $Age_i = 0$. Since the age reduction effort is $0 < q < 1$ then all PM are imperfect repairs.

The CM is performed when necessary whereas PM is carried out only in the summer given to more favourable weather conditions, thus higher accessibility to the turbine. A PM is performed when Equation 6 is valid.

$$t_i - t_{i-1} + Age_{i-1} \geq p \cdot MTTF \tag{6}$$

Notice that t_i is a summer calendar time. The failure distributions and, repair and replacement times of the components are considered to be independent.

Ding & Tian (2012) used the age reduction ratio, q, for the opportunistic maintenance of an onshore wind farm, considering the cost of the imperfect maintenance actions as a function of q^2 times a variable preventive replacement cost plus a fixed maintenance cost. In the present paper each PM is stochastically driven so no fixed maintenance cost is considered. Although the maintenance cost function, Equation 7, is also based on q it additionally increases, however, as the age of the component increases at each PM.

$$C_M = \begin{cases} q^{\frac{MTTF}{Age_i^{acc}}} \cdot C_r & 0 < q < 1 \ \wedge \ Age_i^{acc} > 0 \\ 1 & q = 1 \ for \ CM \Rightarrow Age_i = 0 \end{cases} \tag{7}$$

where C_r is the cost of a new component (see Table 4).

Figure 2 shows the plot of the maintenance cost function in terms of the age reduction effort q and of the age of a component, Age_i^{acc}, at the beginning of a PM and accumulated from the previous maintenance task. The PM cost (in terms of C_r) for a fixed q increases with the age of the component, i.e. it is reasonable to consider that putting the same effort on PM actions, say $q = 50\%$, to improve the condition of a component with an age of 100% of its MTTF is more costly than if its age were to be 75% × MTTF. Thus, a component which is aging even with consecutive PM has increasing maintenance costs. Also, it may be as preventively costly to slightly reduce the age of an old component as significantly improving its condition when it is much younger.

The effective duration times of the CM replacements and PM repairs follow exponential and

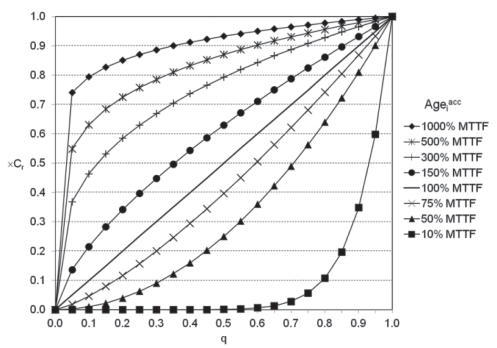


Figure 2. Effect of age and reduction effort on the PM cost.

Table 11. Distributions' parameters of the effective duration of CM and PM actions.

Maintenance category	CM (exponential)	PM (lognormal)	
	λ [day^{-1}]	MTTR [day]	St. dev. [day]
Supply	2.381	0.420	0.126
Crane	0.481	2.079	0.624
Jack-up	0.599	1.669	0.501

lognormal distributions, respectively. Their parameters are given in Table 11 for each maintenance category.

The logistics, weather constraints and the O&M tasks are modelled and simulated using Generalized Stochastic Petri Nets with predicates and Monte Carlo simulation. The q and age dependent cost function for PM repairs (Equation 7) is compared with the q^2 cost function in terms of the effect on the turbine's O&M costs and revenues.

5 GENERALIZED STOCHASTIC PETRI NETS MODEL

Petri nets are a tool that combines graphical with mathematical modelling to analyse discrete event systems. They are adequate to represent the dynamics and behaviour of systems and its maintenance, providing performance outputs (Zio 2009). The GSPN with predicates coupled with MCS are a recent extension of Petri nets and have been proven to be powerful and efficient in modelling the complexity of real systems (Dutuit et al. 1997, 2008, Santos et al. 2012, 2013a, b). The transitions of the GSPN can fire stochastically and deterministically. The predicates can be guards or assignments. The first are preconditions to enable or inhibit the transitions while the second are post-condition messages to update variables when a transition fires. Not to be too extensive, only the GSPN of the PM of the rotor presented in Figure 3 is briefly explained.

The rotor imperfect PM is performed only in the summer, if it is functioning (i.e. *??Rotor_avail*==1 is *true*) and its age is equal to or larger than the predefined age $p \times MTTFrotor$ (i.e. when the *if then else PerformRotor_PM=ite((time()-max(Rotor_lastCM, Rotor_lastPM)+Rotor_age)>=(p×Rotor_MTTF), true,false)*). If so, and the supply vessel is on standby along with the maintenance crew and no other component is in replacement/repair a weather window is generated. Meanwhile, if the rotor fails or the summer ends the PM is aborted (i.e. *NoRotorPM* fires).

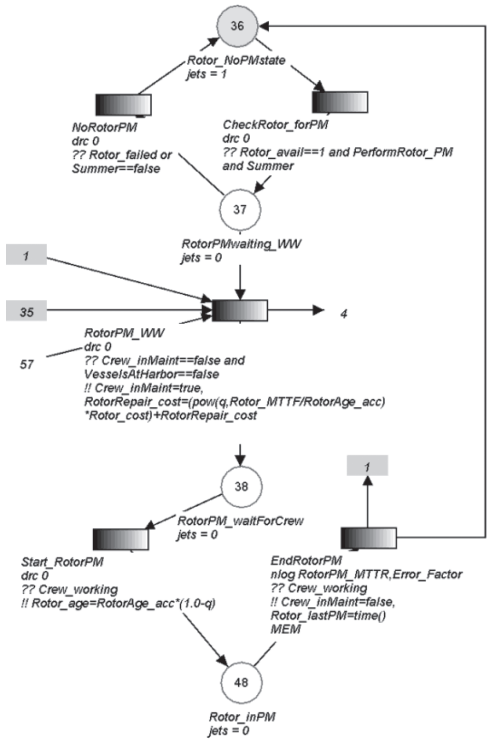


Figure 3. GSPN model of the rotor's PM.

Given that an age reduction ratio, q, is used the rotor's age after the PM is $1 - q$ times its accumulated age since the last maintenance, i.e. $Rotor_age = RotorAge_acc \times (1.0\text{-}q)$ and the accumulated repair cost is $RotorRepair_cost = (pow(q, Rotor_MTTF / RotorAge_acc) \times Rotor_cost) + RotorRepair_cost$ (see Equation 7). The stochastic law of the repair time is lognormal as shown in the transition *EndRotorPM*.

6 RESULTS

To begin with, a convergence analysis of the MCS was performed on the GSPN model considering all of the relevant statistics. The simulations were of 10,950 *days* (i.e. 30 *years*). The convergence of the statistics was achieved when the variation of their values was equal to or less than 0.1%. This occurred when increasing the number of simulations from 9000 to 15,000.

For simplification purposes the models with the q and age dependent, and q-dependent cost functions will be referred from now on as *q^age* and *q^2*, respectively. They were compared in terms of the effect on the turbine's O&M costs and revenues.

For such, a fixed $q = 0.4$ and a set of p-values ranging from 0.1 to 0.9 in steps of 0.1 were considered. The total simulation times were 4.02 and 4.58 minutes for the models with q^2 and q^*age* cost functions, respectively.

Figure 4 shows the mean CM costs incurred with the replacements: new components, mobilizations and demobilizations of the larger vessels (i.e. crane and jack-up), their times at the harbour, going to and staying at the turbine, and to demobilize. The second curve is related with the turbine mean loss of production. The other curve represents the supplier vessel and maintenance crew mean costs due to the CM and PM actions. Since what drives such costs are the failure and repair rates, the logistic times and weather constraints, which are common to both models and do not result from the q^*age* and q^2 cost functions, the models have the same mean costs (i.e. curves).

As the preventive repair threshold parameter, p, is increased until 0.9, the mean times between PM get larger. Accordingly, the failure rates increase giving rise to more failures, thus increasing the mean CM costs as shown in Figure 4. Moreover, the mean costs with the supplier vessel and maintenance crew used in the CM and PM tasks decrease, since the drop in the mean number of PM is larger than the increase in the mean number of CM. However, the rate at which these CM and PM costs decrease is lower than that of the increasing CM costs given that the supplier and crew hourly costs are much smaller than the replacements, but specially than the hourly costs of the larger vessels. Finally, the loss production costs due to the turbine unavailability decrease until $p = 0.5$, stabilizing after that, mainly due to the reduction in the mean number of PM actions.

The q^2 and q^*age* cost functions have only effect on the mean PM repair costs (see Equation 7) as shown in Figure 5.

Considering that the age reduction ratio, q, has a fixed value the mean cost of each PM repair,

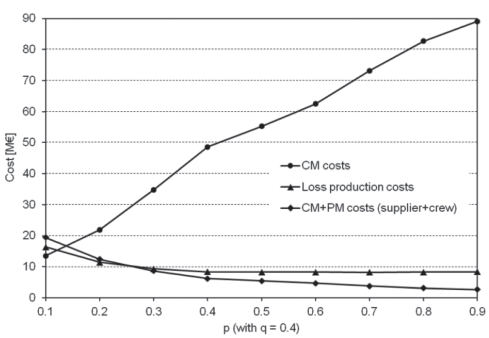


Figure 4. CM and PM costs for both models.

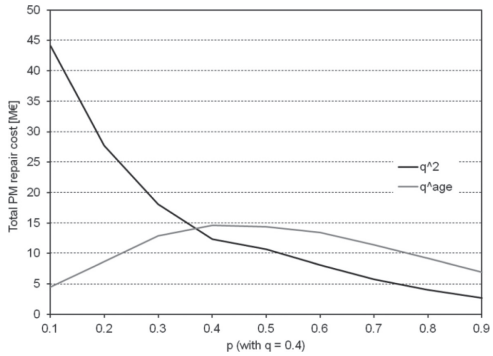


Figure 5. PM repair costs using the two cost functions.

according to the q^2 approach, is always the same for a component independently of its age. In other words, one can vary the time between PM actions (by varying p) that the PM repairs costs "behave" as if the component did not age. This seems counterintuitive, however. The only reason for the decrease in the mean total PM repair costs is the reduction of the mean number of PM repairs due to the increase in the time between PM actions.

On the other hand, the q^*age* cost function is sensitive to the age reduction effort and to the age of a component at each PM. Therefore, although the mean number of PM tasks decreases, as the time between PM increases, the total mean costs get higher due to the aging of the components, reaching is maximum value at $p = 0.4$. As the time between repairs continues to increase the total repair costs decrease given that the impact of the decrease in the mean number of repairs outweighs that of the increasing ages of the components. Also, the aging between consecutive PM repairs is accounted for in the maintenance costs. It seems reasonable that an effort to reduce, for example, the age of a young component by 40% should be less costly than improving its condition in the same percentage when it is older. Also, it may be realistic to consider that is as costly to slightly reduce preventively the age of an old component as is to considerably improve its condition when it is quite younger.

Figure 6 shows the mean total maintenance costs and revenues by varying the p-values. The availability curve is independent of the two cost functions by the same reasons given for the results in Figure 4.

The mean optimal revenues are 20 M€ ($p = 0.3$) and 34.48 M€ ($p = 0.2$), the mean number of PM repairs are 1.33 and 1.94 per component/year, and the turbine's mean availabilities are 90.7% and 88.6% when using the q^2 and q^*age* cost functions, respectively. These availability figures are

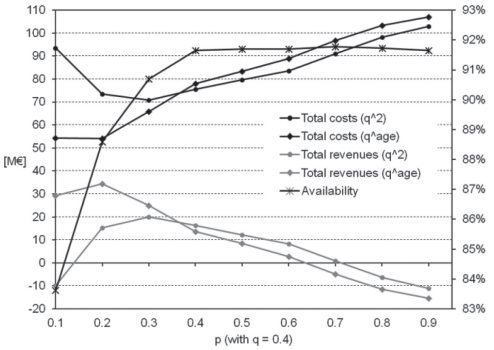


Figure 6. Total maintenance costs and availability using the two cost functions.

somewhat in line with the current offshore wind turbines availability values of 90–95% achieved by the industry (Tavner 2012). All in all, it seems at least as reasonable and realistic to consider the PM cost function that takes into account the age reduction effort and the age of the components.

Despite having been modelled only one offshore wind turbine, the considered maintenance strategy and cost function can be used for a wind farm provided that the dependencies between wind turbines due to sharing common logistic resources are modelled. In such case, the failure and repair models can be assumed the same for equal components in all wind turbines; more repair teams, different numbers of vessels and the use of an helicopter for harsh weather conditions could be introduced in the model to evaluate the impact in the costs, revenues and availability of the wind farm. Also, the use of opportunistic maintenance should be evaluated since it is reasonable to expect that the "simultaneous" maintenance of several wind turbines would be less costly.

7 CONCLUSION

An age-based imperfect PM combined with CM replacements was modelled for an offshore wind turbine using GSPN with predicates coupled with MCS and considering the logistics, times and costs, and weather constraints. The PM repairs were modelled to be performed after a repair threshold age, $p \times MTTF$, of the components. The failure models of the components were obtained from onshore ones using an empirical approach based on stress factors for mechanical systems.

A PM repair cost function dependent on an age reduction ratio, q, and on the age of the components was proposed and compared with a q-dependent cost function in terms of the effect on the O&M costs and revenues of the wind turbine.

Since the cost function is sensitive to the age of the components the total mean repair costs increase with their aging as the time between PM increases up to a point when the impact of the decreasing number of repairs on the costs outweighs that of the aging. This way the aging between consecutive PM repairs is accounted for in the maintenance costs. This approach seems reasonable when compared with the one based only on q given that an effort, in percentage terms (q), to reduce the age of a young component should be less costly than when applying the same effort once the component is older.

Considering a fixed q and varying the time between PM repairs (i.e. varying p-values) the mean optimal revenues were higher for the model with the age-dependent cost function.

ACKNOWLEDGMENTS

This work has been performed within the project Hydro-Environmental Modelling of Multi-Purpose Marine Renewable Energy Platforms (MAREN2), which is partially funded by the Atlantic Area Programme.

REFERENCES

BVG Associates. A Guide to an Offshore Wind Farm. Published on behalf of The Crown Estate.

Barata, J., Guedes Soares, C., Marseguerra, M. & Zio, E. (2002). Simulation Modelling of Repairable Multi-Component Deteriorating Systems for "On Condition" Maintenance Optimization. *Reliability Engineering and System Safety*. 76: 255–264.

Davidson, J. (1994). The Reliability of Mechanical Systems. IMeche (Institute of Mechanical Engineering) Guides for the Process Industries, John Wiley & Sons inc.

Ding, F. & Tian, Z. (2012). Opportunistic Maintenance for Wind Farms Considering Multi-Level Imperfect Maintenance Thresholds. *Renewable Energy* 45: 175–182.

Durstewitz, M. (ed.) (2005). Windenergie Report Deutschland 2004–2005. Kassel: Institut für Solare Energieversorgungstechnik (ISET).

Dutuit, Y., Châtelet, E., Signoret, J.-P. & Thomas, P. (1997). Dependability Modelling and Evaluation by Using Stochastic Petri Nets: Application to Two Test Cases. *Reliability Engineering System Safety* 55(2): 117–124.

Dutuit, Y., Innal, F., Rauzy, A. & Signoret, J.-P. (2008). Probabilistic Assessments in Relationship with Safety Integrity Levels by Using Fault Trees. *Reliability Engineering and System Safety* 93: 1867–1876.

Guedes Soares, C., Caldeira Duarte, J., Garbatov, Y., Zio, E. & Sorensen, J. D. (2010). Framework for Maintenance Planning. Guedes Soares, C. (Ed.). *Safety and Reliability of Industrial Products, Systems and Structures*, London, U.K.: Taylor & Francis Group; pp. 33–52.

International Energy Agency (2012). IEA wind 2011 Annual Report. Available on http://www.ieawind.org/annualreports.html.

Karyotakis, A. (2011). On the Optimisation of Operation and Maintenance Strategies for Offshore Wind Farms. Ph.D. thesis, University College London, London.

Karyotakis, A. & Bucknall, R. (2010). Planned intervention as a Maintenance and Repair Strategy for Offshore Wind Turbines. *Journal of Marine Engineering and Technology*, No. A16: 27–35.

Lindoe (2011). Offshore Renewables Center (LORC) foundation, http://www.lorc.dk/offshore-wind-farms-map/alpha-ventus?os_c = Germany.

Nielsen, J.J. & Sørensen, J.D. (2011). On Risk-Based Operation and Maintenance of Offshore Wind Turbine Components. *Reliability Engineering and System Safety* 96: 218–229.

Rademakers, L.W. & Braam, H. (2002). O&M Aspects of the 500 MW Offshore Wind Farm at NL7 (80 × 6 MW Turbines)—Baseline Configuration. *DOWEC 10080 rev. 2*.

Ribrant, J. (2006). Reliability Performance and Maintenance—A Survey of Failures in Wind Power Systems. MSc thesis, KTH School of Electrical Engineering, Stockholm.

Santos, F.P., Teixeira, A.P. & Guedes Soares, C. (2012). Production Regularity Assessment Using Stochastic Petri Nets with Predicates. In Guedes Soares, C., Garbatov, Y., Sutulo, S., Santos, T.A. (ed.), *Maritime Technology and Engineering*, Lisbon. London: Taylor & Francis Group.

Santos, F.P., Teixeira, A.P. & Guedes Soares, C. (2013a). Maintenance Planning of an Offshore Wind Turbine using Stochastic Petri Nets with Predicates. *Proc. 32nd Int. Conf. on Ocean, Offshore and Arctic Engineering (OMAE2013)*; Nantes, France. Paper OMAE2013-11639.

Santos, F.P., Teixeira, A.P. & Guedes Soares, C. (2013b). Influence of logistic strategies on the availability and maintenance costs of an offshore wind turbine. In Steenbergen, R., van Gelder, P., Miraglia, S., Ton Vrouwenvelder, A. (ed.), *Safety, Reliability and Risk Analysis: Beyond the Horizon*. London: CRC Press, Taylor & Francis Group.

Tavner, P. (2012). *Offshore Wind Turbines: Reliability, availability and maintenance*. Renewable Energy Series 13, London: The Institution of Engineering and Technology.

Van Horenbeek, A., Van Ostaeyen, J., Duflou, J.R. & Pintelon, L. (2013). Quantifying the added value of an imperfectly performing condition monitoring system—Application to a wind turbine gearbox *Reliability Engineering & System Safety*, 111: 45–57.

Zio, E. (2009). Reliability Engineering: Old Problems and New Challenges. *Reliability Engineering and System Safety* 94: 125–141.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Availability modelling and analysis of an offshore wind turbine using Extended Coloured Stochastic Petri Nets

P. Zeiler & B. Bertsche
Institute of Machine Components, University of Stuttgart, Stuttgart, Germany

ABSTRACT: Wind turbines for power generation will be further developed and constructed worldwide. The trend goes towards offshore locations due to the higher wind speeds at sea. For an operator of a wind turbine its technical availability is the crucial factor for a cost-effective operation. In this paper, the availability modelling and analysis of an offshore wind turbine is done based on Extended Coloured Stochastic Petri Nets (ECSPN). The merits of ECSPN in modelling complex, multi-state and multi-component systems with age evolution based on time-dependent failure rates are shown. Corrective, preventive and condition-based maintenance measures as well as periodic replacements are modelled—each with individual age reduction effects. Two different maintenance categories differentiated by the size and weight of the spare parts and logistics involved such as ships and floating cranes are included in the model. The spare parts inventory and the order policy are modelled. The weather windows for accessing the turbine as well as the wind loads of the turbine are also modelled. Numerous interactions and dependencies are included in the model. The influences of different maintenance and logistics strategies on the availability are investigated. Based on the results, the reliability goals and the necessary maintenance strategy for achieving a desired availability can be specified.

1 INTRODUCTION

Wind power is one of the most important forms of renewable energy production. The German Wind Energy Association (BWE) reported in 2013 the construction of wind turbines with a total capacity of approximately 3,000 MW in Germany. In order to operate such a plant economically, despite the high investment costs, life times of about 20 years are provided (IWES 2009). This results in high demands on the reliability of a wind turbine.

In recent years, the trend goes towards offshore wind farms that promise a higher energy yield due to the higher wind speed at sea. These exposed locations provide new challenges on maintenance and repair for operators of wind turbines. Due to meteorological conditions—in particular by wind and waves—the access to offshore wind turbines is significantly limited compared to onshore wind turbines. Therefore, the maintenance strategy is of particular significance.

For the operator of a wind turbine the crucial factor for the cost-effective operation is the technical availability of the system, which results from the reliability and maintenance strategy. Therefore, powerful methods need to be applied to the specification of wind turbine availability.

In the past years many papers have been published in the context of maintenance and logistics modelling as well as availability analysis. Several papers are especially focusing on offshore wind turbines. A recent paper already including a variety of modelling aspects is Santos et al. (2013). It aims for the planning of operation and maintenance activities based on Generalized Stochastic Petri Nets (GSPN). It includes corrective and preventive maintenance but does not consider condition-based maintenance and periodic replacements. The global age evolution of the components in their different load states cannot be modelled due to the limitations of the GSPN. Kahrobaee & Asgarpoor (2013) focuses on maintenance optimization of deteriorating equipment of offshore wind turbines by applying a hybrid analytical-simulation approach. The developed model is limited to constant failure and repair rates and is neglecting the maintenance logistics and resources. The influence of the weather on the turbine load and accessibility is not considered. Roux et al. (2013) investigate the optimization of preventive maintenance through a combined maintenance-production simulation model applying timed Petri nets. The developed model is able to describe a multi-component system, but it is not possible to consider multi-states of the components.

In this paper, the availability of an offshore wind turbine is modelled and analysed based on Extended Coloured Stochastic Petri Nets (ECSPN).

The merits of ECSPN in modelling complex, multi-state and multi-component systems with age evolution based on time-dependent failure rates are shown. Corrective, preventive and condition-based maintenance measures as well as periodic replacements are modelled—each with individual age reduction effects. Two different maintenance categories differentiated by the size and weight of the spare parts and logistics involved such as ships and floating cranes are included in the model. The spare part inventory and the order policy are modelled. The weather windows for accessing the turbine as well as the wind loads of the turbine are also modelled. Numerous interactions and dependencies are included in the model. They need to be considered for a close-to-reality analysis which will serve as a base for the specification of the wind turbine reliability and the supporting maintenance process.

This paper is organized as follows: In section 2 Petri nets are presented, which serve for the modelling and analysis. Modelling availability and complex maintenance strategies is covered by section 3. In section 4 the influence of the specified reliability and maintenance strategy on the achieved technical availability will be investigated in a case study.

2 PETRI NETS

2.1 *Low-level Petri nets*

In (Petri 1962) Carl Adam Petri developed Petri nets as a graphical modelling formalism for state-discrete systems. Petri nets consist of the following basic elements:

- Places, pictured as circles, represent possible states and can contain tokens.
- Transitions, pictured as squares, model possible state changes and therefore the dynamics within the model following specific rules. After a certain precondition, the activation, a transition can fire. The transition then deletes and creates new tokens in the places connected to it. If the transition is a so called timed transition, there is a time delay between activation and firing; otherwise it is called an immediate transition. Within a stochastic Petri net, the time delay can be stochastically distributed.
- Arcs are direct connections between transitions and places and vice versa. They map the logical interrelations.
- Tokens, pictured as filled out circles, are the only dynamic elements within a Petri net. The marking of a Petri net is the assignment of tokens of all places. A marking describes the current state of the modelled system and therefore changes with a firing of a transition.

A simple Petri net model of a repairable component is shown in Figure 1. It consists of two places, representing the states 'operational' and 'failed', and two timed transitions representing the stochastic life time of the component and its maintenance time.

At the beginning the component is in the operational state. This initial marking is shown in the figure. The transition 'Component failure' is activated with the initial marking. After a stochastic delay it fires, which means the component fails. When it fires the token in the place 'Component operational' is deleted and a new token is created in the place 'Component failed'. The new token then activates the following transition 'Component repair' and it fires after a stochastic repair delay. This deletes the token in the input place 'Component failed' and creates a new token in the output place 'Component operational'. The original marking is restored and the lifecycle starts again. The time slice of the token being in the place 'Component operational' is equivalent to the operational availability of the component. The analysis of the model is done by applying a Monte Carlo simulation.

Since the introduction of the original Petri net, many new extended classes of Petri nets have been developed to improve their modelling abilities (see e.g. extended stochastic Petri nets, Pozsgai 2006).

2.2 *Coloured Petri nets*

The class of Coloured Petri Nets (CPN) was developed in (Jensen 1996). In a CPN the anonymous token can carry information therefore they are distinguishable (coloured). The information within the token may affect the activation of transitions and thus influences the dynamic of the Petri net model. The information within the tokens can be passed on and/or can be modified by a firing transition. As the tokens are distinguishable

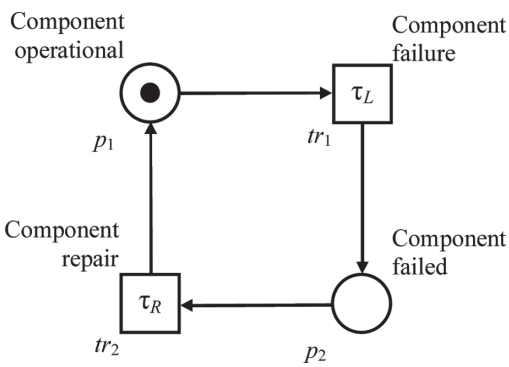


Figure 1. A simple stochastic Petri net model of a repairable component.

identical net parts can be reused for tokens with different colours and models become more compact. On the other hand, coloured Petri nets require textual declarations and additional text inscriptions in the graph to depict the flow of information within the model. Tokens are represented by a text inscription beside the place in a CPN.

Pozsgai developed a Conjoint System Model (CSM) focusing on the close-to-reality modelling of complex technical systems in Pozsgai (2004) and Pozsgai (2006). It consists of a class of Extended Coloured Stochastic Petri Nets (ECSPN) and a Reliability Block Diagram (RBD). An ECSPN allows the modelling of:

- arbitrarily stochastically distributed and/or deterministic time characteristics (life times, maintenance durations),
- various system states and component states including passive states, hot/warm/cold standby redundancies and load sharing,
- manifold dependencies between components, the system and the system's environment, for example common mode failures or failure propagation,
- complex maintenance strategies with corrective and preventive maintenance actions including condition-based maintenance actions,
- failure and maintenance behaviour of pre-aged components,
- queuing behaviour of maintenance/logistic processes and
- activity- and state-dependent operational costs.

Figure 2 shows a CSM version of the anonymous PN model from Figure 1. The system RBD

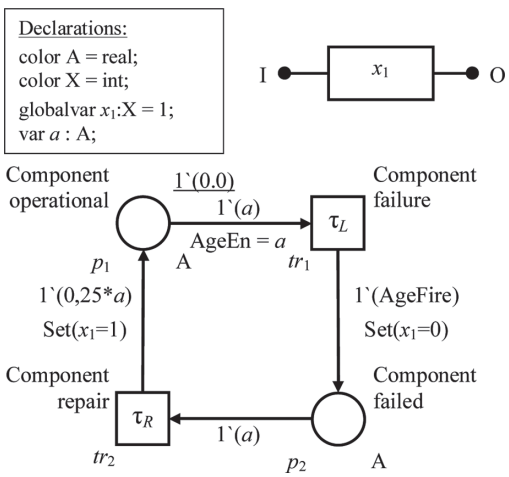


Figure 2. Conjoint system model of a repairable component with age influence.

model can be seen in the upper right corner and the ECSPN component model is located below. In the upper left corner the declarations of the ECSPN model can be seen. The token within the model contains the pre-age of the component, which is considered when calculating the component's stochastic life time. This can be seen in the depiction of the arc inscription 'AgeEn = a'. The arc inscription '0.25*a' represents an age reduction of 75% of the repair measure. The interface between the RBD and the ECSPN is the global component state-variable x_1 which is modified by the arc expression 'Set()'.

Certain advancements and supplements have been implemented and published, whose preliminary last status is represented by (Buck et al. 2011).

3 MODELLING AVAILABILITY AND COMPLEX MAINTENANCE STRATEGIES

The availability modelling based on Petri nets is very powerful. This method allows a comprehensive analysis of an offshore wind turbine. Based on a realistic model, relevant effects on the availability can be taken into account. These are on the one hand, the reliability of the wind turbine and its components, and on the other hand, the maintenance strategy that is being implemented for the system.

The reliability of the system results mainly from the so-called inherent reliability, which basically is the constructive and technically implemented reliability. It results from the relevant structural reliability of the system and the reliability of its components. The inherent reliability is strongly influenced by actual stress of the components during the operation of the plant. Main factor to this are the meteorological conditions, especially the prevailing wind strength.

A failure of one component usually leads to the shut-down of the entire wind turbine. As a result the intact components are usually set in a safe passive state in which they are considerably less strained in comparison to usual operation. This is referred to as a failure dependency, as the failure of one component has influence on the reliability of the other components.

The maintenance strategy includes the type and planning of the intended maintenance activities, as well as the necessary resources. This also includes the related logistics in the form of equipment, maintenance personnel and spare parts. Frequently, dependencies between the maintenance and the availability of a system exist. For example, a maintenance action requires a standstill

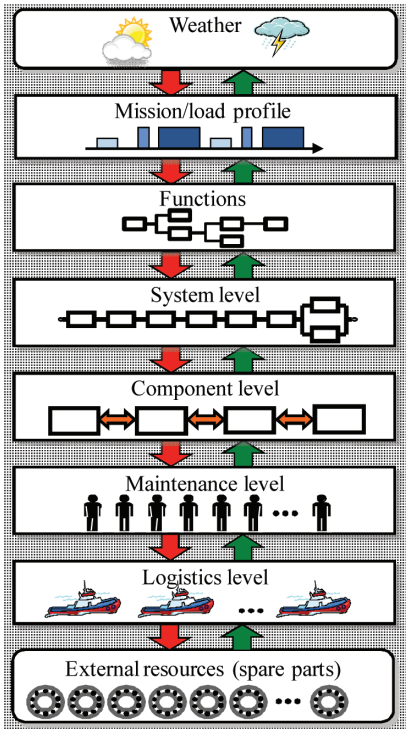


Figure 3. Numerous aspects of availability modelling.

of a plant, which cannot continue to produce during that period. Mostly the available resources are also limited or not available immediately, leading to extended plant downtimes. Therefore, it has to be possible to represent the maintenance process on the one hand and the resulting interdependencies on the other hand in the model.

The numerous aspects of modelling the availability of an offshore wind turbine are illustrated in Figure 3. It can be seen how the different modelling levels are interdependent.

4 AVAILABILITY ANALYSIS OF AN OFFSHORE WIND TURBINE

Especially in the field of wind energy technology availability is a parameter that is used to assess a wind turbine. The availability is defined as the probability that a system is operating satisfactorily at time t (Bertsche 2008). In simple terms, availability is the ratio of the period with full operability to the observation period. In the wind energy industry, mainly the technical availability and energetic availability are used. In particular, the technical availability takes the influence of the reliability and maintenance policy on the availability of the plant into account and is therefore considered in the following.

In the following case study it is shown how an offshore wind turbine can be analysed and evaluated right from the planning phase. The CSM (refer to section 2) is applied to model the turbine and its maintenance process. The Monte Carlo simulation (Pozsgai 2006 and Zio 2013) is used for analysing the model. It allows the analysis of the technical availability using statistical methods. The case study was carried out by using the modelling and simulation package REALIST, which has been developed at the Institute of machine components of the University of Stuttgart. The principal procedure is illustrated in Figure 4.

As a part of the joint project "Increasing the availability of wind turbines" operational data and experience of wind turbines were processed and analysed (IWES 2009). The life times and maintenance periods in this availability analysis are generic but were mainly based on the values shown there. The Weibull distribution was always chosen as the life time distribution.

4.1 *Specification of the wind turbine*

The specification of the wind turbine is done based on its five main components: Rotor System (RS), Gear Transmission (GT), Pitch Control (PC), Hydraulic System (HS) and Control unit and Safety equipment (CS). The turbine system comprises a series structure, i.e. one failed component leads to a shut-down of the turbine.

As noted in section 3, the reliability of wind turbines or their components is mainly influenced by the prevailing wind strength. Therefore, different inherent reliabilities depending on the wind strength were used as a basis for the components: reliability during normal operation (see Table 1), during calm and during a safety shut-down (caused by exceptionally high wind speeds). Additionally a

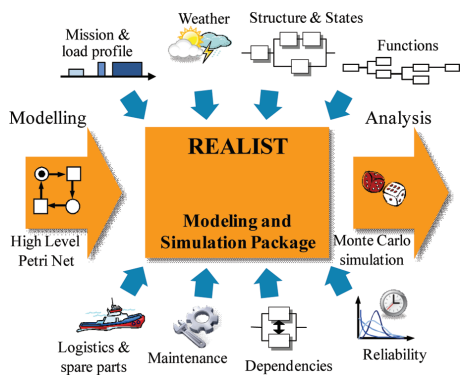


Figure 4. Procedure of availability analysis.

Table 1. Parameter of life time distributions for inherent reliability in "normal" operation.

Component	Scale parameter [h]	Shape parameter
Rotor system	32,000	1.5
Gear transmission	15,000	1.5
Pitch control	12,000	1.5
Hydraulic system	20,000	1.5
Control unit and safety equipment	1,460	1.0

separate reliability has been chosen for the passive state of a component. Each component can fail in each of its states.

During calm (see Table 2) each component would be operational, but operation is not possible due to too low wind speeds.

During safety shut-down (see Table 3) components would be operational, but turbine operation is interrupted caused by exceptionally high wind speeds.

A failure of one component leads to the shut-down of the entire wind turbine. As a result the intact components are set in a safe passive state (during the maintenance of the failed component) in which they are considerably less strained in comparison to usual operation (see Table 4). Components would be operational, but operation is not requested by the system.

Therefore, the reliability model of the turbine is based on multi-level components with individual time-dependent failure rates in each state.

4.2 *Weather model*

The influence of weather on the stress states of the components as well as on the accessibility of the turbine is considered in a weather model.

The duration of the maintenance measures on a wind turbine depends to a significant degree on the accessibility to the system. Very strong winds, storms or swell may prevent or complicate the accessibility. Special equipment is needed for maintenance work. Repairs of rotor blades or replacements of the transmission usually require large floating cranes. These can only be used in moderate weather. Apart from helicopter operations, the accessibility of offshore wind turbines is directly influenced by the wave height (indirectly of the wind speed). During weather conditions with a wave height of more than 1.5 m, called the "weather days", a wind turbine cannot be reached without danger. These boundary conditions were considered in the model of the wind turbine.

The weather conditions are divided into two seasons: winter and summer half year. With the modelled weather parameter, the following weather data (exemplary shown for the winter half year in Table 5) were considered in the analysis.

Table 2. Parameter of life time distributions for inherent reliability in "calm" state (caused by too low wind speed).

Component	Scale parameter [h]	Shape parameter
Rotor system	128,000	1.2
Gear transmission	60,000	1.2
Pitch control	48,000	1.2
Hydraulic system	80,000	1.2
Control unit and safety equipment	1,460	1.0

Table 3. Parameter of life time distributions for inherent reliability in "safety shut-down" state.

Component	Scale parameter [h]	Shape parameter
Rotor system	35,000 h	1.5
Gear transmission	28,000 h	1.2
Pitch control	20,000 h	1.2
Hydraulic system	20,000 h	1.5
Control unit and safety equipment	1,460 h	1.0

Table 4. Parameter of life time distributions for inherent reliability in "passive" state.

Component	Scale parameter [h]	Shape parameter
Rotor system	50,000	1.3
Gear transmission	28,000	1.3
Pitch control	25,000	1.3
Hydraulic system	25,000	1.3
Control unit and safety equipment	1,460	1.0

4.3 *Maintenance strategy & logistics*

The maintenance strategy defines the type and planning of the intended maintenance activities, as well as the necessary resources and logistics.

4.3.1 *Maintenance strategy*

Four different maintenance strategies have been investigated:

– Option 1—Corrective Maintenance (CM): Only corrective measures (i.e. repairs) performed after a failure

Table 5. Weather data for winter half year.

Phase condition	Days/phase	Phases/month
Operation	2.4	10
Operation (with access to turbine)	1.4	10
Operation (w/o access to turbine)	1.0	10
Calm (too low wind speed)	1.1	3
Wind speed too high	0.5	6

- Option 2—Condition-based maintenance (CM+CBM): In addition to option 1, also measures depending on the detectable state (i.e. by a condition monitoring system) are carried out
- Option 3—Preventive Maintenance (CM+PM): In addition to option 1, preventive measures at defined intervals are performed
- Option 4—Combined maintenance strategy (CM+CBM+PM): Includes the corrective, preventive and condition-based measures of the options 1 to 3

The duration of repair time is modelled by a Weibull distribution for each component as listed in Table 6. Each repair requires a spare part. Depending on the spare part size, a ship or a floating crane is required (see section 4.3.2 and 4.3.3).

The preventive and condition-based measures have constant time duration of 12 h. It is assumed that all necessary planned measures can be performed in parallel within one common maintenance action. The maintenance interval is 1,200 h, which is globally defined for all components. A ship is required for a preventive and condition-based measure (see section 4.3.3).

Over the analysed wind turbine life time of 20 years its components are replaced completely at least once and considered as new after that (see Table 7). This planned component replacement is carried out for all four strategy options. This means that maintenance measures aim to keep downtime as a result of unplanned outages or maintenance as low as possible. A component replacement is not possible during the winter half year. If a replacement is due in a winter half year, it is waited until the summer half year begins to start the replacement. A replacement of a component requires a floating crane.

The maintenance actions yield a specific reduction of the component age. A degree of renewal describes a factor. The component age after maintenance is the age before the action multiplied by this factor (see Table 8).

Table 6. Parameter of repair time distributions.

Component	Scale parameter [h]	Shape parameter
Rotor system	48	3.5
Gear transmission	90	3.5
Pitch control	12	3.5
Hydraulic system	12	3.5
Control unit and safety equipment	2	3.5

Table 7. Interval between component replacements.

Component	Replacement interval [h]
Rotor system	87,600
Gear transmission	70,080
Pitch control	105,120
Hydraulic system	87,600
Control unit and safety equip.	87,600

Table 8. Degree of renewal of maintenance actions.

Maintenance action	Degree of renewal
Repair (CM)	0.3
Maintenance (PM or CBM)	0.5
Replacement	0.0

4.3.2 *Spare part logistics*

Spare parts are necessary for each repair of a failed component. Preventive maintenance does not require a spare part. Two spare part policies are considered in the case study:

- Policy 1—Order policy: Without spare part inventory; spare parts are ordered at the supplier only when needed; Spare part delivery has a specific lead time according Table 9.
- Policy 2—Spare part inventory: A spare part inventory is available onshore; if the inventory level falls below a specified value an order for new spare parts is placed.

The spare parts have two different sizes. The share of small and large spare parts for each component is given in Table 10.

4.3.3 *Special equipment*

For the availability analysis the logistics of floating cranes and ships for the transport of spare parts and the implementation of measures has been integrated into the model.

- Ship: Necessary for delivery of small spare parts to the turbine and for performing planned or condition-based maintenance.

Table 9. Spare part lead times.

Component	Lead time [week]
Rotor system	4
Gear transmission	8
Pitch control	4
Hydraulic system	4
Control unit and safety equipment	2

Table 10. Share of spare part size.

Component	Small spare part [%]	Large spare part [%]
Rotor system	65	35
Gear transmission	80	20
Pitch control	92	8
Hydraulic system	94	6
Control unit and safety equipment	100	0

– Floating crane: Necessary for delivery of large spare parts to the turbine and for component replacements.

A ship or a floating crane is only sent to the turbine if the wind is calm. If the wind is not calm, it is waited until it is calm. The trip duration is according to the weather condition. If the turbine is not accessible when the ship or crane arrives, it needs to idle nearby the turbine until it is accessible again. The return trip to the service harbour starts only if the weather condition is well.

4.4 *Turbine model*

The entire model which has been developed based on the values and boundary conditions as described in the sections 4.1 to 4.3 is shown in Figure 5. It is realised by the CSM modelling method. The tool REALIST offers a graphical editor to develop the model.

The model it is thematically decomposed i.e. the model is separated visually into sub models by applying reference places. This allows avoiding a spider web like crossing of connecting arcs all over the model. The model is kept traceable which supports the modelling process especially for such complex scenarios.

In the following the modelling aspects which are implemented by using the ECSPN are shortly described in an overview. In the top part of the model the different operational states and the conditional state transitions are modelled which include also the processing of the pre-age when leaving a state and entering a new one. Therefore,

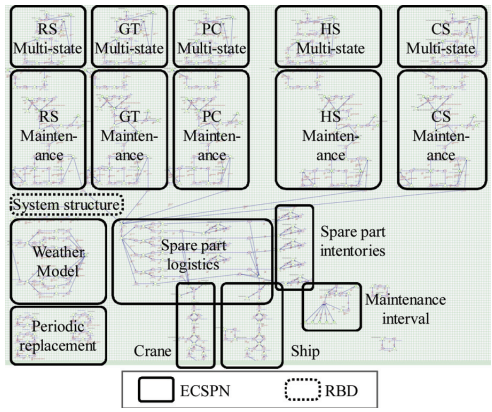


Figure 5. Entire model structured into main modelling topics.

the turbine model is a multi-component system with multi-state components. The components have an individual age evolution in each state based on time-dependent failure rates.

Below the state model, the maintenance process is modelled including the corrective, preventive and condition-based measures as well as component replacements. In the lower part of the model the spare part logistics including the spare part inventories and the special equipment is modelled. The logistic process of two different maintenance categories requiring a ship or a floating crane can be seen. Two auxiliary sub models for generating the trigger for the overall periodic maintenance as well as the periodic replacements are included, too. On the left side the weather model which is simulating the weather phases in summer and winter half year can be observed. By this, the weather windows for accessing the wind turbine and the load states of the turbine components are generated.

Finally the system structure of the turbine is implemented by using a RBD which allows for an efficient generation of the turbine system state.

In Figure 6 a detail of a ship proceeding to the turbine is shown. After a repair order which is put in place p34 an available ship will be sent to the turbine with the spare part after a preparation time modelled by transition tr60. If no ship is available, the repair order needs to wait until one is available. The ship is only sent to the turbine, if the turbine is currently accessible which is modelled by the transition tr65 using the global accessibility variable of the weather model. The trip duration to the turbine is depending on the weather condition. If it is calm, the trip duration is shorter compared to strong wind, which is realised by the two transitions tr67 and tr68 and specific guards, which use the value of the global wind variable of the weather model.

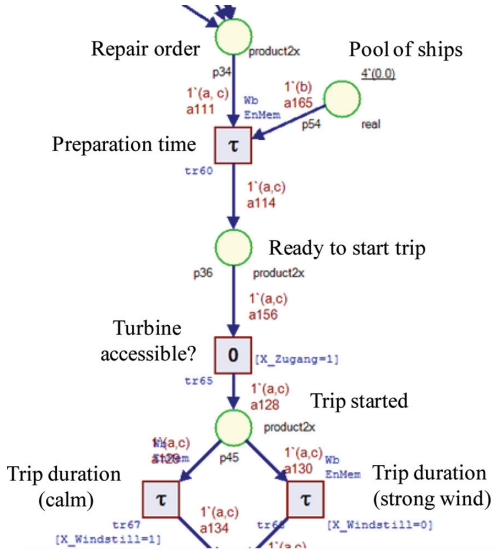


Figure 6. Ship driving with spare part to turbine.

4.5 *Availability without spare part inventory*

The availability analysis has been carried out for all maintenance strategy options described in section 4.3.1. The analysis was done by applying the REALIST simulation and evaluation module.

The spare part logistic is organized according policy 1 (i.e. without spare part, see section 4.3.2). The results of the analysis are given in Table 11. They show the lowest technical availability of 89.5% for option 1. If condition-based measures are carried out in addition to the purely corrective measures, there is a slight increase to 90.1%. In option 3 with additional preventive measures the result is 91.2%. If all measures are combined like in option 4 there is the highest achievable availability of 92.0%.

A technical availability of 98% for an onshore wind turbine can be considered as reference for a comparison with the values in Table 11. Compared to this reference value, the analysed availability of the offshore turbine is considerably lower. That means the higher energy yield of an offshore turbine should at least compensate the lower operation time. It should be mentioned here that the analysed availability of the variants is purely depending on the modelled scenario. Different specification parameters may lead to a different availability or variant ranking.

4.6 *Availability with spare part inventory*

In the second step, all maintenance strategy options are considered in combination with spare part policy 2. The results of the analysis are given in Table 12. They show the benefit of an onshore part inventory on the availability compared to the results in the previous section. Again option 4 achieves the highest availability with a value of 95.9%. That means the onshore inventory increases the availability by almost 4%.

Table 11. Technical availability without spare part inventory.

Maintenance strategy	Technical availability [%]
Option 1 (CM)	89.5
Option 2 (CM+CBM)	90.1
Option 3 (CM+PM)	91.2
Option 4 (CM+CBM+PM)	92.0

Table 12. Technical availability with spare part inventory.

Maintenance strategy	Technical availability [%]
Option 1 (CM)	94.5
Option 2 (CM+CBM)	95.1
Option 3 (CM+PM)	95.7
Option 4 (CM+CBM+PM)	95.9

Table 13. Mean number of failures per component.

Strategy	RS	GT	PC	HS	CS
Option 1	3.3	7.5	8.9	4.9	62.6
Option 2	2.9	6.7	8.7	4.8	62.5
Option 3	1.5	3.3	4.5	2.3	62.5
Option 4	1.4	3.2	4.5	2.2	62.1

The effect of component failures to the turbine availability is quite significant compared to the preventive and condition-based maintenance measures. The time between failure and finished repair depends strongly on the weather and the accessibility of the turbine. In contrary the turbine is still operating until a preventive or condition-based maintenance measure begins. It is important to note, that an instantaneous component failure can also lead to expansive damage on the component or the surrounding elements.

Besides the availability the mean number of failures per component has been investigated during the study in order to further evaluate the different strategy options (results are shown in Table 13).

Compared to the corrective maintenance strategy (option 1), the number of failures can be considerably reduced especially by option 3 and 4. The number of failures for the control unit and safety equipment is relatively high and remains almost

constant in all strategy options. The different maintenance options do not have an effect on the failure number. This stems from the random failure behaviour of these electric and electronic components (modelled by a constant failure rate). The situation can only be improved by a design change, which leads to a significant lower failure rate.

5 CONCLUSIONS

The analysis showed the high influence of the weather on the maintenance logistics. Both the trip duration and the accessibility of the turbine depend on the weather condition. The effect of sudden failures on the availability is higher compared to maintenance actions, as the turbine stands still until the spare part is available and the repair is finished.

Furthermore, the analysis results showed that the control unit and safety equipment causes much more failures compared to the other components. It was shown that it is not possible to reduce these failures by maintenance. Therefore, from reliability specification point of view, the reliability target of the control unit and safety equipment needs to be increased considerably.

The bottleneck of the maintenance strategy is the spare part supply and the accessibility of the turbine. It was shown how an additional spare part inventory contributes to a higher availability. As the accessibility is strongly depending on the weather, the maintenance accesses to the turbine should be reduced to a minimum. This can be achieved by reducing the number of unplanned failures by additional preventive and condition-based maintenance actions.

The availability analysis based on Petri nets allows the consideration of many factors and interactions, and can be performed at an early development stage. Based on the results, the reliability goals and the necessary maintenance strategy for achieving a desired availability can be specified. Many variations can be analysed, compared and optimized. The model enables sensitivity analysis to determine, e.g. how the maintenance periods or condition monitoring quality influences the turbine availability.

Additionally the risk-based development of services for the turbine, e.g. maintenance contracts, can be done based on the analysis results (Zeiler & Bertsche 2014).

For the analysed maintenance strategies further studies for optimizing the maintenance strategy and the supporting logistics as well as the cost aspects will be carried out. Furthermore, the research activities will be extended to an entire wind farm.

REFERENCES

Bertsche, B., 2008. *Reliability in Automotive and Mechanical Engineering*. Berlin Heidelberg: Springer.

Buck, A., Nebel, S. & Bertsche, B., 2011. Maintenance and Cost Modelling of Production Systems with Petri Nets. In *Proceedings of 21st International Conference on Production Research*, Stuttgart.

IWES, 2009. *Final report for the joint project "Increase of wind turbine availability", granted by federal ministry of environment, nature protection and reactor safety (BMU)—sub project: Processing and analysis of operating data and experiences from "scientific program of measurement and evaluation" of the 250 MW Wind assistance measure of the BMU;* Fraunhofer Institut für Windenergie und Energiesystemtechnik (IWES).

Jensen, K., 1996. *Coloured Petri Nets—Basic Concepts, Analysis Methods and Practical Use*. Volume 1. Berlin, Springer.

Kahrobaee, S. & Asgarpoor, S., 2013. A hybrid analytical-simulation approach for maintenance optimization of deteriorating equipment: Case study of wind turbines. *Journal of Electric Power Systems Research* 104(2013): 80–86.

Petri, C.A., 1962. *Kommunikation mit Automaten (Communication with Automats)*. Universität Bonn, PhD thesis.

Pozsgai, P. & Bertsche, B., 2004. *Conjoint Modelling with Extended Coloured Stochastic Petri Net and Reliability Block Diagram for System Analysis. In Proceedings of PSAM 7/ESREL '04,* Berlin, June 14th–18th.

Pozsgai, P., 2006. *Realitätsnahe Modellierung und Analyse der operative Zuverlässigkeitskennwerte technischer Systeme (Close-to-reality modeling and analysis of the operational reliability characteristics of technical systems)*. University of Stuttgart, PhD thesis.

Roux, O., Duvivier, D., Quesnel, G. & Ramat, E., 2013. Optimization of preventive maintenance through a combined maintenance-production simulation model. *International Journal of Production Economics* 143(2013): 3–12.

Santos, F., Teixeira, A. & Guedes Soares, C., 2013. Maintenance Planning of an Offshore Wind Turbine Using Stochastic Petri Nets With Predicates. In *Proceedings of ASME 2013 32nd International Conference on Ocean, Offshore and Arctic Engineering*, Nantes, France, June 9th–14th.

Zeiler, P. & Bertsche, B., 2014. Simulation-Based Risk Management of Product-Service Systems. In *Proceedings of RAMS 2014*, Colorado Springs, USA, January 27th–30th.

Zio, E., 2013. *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. London, Springer.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Maintenance in availability of weapon systems under combat operation—optimization possibilities

T. Smal
Faculty of Security Affairs, Wroclaw, Poland

ABSTRACT: Availability is a parameter which determines (together with credibility) dependability of any technical object including weapon systems. High availability of a weapon system means that such system has high reliability and maintainability and it can be increased due to modelling its survivability and vulnerability. In context of a combat operation, weapon system availability can be improved at the stage of design and production and at the stage of maintenance. An effective systems of service, evacuation and repair are of crucial importance when we consider availability of a weapon system under combat operations. Therefore, maintenance is one of the solutions which can improve availability of a weapon system. The paper presents analysis of functional elements of maintenance system that influence weapon systems' availability under combat operations. The following components were discussed: purchasing of weapon systems, organization of maintenance system, human resources and technical resources connected with maintenance. On the basis of numerous references and personal experience some new optimization possibilities were offered like: *taking into account new factors when purchasing equipment,* modification of maintenance services structures, introducing modern IT platform, reduction and destination of currently used mobile workshops and introducing system of expedient repairs in the field.

1 INTRODUCTION

Logistic system under combat operations is called combat service support and they include: supply, movement and transportation, maintenance, infrastructure and medical support (ALP-4.2(A), 2010). Weapon systems belong to a group of technical objects used in task (random) mode and they require a specific maintenance system, which should be aimed at executing tasks in a specific place and time regardless of circumstances. The properly developed maintenance system can create advantage over an enemy, that is why, the new and diverse solutions should be searched for in order to ensure fighting units availability of weapon systems. Diversification of various solutions and adequate designing of equipment will support logistics units in recovering of weapon systems and can help to create advantage over an enemy by increasing availability of weapon systems.

Availability can be defined as a system ability to fulfil the required functions in certain time and conditions. High availability of a weapon system means that such system has high reliability and maintainability and it can be increased due to proper modelling its survivability and vulnerability (Nowakowski, 2011).

In context of a combat operation, weapon system availability can be improved at the stage of design and production and at the stage of maintenance. Firstly, we can take into account: lessons learned from previous military operations and current and upcoming means of combat and protection systems as well as we can apply modern on board diagnostic systems in order to design and manufacture military equipment which has higher survivability and maintainability and lower vulnerability. Secondly, we can introduce effective systems of service, evacuation and repair in order to increase maintainability of a weapon system (Furch, 2010).

2 WEAPON SYSTEMS AVAILABILITY

There are several definitions of a system (Nowakowski, 2011; Backlund, 2005). One of them says that each complex object, which can be distinguished in researching reality can be called a system given that it determines integrity created by a set of elementary objects and relations between them (Sienkiewicz, 1983). Another one, runs that a system is an existence displaying its existing by the synergetic cooperation of its elements (Bellinger, 2002). A mathematical complement of the mentioned definition is represented by the following equation:

$$S = (E, A, R),\ E = [E_1 \ldots E_n],$$
$$A = [A_1 \ldots A_m],\ R = [R_1 \ldots R_k]$$

where: S—system, E—a set of elements, A—a set of attributes (properties), R—a set of the relation between elements and attributes.

A system can consist of $n > 1$ elements—E, which can have $m \geq n$ attributes, participating in $r \geq n - 1$ relations (equality for the series system). The possible spectrum of elements of some systems could be: physical, energetic, symbolic, computerized, living, conscious, self-conscious. Additionally, they are set in the any configuration of types and elements.

The main aim of logistics should be providing a commander with adequate quantity of means in order to fulfil particular task. To meet this aim it is necessary to implement the latest organizational and technical solutions to the battlefield maintenance system, which proper installation should maximize activities performed by logistics elements. Among components which are essential for trouble-free functioning of maintenance system one can distinguish:

– purchasing of weapon systems;
– organization of system;
– human resources connected with the system;
– technical resources assigned to weapon systems' maintenance.

3 PURCHASING OF MILITARY EQUIPMENT

The first phase in a new model during which new equipment is obtained is called needs defining. From the logistic point of view, one of the important problems is designing maintenance system according to the newly acquired military technology. It should be commenced at the stage, during which the ability to fulfil the needs is analysed. Project of this type of system should contain; among other things, such elements as maintenance (together with repair) and supply systems. Moreover, it should be able to determine accessibility and designing of service appliances altogether with courses and trainings, not to mention that transport devices and IT implementation should be also enclosed within it. Considering the above-mentioned issues will have a great impact on logistical susceptibility of particular object during its maintenance, which consists not only of technical susceptibility (diagnostic, service, evacuation, repair and transport) but also its maintenance needs (Smal & Szukalski, 2009).

Modification of system, which is aimed at acquisition of weapon systems in accordance with its availability, should be carried out by increasing life cycle and combat lifespan of newly manufactured or modernized objects (Vališ & Vintr, 2006), and by designing them on the basis of carried out tests, methodology of quick verification of damages, and last but not least, according to a propose of its recovery and repair methods on battlefield (Vališ & Vintr & Malach, 2012). Determining survivability of the equipment may be conducted by practical tests (Jackson, 2009) or by computer simulations (Wasmund, 2009; Vališ & Vintr, 2006). However, the most reliable results might be obtained only during an experiment. For example, each weapon system purchased by US Army must pass adequate procedures, which reflect its survivability—so called "live fire tests" done by means of live ammunition. Such tests have been done e.g. for F/A-22 plane. It passed and the damages turned out to be far less considerable than it had been assumed. After that, wing, which was built of composite and titanium skeleton, was repaired and it was an excellent opportunity of improving repair methods by using standard BDR kit (Fig. 1).

U.S.A. experiences in that matter have shown that the best solution is to create adequate technologies and algorithms of proceeding, which would be dedicated to particular family or type of equipment (FM 4-30.31, 2006). A positive example of this kind of philosophy of an approach to designing is HMMWV vehicle. In this vehicle, the driver, without any repair kits, is able to carry out particular gears or assemblies with help of Battle Damage Assessment and Repair (BDAR) instruction (TM 9-2320-280-20-1/2/3, 1996).

To sum up, as long as obtaining of new equipment is concerned, requirements of maintenance system should be taken into account. The susceptibility to restore a weapon system availability is higher when an object is:

– designed observing the modularity of assemblies,
– equipped with quick-mounting joints that provide quick assembly and disassembly.



Figure 1. Combat logistics support squadron's personnel cutting expedient repair of F/A-22 plane (Surviac Bulletin, 2002).

– equipped with a possibility of using standard devices and tools in a process of assembly and disassembly,
– secured with base surfaces (openings) of the components in order to use them in a repair process,
– labelled in a way that enables easy and proper assembly of cooperative components of the object,
– constructed in a way that makes an access to the most often damaged assemblies easy and; simultaneously, that enables easy mounting of damaged subassemblies or their repair without a necessity of disassembly,
– designed in a way that gives a possibility to use modern technologies and repair materials in a repair process,
– equipped with dedicated repair manuals in conditions of combat operations, and with special repair kits.

4 ORGANIZATION OF SYSTEM

Maintenance tasks should be conducted by means of recovery and repair mobile elements which are equipped with adequate procedures, tools and materials. Although the fundamental problem is that maintenance services during peacetime usually train and perform tasks as logistic forces and they use stationary maintenance infrastructure, but for the combat purpose they convert themselves into mobile maintenance elements such as: recovery teams, evacuation-repair sections, evacuation teams, etc. (DD/4.2, 2007). In addition to that, because of gradual spending cuts tactical exercises are being abandoned; therefore, above mentioned elements are not executed and there is no opportunity for training and synchronization similar to real environment.

Another organization issue concerns division of military equipment into two groups. The first group is in use to conduct current tasks and training of military units. The second group is stored to support mobilization and war time. A huge part of mobile workshop is assigned to a stored group; therefore, military regulation doesn't allow to use them during peace time. Military mechanics execute service and repair of military equipment during peace using different stuff, thus they don't use specialist tools sets. This fact can lead in the future to the situation where maintenance units act ineffectively during combat operations, because of lack of experience. Having regard to the above, the proposition is to shift almost all mobile workshops to the group in use, and that is going to allow mechanics to gain more experience in using their equipment, as well as, to interchange their tools and materials. These undertakings should give certainty that mechanics will be well-prepared for their tasks (Smal & Smoła, 2011).

The allied countries implement organizational solutions, which facilitate incorporation of system solutions in the scope of maintenance tasks. Such system should be organized in a way which give assistance, as quickly as possible, by entire or partial removal of consumption effects, as well as, damages or malfunctions, of restoration of task capability of military equipment. Time devoted for those actions, in combat conditions, should be sufficiently short. Conducting it, one should try to restore as many of the vehicles as it would be manageable in the shortest time possible. According to this, one should repair, as the main priority, those of vehicles, which cause fewest problems (DD/4.2, 2007 & Stanag 2406, 1995). It is permitted to demount parts from those which are non-operational in order to mount them in those which are still useful. It is also allowed to mend them so they would be able to perform a single task or so they could be used but with some limitations (Smal & Rośkowicz, 2009).

The exchange of information about the occurred problems and previously executed operations is an efficient method of simplifying maintenances tasks (Vališ & Mlynczak & Nowakowski, 2011). The Polish Armed Forces do not have a unified IT system, which would support the maintenance process under combat operations. Furthermore, the units do not gather information on defect statistics of the equipment or the methods of damage elimination. Thus today, there is no way of implementing modern strategies, such as Reliability Cantered Maintenance (RCM) or strategy based on RBI diagnostics or RBM safety oriented strategy in the maintenance of military equipment (Uhl, 1999), as well Prognostics and Health Management (PHM) Technologies (Song & Li, 2009) or Condition Based Maintenance Plus (CBM+). The last mentioned concept seems to be very useful, especially in context of weapon systems sustainment. CBM+ is the application and integration of appropriate processes, technologies, and knowledge-based capabilities to achieve the target availability, reliability, and operation and support costs of weapon systems and components across their life cycle (Fig. 2). CBM+ uses a systems engineering approach to collect data, enable analysis, and support the decision-making processes for system acquisition, modernization, sustainment, and operations (Gang & Bo-Suk & Pecht, 2010).

An additional setback in implementing the above strategies in the usage of military equipment of the Polish Armed Forces, would not only be the lack of knowledge on damage characteristics, but also the shortage of specialized equipment

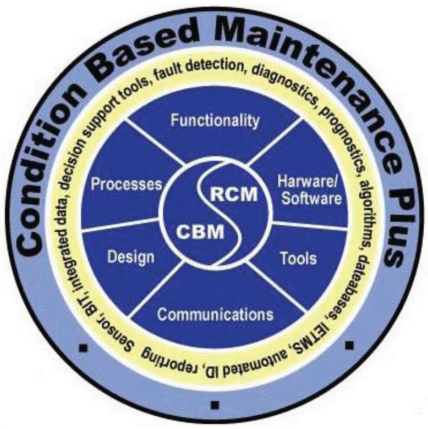


Figure 2. Condition based maintenance plus (http://www.acq.osd.mil/log/mpp/cbm+.html, 2014).

for controlling the state and software, especially with older versions of devices and vehicles and the necessity of baring significant costs of service investments, which would affect the total cost of maintenance (Niziński, 2002).

The leading armies of NATO are ordered to keep a regular repair documentation. For instance, the Armed Forces of USA have a special damage evaluation and executed repairs form, which is transmitted to Survivability/Vulnerability Information Analysis Centre (SURVIAC). An analogical temporary repair realization form was implemented by the NATO standardization document on the basis of American experiences (Stanag 2418, 2009). Gathering and distributing information on combat damages and the methods of dealing with those damages through interactive internet sites is an interesting and useful idea for transferring information on damages and executed repairs. The project was created by the Joint Combat Assessment Team (JCAT) and implemented by SURVIAC to support the reporting system of combat damages of aircrafts (Egner & Mullins, 2009). A web page under the name Combat Damage Incident Reporting System (CDIRS) was used as a data base for all documented combat damages during the operation "Iraqi Freedom". Initially, the page was a source of statistical data, currently it is an interactive data base operating in actual time, thus it can be used directly during combat operations. Additionally, it contains tools enabling data analysis, its distribution to all the involved subdivisions, data search according to specified criteria, e.g. damaged component or the damage's occurrence date etc.

By combining the knowledge and experience of maintenance specialists with the data gathered

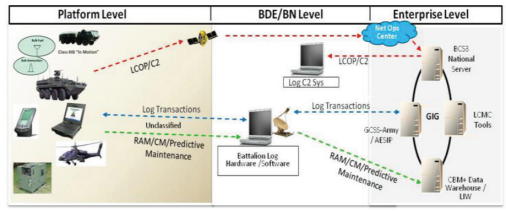


Figure 3. Telemetry combat service support system under combat operation (Presentation obtained from U.S. Army Logistics Innovation Agency, 2012).

in electronic bases, we could develop availability of weapon systems, including remote technical service i.e. telemaintenance. Telemaintenance, in some publications called "Remote Diagnostics & Maintenance (RD&M)", are based on wireless transitions of utilization data of the vehicle (You & Krage & Jalics, 2005). These systems are usually used by companies, which provide long distance transportation and by the military. Considering combat operation circumstances, the telemaintenance system may be very useful, especially in: vehicle's diagnostics performed by the driver, gathering vehicle's diagnostic data by the logistic support line, planning and organizing vehicle's utilization, remote technical support for the driver and the crew, especially in special situations (combat damages, breakdowns) as well as perfecting the construction and the utilization process in order to improve the reliability and efficiency of repairs (Fig. 3).

In sum, functioning organization of the maintenance systems could be significantly improved by:

- modification of maintenance service structures, which realize services and repairs;
- developing and implementing equipment procedures and manuals within the scope of recovery and quick temporary repairs of weapon systems directly within operation zone;
- utilizing modern IT tools to support the service and repair works;
- constant monitoring of the system's functioning and searching for optimization possibilities.

5 HUMAN RESOURCES

Regardless of the type of activity, a man and his intellect is the most significant element of every system. Thus, while discussing the availability of weapon system, we cannot ignore the problem of effective gathering, processing and repeated usage of the experiences of specialists in this field.

Due to permanent restructuring of the Polish Armed Forces, especially the logistic system and

logistic structures, the issue of system usage of the experts' knowledge and experience in the field of military technology repairs is highly neglected. The aging mechanic and engineering staff is another problem. Introducing regular army and recruiting young and inexperienced privates and officers to repair divisions causes them to often not be able to handle the tasks that they are given. A similar situation occurs during trainings for future officers—future commanders of platoons. Their knowledge on the structure and usage of military equipment constantly decreases. This is most likely caused by the fact that they are usually graduates of humanities at high schools, and the number of hours for technical subjects in the military schools is permanently decreased. The problem of experienced mechanics shortage in repair subdivisions is solved by hiring former professional soldiers, who served in such formations. Their knowledge and competences are priceless, but besides current usage of their work, is someone gathering and utilizing their experience? Furthermore, as interviews conducted with commanders of repair battalions indicate, the average age of persons employed as mechanics is constantly increasing. Replacing vacant mechanic positions with positions from the National Reserve Forces program is an additional hindrance in filling the generation gap (Smal & Smoła & Stankiewicz & Szukalski, 2010).

The experiences of allied countries clearly indicate that proper preparation of maintenance personnel is a very significant element of technical support of weapon systems. An appropriate level of training for persons responsible for eliminating damages during combat operations is acquired through permanent conduction of trainings—theoretical and, first and foremost, practical [19, 25] (Fig. 4).

The experiences of other armies indicate that we cannot waste the massive intellectual potential concerning the practical realization of maintenance tasks, which is usually lodged in the older and more experienced mechanics. For example, technologies and field repair systems of technical objects evolve along with the intellectual thought and human imagination. The same techniques, equipment and materials could be used in varied situations and circumstances. It is important that these experiences are gathered, verified and that the fastest and most efficient methods are proposed for usage. This however, will not be possible without proper system solutions.

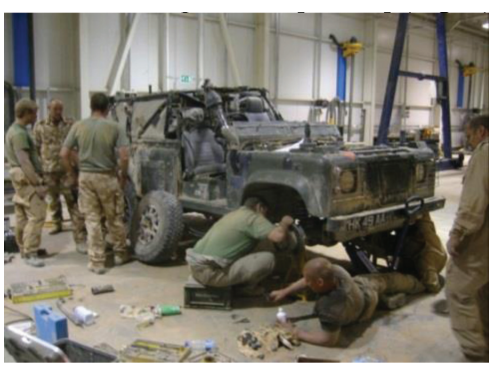


Figure 4. British team practicing expedient repairs (Photo obtained from Combat Service Support Group of NATO Standardization Agency, 2012).

In sum, we must conclude that proper usage of human potential within maintenance of weapon systems at appropriate level of availability should consist in:

- creating or appointing a centre that deals with training and studying technology applications;
- developing a digital platform of gathering, processing and popularizing information on maintenance technologies and procedures with the use of a form proposed in the standardization document common for the entire Armed Forces;
- organizing periodic trainings about maintenance tasks with the participation of experienced instructors—repair specialists in an appointed centre;
- inviting researches and public companies, occupied with the problems of military technology sustainment to participate in distributing the experiences and propagating knowledge on weapon systems availability;
- distributing information on techniques and methods of recovery and repairs among the staff of repair subdivisions, e.g. via periodical bulletins.

6 TECHNICAL RESOURCES

The system of weapon systems maintenance requires usage of technical resources, which differ significantly from the ones commonly used in other fields of economy. Technical potential of maintenance system under combat operations is based on four main elements: recovery vehicles, mobile workshops with universal equipment, specialist tools sets and spare parts kits (Smal & Smoła, 2011).

Recovery vehicles should provide evacuation and repairs of damaged equipment in field conditions. Trucked combat vehicle of Polish Army Land Forces are supported with special recovery vehicles like WZT-2, WZT-3, WPT Mors and Bergepanzer 2A2 (Fig. 5).

The presented vehicles perform well during large scale combat operations with the use of heavy



Figure 5. Recovery vehicle Bergepanzer 2A2 during lifting power pack of tank.

caterpillar equipment. However, the experiences of the components of the Polish Armed Forces from recent abroad operations and equipping the units with AMV Rosomak, indicates that there is a gap concerning wheeled combat vehicles. So far, maintained vehicle KRAZ 255 is being withdrawn from the Army as obsolete and TATRA 815 is being used mostly as semitrailer evacuation vehicle. Due to this, there is a necessity to purchase a new type of vehicle, which will be able to recover wheeled combat vehicles like BRDM or AMV Rosomak and conduct second level BDR for them (Smal & Stankiewicz, 2010). The tasks of such a vehicle would include: sling towing damaged vehicles, evacuation of mired down vehicles, supporting medical services in rescuing people out of damaged vehicles, executing expedient repairs of damaged vehicles in order to restore independent movement, standing overturned vehicles, reloading pallet containers, car bodies and weaponry system modules in field conditions.

In relation to the above, the future vehicle should be designed on a 8×8 basis chassis with large load capacity and increased mobility, furthermore, it should be equipped with among others (Smal & Smoła & Stankiewicz & Szukalski, 2010): an armoured cabin adjusted for weaponry installation, main and supporting winch, a winch for self-evacuation, a hydraulic crane, a hydraulic device for lifting and towing, a hydraulically steered plowshare, a system of supports and anchor bolts ensuring the vehicle's stability during the crane's and winches' operation and specialized equipment for repair works and rescues as well as a power generating unit with a combustion drive and communication means.

By combining the concept of a properly equipped wheeled recovery vehicle with battle damage repair technology, adequate for equipping our army, we could create an evacuation/repair vehicle, which would serve as an evacuation tractor and a repair sets carrier. Thus, the vehicle could prove useful in technical rescue as well as executing expedient on-the-spot repairs. Additionally, such a vehicle would be endued with road rescue equipment and could also be used during civil level crisis operations. At this point, we should again consider qualifications and experience of such a vehicle's crew, which would play a key part in proper realization of the entire element's tasks.

The mobile repair and service workshops located on chassis were designed in order to secure the operation of logistic subdivisions, which secure military actions in field conditions. There are some problems connected with contemporary mobile workshops, which are maintained in land forces, and those are types of workshops, dimensions of bodywork and equipment of workshops.

Currently there are two basic and eight auxiliary workshops maintained in Polish Armed Forces to conduct service and repair of wheeled and trucked vehicles. Basic workshops are supplemented with specialist tools sets at level 1, 2 or 3 dedicated to a given type of vehicle and; as the result, the workshops turn into specialist workshops. There are following kinds of basic mobile workshop: WOP—workshop designed for vehicle service that can be equipped with 5 box of KOR and WRP—workshop designed for vehicle repair that can be equipped with 7 box of KOR. Basic workshops make it possible to conduct a full range of service and repair but only with exchanging of units and parts. They aren't equipped enough to provide full diagnosis, verification, and regeneration of damage units and parts, therefore, there are used as additional auxiliary mobile workshops, among which we include: cylinders filling station, battery recharge station, machining workshop, electromechanical workshop, welding-tin workshop, engine repair workshop, fuel gear workshop, lubrication workshop, evacuation vehicles.

According to the literature the following trends might be considered when talking about the development of mobile workshops (Šafr & Chladil, 2005):

- lowering the types and the number of mobile workshops;
- providing basic technical parameters for land, air and rail transport, and shipment;
- using the functional bodies of a container type for higher organizational logistic levels, providing the maintenance of land combat vehicles used in missions.

Technical solutions examples in allied armies confirm the trend of mobile repair workshops development on the basis of loading containers (Furch & Smal, 2011). Repair subunits of the Land Forces of USA made use of the experiences gathered during utilization of M984 vehicles and PLS and devel-

oped equipment adjusted for executing overhauls and repairs in field conditions (M7 Forward Repair System—FRS). Basing on the solutions for PLS, FRS was created on a flat rack platform and can be moved with HEMTT trucks (Fig. 6). The presented solution significantly optimizes the operation of technical services ensuring higher weapon systems' availability and possibility of reacting to occurring threats under combat operations. FRS is ready to undertake tasks within 5 minutes from the stoppage of the basic vehicle (FRS, 2009). Execution of repairs is possible due to such equipment as: hydraulic crane with 5t load capacity, power generating unit, compressor, combustion unit, power tools, hand tools (ca. 560) and diagnostic devices sets. Constant development of technical solutions for field repair systems of military equipment is a characteristic feature of leading armies.

Having regard to the above and the unification of bolted and pivot connections, as well as, the use of standardized bearing and covering the differences between higher and lower services and repair, there is a proposition to replace the two basic workshops mentioned above with one mobile workshop designed to vehicle service and repair (Smal & Smoła, 2013). Additionally, considering the current trend to minimize parts regeneration, the number of auxiliary workshops should be reduced. The table below shows new configuration of mobile workshops maintained in Land Forces of the Polish Army (Table 1).

The workshops maintained in Polish Army are constructed on the basis of bodywork called "Sarna II" which is totally incompatible with very popular standardized containers (Šafr & Chladil, 2005). The standardized containers are cheap in manufacturing and transport, multi-role and compatible with many kinds means of transport. In most countries of NATO, containers are used as bodyworks for many sorts of workshops (Connors, 2003). The Polish Army will not avoid the same future; still, considering the costs; first of all, exchange and modernization of equipment in currently used workshops should be executed.

Discussing the unification of mobile workshops, basic logistic vehicle-carriers should be considered because there is no understandable reason for vehicles like STAR MAN 944 or 1466 to be purchased as the universal logistic carriers. The analysis of vehicles used by other armies has shown that universal vehicles should be equipped with jib hook to load every cargo in container outlines (all means of transport base on standardized containers). Universal vehicle should also be the basis for semi-trailer evacuation vehicle (Fig. 7). We can obtain high military equipment susceptibility to service and repair thanks to considering the mentioned facts (Smal & Szukalski, 2009).



Figure 6. FRS on a HEMTT-type vehicle during transportation (left), working post after removing from the vehicle (middle) and FRS during repair works (right) (Gray, 2007).

Table 1. Proposition of reducing mobile workshops number and types.

Current status	Proposed changes
WOP—workshop designed for vehicle service	WOR—workshop designed for vehicle service and repair
WRP—workshop designed for vehicle repair	
SŁB—cylinders filling station	SŁB—cylinders filling station
SŁA—battery recharge station	WEM—electromechanical workshop
WEM—electromechanical workshop	
WOM—machining workshop	WOMC—machining and heat treatment workshop
WSB—welding-tin workshop	
WRS—engine repair workshop	WRPP—power packs workshop
WAP—fuel gear workshop	WRUD—additional devices workshop
WOS—lubrication workshop	



Figure 7. The example of universal logistic vehicles which are able to load container cargos.

There are many propositions of solving the problem above. One of them is a container workshop constructed by 52 repair battalions (Fig. 8), but there also are some issues which should be improved. The workshop should be equipped with handle for jib hook to make it possible to load it on universal carrier; a side tent should be replaced by mechanical awning, and drawers should be replaced by mobile workshop wheelchair. Similar workshops effectively operate in other armies of NATO or are being currently created by them (Furch & Těšík & Glos & Marek, 2008).

Similar conditions to stationary should be created for mechanics who are conducting tasks in field conditions; therefore, they should execute service and repair in the same teams, with the same tools, and



Figure 8. The proposition of a new workshop for the Polish Armed Forces.

using the same procedures. The equipment of currently maintained mobile workshops is far different from stationary workshops. The modernization of it was terminated at the end of the 80's, hence over 20 years of technology gap (Smal & Smoła, 2010). The example of that is soldiering iron, which is very obsolete and cannot be used to repair complicated and delicate electronic systems. It is not possible to exchange all mobile workshops with modern container workshops taking into consideration the current economic situation of our country. Therefore, transition solution should be adopted, which main effort would be focused on equipment modernization of currently used workshops including the fact that the modernized equipment will be moved to a new container workshops in the future. Additionally, the purchased tools would be used in stationary workshops at the same time, which should allow to reduce costs. The tools and equipment of mobile workshops should be placed in special mobile workshop wheelchairs or boxes taking into account the specific conditions of maintaining sections activities, especially in the field conditions. It would facilitate moving them between stationary and mobile workshops and during field operation at the damaged vehicles (Smal & Smoła, 2011).

Specialized repair equipment is another element, which may significantly improve the conditions and efficiency of repairs and shorten the time of execution. The contemporary market of power tools and hand tools is very developed. This allows for very precise selection of equipment, according to the needs. Besides the standard durability, anti-corrosive or aesthetic properties, military tools should have several additional features, such as: permissible black colour (oxidation) or khaki green, low weight, multi-functionality, a higher safety coefficient during construction of tools, high ergonomics of the handle enabling longer work and greater torque (Fig. 9).

Pneumatic lifts are incredibly useful tools, which should be at the disposal of maintenance services. They may significantly improve realization of enterprises connected with lifting damaged vehicles in the workshop as well as in the field and facilitate recovery of vehicles mired down during operation. The lifts are elastic containers (bags), filled with exhaust fumes by a hose connected to the exhaust pipe of the repaired or neighbouring vehicles (Fig. 10). The fact that such lifts can be



Figure 9. The example of modern tools: power wrench (left), hammer screwdriver (middle), small gas welder (right).



Figure 10. Using pneumatic lifts for lifting vehicles (www.arbusa.com).

placed directly on the ground (e.g. snow, dirt, etc.), without the necessity of searching for hardened places (places of direct damage) is a significant advantage over the "classic" solutions. Lifting lopsided vehicles is possible, thus unsteadiness of traditional siphons is eliminated, which in turn decreases the probability of injuries.

Proper repair sets enabling elimination of military equipment's damages when access to specialized tools and spare parts is limited is another aspect of maintenance services proper functioning in the context of weapon systems availability (Fig. 11) (Smal & Smoła, 2010). The equipment of our repair subdivisions is mainly the one used during the former "Warsaw Pact" and is not adjusted to contemporary reality, nor the expeditionary character of actions. The ER/BDR repair sets should include the following groups of repair materials: glue composites, materials for eliminating damages of pneumatic, hydraulic and electric installations and plastic elements. They should also include universal repair materials, such as: regeneration tapes, tie bands, fan belts, seals, simmerings, etc. Completing sets should be based on scientific research and years of practical experience, the process should be continuous (Smal & Furch, 2011).

To sum up, modification of technical resources of the weapon system maintenance should include:

– purchasing a new type of recovery vehicle, which will be able to recover wheeled combat vehicle like AMV Rosomak and conduct recovery and repair tasks;



Figure 11. Level 1. BDR kits used by the Dutch (left) and Norwegian (right) armies.

– reduction and destination of mobile workshops type so they are more up-to-date concerning current challenges and needs facing land forces;
– in the first step, an exchange and modernization of equipment should be executed in currently used workshops, and in the second step a new type of container workshops should be introduced;
– proper temporary repairs kits should be introduced to the crews of fighting and recovery vehicles.

7 CONCLUSIONS

The crucial role of efficient and effective maintenance system in the field conditions is highlighted not only in the allied doctrines and rules but also in numerous publications concerning recently conducted combat operations. The appropriate documents allow for execution of improvised and temporary repairs in order to fast restore damaged weapon systems to battle area.

The conducted analysis of maintenance systems in other NATO armies indicates that it is a crucial element of any combat operations. Considering its complexity and significance, the system is being permanently improved and developed by numerous research, analysis and implementation of new concepts and solutions. Therefore, it seems that the process of new weapon systems acquiring should be modified in order to fulfil operation and logistics needs. As far as the battlefield maintenance of weapon systems at the appropriate level of task efficiency is concerned, it is very profitable to the weapon system since it would be characterized by high level of survivability, vulnerability and reparability in case of any damage. Additionally, there are necessary well-trained specialists, appropriate procedures and technologies in order to quickly execute maintenance tasks during combat operations.

It should be highlighted that the mobile repair system and equipment of the Polish Land Forces maintain units is largely obsolete and not adequate to requirements of contemporary battlefield. The rational organizing of maintain system of equipment used in the task mode seems to be matter of urgency. The division of maintain equipment and organization structure into peace and war time seems to be not rational and economic, especially if lack of sources for regular training is taken into consideration. It should be mentioned that the organization and technical solutions adopted in the Polish Land Forces do not fit into an expeditionary nature of operations conducted recently by Polish troops. As the analysis of numerous references have indicated, there are; commonly used by the allied armies, and easy to redeployment, mobile workshops and expedient repairs technologies, as well as, materials during expeditionary operations conducted in the remote battle areas. Another issue concerns a proper personnel preparation to battle damage assessment and repair, which can be achieved by providing permanent trainings for each maintain level personnel and including the gained experiences in handbooks, manuals and digital platforms. Finally, it should be claimed that the changes and modifications concerning the Polish Land Forces mentioned in the chapter are very slow, although they follow trends observed in allied armies.

There are many modern and efficient methods and technologies on the market that can be successfully applied to perform services and repairs of military equipment in the field. Taking this fact into account, an accessible solutions should be searched for by the military by means of numerous comparative experimental studies, as well as, economical and application analysis in order to find the best products and technologies considering specific requirements of a contemporary battlefield.

Statistics is an invaluable tool for collecting, processing and using of all information referring to maintenance of weapon systems, in particular, special computer systems designed for supporting maintenance and supply management like for example Condition Based Maintenance Plus. The use of these systems in the future should allow to eliminate a large portion of faults and defects resulting from faulty design, production technology or used materials and any other engineers solutions, as well as, take advantage of experiences and reports from executed already repairs. The implementation of computer system would support not only current maintenance planning and execution but also: permanent weapon systems improvement, design of new weapon systems, prediction of battle and maintenance faults, planning of recovery and repair operations, as well as, technical potential assessment, cost of repair calculation and stocks record to conducting repairs.

REFERENCES

Alp-4.2(A). 2010. Land Forces Logistic Doctrine.

Backlund, A. 2000. The definitions of system. *Kybernetes* vol. 29, no. 4: 444–451. ISSN 0368-492X.

Bellinger, G. *Outsight*. 2002. Available from: <http://www.radix.net/~crbnblu/musings/>.

Connors, S., C. (Eds) & Foss., Ch., F. (Eds). 2003. *Jane's Military Vehicles and Logistics, 2003–2004*, Jane's Information Group, 24 Edition. ISBN-10 0710625545.

DD/4.2. 2007. *Logistic doctrine of Land Forces* (In Polish). Warsaw: Headquarters of The Polish Land Forces.

Egner, D. & Mullins, D. 2007. *Combat Damage Incident Reporting System (CDIRS). Aircraft Survivability*, no. Summer: 20. Available from: <https://jaspo.wpafb.af.mil/>.

FM 4-30.31 (FM 9-43-2). 2006. *Recovery and Battle Damage Assessment and Repair*.

FRS. 2009. M7 Forward Repair System (FRS), URL: <http://www.armyproperty.com/Equipment-Info/M7-FRS.htm>.

Furch, J. & Těšík, O. & Glos, J. & Marek, J. 2008. In *Proceedings of Armament and Technics of Land Forces.* Liptovský Mikuláš: Akadémia Ozbrojených Síl Generála M.R. Štefánika, ISBN: 978-80-8040-356-0.

Furch, J. 2010. New Trends in a Vehicle Maintenance System. *Advances in Military Technology*, vol. 5, no. 2: 111–119. ISSN 1802-2308.

Furch, J. & Smal, T. 2011. Project on a container workplace to perform the maintenance of land combat vehicles in field conditions. *The Journal of Science of the Gen. Tadeusz Kosciuszko Military Academy of Land Forces*, no. 3: 323–333. ISSN 1731-8157.

Gray, Ch., N. 2007. Standard Automotive tool set: More than Just an improved common set. *Army Sustainment*, no. January-February: 16–17. ISSN 2153-5973.

Gang, N. & Bo-Suk, J. & Pecht, M. 2010. Development of an optimized condition-based maintenance system by data fusion and reliability-centered maintenance. R*eliability engineering & system safety,* vol. 95, issue 7. ISSN 0951-8320.

Jackson, R. 2009. Battle Damage Assessment and Repair (BDAR). *Aircraft Survivability*, 2000, no. Winter: 25–26. Available from: <http://jtcg.jcte.jcs.mil:9101>.

Niziński, S. 2002. *Maintenance of technical object* (In Polish). Warsaw-Sulejowek-Olsztyn-Radom: The Library of Maintenance Problems, Institute of Technology and Maintenance. ISBN 8372042845.

Nowakowski, T. 2011. *Reliability of Logistic Systems* (In Polish). Wroclaw: Publishing office of the University of Technology in Wroclaw. ISBN: 978-83-7493-594-4.

Šafr, G. & Chladil, J. 2005. *The analysis of military repair vehicles* [Research Report]. Vyškov: VTÚPV.

Sienkiewicz, P. 1983. *Engineering of systems* (In Polish). Warsaw: Ministry of Defence. ISBN 83-11-06851-8.

Smal, T. & Rośkowicz, M. 2009. The battlefield maintenance of aircraft equipment (In Polish). *Quartelly Bellona*, 2009, no. 4(659): 170–175. ISSN 1897-7065.

Smal, T. & Szukalski, M. 2009. Logistic susceptibility of military equipment (In Polish). *Logistyka* no. 6, CD-Room. ISSN 1231-5478.

Smal, T. & Smoła, T. & Stankiewicz, G. & Szukalski, M. 2010. *The analysis of organizational and technical possibilities to conduct emergency repairs of military equipment using modern repair technologies* (In Polish) [Research Report]. Wroclaw: The Gen. T. Kościuszko Military Academy of Land Forces, Wroclaw.

Smal, T. & Smoła, T. 2010. Materials and equipment for quick repairs of technical objects (In Polish). *Logistyka* no. 2, CD-Room. ISSN 1231-5478.

Smal, T. & Stankiewicz, G. 2010. Development trends of service and repair means in the Polish Armed Forces (In Polish). *Logistyka* no. 6, CD-Room. ISSN 1231-5478.

Smal, T. & Smoła, T. 2011. Transition modification of mobile workshops system—polemic article. *Deterioration, Dependability, Diagnostics*, Brno: University of Defence: 129–135. ISBN 978-80-260-0633-6.

Smal, T. & Furch, J. 2011. Expedient Repairs—Analysis of Possibilities and Needs. *Advanced in Military Technology*, no. 4. ISSN 1802-2308.

Smal, T. 2011. Battle damage repair systems in selected NATO armies. *Deterioration, Dependability, Diagnostics*, Brno: University of Defence: 33–40. ISBN 978-80-260-0633-6.

Smal, T. & Smoła, T. 2013. Optimization of technical support (In Polish). *Przegląd Wojsk Lądowych* no. 01(061): 56–61. ISSN 1897-8428.

Stanag 2406. 1995. *Land Forces Allied Logistics Doctrine—ALP-9(B).*

Stanag 2418, 2009. *Procedures for expedient repair, including battle damage repair.*

Surviac Bulletin. 2002. F/A-22 Live Fire Repair. Vol. XVIII, issue 2: 1–4. DSN 785-4840. Available from: <www.bahdayton.com/surviac/surviacbulletin.htm>.

TM 9-2320-280-20-1/2/3. 1996. *Technical manual units maintenance of HMMWV, vol. 1, vol. 2, vol. 3.* Washington.

Uhl, T. 1999. *Contemporary development trends of machines monitoring and diagnosing* (In Polish). Warsaw: PAK.

URL: <http://www.arbusa.com/Products/Tow-Straps-And-Recovery-Gear/Exhaust-Jacks/46.aspx>, [cited 2010-08-30].

Vališ, D. & Mlynczak, M. & Nowakowski, T. 2011. How to manage risk? An approach based on standards. *Maintenance problems*, vol. 1, no. 80, p. 137–148. ISSN 1232-9312.

Vališ, D. & Vintr, Z. & Malach, J. 2012. Selected aspects of physical structures vulnerability—state-of-the-art. *Maintenance and Reliability—Eksploatacja i Niezawodność,* vol. 14, no. 3: 189–194. ISSN 1507-2711.

Vališ, D. & Vintr, Z. 2006. Vehicle Maintenance Process Optimisation Using Life Cycle Costs Data and Reliability-Centred Maintenance. *Proceedings of the First International Conference on Maintenance Engineering*. Beijing: Science Press. ISBN 7-03-018064-X.

Vališ, D. & Vintr, Z. 2006. Dependability of Mechatronics Systems in Military Vehicle Design. *Safety and Reliability for Managing Risk—Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006)*. London: Taylor & Francis. ISBN 0-415-41620-5.

Wasmund, T., L. 2000. Advanced Joint Effectiveness Model. In: *Aircraft Survivability*, no. Summer. [cited 2009-06-11]. Available from:<https://jaspo.wpafb.af.mil/>.

You, S. & Krage, M. & Jalics, L. 2005. *Overview of Remote Diagnosis and Maintenance for Automotive Systems*. Reprinted from Vehicle Diagnostics, Detroit: SAE International. ISSN 0148-7191.

Yong-jun, S. & Bing-shang, L. 2009. Application of Prognostics and Health Management Technology in Equipment Maintenance. Vehicle & Power Technology no 2. ISSN 1009-4687.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimum CTV fleet selection for offshore wind farm O&M activities

Y. Dalgic
Department of Naval Architecture, Ocean and Marine Engineering, University of Strathclyde, Glasgow, UK

I. Dinwoodie
Wind Energy CDT, University of Strathclyde, Glasgow, UK

I. Lazakis
Department of Naval Architecture, Ocean and Marine Engineering, University of Strathclyde, Glasgow, UK

D. McMillan
Institute for Energy and Environment, University of Strathclyde, Glasgow, UK

M. Revie
Department of Management Science, University of Strathclyde, Glasgow, UK

ABSTRACT: The focus of this paper is to provide decision support for the selection of a Crew Transfer Vessel (CTV) fleet for the offshore wind farm maintenance operations. This is achieved through analyses of environmental conditions, investigation of failures, and assessment of vessel operations. The developed methodology and analysis enable operators to decide the specification of CTVs which will bring the optimum financial benefit, considering both the enhancement of the offshore wind farm power generation as well as the minimisation of the total O&M cost.

1 INTRODCUTION

Offshore wind is becoming increasingly attractive to developers due to a number of advantages over the onshore environment. These include the availability of offshore areas in which major projects can be developed, the lack of limitations associated with the visual impact and noise of the wind turbines, higher wind speeds, and the lower turbulence levels in the offshore environment. Contrary to these advantages there are a number of increased challenges when moving offshore; wind turbines are situated in the highly corrosive sea environment, and subject to loads that are not often experienced onshore; therefore offshore wind farm operators suffer from greater maintenance issues. Harsher wind and wave conditions limit the operability of these vessels and eventually the accessibility of offshore wind farms. Currently, onshore wind energy costs £74/MWh, alternatively offshore wind energy costs £150/MWh, which the industry has to commit to bringing the cost of offshore wind down to £100/MWh in order to sustain the competiveness and the development in the offshore industry (WindPower Offshore, 2012).

According to a report prepared by WindPower Offshore (2013), the proportion of the CTVs to the number of vessels in the entire offshore wind market is 40.6%, while cabling vessels, jack-up vessels, heavy lift vessels and other vessel account for 21.3%, 16%, 12%, and 10%, respectively. Despite the dominance of the CTVs, there is no regulation specifically for offshore wind farm service vessels (WorldWind Technology, 2013). Technicians performing offshore maintenance are classed as passengers, and therefore if there are more than 12 technicians on-board, this specific vessel is classified as passenger vessel, which introduces extensive safety legislation and decrease operational flexibility. Furthermore, weather conditions restrict access of the CTVs; larger vessel may have better operational capabilities but charter rates escalate quickly. In this respect, it is essential to use the optimal vessels for the jobs involved, but also charter them at the right time at the minimal price.

It has been identified that the minimisation of the vessel costs has significant potential to reduce the overall Operation and Maintenance (O&M) expenditure. Although, CTVs are highly utilised within an offshore project lifecycle, the influence of CTVs on the entire O&M lifecycle cost has not been considered thoroughly. Considering current offshore wind O&M models, it has been identified that the CTV related operations are generally

neglected or modelled in a crude way. As such, the focus of this research is the investigation of optimum CTV fleet size and the examination of different CTV types which bring economic and operational benefits. Considering different climate parameters, failure characteristics of the turbine components, and the operational characteristic of the CTVs, an exhaustive model is presented which provides support for the long term offshore wind O&M planning.

The paper is structured as follows; in Section 2, the common procedures, aspects and issues associated with maintenance of offshore wind farms are presented. Through the observations in that section, a modelling methodology is specified in Section 3. A case study is presented in Section 4 in order to validate the proposed model. In Section 5, the results of the case study are evaluated. Final recommendations are provided in Section 6.

2 LITERATURE REVIEW

2.1 *Economic assessment*

O&M activities represent a significant share of the expenses during the lifecycle of the projects (Kaldellis and Kapsali, 2013). O&M costs can be considered to comprise of labour costs, material costs, access vessels & lifting vessels costs and potential revenue losses. In this respect, it is important to identify the critical elements that can significantly reduce overall costs.

Previous studies have identified that the development of new O&M vessels is particularly important; since the costs for vessels make up 73% of the total O&M costs (Fingersh et al., 2006, Junginger et al., 2004, Krohn et al., 2009, Lazakis et al., 2013). Van Bussel and Zaaijer (2001) showed that irrespective of wind turbine design, the cost of lifting operations by using a vessel accounted for more than 50% of the overall O&M costs. Dinwoodie et al. (2013) evidenced that the proportion of vessel associated costs to the total O&M costs is the largest; therefore optimisation of vessel costs is the key to minimise the overall project costs; considering the fact that economic benefit from producing more energy by increasing the availability does not always leads to higher profits since it may not compensate the increase in the total O&M costs (Santos et al., 2014).

2.2 *O&M activities and available vessels*

Minor failures occur frequently but lead to shorter downtimes and the cost of repairs are cheaper; however, numerous minor failures have the potential to contribute significant downtime. In this respect, Faulstich et al. (2011) studied the failure rates of wind turbine components identifying that the minor failures account for 75% of all turbine failures. In the case of minor failures such as; electrical system, electronic control, sensor and hydraulic system failures, vessels for minor maintenance are utilised in the repair operations. CTVs are used for wind turbine repairs, which do not require heavy equipment transport or heavy crane operations. CTVs can be equipped with dynamic positioning and motion-compensating gangways in order to improve the operability and accessibility but these technologies currently have a high associated cost.

Monohull boats, small catamaran vessels and Small Waterplane Area Twin Hull (SWATH) vessels are generally utilised in minor maintenance operations, which allow operators to keep the cost of minor maintenance operations at acceptable levels. Catamaran configurations are often the preferred choice but operations are restricted to relatively low wave heights (Tavner, 2012). The most distinctive characteristics of these vessels are high speed, small deck spaces, small crane capacities and safe access to wind turbine structures that will allow operators to take quick actions in case of urgent repairs.

3 METHODOLOGY

The developed methodology is illustrated in Figure 1. The overall model consist of four blocks. The inputs of the model are introduced in the Inputs block. The inputs are processed in the Data Process block and then considered for the Simulations block. In the Simulations block, processed climate series, forecasted failure behaviours and vessel accessibility and operability values are synthesised and OPEX calculations are performed. The cost elements which influence offshore O&M activities are then employed along with these results to support the decision making. Final decision choices are determined not only from a power production point of view, but also in terms of cost, revenue and profit.

3.1 *Inputs block*

Wind speed, wave height and wave period observations constitute the climate parameters. Whilst all the climate parameters influence vessel operations, wind speed has also impact on power generation. Failure rates and repair times denote the sequence of minor failures and the time required to repair these failures. The repair time values are the periods associated with actual repairs, excluding the reaction time. Wind farm related attributes represent the number of turbines in the farm, individual turbine capacity

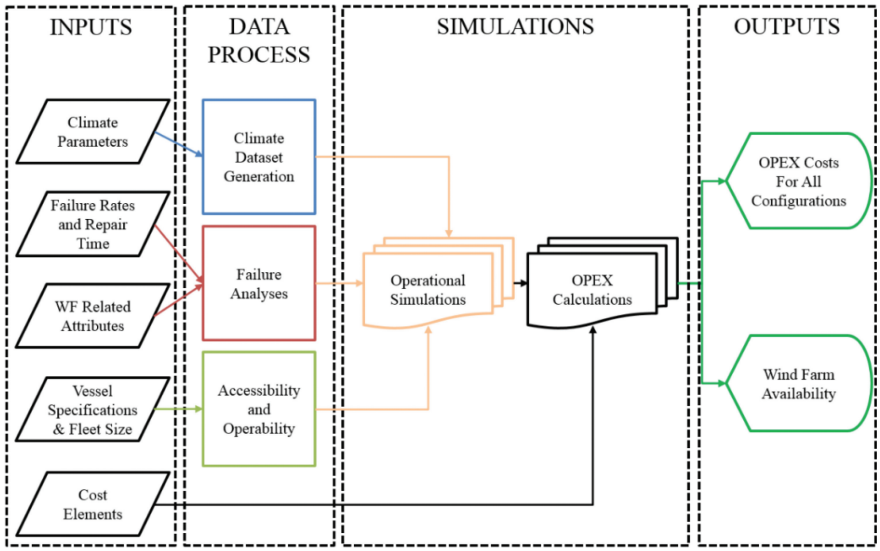


Figure 1. Proposed methodology.

and average distance from O&M port. Vessel specifications and fleet size denote the number of vessels in the fleet; also structural and mechanical properties of these vessels. Cost elements symbolise daily charter cost of vessels, fuel cost, electricity price, and technician annual salaries.

3.2 *Data process block*

Data process block where the datasets from inputs block will be organised and evaluated. In this respect, climate dataset generation, failure analyses, and accessibility & operability calculations are performed prior to the simulations and OPEX calculations. In the following sections, these analyses will be explained in details.

3.2.1 *Climate dataset generation*

The climate dataset for simulation comprises of a synthetic wind speed, significant wave height and wave period time series. These are generated using a Multivariate Auto-Regressive (MAR) model, shown in Equation 1, normalised by the mean of the data μ where X_t is the simulated wind speed at time-step t, n is the number of variables, X_n is a variable state vector, A_n is a matrix of the MAR model coefficients and ε_n is a noise vector with mean zero and covariance matrix of the data, order p (Box and Jenkins, 1970).

$$X_t = \mu + \varepsilon_n + \sum_{i=1}^{p} A_n (X_{n-i} - \mu) \quad (1)$$

In order to apply Equation 1 to a wind and wave data set a transformation must be applied in order that the data set mean and variance are stationary and approximate a Gaussian distribution. It is necessary to apply the Box-Cox transformation described in Equations 2 and 3, where Y_t is the transformed series, Hs is significant wave height and Λ is the transform coefficient. A Fourier series fit of the seasonality observed in the transformed data can then be removed (Soares et al., 1996). The transfer coefficient value that minimises skewness is identified and used to give the closest approximation of a normal data set.

$$Y_t = \frac{Hs_t^{\Lambda-1}}{\Lambda}, \quad for\ \Lambda \neq 0 \quad (2)$$

$$Y_t = T(Hs_t) = ln(Hs_t), \quad for\ \Lambda = 1 \quad (3)$$

Having transformed the data, Equation 1 can be applied to both wind and wave data. The determination of MAR coefficients and model generation is implemented using the arfit algorithm in MATLAB (Schneider and Neumaier, 2001). Order is chosen by optimising Schwarz's Bayesian Criterion and coefficients are estimated using a stepwise least squares estimation process. In order to preserve the variability in performance driven by climate, a unique synthetic time series is generated for each simulation. Using the described methodology the key characteristics of mean and variance as well as annual distribution, access window duration periods and inter-time step correlation are

preserved. In addition, correlation between different climate parameters are preserved.

3.2.2 *Failure analyses*

The wind turbine system failure process is implemented using the methodology developed in (Billinton, 1970). The wind turbine is characterised as a series of subsystems that can each exist in a discrete state during each simulation time-step. The probability of moving from an operating state to a failed or reduced operating state is governed by the hazard rate h(t), which is defined as the probability of observing a failure in a specified time interval. The hazard rate through the life cycle can be represented using the Weibull function shown in Equation 4, where the shape parameter β determines the gradient of the hazard rate and scale parameter ρ corresponds to the frequency of observed failures. This methodology allows for changing hazard function throughout the simulated life time. As a greater understanding of offshore wind turbine failure behaviour is developed through operator experience it will become possible to represent design life changes or impacts of climate and maintenance.

$$h(t) = \rho\beta t^{\beta-1}, \ for \ t \geq 0 \tag{4}$$

At each time-step a uniformly distributed random number, R, in the interval 0 to 1 is generated and used to determine if a failure has occurred using the criteria in Equation 5. Failure transition if:

$$R > (1 - h(t)) \cdot \frac{\Delta t}{8760} \tag{5}$$

Repair is then simulated based on the climate time series. If a turbine is in a failed state it will return to a working state when sufficient access time has been observed or when a series of repair actions have been performed corresponding to a completed maintenance action.

3.2.3 *Accessibility and operability*

CTVs operate in waves; through analysing wind speed and significant wave height values, it is possible to identify the time-steps/days in which the CTVs can operate or stay in the specified port. In the proposed methodology, the transit time delays due to speed reduction under different climate conditions are considered by also analysing the wave period values. In this context, accessibility and operability analyses are constituted from 5 sequential steps;

- Calculation of total calm water resistance
- Calculation of additional wave resistance
- Calculation of total resistance
- Calculation of speed loss in wavy sea
- Calculation of transit time

The total calm water resistance $R_{T\text{-}Calm}$ of the CTVs can be calculated from the Equation 6 and 7;

$$P_E = P_B / \eta_T \tag{6}$$

$$R_{T\text{-}Calm} = P_E / V \tag{7}$$

where P_B = break power; P_E = effective power; η_T = total efficiency of the vessel; and V = vessel speed. In the Equations above, effective power is the necessary power to move the vessel through water, and break power is the power output of the engine without power loss caused by gears, transmissions or friction force.

In heavy seas, waves cause additional resistance on the vessel hull. The most accurate method to calculate additional resistance due to waves is model testing; alternatively, Jinkine and Ferdinande (1973) developed an empirical formulation for predicting the added resistance for fast cargo ships in head seas. The dimensional added resistance is related to the non-dimensional added resistance coefficient by Equation 8,

$$R_{AW} = \sigma_{AW} \ (\rho g \zeta_A^2 B^2 / L) \tag{8}$$

where R_{AW} is non-dimensional added resistant coefficient, σ_{AW} is non-dimensional added resistant coefficient, and ζ_A is wave amplitude; ρ is density of water, g is acceleration due to gravity, B breadth of CTV, and L is length of CTV. The total resistance of the vessel, R_T is the summation of calm water resistance and added resistance due to waves in the ocean (Equation 9).

$$R_T = R_{AW} + R_{T\text{-}Calm} \tag{9}$$

Due to the fact that time-step approach is utilised in the simulations, wave height and wave period values in each time-step will be different which creates variation in added resistance and eventually total resistance of the CTVs. Therefore, the equations above have to be applied to every time-step of the simulations.

Whilst a CTV is traveling in a wavy sea, skipper can keep the power constant and decrease the speed or keep the speed constant and increase the power. In this study the power and thrust of the CTVs will be kept constant and speed will change with the influence of added resistance. In order to calculate the speed loss in each time-step under the condition of constant power and thrust, Equations 10 and 11 derived by Berlekom et al. (1974) and Berlekom (1981) can be utilised.

$$\frac{\Delta V_i}{V_0} = \sqrt{1 + \frac{R_{AW_i}}{R_{T_i}}} \quad (10)$$

$$V_{A_i} = V_0 - \Delta V_i \quad (11)$$

where R_{AWi} = Added resistance at time-step i; R_{Ti} = Total resistance at time-step i, V_0 = Operational speed of CTV; ΔV_i = Speed loss at time-step i; V_{Ai} = Achievable speed at time-step i.

Transit time is calculated through adding the individual distances that are logged in each time-step, which are the multiplication of achievable speed at time-step i and interval (Equation 12). When the summation of these distances become equal to the total distance between port and offshore wind farm, it is accepted that the vessel has approached to the wind farm site (Equation 13).

$$Distance_i = Time\ Step\ interval \times V_{A_i} \quad (12)$$

$$Total\ Distance = \sum_{0}^{i} Distance_i \quad (13)$$

3.3 *Simulations block*

The simulations are performed through synthesising all the processed climate, failure and operational information received from data process block. At the first stage, the failure types and time-steps are identified and assigned to the specified turbines. In the repair strategy, climate parameters and accessibility calculations are considered together. Following the failure identification and allocation, accessible & operable days are identified. Due to the fact that current operational practices are on shift bases, the same approach is adapted in this study; therefore working hours are limited by a specified shift duration. However, climate parameters may not allow CTVs to leave the port or transport technicians to wind farm within specified shift or allow only a limited period in the shift. In this respect, the maximum weather window is calculated in the shift in order to identify the maximum period that the technicians can work.

Additionally, there may be cases that the time spent on the journey might be substantially longer. Therefore, a 'minimum working limit' has to be defined for making a working shift acceptable and cost-effective. The 'minimum working limit' will create an extra constraint for the O&M activities. If the maximum weather window is shorter than the minimum working hour, this specific day is considered as inaccessible day.

The repair simulations are performed on daily bases. After identifying the day that the repair can be performed, a CTV is allocated to the failed turbine. The repairs are cumulative, which means if the repair cannot be completed within a single shift, the remaining part can be completed in the following accessible day. When a repair day is completed, the following day is simulated. If there is failure in that day, the same approach is implemented. Otherwise, the following day is simulated. The simulations are completed when the days simulated reaches the length of the simulations.

3.4 *Outputs block*

Outputs of this study are the average MTTR for all turbine components, average availability, the ratio of completed scheduled maintenance, power produced, power loss, revenue loss, and profit values due to the change of fleet size and CTV capabilities. These outputs provide sufficient information in order to assess the influences of changes and bring a solution for the fleet optimisation problem. Through considering all the parameters, the optimal fleet size and CTV type are decided. Potential alternatives, such as increase in crew size, improvement in failure characteristics, can be investigated following the decision of fleet size and CTV type.

4 CASE STUDY

In order to validate the proposed model, a case study which captures the influence of fleet size variation on MTTR, power production, availability, and profit values, was performed. In the simulations, two different CTVs were examined, which provide not only the flexibility of comparison between the size of fleets, but also the selection of CTVs which brings the most economic advantage. Table 1 shows the specifications of CTVs; CTV-1 has better capability than CTV-2, on the other hand daily charter rate and fuel consumption

Table 1. CTV specifications.

	CTV-1	CTV-2
Vessel type	Catamaran	Catamaran
Length (m)	26	19.1
Demi-hull breadth (m)	3	2
Draught (m)	2.05	1.3
Displacement (tons)	145.7	50
Speed (knots)	24	24
Installed power (kW)	1790	1418
Op. wave height (m)	1.5	1.25
Op. wind speed (m/s)	25	25
Fuel cons. (l/h)	446	316
Charter rate (£/day)	3250	2000
Technician capacity	12	12

values of CTV-2 are less than the values associated with CTV-1.

Tables 2 and 3 represent the failure rates, cost of repairs, required time and the technicians that will be allocated to the turbines. These values are adapted from the reports prepared by Poore and Walford (2008) a Wilkinson and Hendriks (2007). At this stage, it is important to highlight that the knowledge related to failure rates of offshore wind turbines are very limited, therefore, it will be possible to utilise more accurate offshore wind failure rates in the future using the developed modelling framework.

Table 2. Failure rates and repair costs of components.

No.	Failure types	Failure rate (times/year)	Repair cost (£)
1	Manual restart	8.79	–
2	Blade	1.48	20300
3	Pitch system	0.08	7150
4	Hub	0.185	4300
5	Main shaft & bearings	0.185	14000
6	Gearbox	0.08	3250
7	High-speed shaft	0.19	3250
8	Mechanical brake	0.04	2500
9	Generator	0.08	12000
10	Control system	0.24	4150
11	Yaw system	0.12	10800
12	Hydraulic services	0.12	1300
13	Power electrics	0.24	4150
14	Transformer	0.02	15400
15	Tower	0.19	5000

Table 3. Required time and technicians for repairs.

No.	Failure category	Repair time (Hours)	Required tech.
1	Manual restart	1	2
2	Blade	8	2
3	Pitch system	5	2
4	Hub	4	2
5	Main shaft & bearings	4	2
6	Gearbox	4	2
7	High-speed shaft	3	2
8	Mechanical brake	2	2
9	Generator	4	2
10	Control system	4	2
11	Yaw system	3	2
12	Hydraulic services	3	2
13	Power electrics	3	2
14	Transformer	5	2
15	Tower	8	2

Table 4. Additional attributes.

No.	Failure category	
1	Number of simulations	100
2	Number of years	20
4	Number of turbines	100×5 MW
6	Scheduled maintenance	100 man-hour/ year/turbine
7	Electricity price	0.137 £/kWh
8	Staff cost	60000 £/year
9	Fuel cost	0.83 £/litre
10	Distance to shore	20 nmiles
11	Minimum working	2 hours
12	Daily shift	8am–8pm

Table 4 represents the additional attributes required to run the simulations. Due to the fact, the generated climate datasets show variations, 100 different climate datasets are generated prior to the simulations, and these generated climate dataset are utilised for each fleet size. Therefore, the climate influence is captured by running 100 simulations for each fleet size, on the other hand consistency is secured by utilising the same climate datasets for each fleet size.

5 RESULTS

This section presents the simulated results for the specified case studies. Figure 2 demonstrates the annual availability simulated across different CTV configurations. There is an inherent inter-annual variability driven principally by the climate and failure rates which both have significant variability between years. It can be seen that increasing the number and capability of the CTV fleet reduces the degree to which inter annual variation occurs as well as improving average availability. This result is explained due to the increased operational threshold reducing the observed inaccessibility and consequently reducing uncertainty in performance from climate. Increasing the access threshold of CTV fleet further will reduce the variability from climate further but there are practical technology limits and associated costs with improved vessel design.

Figure 3 shows the downtimes of offshore wind turbine components due to minor failures under the influence of fleet size increase. Whilst the left vertical axis represents the component MTTR values, the right vertical axis represent the mean MTTR values for the entire offshore wind turbine system. The values on the horizontal axis is the size of fleet and the values ‘1’ and ‘2’ denote the category of CTV in the fleet. Due to the fact that

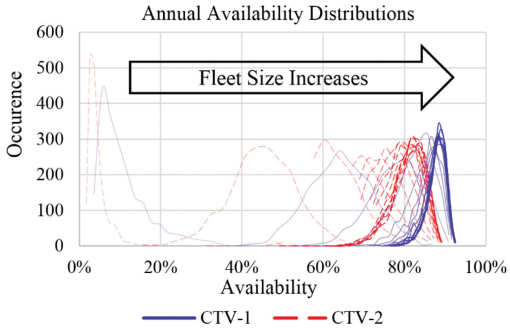


Figure 2. Annual availability distributions.

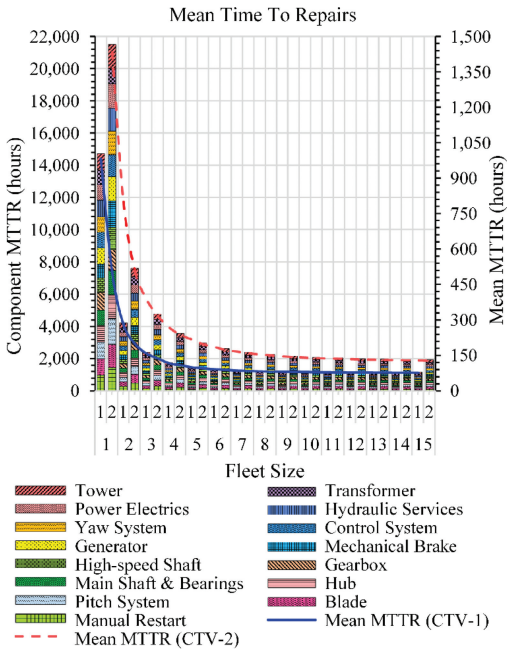


Figure 3. MTTR values for different fleet compositions.

increase in the fleet size provides more flexibility in the O&M activities, the reaction times to failures and eventually the downtimes of the minor failures decrease substantially. As explained in the previous section, the operational capabilities of CTV-2 are lower than CTV-1; therefore, MTTR values are higher for the fleets which consist of CTV-2. Additionally, the improvement on MTTR values decreases with the increase in the size of fleet for both CTV categories.

In contrast to the MTTR values, the power production values escalate with the increase of fleet size regardless of CTV category (Fig. 4). Due to the fact that maximum theoretical power that

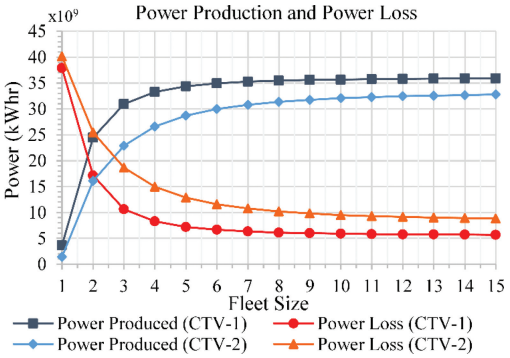


Figure 4. Power produced and power loss.

can be generated is unrelated to the fleet size or CTV capabilities, the power loss values decrease proportional to the increase in power production. The reason that all the graphs in Figure 4 become approximately straight after a critical fleet size is the maximum accessibility has been achieved by the specified vessels.

Wind farm availability and completed scheduled maintenance values are shown in Figure 5. Availability values show similar trends to the power production values and increase when the fleet size becomes larger. For all fleet compositions, the availability values are lower for the fleets with CTV-2. The reason is the number of accessible days within a year for CTV-2 is lower than the number of accessible days for CTV-1. Therefore, it will not be possible to reach equivalent productivity by chartering a larger number of CTV-2 s. With regard to completed scheduled maintenance values, it can be seen that scheduled maintenance tasks can be completed within simulation period in both cases; however the size of the CTV-2 fleet has to be larger to achieve comparable performance with the CTV-1 fleet.

When the distribution of costs that contribute to total O&M cost is analysed, the transport cost which is the summation of fuel cost and daily charter rate cost, dominates the total O&M cost as shown in Figure 6. The vertical axis represents the costs associated with each cost attribute; the values on the horizontal axis is the size of fleet and the values '1' and '2' denote the category of CTV in the fleet. At this stage, it is important to highlight that the O&M tasks in this study are the repairs due to minor failures of the turbine components; therefore the values in Figure 6 represent the costs associated with minor O&M activities. The staff cost is directly proportional to the fleet size; therefore the staff cost increases £720,000/per-year when a new CTV is added to the existing fleet. The red and blue lines show the total O&M cost which is always

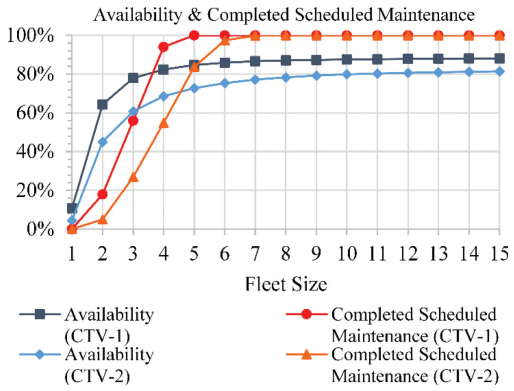


Figure 5. Availability and completed scheduled maintenance.

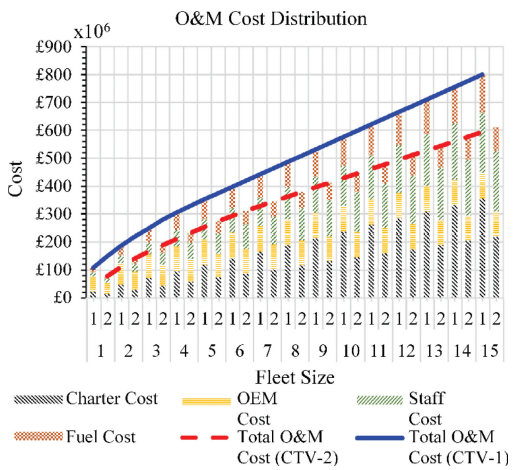


Figure 6. O&M cost distribution.

higher for the CTV-1 fleets than CTV-2 fleets due to higher daily charter rate and fuel consumption of CTV-1.

Considering these results, the escalation of fleet size brings a reduction in MTTR and lost revenue, increased power production, availability, and completion of scheduled maintenance values; however, there is a corresponding increase in all aspects of the costs. In this context, the optimum size of the fleet has to be defined through assessing the revenue loss and profit values; because the revenue and profit values reflect the level of economic benefits achieved through increasing the fleet size. In this respect, Figure 7 shows how these features are formed. For the CTV-1 fleets, financial loss decreases and profit increases until fleet size reaches a fleet of 7 vessels. If the CTV-1

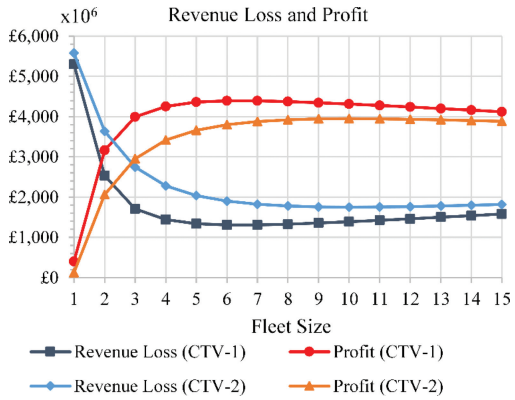


Figure 7. Revenue loss and profit.

fleet size becomes larger than 7, the profit starts to decrease and therefore revenue loss increases. This is because, extra costs cannot be covered anymore by the production increase. From the CTV-2 point of view, optimum fleet size is 10 vessels. As for the CTV-1 fleet, revenue loss decreases and profit increases until fleet size reaches 10. Therefore, the optimum fleet sizes for CTV-1 is 7, for CTV-2 is 10.

When the simulation results are compared between CTV categories, CTV-1 clearly shows both operational and economic benefits. Although, CTV-2 has lower fuel consumption and daily charter rate, the number of days accessible by CTV-2 is significantly low; thus the utilisation of CTV-2 is low. This situation causes a substantial decrease in the availability and profit values.

6 FINAL DISCUSSION AND CONCLUSION

This article relates to the current issues of the offshore wind O&M cost optimisation; considering the influence of varying fleet sizes and CTV characteristics. A model was introduced with the objective of identifying the most cost effective CTV and the optimum fleet which brings economic and operational benefits. In order to assess the accuracy of the proposed model and to generate realistic results, the model was applied to a case study wind farm.

The results indicate that a CTV with better capability brings great economic and operational advantages, even though that CTV has higher daily OPEX cost. It is also identified that the profit increases and the financial loss decreases until the fleet size is reached an optimum level. On the other hand, the fleets that are larger than optimum result

in an increase in the total O&M cost which cannot be compensated by the economic benefit from producing more energy.

REFERENCES

Berlekom, W.B.V. 1981 Wind Forces on Modern Ship Forms—Effects on Performance. *Transactions of the North East Institute of Engineers and Shipbuilders,* 97.

Berlekom, W.B.V., Tragardh, P. & Dellhag, A. 1974 *Large tankers—Wind coefficients and speed loss due to wind and sea*, Royal Institution of Naval Architects.

Billinton, R. 1970 *Power system reliability evaluation,* New York, Gordon and Breach.

Box, G.E.P. & Jenkins, G.M. 1970 *Time series analysis: forecasting and control,* San Francisco; London, Holden-Day; [Maidenhead]: Distributed by McGraw-Hill.

Dinwoodie, I., Mcmillan, D., Revie, M., Lazakis, I. & Dalgic, Y. 2013 Development of a Combined Operational and Strategic Decision Support Model for Offshore Wind. *Energy Procedia,* 35, 157–166.

Faulstich, S., Hahn, B. & Tavner, P.J. 2011 Wind turbine downtime and its importance for offshore deployment. *Wind Energy,* 14, 327–337.

Fingersh, L., Hand, M. & Laxson, A. 2006 Wind Turbine Design Cost and Scaling Model. National Renewable Energy Laboratory.

Jinkine, V. & Ferdinande, V. 1973 A method for predicting the added resistance of fast cargo ships in head waves. *International Ship Building Progress,* 21.

Junginger, M., Faaij, A. & Turkenburg, W.C. 2004 Cost reduction prospects for the offshore wind energy sector. *Wind Engineering,* 28, 97–118.

Kaldellis, J.K. & Kapsali, M. 2013 Shifting towards offshore wind energy-Recent activity and future development. *Energy Policy,* 53, 136–148.

Krohn, S., Morthorst, P.-E. & Awerbuch, S. 2009 The Economics of Wind Energy. Brussels, EWEA.

Lazakis, I., Turan, O. & Rosendahl, T. 2013 Modelling of vessel and equipment cost for the maintenance activities of an offshore tidal energy array. *Proceedings of the PRADS2013, 20–25 October 2013.* Changwon City, Korea.

Poore, R. & Walford, C. 2008 Development of an Operations and Maintenance Cost Model to Identify Cost of Energy Savings for Low Wind Speed Turbines. Washington, USA, National Renewable Energy Laboratory.

Santos, F.P., Teixeira, A.P. & Soares, C.G. 2014 Influence of logistic strategies on the availability and maintenance costs of an offshore wind turbine. *Safety, Reliability and Risk Analysis: Beyond the Horizon, 29 September–2 October.*

Schneider, T. & Neumaier, A. 2001 Algorithm 808: ARfit—a matlab package for the estimation of parameters and eigenmodes of multivariate autoregressive models. *ACM Transactions on Mathematical Software* 27, 58–65.

Soares, C.G., Ferreira, A.M. & Cunha, C. 1996 Linear models of the time series of significant wave height on the Southwest Coast of Portugal. *Coastal Engineering,* 29, 149–167.

Tavner, P. 2012 *Offshore Wind Turbines: Reliability, availability and maintenance,* London, UK, The Institution of Engineering and Technology.

Van Bussel, G.J.W. & Zaaijer, M.B. 2001 Reliability, availability and maintenance aspects of large-scale offshore wind farms, a concepts study. *Proceedings of MAREC Marine Renewable Energies Conference, March 2001.* Newcastle, UK.

Wilkinson, M. & Hendriks, B. 2007 Report on Wind Turbine Reliability Profiles. ReliaWind Project.

Windpower Offshore 2012 Global Offshore, Special Report. London, UK.

Windpower Offshore 2013 Vessels and Access, Special Report. London, UK.

Worldwind Technology 2013 Steering a course through offshore wind energy regulations. London, UK.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Practical aspects of the application of RCM to select optimal maintenance policy of the production line

M. Jasiulewicz-Kaczmarek
Poznan University of Technology, Poznan, Poland

ABSTRACT: The most known and diffused third generation maintenance management systems is the Reliability-Centered Maintenance (RCM). RCM focuses on the system functions and directs maintenance efforts at those parts and units where reliability is critical. One of the issues with the conventional RCM process is that the analysis takes time and consequently, the results of the program accrue after a substantial period of time. Considering the fact that there is not enough time nor money to follow the full RCM procedure, the approach to the methodology has been modified. In the paper the case is introduced to present application of modified RCM to determine the optimal maintenance strategies mix for an equipment in the way more efficient comparing to classic RCM approach.

1 INTRODUCTION

1.1 *Technical object*

Profitability improvement is one of the most important tasks for the industry. This improvement can be achieved by increasing the availability of the system and by reducing the total associated maintenance costs. In pursuit of continuous improvement, two complementary methodologies that reflect various focuses are available (uptime) of physical assets, these methodologies are (Jardine & Tsang 2013): Total Productive Maintenance (TPM)—a people-centered methodology and Reliability-Centered Maintenance (RCM)—an asset-centered methodology. These methodologies require the maintenance and production departments to operate with synergy to discern and avoid potential problems. The maintenance objectives are focused on production needs, i.e. to reduce manufacturing lead-times and increase flexibility. TPM emphasizes integration between production and maintenance practices and the systematic and continuous improvement, in order to maximize the Overall Equipment Effectiveness (OEE) performance index. RCM focuses on the system functions and directs maintenance efforts at those parts and units where reliability is critical (Garg & Deshmukh 2006).

In the paper, the author presents a case study of RCM implementation in one of the manufacturing companies in order to improve the maintenance scheduling and maintenance strategy in the production line. The implementation of RCM was carried out in 4 stages; preparation, system analysis, decision making, implementing and feedback. In order to determine system functions, functional requirements, functional failures, as well as cause and consequences of functional failures, the FMECA technique can be adopted.

2 MAINTENANCE

Nowadays along with the rapid development of industries in the world and organizations attempt for the continuity of production and also the increase of influence in the market, the decrease of the production cost and the attempt to set up the process of production, have turned to the most important challenges of production organizations. To reach to this goal continuity of production and also decrease of operation costs are set on the high agenda of production managers. (Swanson 1997). Maintenance costs are a major part of the operating costs of all manufacturing or production plants. Depending on the specific industry, maintenance costs can represent between 10 and 40% of the costs of goods produced.

Today, maintenance has become a management issue, with its function as a contributor towards profit (Jasiulewicz-Kaczmarek 2013a). This indicates the need for the maintenance operation to align with the business objectives and increase value for the enterprise. Thus, the choice of the right maintenance strategies, i.e. the best mix of corrective, preventive, condition-based, and proactive maintenance for the equipment is fundamental. Throughout the years several approaches to enhance the maintenance management have been developed and applied to a wide variety of organizations and systems (Bevilacqua & Braglia 2000;

Pun et al. 2002; Jafari et al. 2008; Selvik & Aven 2011; Wang et al. 2012). The most known and diffused third generation maintenance management systems is the Reliability-Centered Maintenance.

3 RELIABILITY-CENTERED MAINTENANCE

3.1 *RCM history*

Reliability-Centered Maintenance is one of the well-established systematic methods for selecting applicable and suitable maintenance operation types (Kumar et al. 2007). It originated in the civil aircraft industry in the 1960s with the introduction of the Boeing 747 series, and the need to lower PM costs in attaining a certain level of reliability. The results were successful and the methodology was developed further. In 1975, the U.S. Department of Commerce defined the concept RCM and declared that it should be used in all major military systems (Nowlan & Heap 1978). In the 1980s, the Electric Power Research Institute (EPRI) introduced RCM into the nuclear power industry. Today RCM is used or being now expanded to several industry fields (Abdulrohim et al. 2000; Deshpande & Modak 2002; Afefy 2010; Ramli & Arffin 2012; Narnaware et al. 2014).

3.2 *RCM approach and methodology*

Moubray (1997) defines RCM as "a process used to determine what must be done to ensure that any physical asset continues to do what its users want it to do in its present operating context", characterizing RCM as a process to establish the safe minimum levels of maintenance. The definition however is quite general. The more detailed approach is presented in IEC 60300-3-11 standard, in which RCM is defined as "a method to identify and select failure management policies to efficiently and effectively achieve the required safety, availability and economy of operation" (IEC 60300-3-11:2009). RCM methodology has three major goals (Moubray 1997):

- to increase safety and reliability of systems by focusing on the most significant functions (RCM is concerned mainly with what we want the equipment to do, not what it actually does),
- to prevent or to mitigate the consequences of failures, not to prevent the failures themselves (the consequences of a failure disagree depending on where and how items are installed and operated),
- to decrease maintenance costs by escaping or removing maintenance actions that are not strictly necessary.

Hence, determining the operating context and what the user wants the equipment to do is the starting point for the RCM process, which is applied by asking and answering the following seven questions (Moubray 1997):

- What are the functions and associated performance standards of the machine in its present operating context?
- In what way does it fail to fulfil its functions?
- What causes each functional failure?
- What happens when each failure occurs?
- In what way does each failure matter in respect of the environment, human safety, losses, and expenses?
- What can be done to predict or prevent each failure?
- What should be done if a suitable proactive task cannot be found?

To perform RCM analysis are employed the following tools and expertise:

- design, engineering and operational knowledge of the system,
- condition-monitoring techniques,
- risk-based decision making (the frequency and the consequence of a failure in terms of its impact on safety, the environment and operations),
- Failure Modes, Effects and Criticality Analysis (FMECA), this analytical tool helps answer questions 1 through 5 (the FMECA is composed of two separate analyses: the Failure Mode and Effects Analysis (FMEA) and the Criticality Analysis (CA); the FMEA analyzes different failure modes and their effects on the system while the CA classifies or prioritizes their level of importance based on failure rate and severity of the effect of failure; the ranking process of the CA can be accomplished by utilizing existing failure data),
- RCM decision flow diagram, this diagram helps answer questions 6 and 7.

The aim of RCM is to optimize, in a systematic way, the mix of the main maintenance practices, i.e. corrective, preventive, condition-based, and proactive, that must be adopted by the maintenance staff of a firm. These main maintenance policies, rather than being applied independently, are integrated to take advantage of their respective strengths in order to maximize facility and equipment reliability while minimizing life-cycle costs.

Successful application of RCM requires a good understanding of the equipment and structure, as well as the operational environment, operating context and the associated systems, together with the possible failures and their consequences. It means that running RCM analysis in a company requires some specific knowledge and experience from the

Table 1. Classification of streamlined RCM concepts (Pintelon & Parodi-Herz 2008).

Example	Characteristics	Pitfalls
Retro-active approach	Starts from the existing maintenance plan. Determines the failure mode for all maintenance tasks and implements the last RCM steps for these.	Quite time-consuming to find the failure modes for all tasks. "Functions" are detected on ad hoc basis. It Implies that the existing maintenance plan is good.
Criticality approach	Limits the implementation to critical functions and/or failures for these a full RCM analysis is performed.	Often determines criticality on an ad hoc basis or uses criticality tools which are less reliable than the RCM approach.
Troublemaker approach	Carries out a full RCM analysis for critical equipment only. Critical equipment is defined here as bottleneck equipment, which had a lot of maintenance problems in the past or is critical in terms of safety hazards.	Idem as above, although here all RCM steps are followed which guarantees a "full picture".

members of the team responsible for the analysis. The IEC 60300-3-11:2009 standard introduces requirements within this area, especially stressing:

– knowledge of and experience with the RCM process,
– detailed knowledge of the item and the appropriate design features,
– specialist knowledge of constraints, such as safety and environmental legislation, regulation, etc.
– knowledge of the maintenance techniques and tools,
– knowledge of costs.

3.3 *RCM related concepts*

In the 1970s, and still today, RCM was a major challenge in many industries because it changed the focus of PM from bringing back the systems to a "perfect" state to maintaining the system in a good "functional" state. RCM as such has proven to be a very valuable concept, focusing on reliability and paying attention to safety and environment. Its structured approach ensures asset sustainability. However, there are some drawbacks that should be kept in mind and, if possible, remedied. RCM implementation is complex, time consuming and is not straightforward. Hence, it should be implemented in a controlled fashion with total support of all levels of the organizations. In the literature one can find many RCM-related concepts such as Gits, Coetzee, BCM, RBCM, streamlined RCM, and so forth (Pintelon & Parodi-Herz 2008). All of them adopt RCM principles with the intention of solving some of its shortcomings. Although streamlining sounds attractive it should be carefully applied, in order to keep the RCM benefits. Table 1 provides a picture of popular streamlined RCM approaches.

In many enterprises RCM methodology is an element of TPM approach realization (Ben-Daya

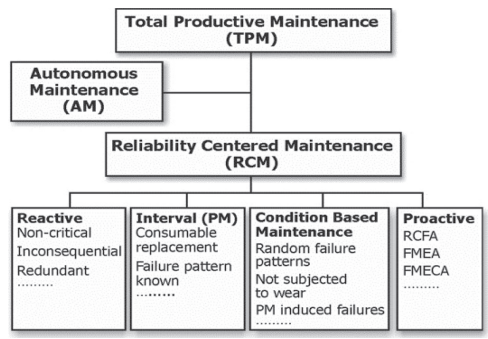


Figure 1. Relation between TPM, RCM and other maintenance approaches.

2000). TPM is a holistic approach building technical culture, based on team work and common goals. Simultaneous application of TPM and RCM contributes to synergy effect within maintenance area. The effect is possible thanks to combination of knowledge of maintenance engineers (RCM) and machines operators (TPM)—participation in striving for a common goals. The relations between TPM and RCM is introduced in the Figure 1.

4 CASE STUDY

The RCM practice was used to assist the company in focusing their maintenance activities based on the criticalities of the equipment by applying the FMECA. For over six years the company benefits from TPM approach application. Predefined pillars of TPM are being developed according to general methodology developed by JIPM, with respect to needs and constraints identified in a company. Regular training sessions concerning methods and techniques for continuous improvement are organized periodically for managers and operators in a

production process, as well as for maintenance staff, new standards for performance are being developed and procedures and instructions applied so far are inspected and modified whenever needed.

The aim of RCM was to reduce the number of maintenance checklist and to improve significantly the integrity of maintenance practice, by, among others, optimization of performance of maintenance staff and of operators realizing technical services within Autonomous Maintenance (AM) pillar.

RCM analysis was to be conducted for one of the production lines composed of 11 machines. The line works in three-shifts system and breakdown of any of the machines results in stoppage of the entire line.

One of the issues with the conventional RCM process is that the analysis takes time and consequently, the results of the program accrue after a substantial period of time. Considering the fact that there is not enough time nor money to follow the full RCM procedure, the approach to the methodology has been modified. The modification introduces one basic change into the process. Instead of looking forward, into the future and thinking about "potential breakdowns", their causes and consequences, it is necessary to look into the past, at breakdowns which has already happened. The benefit from the approach is substantial decrease in time and costs of analysis, making it practically applicable in the company.

The implementation of RCM was carried out in 4 stages; preparation, system analysis, decision making, implementing and feedback.

At the beginning of preparation stage, a project group was established from various departments and all relevant equipment documentations are collected such as breakdown reports, maintenance history records, current maintenance checklists, operation manuals, safety and environmental incident reports, production and quality reports and service reports. Also the equipment was listed accordingly to their respective shop in order to clarify the status of every parts availability. Analysis of data on production line covered two years period. The goal of analysis was to identify machines characterized with the greatest unreliability, as well as time and cost consuming repair process (failure removing and production losses). Identification of a machine to be subject of further analysis is based on Pareto analysis, according to which in each set or group of objects there is a small subset much more important than others. Basing on the data gathered on failures of production lines resulting from failures of all the machines Pareto graph was made (Fig. 2). In the chart, the columns represent the number and downtime connected with removing failures detected. Analysis of the two parameters proves that the machine critical for the line is M1, for which average time of repair was calculated as t = 0,61 h. Furthermore, analysis of costs emerging from failures removal was conducted for every machines. Taking into consideration the number of failures, time and cost of their removal the decision was taken to conduct further analysis for M1 machine.

In the next stage analysis of failures of M1 workstation was conducted. The goal of the analysis was identification of a component of the machine causing the greatest losses. Decomposition of the machine was conducted and basing on historical data on number of failures and downtime caused by failures of each component Pareto chart was drawn, as presented in the Figure (Fig. 3).

The area critical for M1 is foiling subsystem M1U1. Decomposition of M1U1 to basic components was conducted as presented in the Figure 4.

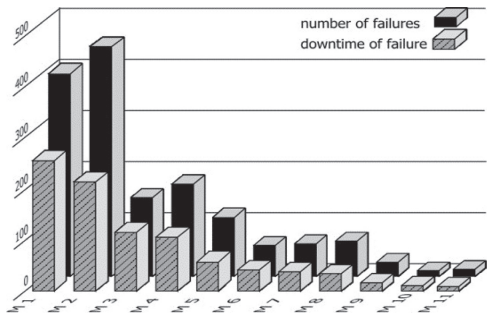


Figure 2. Pareto chart for a production line.

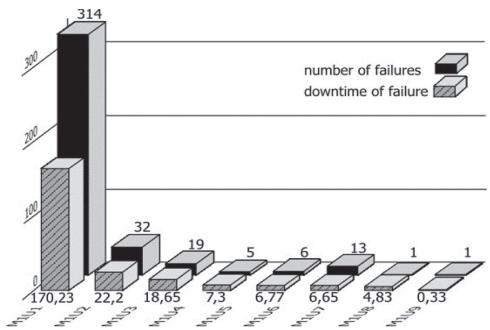


Figure 3. Pareto analysis for M1.

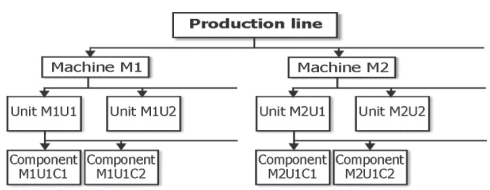


Figure 4. Decomposition of M1 to subassemblies and components.

Based on maps of losses (Pareto analysis) the 8 most critical components of the device were selected. In the next step functions of components were identified for all the components (F), which was followed by characterization of all possible Functional Failures (FF), described all possible Failure Mode (FM) and the effects of each failure mode were specified in reference to: line downtime, spare parts purchase costs and working time purchase costs for maintenance staff (Table 2).

In the next step, criticality of each failure was assessed. Methodology applied for the assessment was FMECA. FMECA is a tool used to help on setting priorities for the definition of maintenance tasks based on the analysis of the failure modes of components and their respective effects in a system. The effects of a failure depend on:

- the consequences (impact) of the failure in the operational environment,
- the conditions (occurrence) under which the failure happens.

Failure of a machine potentially influences performance, quality of a product, safety and many others. Hence, gravity of consequences of failures influences mostly which actions are to be taken to avoid predefined failures. That is why the following factors determining the impact of failures were identified in the company:

- safety (S)—analyze the impact of the failure mode on the safety of the workers in the area of occurrence (risk of accidents due to the failure),
- environment (E)—analyze the impact of the failure mode on the environment on its area of occurrence (risk of environmental accidents due to the failure),
- quality (Q)—analyse the impact of the failure mode on the quality of product (risk of quality defects due to the failure),
- production (P)—analyze the impact of the failure mode on the production, productivity or efficiency of processes (risk of time/material losses due to the failure etc.).

Assessment of impact of a failure on each of predefined factors was based on four levels scale, where 0—no impact; 1—low impact, 2—medium impact, 3—high impact. The example of assessment of influence of a failure on production is introduced in the Table 3.

It needs to be stressed that downtime parameters "a" and "b" presented in the table are individual for each company, hence each team should assess them by itself. Taking general data based on literature analysis may lead to mistaken decisions in some cases. In the next step the team conducted assessment of influence of the failure mode on the safety, environment, quality and production.

Table 2. Definition of function, functional failures and possible failure mode for M1U1C1 component—the example.

Component/code	F	FF code	FM code
Gum covered cylinders/ M1U1C1	Keeping foil strained while cutting	No cutting M1U1C1.1	Contaminated cylinders M1U1C1.1.1
		Foil creasing M1U1C1.2	Cylinders pressure wrongly adjusted M1U1C1.2.1
		Foil creasing M1U1C1.2	Used surfaces of cylinders M1U1C1.2.2
		Cutting impossible M1U1C1.3	Change in properties M1U1C1.3.1
		Foil got stuck in between cylinders M1U1C1.4	Leading rods wrongly adjusted M1U1C1.4.1

Table 3. Impact of a failure on production.

Index	Description
0	The occurrence of the failure has no effect at all
1	The occurrence of the failure can cause stoppages < "a" min
2	The occurrence of the failure can cause stoppages between "a" min and "b" hours and/or small increment in materials consumption
3	The occurrence of the failure can cause stoppages > "b" hours and/or significantly increase materials consumption

Table 4. Impact of a failure—M1U1C1 component.

Component code	FM code	Impact (I) S	E	Q	P	S + E + Q + P
M1U1C1	M1U1C1.1.1	0	0	1	1	2
	M1U1C1.2.1	0	0	1	1	2
	M1U1C1.2.2	0	0	1	3	4
	M1U1C1.3.1	0	0	1	3	4
	M1U1C1.4.1	0	0	1	2	3

Table 5. The occurrence of failure defined by frequency.

Index	Description
0	Potential failure: MTBF = ∞
1	MTBF > "m" operating hours
2	"n" < MTBF < "m" operating hours
3	MTBF < "n" operating hours

Table 6. Occurrence and criticality—M1U1C1 component.

Component code	FM code	Occurrence (O) P	R	D	C = I + O	Cause
M1U1C1	M1U1C1.1.1	3	1	1	7	No sensorial inspection
	M1U1C1.2.1	3	1	2	8	No sensorial inspection
	M1U1C1.2.2	3	3	2	10	No CBM
	M1U1C1.3.1	3	3	2	10	No modification
	M1U1C1.4.1	1	2	2	8	No sensorial inspection

The example of the assessment of influence of M1U1C1 is introduced in the Table 4.

After influence analysis, occurrence was assessed. The occurrence of failures was defined through:

- frequency (F)—analyse how often the failure mode occurs in the equipment (MTBF of the failure mode), (Table 5),
- repair (R)—analyse how difficult the repair/restoration of the failure is (time and cost),
- detection (D)—analyse how difficult it is to detect in advance the occurrence of the failure (before it happens).

The Criticality (C) of the failures can be defined based on the analysis of all of their effects (impact and occurrence) and the interaction of those factor.

In the company criticality was assessed as a sum of all components of impact and occurrence. The example of occurrence and criticality assessment for M1U1C1 and causes for the situation identified are presented in the Table 6.

The analysis of the Criticality index provides organization with ability to prioritize action in order to reduce the effect of the failure modes on the equipment. The principle followed by the company is that analysis has to be continued for influence values are identified in the given range (S or E ≥ 2) or (P or Q = 3) or criticality C ≥ 7, for the other cases it is necessary to examine whether performance standards are satisfactory and keep

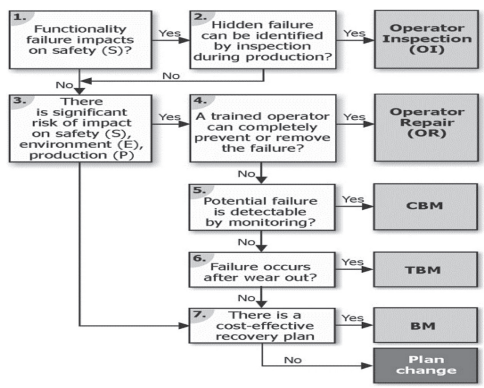


Figure 5. Decision-making process diagram.

them, in the other cases it is necessary to develop new or verify existing standards.

The next task of the team was definition of actions which have to be performed for each failure. Based on the diagram (Fig. 5), the team chose a PM effective tasks (Table 7).

In the next step, results of analyses conducted were translated into actions on operative level. Operative actions were assigned to their performers (depending on to whom the job is assigned: operators (AM)/maintenance staff (PM)), scheduled and resources necessary for their execution were identified as well. Considering changes of performers responsible for predefined actions,

Table 7. Maintenance tasks selection.

Function	FF code	FM code	Questions 1	2	3	4	5	6	7	Task
Keeping strained foil during cutting	M1U1C1.1	M1U1C1.1.1	N		P	Y				OR
	M1U1C1.2	M1U1C1.2.1	N		P	Y				OR
	M1U1C1.2	M1U1C1.2.1	N		P	N	Y			CBM
	M1U1C1.3	M1U1C1.3.1	N		P	N	Y			CBM
	M1U1C1.4	M1U1C1.4.1	N		P	Y				OR

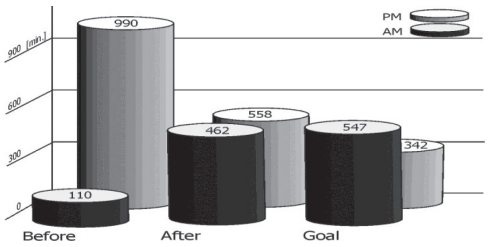


Figure 6. Inspection AM-PM/month.

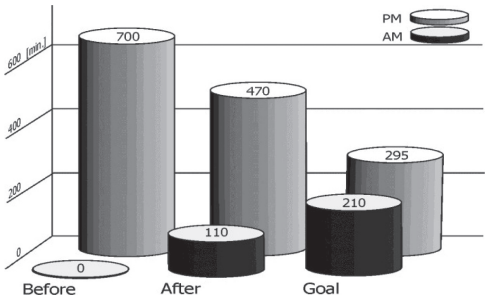


Figure 7. Lubrication AM-PM/month.

competence gaps were identified and training sessions were scheduled, supported by documents (procedures and instructions) developed to provide correct realization actions. To cope with new challenges considering lead time the analysis of availability of spare parts and exploitation materials was conducted.

The next stage was implementation of changes developed for previously binding standards of repairs planning, inspections conducting and smearing followed by assessment of changes efficiency.

It was confirmed that the implementation of RCM gave great success. Changes in number of breakdowns were noticed three months after implementation of the program. Comparing the number of breakdowns observed within three months

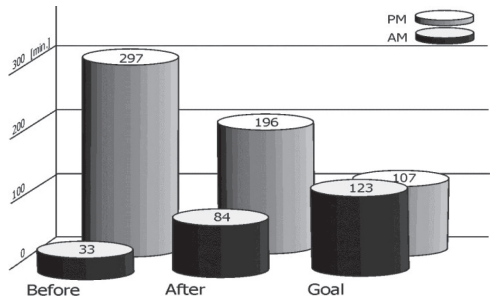


Figure 8. Overhauls AM-PM/month.

after implementation of the program to equivalent period of the last year the decrease percentage was 38%. Major improvements were also obtained in: structure of the work execution (Figs. 6–8), maintenance costs, unscheduled machine failures, repair downtime, and spare parts inventory.

RCM is a living process, therefore the practices applied have to be systematically analyzed and verified adequately to needs of an organization. programs monitoring machines condition and training sessions improving skills and knowledge of employees support solutions an organization benefits from and provide current and periodical information enabling assessment of their efficiency. The proposal and example of comprehensive maintenance assessment, based on the values of standardized and aggregated ranks of technical objects, in the context of exploitation measurements is included in (Młyńczak 2007; Loska 2013; Pourjavad et al. 2011).

5 CONCLUSION

Analysis of contemporary approaches to maintenance of technical objects leads to the conclusion that they represent approach to identification and solving problems, as well as interpretation of maintenance place different comparing to the one promoted in previous years. The new approach is

characterized mainly by (Jasiulewicz-Kaczmarek 2005; Młyńczak & Nowakowski 2006; Laskowski & Łubkowki 2013; Jasiulewicz-Kaczmarek 2013b):

– Preserving functions realized by machines and equipment instead of maintaining them only,
– Avoiding, reducing or eliminating failures instead of preventing them,
– Defining frequency of maintenance actions based on failure symptoms instead of relying on indexes of unreliability of machines and equipment,
– Self-reliant development of maintenance program at reasonable consideration of producer instructions instead of making producer the only party responsible for their definition,
– accepting uncertainty as an element of decision making when selecting maintenance methodology,
– common use of IT tools for identification.

The most known and diffused third generation maintenance management systems is the Reliability-Centered Maintenance. The primary focus of RCM is to achieve a high level of understanding of the failure modes/causes, the likelihood of occurrence and the related effects, then to define a maintenance plan that prevents or proactively addresses the potential causes of failure in such a way that the overall cost of doing business is reduced.

The selection of the maintenance policies mix is a very important task for a firm. This job is often carried out on the basis of qualitative and subjective choices, thus relying only on the human factor. This fact may lead to the adoption of the wrong maintenance strategies, reducing productivity as well as profitability. Methodology applied for RCM limits subjectivism in decision making process.

The study was carried out at one of manufacturing plant in Poland which has implemented RCM to improve their current PM task. The RCM practice has been implemented directly in order to improve maintenance scheduling and maintenance strategy in their production line. Prepared maintenance scheduled leads to saving in maintenance cost in each category (e.g. cost of downtime, cost of maintenance labor, cost of parts, etc.). It is concluded that Reliability Centered Maintenance is effective maintenance ensuring all through that maintenance induced failures are either eliminated or minimized. It did not require complex numerical calculation. The important factor enhancing success of the program was the fact that it was established as an element of TPM system already functioning in the company. Hence, the decision was premeditated and its realization was properly provisioned in terms of resources, including human resources, knowledge, data and information, now and before meticulously collected and available. To some extent, it limited potential problems emerging from RCM methodology application. However, there were some limitations identified in a company and related with application range as it was to be applied for all the production lines and machines. The first problem identified was high labor-consumption of the methodology (even though there were some simplifications introduced), thus its application should be the consequence of thorough analysis of enterprise's needs. Secondly, methodology is not useful for typical equipment, including gears or clutches, thirdly, it requires highly qualified staff, fourthly, it should be applied for devices and components of high criticality and finally, each enterprise should develop its own plan with respect to strategy, goals and problems specific for a company, production process and condition of machines.

REFERENCES

Abdulrohim, S.A., Salih, O.D., Raouf, A. 2000. RCM Concepts and Application: A Case Study, *International Journal of Industrial Engineering* 7(2): 123–132.

Afefy, I.H. 2010. Reliability-Centered Maintenance Methodology and Application: A Case Study, *Engineering* 2: 863–873.

Ben-Daya, M. 2000. You May Need RCM to Enhance TPM Implementation, *Journal of Quality in Maintenance Engineering* 6(2): 82–85.

Bevilacqua, M. & Braglia, M. 2000. The analytic hierarchy process applied to maintenance strategy selection, *Reliability Engineering & System Safety* 70: 71–83.

Deshpande, V.S. & Modak, J.P. 2002. Application of RCM to a medium scale industry, *Reliability Engineering System Safety* 1(77): 31–43.

Garg, A. & Deshmukh, S.G. 2006. Maintenance management: literature reviews and directions, *Journal of Quality in Maintenance Engineering* 12: 205–238.

IEC 60300-3-11:2009 Dependability management. Part 3–11: Application guide—Reliability centred maintenance.

Jafari, A., Jafarian, M., Zareei, A. Zaerpour, F. 2008. Using fuzzy Delphi method in maintenance strategy selection problem, *Journal of Uncertain Systems* 2: 289–298.

Jardine, A.K.S. & Tsang, A.H.C. 2013. *Maintenance, replacement, and reliability: theory and application*, 2nd ed. Published by CRC Press.

Jasiulewicz-Kaczmarek, M. 2013a. Role and contribution of maintenance in sustainable manufacturing, 7th IFAC Conference on Manufacturing Modelling, Management, and Control. In N. Bakhtadze et al. (ed.), Series Title: *Manufacturing Modelling, Management, and Control* 7(1): 1146–1151. Publisher: International Federation of Automatic Control.

Jasiulewicz-Kaczmarek, M. 2013b. Sustainability: Orientation in Maintenance Management—Theoretical Background. In P. Golinska et al. (ed.), *Eco-Production and Logistics. Emerging Trends and Business Practices*: 117–134. Berlin Heidelber: Springer—Verlag.

Jasiulewicz-Kaczmarek, M. 2005. Współczesne koncepcje utrzymania ruchu infrastruktury technologicznej przedsiębiorstwa. In M. Fertsch & S. Trzcieliński (ed.), *Koncepcje zarządzania systemami wytwórczymi*: 127–134. Poznan: Publishing Hause of Poznan University of Technology.

Kumar, S., Chattopadhyay, G., Kumar, U. 2007. Reliability improvement through alternative designs — a case study. *Reliability Engineering and System Safety* 92(7): 983–991.

Laskowski, D. & Łubkowki, P. 2013. The end-to-end rate adaptation application for real-time video monitoring, *Advances in Intelligent Systems and Computing* 224: 295–305. Switzerlan Springer International Publishing AG.

Loska, A. 2013. Exploitation assessment of selected technical objects using taxonomic methods. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 15(1): 1–8.

Loska, A. 2012. Remarks about modelling of maintenance processes with the use of scenario techniques. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 14(2): 5–11.

Młyńczak, M. 2007 Queuing system with variable server number. *Eksploatacja i Niezawodność-Maintenance and Reliability* 4: 63–65.

Młyńczak, M. & Nowakowski, T. 2006. Rank reliability assessment of the technical object at early design stage with limited operational data—a case study, *International Journal of Automation and Computing* 3(2): 169–176.

Moubray, J. 1997. *Reliability Centred Maintenance*. 2nd ed. Oxford: Butterworth-Heinemann.

Narnaware, V.S., Gosavi, G.D., Jadhav, P.V., Gorle, R.D. 2014. Implementation of Reliability Centered Maintenance in air compressor unit, *International Journal of Mechanical Engineering and Technology* 5(1): 26–32.

Nowlan, F.S. & Heap, H.F. (1978). *Reliability-Centered Maintenance*. Springfield, VA: National Technical Information Service, U.S. Dept. of Commerce.

Pintelon, P. & Parodi-Herz, A. 2008. Maintenance: An Evolutionary Perspective. In K.A.H. Kobbacy, D.N.P. Murthy (ed.), *Complex System maintenance Handbook*, pp. 21–48.

Pourjavad, E., Shirouyehzad, H., Shahin A., 2011. Analyzing RCM Indicators in Continuous Production Lines A Case Study, *International Business Research* 4(4): 115–123.

Pun, K.-F., Chin, K.-S., Chow, M.-F. Lau, H.C.W. 2002. An effectiveness-centred approach to maintenance management, *Journal of Quality in Maintenance Engineering* 8: 346–368.

Ramli, R. & Arffin, M.N. 2012. Reliability Centered Maintenance in Schedule Improvement of Automotive Assembly Industry, *American Journal of Applied Sciences* 9(8): 1232–1236.

Selvik, J.T. & Aven, T. 2011. A framework for reliability and risk centered maintenance, *Reliability Engineering & System Safety* 96: 324–331.

Swanson, L. 1997. An empirical study of the relationship between production technology and maintenance management. *International Journal of Production Economics* 53: 191–207.

Wang, W., Hussin, B. & Jefferis, T. 2012. A case study of condition based maintenance modelling based upon the oil analysis data of marine diesel engines using stochastic filtering, *International Journal of Production Economics* 136: 84–92.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Hidden Markov Models for diagnostics and prognostics of systems under multiple deterioration modes

Thanh Trung Le, Florent Chatelain & Christophe Bérenguer
GIPSA-Lab, University of Grenoble Alpes, Grenoble, France
GIPSA-Lab, CNRS, Grenoble, France

ABSTRACT: Multi-state systems have recently attracted a great deal of interest with regards to reliability and maintenance. Since most mechanical equipment operates under some sorts of stress or load, it tends to degrade over time, thus possibly resultingin discrete degradation states (damage degrees), ranging from perfect functioning to complete failure. Over recent years, Hidden Markov Models (HMMs) have been applied to model these discrete degradation states for diagnostic and prognostic purposes. However, most of the reported researches on HMMs for multi-state equipment in the literature consider only one degradation mechanism of degradation processes. The present paper proposes a novel model called Multi-Branch HMM (MB-HMM) to deal with deterioration processes modeling under multiple competing modes. To illustrate the proposed approach, a numerical study is given.

1 INTRODUCTION

Condition-Based Maintenance (CBM) plays nowadays an important role in the maintenance of engineering systems since it has the ability to recommend in advance proper maintenance actions by basing on the information collected from condition monitoring (Jardine et al. 2006).. Within a CBM program, diagnostics and prognostics are two important aspects where the former deals with fault detection, isolation and identification when it occurs and the latter helps to assess the current health state of the system and predict the remaining time before a failure occurs. An accurate prediction of the Remaining Useful Life (RUL) could provide ample time for maintenance engineers to schedule a repair, and to acquire replacement components before they actually fail (Zhang et al. 2005). Due to the stochastic nature of the deterioration, stochastic processes have been adapted to model the deterioration processes and have shown the promising results within the CBM framework (Van Noortwijk 2009, Le Son et al. 2012, Wang and Wang 2012).

As a stochastic process, Hidden Markov Model (HMM) has been successfully applied in many domains, such as Speech recognition, genes and Deoxyribonucleic acid (DNA) analysis (Rabiner 1989) thanks to its strong mathematical basis. In the CBM context, HMMs can divide equipment conditions into several meaningful states, such as "good", "minor defect", "maintenance required" and "failure" and therefore easy to understand (Si et al. 2011). They can also characterize the stochastic relationship between the features extracted from condition monitoring data and the actual health states of the equipment. For these reasons, HMMs, in the recent year, are being more and more investigated to be used as an efficient tool for the deterioration modeling and the RUL estimation (Wang and Wang 2012). For example, Baruah et al. employed HMMs for carrying out both the diagnostics and the prognostics for metal cutting tools (Baruah and Chinnam 2005). In (Zhang et al. 2005), the authors used the HMMs to construct a health/degradation index representing the current system health status. This index was then fed into an adaptive prognostic scheme in order to estimate the RUL of a bearing. In order to better represent the real degradation mechanism, several extensions of HMMs have being adopted in the literature, such as Mixture of Gaussian HMM (Tobon-Mejia et al. 2012), age-based HMM (Peng and Dong 2011), segmented HMM (Geramifard et al. 2012), segmented Hidden Semi-Markov Model (Dong and He 2007), etc.

To our best knowledge, almost all of the HMM-based frameworks in the literature consider only the mono-mode case, meaning that there is only one degradation mode occurring at one time. In practice, however, multiple degradation modes could exist in competition. In this paper, we propose a new HMM-based structure called Multi-Branch Hidden Markov Model (MB-HMM) to deal with this problem. In order to evaluate the effectiveness of the proposed model with respect

to a traditional mono-branch HMM, a simulation study is implemented.

The remainder of the paper is organized as follows. Section 2 is devoted to review some basic theories of HMMs. Section 3 describes the extension to MB-HMM and its application for diagnostics and prognostics. To illustrate the methodology, a comparative study is introduced in the section 4. Conclusion follows in Section 5.

2 METHODOLOGY

2.1 *Basic theory of Hidden Markov Model*

Hidden Markov Model is an extension of the Markov chain in which the state process are latent and can be only revealed through an observation process. This is where the word "hidden" comes from. In the deterioration modeling framework, the hidden state process represents the health states of the equipment, while the observations can be measurable signals such as the vibration signals or the features extracted from condition monitoring data. The relation between these two processes is represented by a probabilistic model. Figure 1 illustrates an example of an HMM model.

Mathematically, the complete specification of an HMM consists of the following elements (Rabiner 1989)

- N, the number of states in the model
- M, the number of distinct observation symbols per state, i.e., the discrete alphabet size
- A finite set of hidden states, i.e., $S = \{S_1, S_2, ..., S_N\}$
- A state transition probability distribution, i.e., $A = \{a_{ij}\}$, where $a_{ij} = P(q_{t+1} = S_j | q_t = S_i)$
- An observation symbol probability distribution, i.e., $B = \{b_j(k)\}$ where $b_j(k) = P(Y_k | q_t = S_j)$, $1 \le k \le M$
- An initial state probability distribution, i.e., $\pi = \{\pi_i\}$ where $\pi_i = P\{q_t = S_i\}$, $1 \le i \le N$

For convenience, in this study, an HMM is represented by a compact notation $\lambda = (A, B, \pi)$.

2.2 *HMM topology selection*

In order to apply the HMM model for the deterioration modeling framework, one question is naturally raised: Given the observations, how one can choose/select a proper topology of the model. For instance, how can we choose the type of the model, how many states should be used or which observation probability distribution is suitable? These questions will be answered in this subsection.

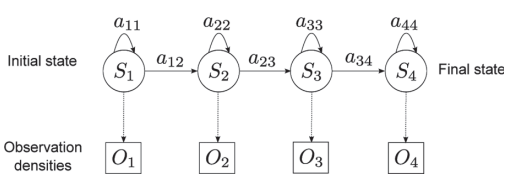


Figure 1. A five state left-right HMM.

2.2.1 *HMM type selection*

There are several types of HMMs existing in the literature, such as the ergodic HMM or the left-right (Bakis) model (Rabiner 1989). Since the deterioration processes are often irreversible in reality, components cannot come back from a bad health state to a better one as time progresses. For this reason, the left-right HMM model is chosen to be investigated. More precisely, the used left-right model in this study has the characteristic that the state index can either stay the same or increase by one. In other words, the components can only stay in the current health state or move to the next one. In this case, the coefficients of the transition matrix of the model satisfy the following properties:

$$\begin{aligned} a_{ij} &= 0, \qquad j < i \\ a_{ji} &= 0, \qquad j > i+1 \\ a_{NN} &= 1, \\ a_{Ni} &= 0, \qquad i < N \end{aligned}$$

The state S_N is considered as the final (failure) state.

2.2.2 *Observation model selection*

The observations are usually considered as discrete symbols, hence discrete probability densities are used to model the observation probabilities. However, in the framework of machine condition monitoring, the observations obtained are typically continuous signals (Tobon-Mejia et al. 2012). In this case, the continuous HMM possessing a continuous probability density function (pdf) to model the emission probabilities could give a better accuracy in diagnostics, compared to the discrete HMM (Wang and Wang 2012). However, to ensure that the parameters of the HMM can be estimated in a convenient way, the observation pdf should be elliptically symmetric densities or mixtures of elliptically symmetric pdf (Rabiner et al. 1985). For this reason, the Gaussian pdf is used in this study as the observation model:

$$b_j(O) = \mathcal{N}(O, \mu_j, \Sigma_j), \qquad 1 \le j \le N$$

where μ_j and Σ_j are the mean vector and covariance matrix in state S_j.

2.2.3 *Number of states selection*

Selecting the number of states in an HMM model is always an interesting but difficult question. It exists several methods as well as criteria for this selection purpose, such as Akaike Information Criterion (AIC), Bayes Information Criterion (BIC), Cross-validation, etc. (Knoblauch 2004). In this study, we investigate the use of BIC for selecting the number of state N.

The Bayes Information Criterion (BIC) is defined as follow

$$BIC = -2\mathcal{L} + k\log N \tag{1}$$

where $\mathcal{L}$ is the log-likelihood function; k is the number of free parameters to be estimated and N is the number of data points in observation sequences $\mathbf{O}$. The chosen model will be the one having the minimum BIC value.

3 EXTENSION TO MULTI-BRANCH HIDDEN MARKOV MODEL

3.1 *General principles*

The idea of the multi-branch HMM have been appeared in the literature and have mainly been applied for the applications of handwriting recognition (Lee, Kim, & Kim 2001, Wang, Brakensiek, Kosmala, & Rigoll 2001). In this section, we will present the general principle of MB-HMM for modeling degradation processes under different modes. An example of a two-branch HMM is presented in the Figure 2.

Such a multi-branch model is suitable to model the equipment deterioration process which could follow different modes due to different changes of the operating condition. Considering the propagation of the crack appearing in a bearing. In a normal condition, the bearing operates normally. However, when more stress is applied on it, the crack could initiate and then propagate with different rates. The more stress applied, the more quickly the crack propagates. In the MB-HMM model, each constituent branch is dedicated to model a different deterioration mode. It is worth noting that the observations emitted from the corresponding states in different constituent branches could be similar (e.g. having the same probability distributions). The only thing that distinguishes the branches is the rate of deterioration which is represented by the transition probabilities.

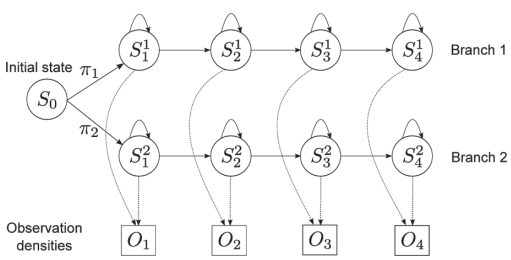


Figure 2. Example of a two-branch HMM.

There are some important assumptions that must be made in constructing the model. Firstly, once the equipment has degraded following one mode, it will follow that mode until it reaches the end of its life. There is hence no connection between the branches. The second assumption is that, the normal condition can last very long with no special characteristics in the measurement. We are interested in the deterioration process, with the purpose of assessing the deterioration level of equipment as well as predict its residual lifetime when it has suffered a problem. For this reason, the initial state can be assumed as a dummy state with no emission of observation. Each branch can therefore be seen as a single model and is assigned an *a priori* probability π_k as shown in the Figure 2. These *a priori* probabilities satisfy:

$$\pi_k = P(\lambda_k) = K_k/K, \qquad \sum_{k=1}^{M} \pi_k = 1 \tag{2}$$

where λ_k denotes the constituent HMM for branch k, K_k is the number of training data sequences corresponding to mode k, K is the total number of training data sequences and M is the total number of branches of the MB-HMM.

3.2 *MB-HMM for diagnostics and prognostics*

The application of MB-HMM for diagnostics and prognostics can be implemented in two phases, as shown in Figure 3.

In the off-line phase, the training data is classified into M different groups and then, each constituent HMM model is trained individually with the data in the corresponding group. At this step, the well-known Baum-Welch algorithm can be used without any modifications. In the next step, the number of data in each group is used to assign the *a priori* probabilities for each model (equation (2)). Finally, a trained MB-HMM model is obtained.

In the online phase, the diagnostics involves two sessions. In the first session, the mode that the equipment is following must to be identified. This goal can be achieved by using the decision theory. For instance, the model that has the maximum *a posterior* probability, given the data, can be chosen

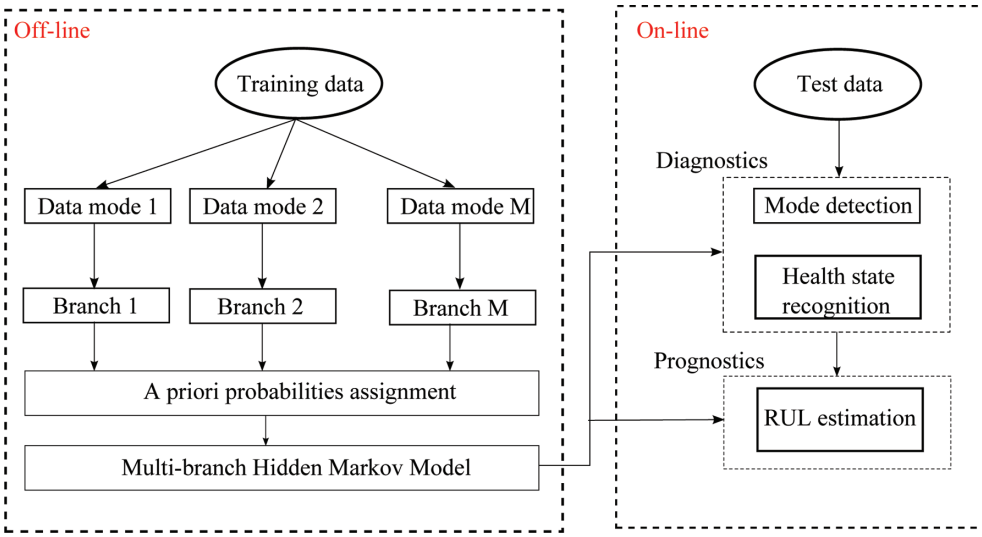


Figure 3. Proposed MB-HMM framework for diagnostics and prognostics.

in order to minimize the misclassification rate, (Bishop et al. 2006). That is:

$$\hat{k} = \arg\max_{k} P\left(\lambda_k | \mathbf{O}\right) \tag{3}$$

Note that, using Bayes' theorem, these *a posteriori* probabilities can be calculated as follows:

$$P(\lambda_k | \mathbf{O}) = \frac{P\left(\mathbf{O} \mid \lambda_k\right) P\left(\lambda_k\right)}{\sum_{k=1}^{M} P\left(\mathbf{O} \mid \lambda_k\right) P\left(\lambda_k\right)} \tag{4}$$

where $P\left(\mathbf{O}|\lambda_k\right)$ is the likelihood of the model λ_i given the data $\mathbf{O}$ and can be calculated thanks to the popular forward-backward algorithm. $P(\lambda_k)$ is calculated from equation (2).

After having identified the deterioration mode, the next stage of the diagnostics is to recognize the actual health state of the equipment. This is carried out in two steps consisting of finding the single state sequence (path) which is the most probable one representing the given test data, and considering the final state as the actual health state. The first step is done thanks to the well-known Viterbi algorithm. Let q_t denote the equipment state at time t and $Q = (q_1, q_2, \ldots, q_t)$ denote a path till the current time. Given the estimated mode, the most probable path is the one that gives the maximum joint probability of the path and the observation:

$$Q^* = \arg\max_{Q_{\hat{k}}} P\left(\mathbf{O}, Q_{\hat{k}} \mid \lambda_{\hat{k}}\right) \tag{5}$$

where Q_i represents a possible path within the mode i. The actual health state of the equipment is the final one of the path Q^*.

3.2.1 *RUL calculation*

Given the deterioration mode and the current health state estimated from the diagnostic stage, the RUL estimation can be conducted the same as in a single HMM case and is straightforward. In the MB-HMM framework, this estimation, however, strongly dependson the mode detection. Indeed, a wrong deterioration mode detection may result in a large bias in the RUL estimation. For example, if a crack propagates with a high rate, the detection of a low rate mode may lead to an extremely larger value of the RUL than the actual one. This phenomenon often occurs at the beginning of a defect propagation since the observations are insufficient to show an obvious deterioration trend. In this study, the Bayesian Model Averaging (BMA) technique (Hoeting et al. 1999) is implemented to tackle this problem. The RUL distribution is calculated as an average of the posterior distributions under each constituent model, weighted by their posterior model probability:

$$P\left(\mathrm{RUL}|\mathbf{O}\right) = \sum_{k=1}^{M} P\left(\mathrm{RUL}|\lambda_k, \mathbf{O}\right) P\left(\lambda_k|\mathbf{O}\right) \tag{6}$$

where $P(\lambda_k|\mathbf{O})$ is calculated from the equation (4).

The RUL estimation now turns to the estimation of the individual RULs under each constituent HMM, which is straightforward and can be

computed in a recursive way as follows. Given the test data, the health state of equipment is identified thanks to the Viterbi algorithm. The RUL can be defined as the necessary time steps to reach for the first time the final state S_N from the current state S_i ($i < N$):

$$\mathrm{RUL} = min\{ n \geq 0 : q_{t+n} = S_N \mid q_t = S_i \} \tag{7}$$

where q_t denote the health state at the time t. By this definition, the RUL can be seen as a discrete variable and its probability mass function is given by

$$P(RUL = n | q_t = S_i) = P(q_{t+n} = S_N, \\ q_{t+n-1} \neq S_N, \ldots, q_{t+1} \neq S_N | q_t = S_i) \tag{8}$$

Denote $h_i^{(n)} = P(RUL = n \mid q_t = S_i)$. Since the model is strictly one-order left-right topology HMM, the RUL can be calculated by the following backward recursive equations:

At state S_{N-1}:

$$h_{N-1}^{(1)} = a_{(N-1)N} \tag{9}$$

$$h_{N-1}^{(n)} = a_{(N-1)(N-1)} h_{N-1}^{(n-1)} \tag{10}$$

At state S_{N-2}:

$$h_{N-2}^{(1)} = a_{(N-2)N} \tag{11}$$

$$h_{N-2}^{(n)} = a_{(N-2)(N-2)} h_{N-2}^{(n-1)} + a_{(N-2)(N-1)} h_{N-1}^{(n-1)} \tag{12}$$

……

At state S_i

$$h_i^{(1)} = a_{iN} \tag{13}$$

$$h_i^{(n)} = a_{ii} h_i^{(n-1)} + a_{i(i+1)} h_{i+1}^{(n-1)} \tag{14}$$

where a_{ij} is the transition probability from state S_i to state S_j and is obtained from the transition matrix A.

After calculating all the individual components, the RUL estimation under the MB-HMM can be accomplished by the equation (6).

4 NUMERICAL EXAMPLES

4.1 *Fatigue Crack Growth model for data generation*

To evaluate the proposed MB-HMM-based diagnostic and prognostic framework performance, it is necessary to have the data which represent several different deterioration modes. In this section, the Fatigue Crack Growth (FCG) model is used to model the crack appearing and propagating within a bearing and to generate both the training as well as the testing data. The FCG is chosen since it has been widely used to describe the crack propagation in the literature (Huynh et al. 2012, Myotyri et al. 2006). The bearing is supposed to operate under different operation conditions so that the crack will propagate with different rates which represent different deterioration modes for our purpose.

4.1.1 *Fatigue Crack model*

The FCG model is constructed based on the popular Paris-Erdogan equation to express the crack growth rate:

$$\frac{dx}{dt} = C(\Delta K)^n \tag{15}$$

where x is the crack depth, t is the time, ΔK is the stress intensity amplitude and C and n are constant depending on the material property. It is shown that ΔK is roughly proportional to square root of crack depth x by a factor β: $\Delta K = \beta\sqrt{x}$ (Myotyri et al. 2006).

To take into account the stochastic aspect of the crack propagation, equation (15) could be discretized and then randomized by adding a multiplicative factor following a log-normal distribution as follows:

$$x_{t_i} = x_{t_{i-1}} + e^{w_{t_i}} C\left(\beta e \sqrt{x_{t_{i-1}}}\right)^n \Delta t \tag{16}$$

where w_{t_i} are independent and identically distributed according to a Normal distribution $\mathcal{N}(0, \sigma_w^2)$, $0 < x_{t_{i-1}} < x_{t_i} < \infty$. This discretized and randomized model allows us to determine recursively the crack depth x_{t_i} at time t_i given the previous depth $x_{t_{i-1}}$ and the model parameters. By this way, the deterioration data can be generated.

For modeling different deterioration modes, the factor β is considered to be a function $\beta(e)$ of the operating environment state e as below (Huynh et al. 2012):

$$\beta(e) = \beta_b \cdot e^{\gamma_e} \tag{17}$$

where β_b is the base stress level of system, the values $\gamma_e \geq 0$, $e = 1, 2, \ldots, M$ determine the level of extra stress linking with the state e of the environment. Obviously, from the equations (16) and (17), the propagation rate is directly proportional to the parameters γ_e: the greater the value of γ_e is, the more quickly the crack propagates.

4.1.2 *Observation model*

The actual crack depth is difficult to be directly and accurately measured because of several different reasons (Huynh et al. 2012). Hence, we need an observation model to represent the relationship between these actual values and the measure ones. In this study, the measurement is assumed to be the sum of the actual crack depth and a zero-mean Gaussian noise. Let X denote the crack depth and Y denote the corresponding measurement, the observation model is:

$$Y = X + \xi \tag{18}$$

where $\xi \sim N\left(0, \sigma_\xi^2\right)$ is the measurement error.

4.2 *Application of MB-HMM for FCG data*

In this section, the bearing is supposed to operate under two different environments and therefore the crack propagates in two different rates. A two-branch HMM is chosen to represent these two deterioration modes. The following parameters of the FCG model are chosen: $C = 0.005$, $n = 1.3$, $\beta_b = 1$, $\sigma_w = 1.7$, $\Delta t = 1$, $\gamma_e = [0\ 0.75]^T$, $\sigma_\xi^2 = [5 \quad 10]^T$ where the subscript T denotes the transpose of a vector. The different variance values of σ_ξ^2 mean that the measurement error may depend slightly on the operating condition.

The bearing is supposed to be failed once the crack depth reaches a critical level $d = 100$. 100 data curves have been generated by using the FCG model with the above parameters and used as the training data. Figure 4 illustrates this training data set.

In this study, the number of deterioration modes is assumed to be known beforehand. Therefore, "kmeans" tool is used to classify the failure times into 2 "clusters". Based on this, the training data can be separated into two groups, which is then used to train different branches of the MB-HMM.

In order to train each constituent model, it is necessary to determine the number of states of each model. This task is done by using the BIC criterion. Figure 5 illustrates the BIC values with respect to different state numbers for a branch of the MB-HMM.

Since the crack propagation herein is a continuous process, the increase in the states number N will obviously reduce the BIC value. To avoid the overfitting situation, it is sufficient to take the "knee" point on the BIC curve. The value $N_{statesmode1} = 10$ is hence chosen for this example.

After having determined the number of states, each model is trained thanks to the Baum-Welch algorithm. The next step is to assign the *a priori* probability for each branch (equation (2)) and the result are: $\pi_1 = 0.41$ and $\pi_2 = 0.59$.

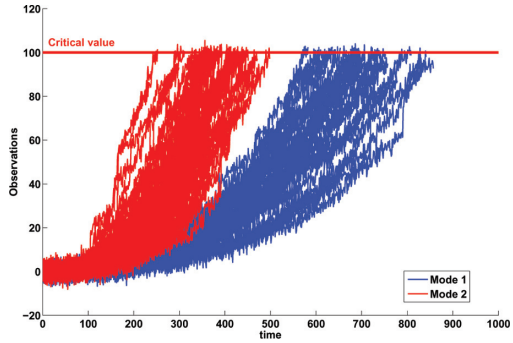


Figure 4. Two-mode training data.

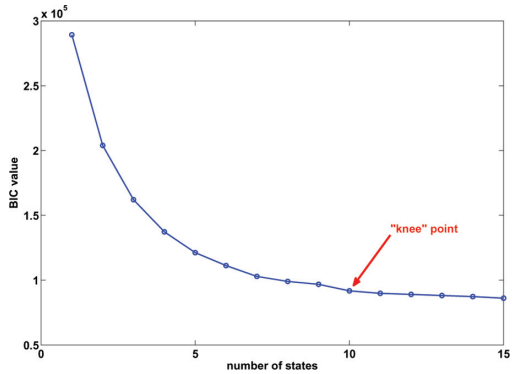


Figure 5. BIC for number of state selection.

An MB-HMM is obtained and the offline phase is terminated.

We now move to the on-line phase. One data curve representing the propagation of the crack depth from the beginning to the end of bearing life is also generated by the FCG model. This curve serves as the test data and is shown in the Figure 6 (upper sub-figure). Only the red part till the actual time $t_{act} = 100\ h$ are assumed to be observable. The estimated RUL pdf is illustrated in the lower sub-figure of the Figure 6.

To simulate the on-line RUL estimation problem, the actual time t_{act} is gradually replaced by 30 h towards the failure. After each replacement, more information about the deterioration is achieved and the diagnostic and prognostic procedures are re-implemented. Figure 7 represents the mean value of the estimated RUL associated with the 95% confidence interval. It can be realized that, at the early instances, the lack of information due to the limited observations results inthe bias and large variance in the RUL estimation. However, the actual values always lie within the 95% confidence interval. As the time passes, the length of the

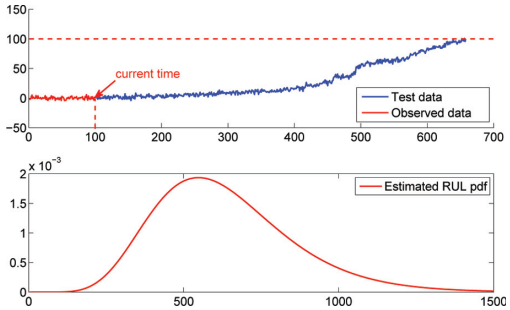


Figure 6. Observations and RUL estimation at t_{act} = 100 *h*.

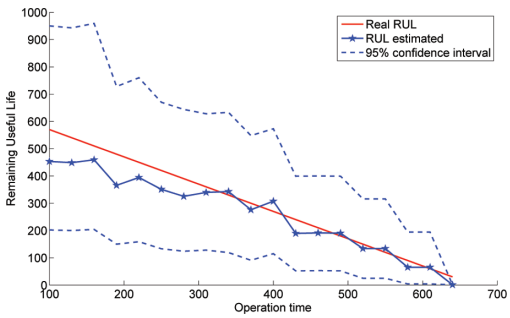


Figure 7. RUL estimation at different time instances.

confidence interval significantly decreases and the estimated RUL converges to the real value. This demonstrates demonstrates the accuracy of the proposed RUL estimation method.

4.2.1 *MB-HMM vs average HMM*

Investigating the advantage of the proposed approach naturally raises a question: given the same data set, which method between the one using the proposed MB-HMM and the one using only an "average" HMM will give the better performance in RUL prediction. To answer such question, a comparative study is given in this section with 100 test data curves. The prognostic performance of each method is characterized by the Root Mean Squared Error (RMSE) metric.

For notation convenience, we denote the average HMM by AVG-HMM. In the training phase, the training data set in the previous section is not grouped and is used as a whole to train only one AVG-HMM. This model is then used in the online phase to estimate the RUL. At $t_{act} = 100\ h$, we obtain $\mathrm{RMSE}_{\mathrm{AVG-HMM}} = 74.4$. Compared to the corresponding result of the MB-HMM: $RMSE_{MB-HMM} = 52.5$, it can be concluded that the MB-HMM give a better performance in RUL

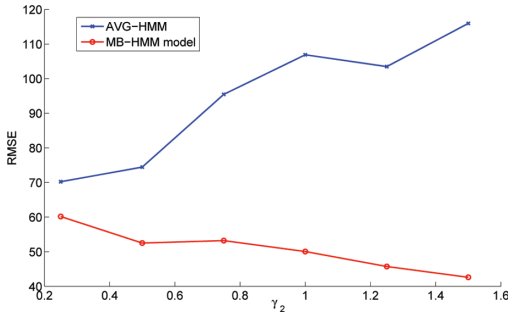


Figure 8. Prediction RMSE vs γ_2.

estimation compared with the AVG-HMM for this case.

Another interesting question raised in evaluating the advantages of the proposed MB-HMM is: does the above conclusion still hold in case that the two propagation rates are not quite different, or in case that there are two obvious trends in the training data? To answer this question, it is necessary to define a "distance" between two deterioration modes. In this study, the "mode distance" is defined by the gap between the two propagation rates and can be changed through the parameter γ_e of the FCG model. Indeed, as indicated in the section 4.1.1, the propagation rate of a crack is directly proportional to γ_e. The greater the value of γ_e is, the more quickly the crack propagates. Therefore, by fixing γ_1 and do varying γ_2, the mode distance is changed. Figure 8 shows that, when the distance between modes increases, the RMSE given by MB-HMM approach decreases while with AVG-HMM, the RUL prediction error increases. It can be concluded that the larger the distance between deterioration modes is, the better performance in RUL estimation it is given by the proposed MB-HMM approach, in comparison to an "average" HMM.

5 CONCLUSION

The present paper proposes a novel model called multi-branch Hidden Markov Model (MB-HMM) to deal with the deterioration modeling problem in case that there are several competing modes existing in deterioration mechanism of equipment. A diagnostic and prognostic framework based on the proposed model is also given. The actual health state recognition and the RUL estimation can be implemented in the same way as the traditional HMM. However, by using different HMM models for different modes, together with the *a priori* probabilities of each model, the MB-HMM shows a very promising result in dealing with the multi-mode deterioration mechanism.

Future research will be focused on the extension of the MB-HMM to a multi-branch Hidden semi-Markov Model (MB-HSMM) due to the fact that the state sojourn time of an HMM follows an exponential distribution, which may not be hold in practice. Another possible extension of the model is the ability of transition between the states of the different branches. The proposed model and the extension should also be validated on the data of real systems.

ACKNOWLEDGEMENT

This work is a part of the Ph.D research work of Thanh Trung LE in the framework of SUPREME ("SUstainable PREdictive Maintenance for manufacturing Equipment") project, funded by the European Comission in FP7 Programme, under the Factories of the Future PPP.

REFERENCES

Baruah, P. & R.B. Chinnam (2005). Hmms for diagnostics and prognostics in machining processes. *International Journal of Production Research 43*(6), 1275–1293.

Bishop, C.M. et al. (2006). *Pattern recognition and machine learning*, Volume 1. springer New York.

Dong, M. & D. He (2007). A segmental hidden semi-markov model (hsmm)-based diagnostics and prognostics framework and methodology. *Mechanical Systems and Signal Processing 21*(5), 2248–2266.

Geramifard, O., J.-X. Xu, J.-H. Zhou, & X. Li (2012). A physically segmented hidden markov model approach for continuous tool condition monitoring: Diagnostics and prognostics. *Industrial Informatics, IEEE Transactions on 8*(4), 964–973.

Hoeting, J.A., D. Madigan, A.E. Raftery, & C.T. Volinsky (1999). Bayesian model averaging: a tutorial. *Statistical science*, 382–401.

Huynh, K.T., A. Barros, & C. Bérenguer (2012). Adaptive condition-based maintenance decision framework for deteriorating systems operating under variable environment and uncertain condition monitoring. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 226*(6), 602–623.

Jardine, A.K., D. Lin, & D. Banjevic (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical systems and signal processing 20*(7), 1483–1510.

Knoblauch, D. (2004). Data driven number-of-states selection in hmm topologies. In *INTERSPEECH*.

Le Son, K., M. Fouladirad, A. Barros, E. Levrat, & B. Iung (2012). Remaining useful life estimation based on stochastic deterioration models: A comparative study. *Reliability Engineering & System Safety*.

Lee, J.J., J. Kim, & J.H. Kim (2001). Data-driven design of hmm topology for online handwriting recognition. *International journal of pattern recognition and artificial intelligence 15*(01), 107–121.

Myotyri, E., U. Pulkkinen, & K. Simola (2006). Application of stochastic filtering for lifetime prediction. *Reliability Engineering & System Safety 91*(2), 200–208.

Peng, Y. & M. Dong (2011). A prognosis method using age-dependent hidden semi-markov model for equipment health prediction. *Mechanical Systems and Signal Processing 25*(1), 237–252.

Rabiner, L.R. (1989). A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE 77*(2), 257–286.

Rabiner, L. R., B.-H. Juang, S. Levinson, & M. Sondhi (1985). Some properties of continuous hidden markov model representations. *At&T Technical Journal 64*(6), 1251–1270.

Si, X.-S., W. Wang, C.-H. Hu, & D.-H. Zhou (2011). Remaining useful life estimation–a review on the statistical data driven approaches. *European Journal of Operational Research 213*(1), 1–14.

Tobon-Mejia, D.A., K. Medjaher, N. Zerhouni, & G. Tripot (2012). A data-driven failure prognostics method based on mixture of gaussians hidden markov models. *Reliability, IEEE Transactions on 61*(2), 491–503.

Van Noortwijk, J. (2009). A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety 94*(1), 2–21.

Wang, M. & J. Wang (2012). Chmm for tool condition monitoring and remaining useful life prediction. *The International Journal of Advanced Manufacturing Technology 59*(5–8), 463–471.

Wang, W., A. Brakensiek, A. Kosmala, & G. Rigoll (2001). Multi-branch and two-pass hmm modeling approaches for off-line cursive handwriting recognition. In *Document Analysis and Recognition, 2001. Proceedings. Sixth International Conference on*, pp. 231–235. IEEE.

Zhang, X., R. Xu, C. Kwan, S.Y. Liang, Q. Xie, & L. Haynes (2005). An integrated approach to bearing fault diagnostics and prognostics. In *American Control Conference, 2005. Proceedings of the 2005*, pp. 2750–2755. IEEE.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Application of the Maintenance Rule to Nuclear Power Plant systems through Bayesian Networks

Dillyane P. Dionizio
Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

P.L.C. Saldanha
Comissão Nacional de Energia Nuclear, Rio de Janeiro, Brazil
UBM—Centro Universitário de Barra Mansa, Rio de Janeiro, Brazil

P.F. Frutuoso e Melo
Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

ABSTRACT: Recently, Bayesian Networks (BNs) have been discussed in the field of maintenance management. The purpose of this paper is to present the results of the BN application to maintenance models of Nuclear Power Plant (NPP) safety systems. The Maintenance Rule (MR) is a methodology to check the effectiveness of maintenance carried out in NPPs and plant configuration control. An expert panel determines the relationship between the selected Structures, Systems and Components (SSCs) and the plant safety within the MR scope. The SSCs are monitored to verify whether their performance meets the established criteria or whether they need undergo a specific maintenance program. For analyzing the adequacy of the methodology, a case study was developed concerning the Emergency Diesel Generators (EDGs) and compared with previous studies. The results have been achieved faster and satisfactorily when experts' opinions are required. This study demonstrates the flexibility of this framework when applied to reliability evaluations of systems under the MR.

1 INTRODUCTION

The Brazilian Monitoring Program for Maintenance Effectiveness (PMEM) is based on the NRC Maintenance Rule (MR) NRC (2012).

The purpose of this paper is to model through a Bayesian Network, BN, a safety system of a German nuclear power plant design within the scope of MR, allowing for making decisions based on the BN probabilities as to which components and subsystems might undergo dependent failures.

The use of BNs in this context aims at assessing their ability to present the modeling of a safety system failure, considering the dependent failure events that might be involved.

The reliability considering the whole set of subsystems through the BN makes it possible to identify subsystems that require more effective actions, thus seeking to keep the reliability index within the required limit.

The BN allows the production of new results, in accordance with the demand of information, assuming the addition of new variables, updated data and hence update the reliability calculation.

For analyzing the methodology adequacy, a case study was developed concerning the emergency diesel generators and compared with previous studies.

The calculations for the modeled BN were carried out through the Netica™ (2014) program. The obtained results were satisfactory and demonstrated that modeling by means of BNs is adequate for classification of MR categories for equipment having several subsystems, such as EDGs. The analysis can be performed more consistently by monitoring the system performance through its operational tests and also the results can help set operational testing for its subsystems.

2 SURVEY OF MAINTENANCE RULE

The Maintenance Rule (MR) is a requirement established by the U.S. Nuclear Regulatory Commission (NRC) to check the effectiveness of maintenance carried out in nuclear plants, and to plant configuration control. The control of plant configuration is necessary to verify the impact of the maintenance of an out of service safety device on plant safety. The MR technique was consolidated in the U.S. in 1996. MR classifies Structures, System or Components (SSCs) into two

categories: Category (a)(2), the SSCs that reach the intended performance demonstrate that the preventive maintenance is being appropriately performed, and Category (a)(1), which stands for the SSCs that do not fulfill Category (a)(2), and must have established goals, so that the discrepancies can be revised and then return to Category (a)(2).

NRC requirements establish that all SSCs can be evaluated to verify the pertinence of their inclusion in MR. If the SSC is directly related to safety, can mitigate accidents or transients, is part of Emergency Operational Procedures (EOPs), can prevent other SSC of performing their safety functions, or causes a reactor shutdown or a safety system actuation, the SSC will be put within the MR scope. Otherwise, it remains under the existing maintenance program, outside the MR scope. The MR simplified flowchart may be found in (NRC, 2014).

The MR also requires that before performing maintenance activities the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.

The Nuclear Engineering Institute (NEI) issued the report NEI (1996). This document is a guideline for applying the Maintenance Rule to Nuclear Power Plants. Section 11.0 of NEI (1996) consolidates the assessment and management of the increase in risk that may result from the proposed maintenance activities.

An expert panel determines the relationship between the selected SSC and plant safety within the MR scope (high or low significance). Finally, SSCs are monitored to verify whether their performance meets the established criteria or whether they can undergo a Maintenance Preventable Functional Failure (MPFF).

A periodic evaluation of the reliability and unavailability balance is scheduled, according to the MR, at each refueling cycle or every two years.

3 GENERAL ASPECTS OF BAYESIAN NETWORKS

One of the most attractive features of the Bayesian formulation in causal models is the ease of making predictions as to future events, such as the outcome of a social episode, the outcome of a given test and the prognosis of a disease, Pearl (1998).

The modeling using Bayesian Networks (BN) allows the organization of knowledge in a given area, or in a given system to map causes and effects, automatically generating predictions or decisions, even with sparse data. Bayesian inference also enables the production of new results, in accordance with the demand of information, assuming the addition of new variables, data update and aggregation of expert opinion when needed.

Bayesian networks consist of a qualitative part (an acyclic directed graph, where nodes represent stochastic variables) and a quantitative part (a set of conditional probability functions), Langseth et al. (2009).

A Bayesian network is a directed acyclic graph, where the nodes represent the system variables and arrows symbolize dependencies or cause-effect relationships between variables. A BN is defined by a set of nodes and a set of directed arcs. A probability is associated with each node state. This probability is defined a priori for a root node and is calculated by inference for the others, Weber et al. (2012).

Celeux et al. (2006) define a Bayesian network as:

- a set of variables V, defining the vertices, and a set of edges between variables;
- each variable has a finite number of unique states;
- variables and edges define an acyclic directed graph, denoted by $G = (V,E)$;
- each variable Y with parents $X_1, \ldots, X_n$, is associated with a conditional probability $P(Y|X_1, \ldots, X_n)$. When a variable has no parents, a marginal probability $P(Y)$ is associated to it.

The name Bayesian network stems from the known Bayes theorem. In a BN, the joint probability can be written as

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid pa(X_i)) \quad (1)$$

where $pa(X_i)$ is the set of parents of vertex X_i, Celeux et al. (2006).

The modeling using Bayesian networks has become increasingly common to treat problems in which the joint use of information from the monitoring and evaluation of a system are fundamental. It allows the creation of diagrams to organize data through a mapping between causes and effects, thus enabling the automatic generation of predictions or decisions even with incomplete knowledge.

Bayesian networks are a brief way to represent conjunctions of probabilities, presenting in a direct and structured way the dependencies between the variables of a domain, Martins (2013).

Cai et al. (2013) discuss the use of BNs to assess the maintenance of subsea Blowout Preventer (BOP) control systems. Neil & Marquez (2012) discuss the use of hybrid BNs the estimate the availability of renewable systems. Jones et al. (2010) apply BN modelling for maintenance planning in a manufacturing industry, while Melo & Sanchez (2008)

discuss delays related to software maintenance by BNs. Celeux et al. (2006) use a BN modeling to discuss preventive maintenance from expert opinions related to a nuclear plant mechanical systems degradation.

4 CASE STUDY

The case study was developed concerning the Emergency Diesel Generators (EDG) and was prepared considering data from published operating experience, according to NRC (1999), Brazilian NPPs operational experience, and the Joint Research Centre, JRC, a reference center of science and technology for the European Union, JRC (2013) concerning plant start-up, load run and subsystems failures. The failures recorded in JRC (2013) for EDG tests can be raised by the cycle operation. For subsystems, the survey could be done only by the accumulation of failures considering the entire period. Thus, the results can only be compared by the failures accumulated in the total period. Each cycle lasts 450 days approximately, with downtime intervals of 30 days for the reactor core refueling and plant maintenance.

The EDG has five auxiliary systems (KWU, 1984). Figure 1 shows the boundary and support systems of EDG:

1. Cooling Water System (XJG), which is designed to remove the heat generated in the engine, in the air for combustion system and in the lube oil system;
2. Lube Oil System (XJV), which is designed to supply oil to lubricate the moving parts of the engine and dissipate heat (while the diesel unit is on standby, this system is preheated and kept in constant recirculation);
3. Fuel System Oil (XJN) provides fuel for engine operation and also executes speed control and engine shutdown;
4. Start Air System (XJP) stores pressurized air tanks and when the start-up is requested, injects air into the engine, with a tank capacity of seven sequential starts;
5. Combustion Air and Exhaust Gas Systems (XJQ/XJR), the XJQ collects, and filters and stores the combustion air and XJR controls the air temperature and extracts the gas from the combustion engine.

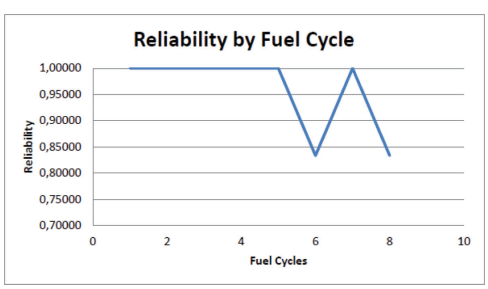


Figure 1. EDG reliability profile during the cycles 1 to 8.

The EDG operate in standby. The reliability and availability assessment are performed through operational tests (or periodical or surveillance tests) or actual demands (cases of postulated events). For this case study, the failures recorded in the operational tests as unsuccessful tests were considered, ETN (2013).

The reliability of emergency diesel generators is one of the major factors affecting the core damage probability in the event of a blackout. Therefore, it is necessary to achieve high reliability and keep it, in order to significantly contribute to ensuring the supply of emergency power to safety systems during blackout. The reliability must be hold within a range of not less than 5%, the minimum acceptable reliability is 95%. Another performance criterion is the maximum acceptable unavailability of 5%, NRC (2007). In this case study, only the criterion on the minimum acceptable reliability is used.

The reliabilities of EDGs are verified through the operating tests demands at intervals of 30 days. Reliabilities are considered at starting and under load run, according to, Vajgel (2009):

$$R_i = 1 - \left({}^{n^o SF}/_{n^o TT} + {}^{n^o RF}/_{n^o TT} \right) \quad (2)$$

– nºSF number of stating failures in operational tests
– nºRF number of loading run failures in operational tests
– nºTT number of total operational tests

Table 1. DG reliability and Maintenance Rule category by fuel cycle.

C[1]	Dem[2]	SF[3]	RF[4]	FP[5]	R[6]	MR[7]
1	32	0	0	0	1	a(2)
2	19	0	0	0	1	a(2)
3	18	0	0	0	1	a(2)
4	24	0	0	0	1	a(2)
5	22	0	0	0	1	a(2)
6	24	4	0	0,167	0,833	a(1)
7	19	0	0	0	1	a(2)
8	28	4	0	0,142	0,857	a(1)
	186[8]	8[8]	0	0,043[8]	0,957[8]	a(2)

1. Fuel Cycle; 2. Demands by Surveillance Tests (ST); 3. Start Failures; 4. Run Failures; 5. Probability of Failure (total); 6. Reliability; 7. Maintenance Rule Category; 8. Total values considering Cycle-1 to Cycle-8 period.

Table 2. DG sub-systems reliability and Maintenance Rule Category (8 fuel cycles).

SSy[1]	F[2]	D[3]	FP[4]	R[5]	MR[6]
XJN	11	186	0,059	0,941	a(1)
XJV	1	186	0,005	0,995	a(2)
XJP	5	186	0,027	0,973	a(2)
XJG	3	186	0,016	0,984	a(2)
XJQ	1	186	0,005	0,995	a(2)
XJY	0	186	0,000	1,000	a(2)
XKY	0	186	0,000	1,000	a(2)

1. Sub-Systems; 2. Failures by Surveillance Tests (ST) demands; 3. Demands by ST considering Cycle-1 to Cycle-8 period; 4. Failure Probability (total); 5. Reliability; 6. Maintenance Rule Category.

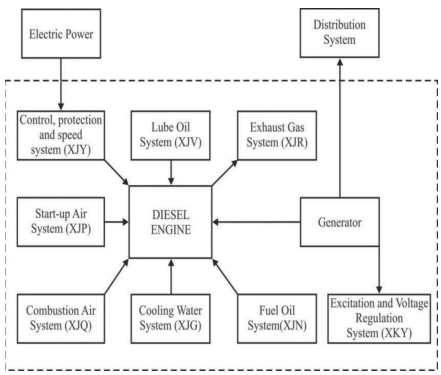


Figure 2. Boundary and support systems (sub-systems) of emergency diesel generator.

The failures were considered in parts, subsystems and systems, which required the maintenance crew intervention. According to NRC (1987), failures can be defined as: critical (they cause the finish of one or more functions of equipment); degraded (they occur gradually and partially, but the equipment/component continues operating); and incipient (they are imperfections that describe the state or condition of an item). Failures considered in the case study were those (critical or degraded) that prevented the continuity of operational tests.

Table 1 presents per cycle the results of EDG tests without success (per cycle), the reliability loss and MR categorization. The reliability loss is calculated according to Eq. (2). Figure 1 shows the reliability profile. The EGD showed a cumulative reliability of 95.7% considering the eight cycles, being classified as a(2). Note that at the end of Cycle 8, its reliability was 85.7%.

Table 2 shows the failures of operational testing (testing without success) for EDG subsystems, considering the eight fuel cycles and the same number of operational tests performed. The subsystem XJN presented a reliability lower than 95% and was classified as a(1), according to the MR requirements. All other subsystems analyzed met the established criteria and were classified as a(2).

With the information from Table 2 and the structure of Figure 2 (boundary and sub-systems of emergency diesel generators), a BN modeling was performed in order to measure the joint probability (the reliability of EDG calculated considering the influence of the subsystems behavior).

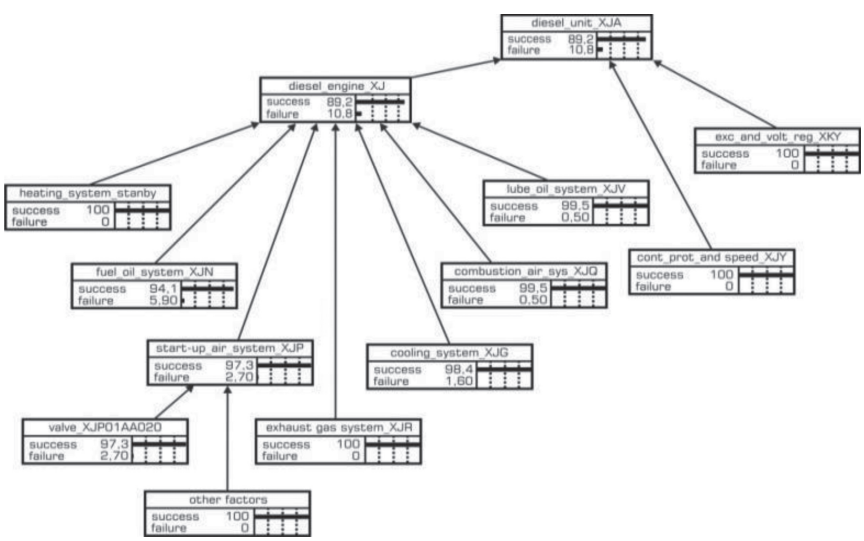


Figure 3. Bayesian network of EDG.

Table 3. Probabilities computed by the Bayesian network.

System	Success	Failure
XJY	1.000	0.000
XKY	1.000	0.000
Diesel motor XJ	0.892	0.108
Others factors	1.000	0.000
Standby heat system	1.000	0.000
XJQ	0.995	0.005
XJN	0.941	0.059
XJR	1.000	0.000
XJG	0.984	0.016
XJV	0.995	0.005
XJP	0.973	0.027
XJA	0.892	0.108
Valve XJP01AA020	0.973	0.027

The probability of failure and reliability were calculated using data obtained from selected publications, JRC (2013) and NRC (1987).

The reliabilities for the subsystem were used as input data for the Bayesian network.

The reliabilities per cycle were used for comparison purposes with the EDG reliability from the BN. The BN was generated through the Netica™ (2014) program. Figure 3 shows the BN and Table 3 shows the calculated probabilities from the BN.

5 CONCLUSIONS

The advantage of the use of a Bayesian Network, in this case, consisted in the fact that it allowed evaluating all the variables involved in the process, the dependency relationships between them and the estimated joint system reliability (considering that perfect EDG functionality depends on the reliability of each subsystem).

The EDG had an accumulated reliability for 8 cycles of 95.7% and was classified as a(2), but its reliability in the end of cycle 8 was 85.7% and would, thus, be classified as a(1) (reliability < 95%). The reliability presented in the last cycle is a more realistic estimate than the accumulated reliability of 8 cycles.

The reliability considering the whole set of subsystems through the BN makes it possible to identify subsystems that require more effective actions, thus helping keep the reliability index within the required limit.

The BN allows the production of new results, in accordance with the information demand, assuming the addition of new variables and updated data and hence update the reliability calculation.

Thus, classification of Maintenance Rule as a(2) or a(1) for equipment having several subsystems, such as the EDG, can be performed more consistently by monitoring their performance through their operational tests and also as a the result set operational testing of its subsystems.

REFERENCES

Cai, B., Liu, Y., Fan, Q., Zhang, Y., Yu, S., Liu, Z., Don, X. 2013, "Performance evaluation of subsea BOP control systems using dynamic Bayesian networks with imperfect repair and preventive maintenance", *Engineering Applications of Artificial Intelligence*, vol. 26, pp. 2661–2672.

Celeux G., Corset F., Lannoy A., B. Ricard B. 2006, "Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable way", *Reliability Engineering and System Safety*, vol. 91, pp. 849–856, 2006.

ETN 2013, Eletrobrás Termonuclear S.A., Final Safety Report, Central Nuclear Almirante Álvaro Alberto, Angra II, FSAR, Rev. 13, Brasil, 2013.

Jones, B., Jenkinson, I., Yang, Z., Wang, J. 2010, "The Use of Bayesian network modelling for maintenance planning in a manufacturing industry", *Reliability Engineering and System Safety*, vol. 95, pp. 267–277.

JRC 2013, Events Related to Emergency Diesel Generators, JRC—European Commission Joint Research Centre Institute for Energy and Transport, Netherlands, 2013.

KWU 1984, PWR 1300 MW Technology Course, Personnel Training Service, Kraftwerk Union AG, Erlangen, 1984.

Langseth, H., Nielsen, T., Rumí, R., Salmerón, A. 2009, "Inference in hybrid Bayesian networks", *Reliability Engineering and System Safety*, vol. 94, pp. 1499–1509, 2009.

Martins, M. 2013, Considerations on Reliability and Risk Analysis (in Portuguese), Habilitation Thesis, Department of Naval and Offshore Engineering, Polytechnic School, University of São Paulo, São Paulo, SP, 2013.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Experience on risk-informed approach to Allowed Outage Time changes due planned maintenance

P.L.C. Saldanha
Comissão Nacional de Energia Nuclear, Rio de Janeiro, Brazil
UBM—Centro Universitário de Barra Mansa, Rio de Janeiro, Brazil

P.F. Frutuoso e Melo
Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

ABSTRACT: This paper presents the experience obtained on the application of Allowed Outage Times (AOT) changes due to planned maintenance to safety systems of the $n + 2$ ($4 \times 50\%$) redundancy design criteria. With the unit in power, Technical Specifications (TS) state that the AOT for one emergency diesel generator is 14 days. After this period, the unit should go to cold shutdown if the emergency diesel generator still remains unavailable. However, 30 days are necessary for planned maintenance. It focuses on the evaluation of Risk-Managed Technical Specifications by EPRI (2006) methodology with risk informed decision making of changes to allowed outage times as a result of planned maintenance observing the Maintenance Rule requirements, and it is supported by the US Nuclear Regulatory Commission requirements. The results show that the maintenance of emergency diesel generators for 30 days does not cause a significant increase of plant risk.

1 INTRODUCTION

Over the last fifteen years a Probabilistic Safety Analysis (PSA) has been issued for most nuclear power plants in the world. General guidelines for issuing these PSAs have been followed both by guidance of the International Atomic Energy Agency (IAEA) and also of the U.S. Nuclear Regulatory Commission (NRC), so that these analyses are of sufficiently high quality to be used.

The modern approach is to apply an integrated decision-making process that combines the insights from the deterministic approach and the probabilistic analysis with further requirements, where applicable (legal, regulatory, cost-benefit, etc) in making decisions. This approach is being increasingly applied by regulatory bodies in making decisions about safety issues (including plant licensing) at nuclear facilities and in organizing their activities so that their resources are more efficiently used and there is a reduction in the unnecessary burden on licensees without compromising safety.

The use of risk information by a regulatory body as part of an integrated decision making process addresses the way in which risk information is being used as part of an integrated process in making decisions about safety issues at nuclear plants—commonly referred to as risk-informed decision making, and how risk information is being used by regulatory bodies as an input into the activities that they carry out—sometimes referred to as risk-informed regulation.

The risk-informed approach aims to integrate in a systematic manner quantitative and qualitative, deterministic and probabilistic safety considerations to obtain a balanced decision. In particular, there is explicit consideration of both the chances of events and their potential consequences together with such factors as good engineering practice and sound managerial arrangements. The basic components of risk, chances of occurrence and consequence, are based on sound knowledge or data from experience, or derived from a formal, structured analysis such as a PSA.

This paper focuses on the evaluation of Risk-Managed Technical Specifications by EPRI (2006) methodology with risk informed decision making of changes to allowed outage times as a result of planned maintenance observing the Maintenance Rule (supported by the US Nuclear Regulatory Commission requirements) The case study is related to plan emergency diesel generator maintenance.

The results show that the maintenance of emergency diesel generators for 30 days does not cause a significant increase of plant risk.

2 REGULATORY DOCUMENTATION CONCERNING RIDM

PSA is a methodology that can be applied to provide a structured analysis process to evaluate the frequency and consequences of accidents scenarios in nuclear power plants. NRC first applied PSA in the Reactor Safety Study (NRC, 1975). An important initiative (NRC, 1988) was the issuance of Generic Letter GL-88-20, which originated the program known as IPE, Individual Plant Examination, NRC (1988). This is because the Reactor Safety Study did not consider each plant individually in the risk assessment.

Since that time, NRC has been using risk assessment and directing the issuance of decisions on complex items associated with or related to safety, such as: (a) total loss of power (station blackout); (b) Anticipated Transients Without reactor Shutdown (ATWS); (c) Pressurized Thermal Shock events (PTS); and (e) Maintenance Rule.

NRC issued the Probabilistic Safety Assessment Policy Statement (NRC, 1995), which incorporated risk assessment as a tool in the regulatory process. It consists of elements that have originated the Risk-Informed Decision Making (RIDM) and the Performance Based Regulation (PD).

The following PSA-based RIDM regulatory guides were issued: (a) changes in the bases of the specific plant licensing, RG-1.174 (NRC, 2011a); (b) assessment of changes and implementation of technical specifications, RG-1.177 (NRC, 2011b); (c) in-service inspections in pipes, RG-1.175 (NRC, 1998) and RG-1.178 (NRC, 2003); (d) an approach to determine the technical quality of PSA results for RIDM, RG 1.200 (NRC, 2009a) (e) fire protection, RG 1.205 (NRC, 2009b). Many of the current regulations, based on deterministic requirements, cannot be quickly replaced.

Regulatory Guide 1.174 (NRC, 2011a) describes the approach accepted by NRC to assess the nature and impact of Licensing Basis Conditions (LBC) by considering engineering aspects and application of risk insights.

Regulatory Guide 1.200 (NRC, 2009a) describes the approach accepted by NRC to determine that PSA quality, in part or in whole, is sufficient to assure its results so that they can be used in regulatory decision making. Figures 1 and 2 show, respectively, the role of NRC regulatory guides in RIDM and NRC approach for RIDM.

The International Atomic Energy Agency, IAEA, has, over the past year, sponsored and promoted activities and issued technical documents related to RIDM. Among the latest highlights are IAEA (2010) and IAEA (2011).

IAEA (2010) was prepared with the participation and contributions of experts from Belgium,

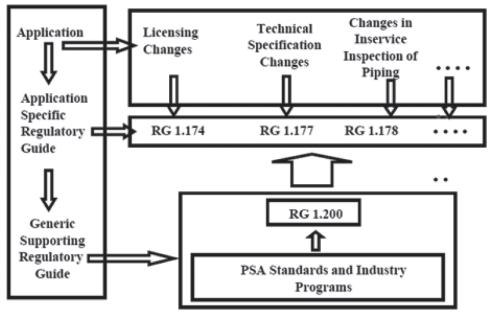


Figure 1. Role of NRC regulatory guides in RIDM.

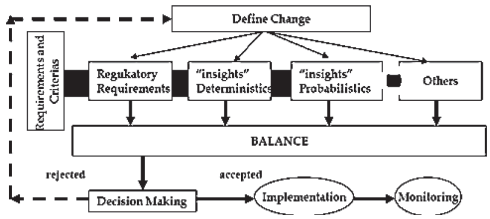


Figure 2. NRC approach for RIDM.

the Czech Republic, Finland, the Netherlands, Sweden, Switzerland and the United States of America. In-service inspection is an integral part of defense in depth programs for nuclear power plants, to ensure safe and reliable operation. Traditional in-service inspection programs were developed using deterministic approaches. However, as probabilistic approaches are being developed, risk insights are being used to optimize in-service inspection programs by focusing in-service inspection resources on most risk significant locations.

IAEA (2011) is intended to promote a common understanding among the international nuclear community (designers, suppliers, constructors, licensees, support organizations and regulators) of how the concept of risk can be used in making safety decisions relating to nuclear installations. The integration of operating experience, deterministic considerations, probabilistic considerations, consideration of uncertainties and other factors serves to help ensure coherent and balanced decisions.

3 TECHNICAL SPECIFICATION, MAINTENANCE RULE AND RISK-MANAGED TS

Technical Specifications are specifications regarding the characteristics of nuclear power plants (variables,

systems or components) of overriding importance to nuclear safety and radiation protection, which is an integral part of plant operation authorization. The technical proposal should be accompanied by a summary of the bases, including the following topics: 1) safety limits, 2) setting limits safety system, 3) limiting conditions of operation, 4) requirements for inspections and periodic tests, 5) design features not included in previous topics, 6) administrative controls, and 7) radioactive effluents.

Limiting Conditions of Operation (LCO) are the minimum levels of performance or capacity or operating system components required for the safe operation of nuclear plants, as defined in technical specifications. The requirements for inspections and periodic (or surveillance) tests (SR) are conditions for the test, calibration or inspection, to ensure: (a) maintaining the necessary quality of systems and components of a plant, (b) facility operation within safe limits, and (c) meeting the boundary conditions of operation.

According Martorell et al. (2012), safe operation of nuclear power plants depends on the Technical Specifications (TS), so that TS are part of the Licensee Basis (LB) to operate a NPP, which were established taking into account mainly deterministic criteria. The development of PRA (Probabilistic Risk Assessment) and its application since the early 80's to analyze TS changes has brought the opportunity to review TS consistency from a risk viewpoint, i.e., addressing the impact of the changes on plant safety on the basis of the risk information provided by the PSA, with particular attention to the role of the Allowed Outage Times (AOT) included within the Limiting Conditions of Operation (LCO). Martorell et al. (2012) focus on the use of importance analysis. A case study that focuses on an AOT change of the accumulators system of a nuclear power plant using a Level 1 PSA is provided.

The Maintenance Rule (MR) is a requirement established by the U.S. Nuclear Regulatory Commission (NRC) to check the effectiveness of maintenance carried out in nuclear plants, and to plant configuration control. The control of plant configuration is necessary to verify the impact of the maintenance of a safety device out of service on plant safety. The MR technique was consolidated in the U.S. in 1996.

MR classifies Structures, System or Components (SSC) into two categories: Category (a)(2), the SSCs that reach the intended performance demonstrate that the preventive maintenance is being appropriately performed, and Category (a)(1), which stands for the SSCs that do not fulfill Category (a)(2), and must have established goals, so that the discrepancies can be revised and then return to Category (a)(2).

NRC requirements establish that all SSCs can be evaluated to verify the pertinence of their inclusion in a MR. If the SSC is directly related to safety, can mitigate accidents or transients, is part of Emergency Operational Procedures (EOP), can prevent other SSC of performing their safety functions, or causes a reactor shutdown or a safety system actuation, the SSC will be put within the MR scope. Otherwise, it remains under the existing maintenance program, outside the MR scope. The MR also requires that before performing maintenance activities the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.

The Nuclear Engineering Institute (NEI) issued the report NEI (1996). This document is a guideline for applying the Maintenance Rule at Nuclear Power Plants. Section 11.0 of NEI (1996) consolidates the assessment and management of the increase in risk that may result from the proposed maintenance activities.

The Electric Power Research Institute (EPRI) has assessed the role of probabilistic safety analysis in the regulation of nuclear power plant Technical Specification, EPRI (2006). This report presents a framework and associated general guidance for implementing Risk-Managed Technical Specifications, RMTS, as a partial replacement for existing Technical Specification, with the following objectives: a) to provide utilities with an approach for developing and implementing nuclear power station Risk-Managed Technical Specifications programs; and b) to complement and supplement existing successful configuration risk management applications such as the Maintenance Rule.

The guidance, EPRI (2006), is applicable to the determination of Risk-Informed Completion Time (RICTs), Risk-Management Action Times (RMATs) and specification of appropriate compensatory Risk-Management Actions (RMAS) applicable to Technical Specification requirements.

Risk management thresholds for RMTS program application are established quantitatively by considering the magnitude of the instantaneous Core Damage Frequency (CDF) and the Incremental Core Damage Frequency (ICDF) for the plant configuration of interest. The incremental frequency values are measured from their respective "no-maintenance" or "zero-maintenance" baseline frequencies as determined via PSA.

Thresholds for risk management actions may be established quantitatively by considering the magnitude of increase of the core damage frequency for the maintenance configuration. This is defined as the incremental CDF. The incremental CDF,

ICDF, is the difference in the "configuration-specific" CDF_s and the baseline (or the zero maintenance) CDF_{ZM}. The configuration-specific CDF_s is the annualized risk rate considering with the out-of-service equipment unavailability:

$$ICDP = (CDF_S - CDF_{ZM})/yr \quad (1)$$

This reflects more closely the plant actual configuration during the maintenance activity. Plants should consider duration factors when setting risk management thresholds. This may be either the duration of a particular out-of-service condition, or a specific defined work interval (e.g. shift, week, etc). The product of the incremental CDF and duration is expressed as a probability (e.g., Incremental Core Damage Probability—ICDP).

Guidance for evaluating temporary risk increases by considering configuration-specific risk is provided in NEI (1996). The risk management thresholds presented in Table 1 provides the basis for RMTS program implementation, the quantitative risk management thresholds and RMTS action guidance as well as a comparison of the respective applicable Maintenance Rule thresholds.

By EPRI (2006), in a RMTS program the 10^{-6} threshold for ICDP, is referred to as Risk Management Action (RMA) threshold and the RMAT is the corresponding risk management action time. The 10^{-5} threshold for ICDP is referred to as Risk Informed Completion Time (RICT) Thresholds. These thresholds are deemed appropriate for RMTS programs because they relate to integrated plant risk impacts that are occasional and temporary in nature and are consistent with NRC (2011a) and NRC (2011b).

Table 1. RMTS quantitative risk management thresholds.

Criterion	MR RMG*	RMTS RMG**
CDF		
$\geq 10^{-3}$ events/yr	Careful consideration before entering the configuration	Voluntary entrance into configuration prohibited. If in configuration due to emergent event, implement appropriate risk management actions
ICDP		
$\geq 10^{-5}$	Configuration should not normally be entered voluntarily	Follow technical specification requirements for required action not met
$\geq 10^{-6}$	Assess non-quantifiable factors; and establish compensatory risk management actions	RMAT and RICT requirements apply; Assess non-quantifiable factors; and Implement compensatory risk management actions
$<10^{-6}$	Normal work controls	Normal work controls

*Maintenance Rule Risk Management Guidance; **RMTS Risk Management Guidance.

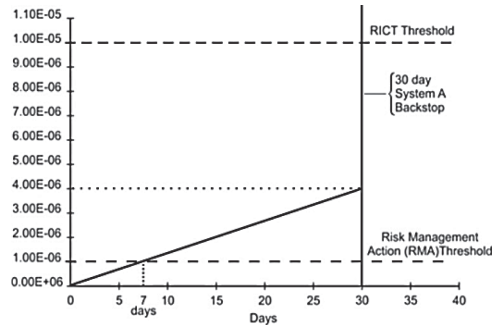


Figure 3. Configuration of risk management RMAT and RICT calculation.

Figure 3 provides a simple example of the RMTS process for inoperability of equipment followed by an emergent event which modifies the risk profile causing changes in the plant configuration RMAT and RICT values.

This example is intended to demonstrate the application of these values in a RMTS program. At $t = 0$, the RMTS equipment becomes inoperable for a duration anticipated to exceed the front-stop CT. In this configuration, RMAT and RICT are calculated.

4 RISK MANAGEMENT NPP

Risk management in nuclear power plants owned by Utility, aims at the monitoring and control of operational settings (unavailability of equipment and/or alignment systems) that imply risks to industrial installation of plants, the ownership and general public, or not directly involved in operating activities.

Risk management adopts the figure of merit frequency of damage to the reactor core to any interference on the tolerability of operational risk.

Risk management by APS during power operation covers: the testing activities; routine or planned corrective maintenance; and the activities of unplanned corrective maintenance.

The CDF calculated for a given plant configuration, in which one set of components is maintenance activities, is compared to the background risk to CDF. The acceptance criteria are defined for the instantaneous and the cumulative risks.

Table 2. Risk ranges depending on CDF.

CDF	Range	Tolerability
CDF < 10^{-4}	GREEN	Usual risk—controls work and usual tasks are developed without constraint having as principle prevent entry into YELLOW range.
$10^{-4} \leq$ CDF < 10^{-3}	YELLOW	Tolerable risk—risk management actions should be implemented seeking to limit the time spent in this band having as principle prevent entry into the RED.
CDF ≥ 10^{-3}	RED	Intolerable risk—risk management actions should be implemented seeking to limit the length of stay in this range for more severe levels as set out for the YELLOW band, under the guidance and strict permission of the Plant Supervisor, having in principle the immediate return the ranges or YELLOW or GREEN.

For the instantaneous risk, the based CDF should be calculated by assuming that all the components considered in the PSA are available to perform their functions (all basic events in test and maintenance should be considered as zero).

The configuration is classified by a criterion of range represented by a color, as the level of risk: GREEN, YELLOW or RED.

The values associated with the boundaries between the stripes and the tolerability of the risk posed is shown in Table 2.

Risk assessment of maintenance for the Unit in power activities are carried out with EOOS software, EPRI (2004), based on the model developed with the EPRI (2005).

The criteria adopted for the management of risk are based on the core damage frequency, CDF. The value of the CDF for PSA Level 1 is 2.3 10^{-5}/year.

5 CASE STUDY

The case study is related to planning maintenance whose completion time exceeds the established Allowable Outage Time of TS and to evaluate the application of EPRI (2006). The NPP is typical nuclear power plant of Siemens/KWU design. This design applies for safety systems of the *n*+2 (4 × 50%) redundancy design criteria.

With the unit in power, the TS states that unavailability (out of service) of one emergency diesel generator is 14 days (AOT or CT).

After this period, the unit should go to cold shutdown if the condition of the emergency diesel generator still remains unavailable.

With the application of the requirements of EPRI (2006) and NEI (1996) and using compensatory measures, the completion time was extended to 30 days for the emergency diesel generator maintenance. Table 3 and Figure 4 show the results for each emergency diesel generator.

It can be seen that risk management actions are necessary to complete the required AOT extension for DG-A, DG-B and DG-D. For DG-C RMAT is 30 days.

With the results of the quantitative evaluation, the monitoring conditions of maintenance activities were established.

The maintenance activities were authorized by the regulatory body that followed the services during the 30 days and has considered satisfactory in meeting the requirements established.

Maintenance activities were conducted in two GDs. These were performed on time and meeting the established criteria. The results demonstrate that

Table 3. Results of case study quantitative risk management thresholds.

Eq.	CDF_S	CDF_{ZM}	ICDP	$ICDP_{30}$	NWC	RMA
DG-A	3.53	1.82	1.71	1.4	22	8
DG-B	3.33	1.82	1.48	1.2	27	3
DG-C	3.10	1.82	1.28	1.0	30	–
DG-D	3.62	1.82	1.80	1.5	17	13

Eq.—Equipment; CDF_S—configuration-specific (10^{-6}/yr); CDF_{ZM}—the zero maintenance (10^{-6}/yr); ICDP—incremental core damage frequency (10^{-6}/yr); $ICDP_{30}$—incremental core damage frequency 30 days (10^{-6}/yr); NWC—Normal work control (days); RMA—Risk Management Actions (days).

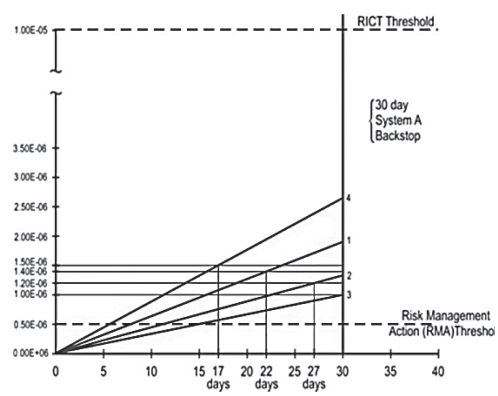


Figure 4. Case study configuration of risk management RMAT and RICT calculation.

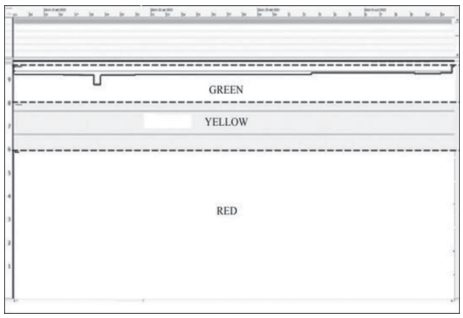


Figure 5. Case study CDF configuration profile during the 30 days maintenance of GD-B.

maintenance of the emergency diesel generators for 30 days does not cause a significant increase on plant risk. Figure 5 shows the profile of the CDF of the plant during the maintenance GD-B period.

6 CONCLUSIONS

Whereas PSA follows the requirements for an integrated decision-making process, the EPRI methodology is appropriate, allowing for consistent decision making.

According to EPRI (2006), a particular configuration change shall be limited to a period of 30 days by technical specifications.

This period was judged by EPRI as an administrative boundary prudently conservative risk management in maintenance activities.

It is noteworthy that, according to the use of risk management for the unit risk assessment, any other component/equipment that is declared inoperable simultaneously with maintaining a given DG and that affects the configuration of the unit may be returned to the original TS completion time.

Maintenance activities were conducted in two GDs. These were performed on time and meeting the established criteria. The results demonstrate that maintenance of the emergency diesel generators for 30 days does not cause a significant increase on plant risk.

REFERENCES

EPRI (2004). *Equipment Out of Service*, version 4.1, Data Systems & Solutions Electric Power Research Institute. Palo Alto, CA, USA.

EPRI (2005). *Fault Tree Analysis System. CAFTA 5.2 software*. Data Systems & Solutions/Electric Power Research Institute, Palo Alto, CA, USA.

EPRI (2006). *Risk-Managed Technical Specifications*: Report 1011758, Electric Power research Institute, Palo Alto, CA, USA.

IAEA (2010). *Risk-informed in-service inspection of piping systems of nuclear power plants: process, status, issues and development*, IAEA nuclear energy series, ISSN 1995-7807, International Atomic Energy Agency, Vienna, Austria.

IAEA (2011). *A framework for an integrated risk informed decision making process: a report by the International Nuclear Safety Group*, INSAG series, ISSN 1025-2169, No 25, International Atomic Energy Agency, Vienna, Austria.

Martorell, S., Villamizar, Villanueva, J.F., Carlos, S., & Sánchez, A.I. (2012). *Importance analysis in risk-informed decision-making of changes to Allowed Outage Times addressing uncertainties*, Advances in Safety, Reliability and Risk Management, Bérenguer, Grall, Guedes Soares (eds), Taylor and Francis, London, pp 2143–2151.

NEI (1996). *Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants*, Section 11—Assessment of Risk Resulting from Performance of Maintenance Activities, NUMARC 93-01 Revision 3, Nuclear Engineering Institute, USA.

NRC (1975). *Reactor Safety Study—An Assessment of Accident Risks* in US Commercial Nuclear Power Plants. WASH-1400, NUREG-75/014, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (1988). *Individual Plant Examination for Severe Accident Vulnerabilities*—10 CFR 50.54(f). Generic Letter GL-88-20, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (1995). *Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities, Final Policy Statement*. Federal Regulation-60FR 42622, Nuclear Regulatory Commission, Wash ington, DC, USA.

NRC (1998). *An Approach for Plant-Specific, Risk-Informed Decision Making: Inservice Testing Assurance*, RG-1.175, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2000). *Reactor Oversight Process*, NUREG-1649, US Nuclear Regulatory Commission, Washington, DC.

NRC (2001). *Technical Committee Meeting on Risk Informed Decision Making (RIDM)*, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2003). *An Approach for Plant-Specific, Risk-Informed Decision Making: Inservice Testing Inspection of Piping*, RG-1.178, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2009a). *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, RG-1.200, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2009b). *Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants,* RG-1.205, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2011a). *An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, RG-1.174, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2011b). *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications*, RG-1.177, Nuclear Regulatory Commission, Washington, DC, USA.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Expert system for means of transport maintenance processes performance. A comparative analysis for various types of rail vehicles

T. Nowakowski & S. Werbińska-Wojciechowska
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: In the presented paper, the authors' research work is focused on the comparative analysis of developed expert system for transportation means' maintenance processes performance implementation in various rail buses exploitation processes performance. As a result, in the Introduction section, the transportation means' maintenance processes issues and a briefly literature overview in the research area are discussed. In the next Sections, the decision support system and expert system for means of transport maintenance processes performance are described. Following this, the case studies of transportation systems performing in Lower Silesia province, Poland is provided. The work ends up with summary and directions for further research.

1 INTRODUCTION

Effective performance of transportation systems needs proper operational management performance on the one hand, and adequate maintenance performance determination on the other. The decision relevance strictly depends on their accuracy and dedicated decision time. Moreover, it influences the dependability state of the system (Babiarz 2006, Kierzkowski 2010, Valis and Vintr 2006).

The maintenance strategy selection is a complex process, thus it may be supported by decision support systems implementation (Nowakowski & Werbińska-Wojciechowska 2013, 2012a). Such systems can support chosen or every step of manager's decision making process, such as: data gathering, problem definition, problem classification, information model designing, model solution, or optimization process performance (Grobarek et al. 2007).

The Decision Support System (DSS) concept is extremely broad and its definitions may vary depending on the author's point of view and the way of its use (DSS 2002). It may be defined as "… *an interactive computer-based system that helps decision makers utilizes data and models to solve unstructured problems*" (Despres & Rosenthal-Sabroux 1992). The literature review in the research area of DSS designing and applications issues may be found e.g. in (Arnott & Pervan 2008, Asemi et al. 2011, Despres & Rosenthal-Sabroux 1992, Eom 2001, Grobarek et al. 2007, Jankowski & Laskowski 2012, Jodejko-Pietruczuk & Plewa 2012, Lubkowski & Laskowski 2013, Power 2008, Sharda et al. 1988, Vintr & Valis 2012, Zhengmeng & Haoxiang 2011).

In the literature, there can be found a lot of works dedicated to DSS developed for means of transport maintenance processes (see e.g. (Bojda et al. 2010, Kacprzak et al. 2011, Martland et al. 1990, Wachnik & Drzewiecki 2011, Zhang et al. 2011, Zhu 1996)).

In the area of passenger transportation processes performance, the DSS issues being analysed in the literature regarded to e.g. timetable adjustments (e.g. (Mendes-Moreira et al. 2009)), transportation system planning process supporting (e.g. (Burla et al. 2009, Han 2006, Kamath et al. 2011)), traffic control (e.g. (Borne et al. 2003, Ossowski et al. 2005, 2004)), or transportation system safety during emergencies (e.g. (Yoon et al. 2008)).

The convenient approach for solving the maintenance management problems is expert system implementation. The expert system may be defined as an *intelligent computer program that uses knowledge and inference procedures to solve problems that are difficult enough to require significant human expertise for their solution* (Angeli 2010). The main components in an expert system development include: knowledge acquisition, choice of knowledge representation, the coding of knowledge in a knowledge base, the development of inference procedures for diagnostic reasoning, and the development of input-output interfaces (Venkatasubramanian et al. 2003).

Following this, the authors have investigated the problem of decision support system for transportation means' maintenance process performance by development of DSS conception (see e.g. (Bojda & Werbińska-Wojciechowska 2012)), expert system definition (see e.g. (Nowakowski & Werbińska-Wojciechowska 2012a)), data uncertainty analysis (see e.g. (Nowakowski & Werbińska-Wojciechowska 2012b)), or initial analysis of

expert system implementation possibilities (see e.g. (Bojda et al. 2014)). As a result, the focus of this study is to investigate the implementation possibilities of developed expert system for different types of means of transport when their exploitation databases differ. Thus, in the next Sections, the conception of DSS for means of transport maintenance processes performance and Expert system are investigated. The work ends up with discussion about analysis results of expert system implementation in the case companies maintenance decision processes performance.

2 DECISION SUPPORT SYSTEM IN MEANS OF TRANSPORT MAINTENANCE PROCESSES PERFORMANCE

The purpose of the developed DSS performance is connected with possible maintenance strategy (traditional/DTA based) for technical object definition based on chosen maintenance and dependability indicators' values. The solution is based on decision rules implementation. These decision rules are the base for computer procedure of decision support definition.

The general decision support program's structure is given in the Figure 1. The example of decision rules edition process is given in (Nowakowski, 1999). For more information we recommend reading e.g. in (Bojda et al. 2014, Bojda & Werbińska-Wojciechowska 2012, Nowakowski & Werbińska-Wojciechowska 2014, 2013).

The main *assumptions* taken during the DSS development encompass (Bojda & Werbińska-Wojciechowska 2012):

- performance of a multi-component (or complex), repairable transportation system investigation,
- investigation of maintenance strategies for systems with and without components dependence,
- corrective maintenance strategy omission,
- condition-based maintenance models omission,
- maintenance information management models omission,
- cannibalization maintenance models omission.

Following these considerations, in the DSS development process we examine various types

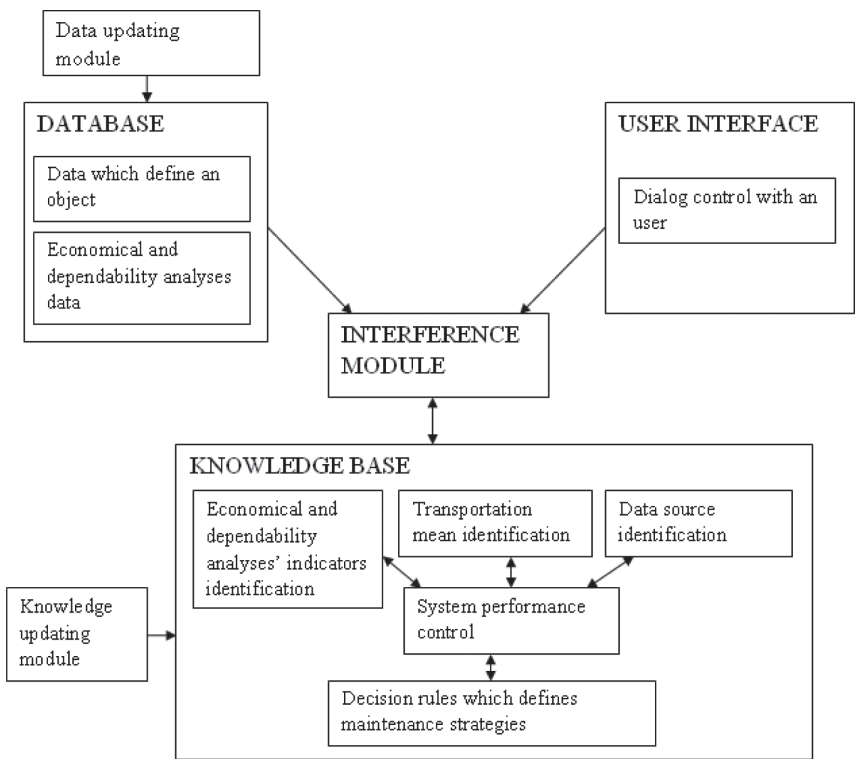


Figure 1. The structure of DSS for means of transport maintenance process performance (Nowakowski & Werbińska-Wojciechowska, 2012).

of maintenance policies for multiunit or complex systems, which are the most commonly used (for review see e.g. (Nowakowski & Werbińska, 2009)).

The development of DSS in the analysed area regards input data, conclusions and decision rules definition. The main *input data* which are necessary to be used in a DSS performance can be classified into three groups (Bojda & Werbińska-Wojciechowska 2012):

- general data, which describe transportation system performance,
- data which describe the actual state of transportation system,
- data which describe the maintenance costs of transportation system performance.

The decisions are made based on the information about the state of a system, maintenance costs and data accessibility. These input data being defined more precisely and quantified are used to develop *decision rules*, which are the simple logical sentences. More information can be found in (Bojda et al. 2014, Bojda & Werbińska-Wojciechowska 2012, Nowakowski & Werbińska-Wojciechowska 2014, 2013).

Table 1 shows a list of basic maintenance strategies included in the DSS with the main information necessary to be gathered to implement the DSS in the area of real-life transportation systems performance. In the Table 2, there are defined main input data.

Table 1. List of maintenance strategies included in the DSS (with index) (Bojda & Werbińska-Wojciechowska 2012).

PM strategy index	PM strategy definition
t_1	Age Replacement Policy (ARP) with minimal repair
t_2	Age Replacement Policy with CF
t_3	Age Replacement Policy for multi-unit system with cost constrains
t_4	Age Replacement Policy for multi-unit system with availability constrains
t_5	Block Replacement Policy (BRP) with minimal repair
t_6	Block Replacement Policy with CF
t_7	Block Replacement Policy for multi-unit system with common cause shock failure
t_8	Block Replacement Policy for multi-unit system with availability constrains
t_9	Block Replacement Policy for multi-unit system with 3 types of maintenance
t_{10}	Repair Limit Policy (RLP) with imperfect repair
t_{11}	Repair Limit Policy with minimal repair
t_{12}	Repair Limit Policy with CF
t_{13}	(L-u,L) policy
t_{14}	Opportunistic Maintenance Policy (OMP) with CF
t_{15}	(τ,T) policy with costs
t_{16}	(τ,T) policy with availability
t_{17}	Simple Group Maintenance Policy (GMP)
t_{18}	Simple Group Maintenance Policy (GMP) with minimal repair
t_{19}	Simple T-policy
t_{20}	Simple T-policy with minimal repair
t_{21}	m—failure policy
t_{22}	(m, T) policy
t_{23}	Delay Time Model (DTM) for multi-unit systems
t_{24}	Delay Time Model for multi-unit systems with imperfect inspections
t_{25}	Delay Time Model for complex systems and non-negligible RT
t_{26}	Delay Time Model for complex systems
t_{27}	Delay Time Model for complex systems with imperfect inspections

t_f—time moments of failure occurrence.
t_{RT}—time moments of repair action finishing

Table 2. The necessary input data for DSS implementation.

Index	Input data definition
Np	Number of means of transport in a system
TE	Time horizon of observation performance
L	Type of components dependency
RS	Type of system's reliability structure
Z_F	Type of system failure
t_f	Time moments of failure occurrence
ZM	Type of maintenance processes performance
t_{RT}	Time moments of maintenance actions finishing
T_p	Time of preventive maintenance performance
T_c	Time of corrective maintenance performance
T_{nm}	Time of minimal repair performance
T_{in}	Time of inspection action performance
T_{dw}	Downtime of a system
$E[h]$	Expected value of delay time
c_{cor}	Cost of corrective action performance
c_{op}	Operational cost per unit of time
c_w	Cost per unit of preventive action performance
c_p	Penalty cost
c_{dw}	Cost of system downtime
c_{nm}	Cost per unit of minimal repair performance
c_i	Cost of inspection performance
$C_{mn}^{\max}$	Maximal acceptable cost of corrective action performance

3 EXPERT SYSTEM APPLICATION

The expert system is based on EXSYS Professional system implementation. Exsys Corvid, is a

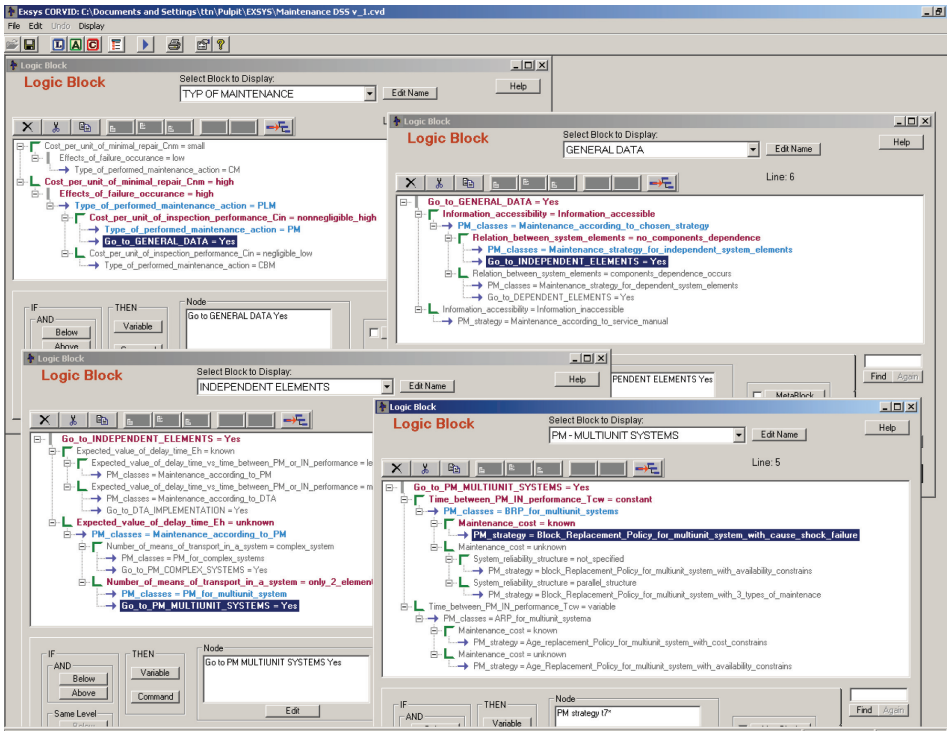


Figure 2. Rule decision window for t_7 strategy selection.

development environment suitable for any type of knowledge automation system project—anywhere expert advice and answers need to be distributed or accessed (Exsys 2011). The example of decision rules edition process is given in (Nowakowski 1999, Nowakowski & Werbińska-Wojciechowska 2014) and the introduction to the presented problem is given e.g. in (Bojda & Werbińska-Wojciechowska 2012, Nowakowski & Werbińska-Wojciechowska 2012a, b). The detailed description of DSS building process is given in (Bojda et al. 2014, Bojda & Werbińska-Wojciechowska 2012, Nowakowski & Werbińska-Wojciechowska 2014, 2013, 2012a, b).

An exemplary DSS screen of Rule decision window is given in Figure 2.

4 EXPERT SYSTEM IMPLEMENTATION

4.1 *Case studies—regional and local passenger transportation systems*

The developed expert system was applied to select maintenance strategies for two types of rail vehicles being operated in two different passenger transportation systems located in Lower Silesia, Poland.

The first type of rail vehicles—rail buses are used in regional passenger transportation system. The operator puts into service small- and middle-sized diesel rail vehicles, running mostly as single train sets, rarely coupled. Currently 21 rail buses dating from 2004 to 2011 are used, being built mostly by one manufacturer or his subsidiaries. The research analysis covered 8 single car rail buses of particular type X.

The system covers several routes operated daily by Lower Silesian Railways Company on mixed-traffic railway infrastructure which is partially single and double track. The network is of irregular form with central station in Legnica, supplemented by the only service depot for the car fleet located nearby. More information can be found e.g. in (Bojda et al. 2014).

The second type of rail vehicles—trams by Skoda are used in city transportation system performing in Wroclaw city, Poland. The municipal transport services are provided by a common carrier. In March 2012, the city carrier had a total of 416 passenger tram cars (*Urban* …, 2012), including 48 cars of Skoda (17 cars of Skoda 16T and 31 cars of Skoda 19T).

The tram network covers the most area of the city, and is supplemented by four service depots. More

information can be found e.g. in (Nowakowski & Werbińska-Wojciechowska in prep.).

4.2 *Maintenance data for presented case companies' rail vehicles*

To implement expert system in the area of maintenance management decision process performance, there were collected data about rail buses' and trams operational processes performance. In the case of rail carriers, the period of research analysis encompasses 43 months (152 568 working hours), from December 2008 to June 2012. The operational data are taken from their operational books which are prepared by department of tram maintenance employees. These operational books are located in every rail buses, and are filled in by engine drivers, warehousemen, and service engineers.

Every engine driver should fill in the date, hour and place of beginning/finishing his work. Moreover, some additional information should be taken into account, like e.g. all failures and irregularities detected during operational process performance.

In the case of trams performance, the period of research analysis covers time from January to December of 2011. The operational data include the recording of all events associated with the operational process of rail vehicles (Skoda 16T, 19T) and their maintenance actions that have been recorded in the technical book and emergency exits book.

The gathered data contain e.g. the information about the date of the event, the number of the wagon; failure information, maintenance information (e.g. type of repair, date of repair). In some cases, there are given extra information about a time of incident notification, time of damaged tram substitution, but such contributions was less (about 30%).

The collected data give the authors information e.g. about types of failures occurred in the system, their occurrence frequency. There were also obtained information about maintenance actions performance (planned/unplanned). Following this, the transportation system characteristics can be obtained. The exemplary transportation systems characteristics for time between failures of defined types of rail vehicles are presented in Figures 3–5.

For more deeply analysis of obtained operational data and rail cars dependability characteristics we recommend reading e.g. (Bojda et al. 2014, Nowakowski & Werbińska-Wojciechowska in prep.).

Another problem regards to economical parameters estimation. There were obtainable corrective and preventive maintenance actions' costs only for one case company—regional carrier. More information can be found in (Bojda et al. 2014). In the second case, maintenance manager has to base only on operational input data to select maintenance strategy.

To sum up, the analysis of rail cars operational processes performance gives the possibility to gather

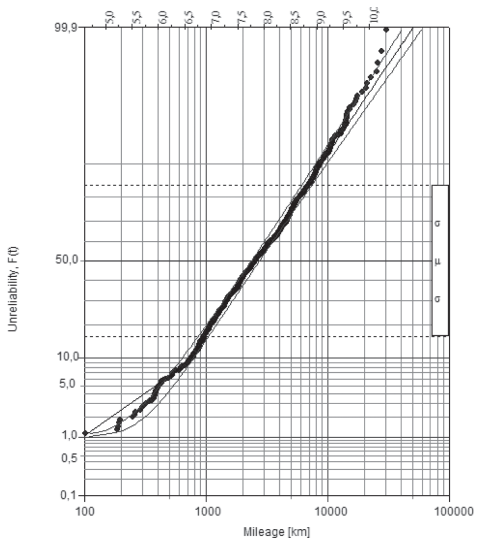


Figure 3. The cumulative distribution function of rail buses time between failures [mileage] (Log-normal distribution: $\mu = 7.8517$, $\sigma = 0.9673$) (Nowakowski & Werbińska-Wojciechowska 2014).

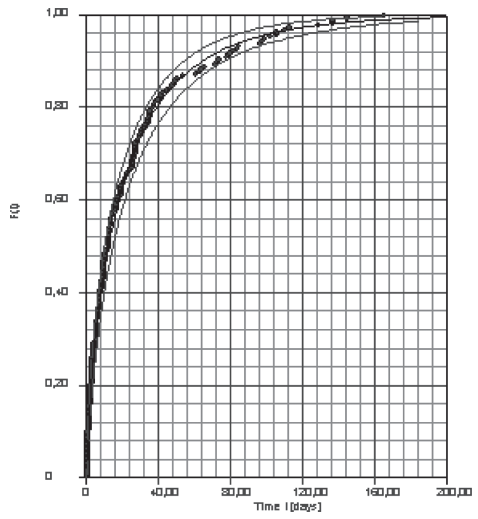


Figure 4. The cumulative distribution function of rail buses Skoda 16T time between failures [days] (Weibull distribution with parameters: $k = 0.7144$, $\lambda = 19.9665$, $\gamma = 0.7800$, $\rho = 0.9739$) (Nowakowski & Werbińska-Wojciechowska in prep.).

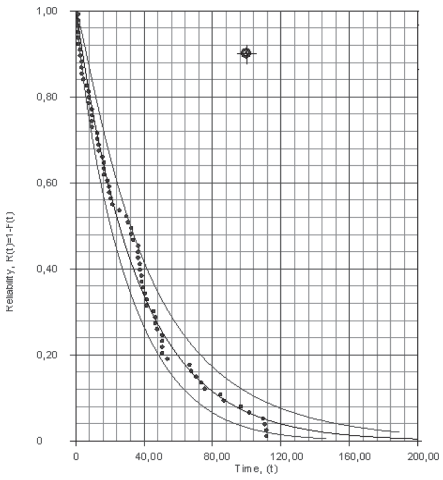


Figure 5. The reliability function of rail buses Skoda 19T [days] (Weibull distribution with parameters: k = 0.9881, λ = 36.4833, γ = 0.3750, ρ = 0.9771) (Nowakowski & Werbińska-Wojciechowska in prep.).

main operational and maintenance data, necessary for maintenance strategy selection process. However, not all necessary DSS's input parameters (presented in the Table 2) were defined during research analysis performance. The comparison of accessible for case companies input data is presented in the Table 3.

In the Table 4, there is presented the correlation between necessary input data and maintenance strategies defined in the expert system (where system reliability structure: 0—a series structure, 1—a parallel structure, 2—a k-out-of-n structure, 3—not specified). For more information see (Bojda & Werbińska-Wojciechowska 2012).

For example, for both the analysed transportation systems there were no possibility to define if, and what kind of components dependency occur. The system reliability structure wasn't also defined. Additionally, there were also no possibilities of delay time parameter estimation. The problem with economic data gathering process is also visible for the case of Skoda trams.

Following this, in the next Section, there is presented the developed expert system implementation in rail cars' maintenance strategy selection process.

4.3 *Maintenance strategy selection for case companies' rail vehicles with expert system application*

In the next step of research analysis authors have implemented the developed expert system for one of the defined maintenance strategies selection process performance. During the decision process, there has to be answered few questions regarding e.g. types

Table 3. The accessibility of necessary input data for DSS implementation for the analysed rail cars.

	Accessibility(+)/inaccessibility(–) of operational data	
Index	Rail buses (1st case company)	Skoda trams (2nd case company)
Np	+	+
TE	+	+
L	–	–
RS	–	–
Z_F	+	+
t_f	+	+
ZM	+	+
t_{RT}	+	+
T_p	+	+
T_c	+	+
T_{nm}	–	+
T_{in}	–	+
T_{dw}	+	+
$E[h]$	–	–
c_{cor}	+	–
c_{op}	–	–
c_w	+	–
c_p	–	–
c_{dw}	+	–
c_{nm}	–	–
c_i	–	–
$C_{mn}^{\max}$	–	–

of the performed maintenances, types of occurred failures, or components dependency occurrences.

For the case of rail buses, the expert system indicates, that the best maintenance strategy for analysed transportation system is t_8—*Block Replacement Policy for multi-unit system with availability constrains*. This result is connected with e.g. lack of information about system reliability structure. Another simplification regards to impossibility of delay time and elements dependency definition. As a result, authors underline, that the rail cars operational process performance should be broadly analysed in order to gather the necessary but not obtained input data for expert system fully implementation.

For the case of Skoda trams, the maintenance strategy selection process is limited to those policies, which uses reliability/availability as optimization criteria. In that case, expert system support maintenance manager with choosing the same maintenance strategy—t_8—*Block Replacement Policy for multi-unit system with availability constrains*. This is also connected with the time between planned maintenance actions performance which is suggested to be constant.

Table 4. The correlation between maintenance strategies implemented in the DSS and necessary input data (Bojda & Werbińska-Wojciechowska 2012).

PM strategy	General data			Dependability data												Economical data								Performance criterion
	Np	*TE*	*L*	*RS*	Z_F	t_f	*ZM*	t_{RT}	T_p	T_c	T_{nm}	T_{in}	T_{ew}	T_{rx}	T_{dw}	c_{cor}	c_{nm}	c_{op}	c_w	c_i	c_P	c_{dw}	$C_{mn}^{\max}$	
ARP																								
t_1		∞	–		+	+	+						+				+		+					Costs
t_2		∞	–		+	+	+						+			+		+	+					Costs
t_3	+	∞	–	0	+	+	+		+	+			+			+			+					Costs
t_4	+	∞	–	2	+	+	+			+			+	+										Availability
BRP																								
t_5		∞	–		+	+	+				+		+				+		+					Costs
t_6		∞	–		+	+	+				+		+				+		+					Costs
t_7	+	∞	–	0	+	+	+						+		+									Availability
t_8	+	∞	–	3	+	+	+						+											Availability
t_9	+	∞	–	1	+	+	+						+				+		+		+			Costs
RLP																								
t_{10}		∞	–		+	+	+												+				+	Costs
t_{11}		∞	–		+	+	+										+		+				+	Costs
t_{12}		∞	–		+	+	+						+							+			+	Costs
OMP																								
t_{13}	+	∞	+	3	+	+	+						+			+	+		+					Costs
t_{14}	+	∞	+	3	+	+	+						+			+			+					Costs
t_{15}	+	∞	+	3	+	+	+		+	+			+	+		+			+					Costs
t_{16}	+	∞	+	3	+	+	+		+	+			+	+										Costs
GROUP MP																								
t_{17}	+	∞	+	3	+	+	+		+	+			+											Availability
t_{18}	+	∞	+	3	+	+	+		+	+	+		+											Availability
t_{19}	+	∞	+	3	+	+	+						+					+	+					Availability
t_{20}	+	∞	+	3	+	+	+						+						+					Costs
t_{21}	+	∞	+	3	+	+	+						+		+	+			+		+	+		Costs
t_{22}	+	∞	+	3	+	+	+						+		+	+			+		+	+		Costs
t_{23}	+	∞	–	3	+	+	+		+	+		+	+						+	+	+			Costs
t_{24}	+	∞	–	3	+	+	+		+	+	+	+	+			+			+	+				Costs
DTA POLICIES																								
t_{25}		∞	–		+	+	+	+				+	+		+									Downtime
t_{26}		∞	–		+	+	+					+	+			+			+	+				Costs
t_{27}		∞	–		+	+	+					+	+			+			+	+				Costs

5 CONCLUSIONS

The discussed issue is a continuation of research work connected with developing a decision support system for transportation means' maintenance processes performance. The system gives decision makers a hint which one from the defined maintenance strategies is the most advisable to implement in a defined circumstances. However, the conclusions are strictly determined by the type and likelihood of obtained operational data. In the presented case studies not all the necessary information can be put into the system. Following this, the decision process cannot be conducted in a proper manner.

Moreover, there is a problem with data uncertainty. Some research works which consider uncertainty problem in decision support system performance are given in (Nowakowski & Werbińska-Wojciechowska 2012b). As a result, the discussion about the input data reliability and its influence on decision process results will be the point of authors' further research works.

REFERENCES

Angeli, C., 2010. Diagnostic expert systems: from expert's knowledge to real-time systems. In: *TMRF e-Book, Advanced Knowledge Based Systems: Model, Applications & Research*. Sajja & Akerkar (eds.), vol. 1: 50–73.

Arnott, D., Pervan, G., 2008. Eight key issues for the decision support systems discipline. *Decision Support Systems* 44: 657–672.

Asemi, A., Safari, A., Asemi Zavareh, A., 2011. The Role of Management Information System (MIS) and Decision Support System (DSS) for Manager's Decision Making Process. *International Journal of Business and Management* 6(7): 164–173.

Babiarz, B., 2006. An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping*, Vol. 83, No. 4/2006: 230–235.

Bojda, K., Dziaduch I., Nowakowski T., Werbińska-Wojciechowska S., 2014. Decision support system for means of transport maintenance processes performance. A case study of rail buses. In: *Safety, reliability and risk analysis: beyond the horizon: proceedings of the European Safety and Reliability Conference, ESREL 2013*, Amsterdam, The Netherlands, 29 September–2 October 2013. Steenbergen R.D.J.M. (eds). Leiden: CRC Press/ Balkema: 909–919.

Bojda, K., Młyńczak, M., Restel, F.J., 2010. The concept of software support system for the management of railcar operation (in Polish). *Proc. of TRANSCOMP—XIV International Conference Computer Systems Aided Science, Industry and Transport, Zakopane, Poland, 2010*.

Bojda, K., Werbińska-Wojciechowska, S., 2012. Data accessibility problem in transportation means' maintenance performance. In Stachowiak A. (ed.), *Transport—strategical and operational issues:* monograph: 69–87. Poznan: Publishing House of Poznan University of Technology.

Borne, P., Fayech, B., Hammadi, S., Maouche, S., 2003. Decision Support System for Urban Transportation Networks. *IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews* 33(1): 67–77.

Burla, M., Laniado, E., Romani, F., Tagliavini, P., 2001. The Role of Decision Support Systems (DSS) in Transportation Planning: the Experience of the Lombardy Region. *Proc. of Seventh International Conference on Competition and Ownership in Land Passenger Transport, Molde, Norvay, 25–28 June 2001*.

Decision Support Systems, 2002. Available at: http://diuf.unifr.ch/ds/courses/dss2002/pdf/DSS.pdf.

Despres, S., Rosenthal-Sabroux, C., 1992. Designing Decision Support Systems and Expert Systems with a better end-use involvement: A promising approach. *European Journal of Operational Research,* 61: 145–153.

Eom, S.B., 2001. Decision Support Systems. In: *International Encyclopedia of Business and Management*, 2nd Edition, Warner M. (ed.). London: International Thomson Business Publishing Co.

Exsys Corvid Knowledge Automation Expert System Development Manual, 2011. Exsys Inc. www.exsys.com. (30.09.2012r.).

Grobarek, I., Grzywański, Ł., Mączka, I., Tomalik, D., Twórz, K., 2007. *Dependability of decision support systems* (in Polish). http://www.ioz.pwr.wroc.pl/Pracownicy/mercik/zbiory/Prezentacje%202007/z3-opracowanie.pdf (22.03.2012).

Han, K., 2006. *Developing a GIS-based Decision Support System for Transportation System Planning*. AASHTO GIS-T. www: http://www.gis-t.org/files/gnYKJ.pdf (23.03.2012).

Jankowski, D., Laskowski, D., 2012. Increasing the robustness of the telephone service of the heterogeneous environment with using open source solutions. *Dependability and Computer Systems*, WUT, Wroclaw: 37–52.

Jodejko-Pietruczuk, A., Plewa, M., 2012. Reliability based model that supports decision making about recovery options in the area of reverse logistics. *Proc. of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM 11 & ESREL 2012*: 4555–4562.

Kacprzak, M., Kulinowski, P., Wędrychowicz, D., 2011. Computerized information system used for management of mining belt conveyors operation. *Eksploatacja i Niezawodnosc—Maintenance and Reliability,* 2: 81–93.

Kamath, M., Srivathsan, S., Ingalls, R.G., Shen, G., Pulat, P.S., 2011. TISCSoft: A Decision Support System for Transportation Infrastructure and Supply Chain System Planning. *Proc. of the 44th Hawaii International Conference on System Sciences*.

Kierzkowski, A., 2010. Reliability models of transportation system of low cost airlines. *Reliability, risk and safety: back to the future.* eds. Ale, B.J.M., Papazoglou, J.A., Zio E., Raton, B.: CRC Press: 1325–1329.

Lubkowki, P., Laskowski, D., 2013. The end-to-end rate adaptation application for real-time video monitoring. *Advances in Intelligent Systems and Computing*, Springer International Publishing AG, Switzerland, Vol. 224: 295–305.

Martland, C.D., McNeil, S., Acharya, D, Mishalani, R., 1990. Applications of expert systems in railroad maintenance: scheduling rail relays. *Transportation Research Part A: Policy and Practice,* 24A(1): 39–52.

Mendes-Moreira, J., Duarte, E., Belo, O., 2009. A decision support system for timetable adjustments. *Proc. of the XIII Euro Working Group on Transportation Meeting (EWGT 2009)—September 2009.*

Nowakowski, T., 1999. *Methodology for reliability prediction of mechanical objects* (in Polish). Wroclaw: Research work of the Institute of Machine Designing and Operation, Wroclaw University of Technology.

Nowakowski, T., Werbińska-Wojciechowska, S., (2014). Problems of rail vehicles dependability assessment. Case study. (in Polish). *Article prepared for XXI Konferencja Naukowa POJAZDY SZYNOWE 2014,* 26th–28th May, 2014, Wroclaw.

Nowakowski, T., Werbińska-Wojciechowska, S., 2014. Data gathering problem in decision support system for means of transport maintenance processes performance development. In: *Safety, reliability and risk analysis: beyond the horizon: proceedings of the European Safety and Reliability Conference, ESREL 2013*, Amsterdam, The Netherlands, 29 September–2 October 2013. Steenbergen R.D.J.M. (eds). Leiden: CRC Press/Balkema: 899–907.

Nowakowski, T., Werbińska-Wojciechowska, S., 2013. Computer decision support system in means of transport maintenance processes performance (in Polish). *Critical infrastructures dependability. Proc. Conf. XLI Winter School of Reliability*. *Szczyrk, January, 6–12 2013.* Radom: Institute of Exploitation Technology Publ. House.

Nowakowski, T., Werbińska-Wojciechowska, S., 2012a. Means of transport maintenance processes performance. Decision support system. *Proc. Carpathian Logistics Congress, CLC' 2012. Jesenik, Czech Republic, November 7th–9th 2012*. Ostrava: Tanger.

Nowakowski, T., Werbińska-Wojciechowska, S., 2012b. Uncertainty problem in decision support system for means of transport maintenance processes performance development. *Journal of KONBiN,* 3: 173–192.

Nowakowski, T., Werbińska, S., 2009. On problems of multicomponent system maintenance modeling. *International Journal of Automation and Computing,* 6(4): 364–378.

Ossowski, S., Fernandez, A., Serrano, J.M., Perez-de-la-Cruz, J.L., Belmonte, M.V., Hernandez, J.Z., Garcia-Serramp, A.M., Maseda, J.M., 2004. Designing Multiagent Decision Support System The Case of Transportation Management. *Proc. of AAMAS'04, July 19–23 2004*. New York, USA.

Ossowski, S., Hernandez, J.Z., Belmonte, M-V., Fernandez, A. Garcia-Serrano, A., Perez-de-la-Cruz, J-L., Serrano, J-M., Triguero, F., 2005. Decision support for traffic management based on organisational and communicative multiagent abstractions. *Transportation Research Part C*, 13: 272–298.

Power, D.J., 2008. Understanding Data-Driven Decision Support Systems. *Information Systems Management,* 25(2): 149–154.

Sharda, R., Barr, S.H., McDonnell, J.C., 1988. Decision support system effectiveness: a review and an empirical test. *Management Science,* 34(2): 139–159.

Urban transport in quantity 2011 (in Polish), 2012. Chamber of Urban Transport, Warsaw.

Valis, D., Vintr, Z., 2006. Vehicle Maintenance Process Optimisation Using Life Cycle Costs Data and Reliability-Centred Maintenance. In: *Proceedings of the First International Conference on Maintenance Engineering. Beijing*: Science Press.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., Yin, K., 2003. A review of process fault detection and diagnosis Part III: Process history based methods. *Computers and Chemical Engineering,* 27: 327–346.

Vintr, Z., Valis, D., 2012. A Tool for Decision Making in k-out-of-n System Maintenance. *Applied Mechanics and Materials*, Vol. 110–116: 5257–5264.

Wachni, R., Drzewiecki, A., 2011. Maintenance Management System of railway vehicles (MMS) (in Polish). In: *Scientific Papers of Silesian University of Technology, Series: Transport* 73, 1861: 115–123.

Yoon, S.W., Velasquez, J.D., Partridge, B.K., Nof, S.Y., 2008. Transportation security decision support system for emergency response: A training prototype. *Decision Support Systems,* 46: 139–148.

Zhang, P., Zhao, S-W., Tan, B., Yu, L-M., Hua, K-Q., 2011. Applications of Decision Support System in Aviation Maintenance, Efficient Decision Support Systems—Practice and Challenges in Multidisciplinary Domains. Prof. Chiang Jao (Ed.). InTech. http://www.intechopen.com/books/efficient-decision-support-systems-practice-and-challenges-in-multidisciplinary-domains/applications-of-decision-support-system-in-aviation-maintenance.

Zhengmeng, Ch., Haoxiang, J., 2011. A Brief Review on Decision Support Systems and its Applications. *Proc. of International Symposium on IT in Medicine and Education (ITME) 2011, 9–11. December 2011*, vol. 2: 401–405.

Zhu, K.X., 1996. Sensor-based Condition Monitoring and Predictive Maintenance—An Integrated Intelligent Management Support System. *Intelligent Systems in Accounting, Finance and Management,* 5: 241–258.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A Colored Petri Net model for railway track maintenance with two-level inspection

Hui Shang
ICD, LM2S, CNRS, UMR, Troyes University of Technology, Troyes, France

Christophe Bérenguer
GIPSA-Lab, University of Grenoble Alpes, Grenoble, France
GIPSA-Lab, CNRS, Grenoble, France

ABSTRACT: Track fault may cause the derailment and it is one of the major contributors to railway maintenance costs. Gauge spread is one of the track faults. Maintenance and speed restriction should be taken according to the inspection results. Visual Inspection (VI) can only detect poor fastening and static gauge spread. Train Recording Vehicle (TRV) detects the loaded gauge spread. The inspection frequencies are required in Standards, but they should happen at a greater frequency if the recommendations are insufficient. Two inspection schemes are introduced for a railway section. One scheme considers that VI and TRV are periodic; another assumes that TRV interval depends on the number of identified defects. In this paper we propose a risk and maintenance model based on a hierarchical Colored Petri Net (CPN) for a railway section, since CPN is flexible enough to model the component deterioration process and the different inspection schemes. The CPN model considers not only the maintenance process for observed component states but also the accident scenarios. According to Monte Carlo simulation results, the model can be used to evaluate the inspection policies.

1 INTRODUCTION

Railway industry concerns the performance of railway system and railway assets management tries to reduce the railway accidents and the maintenance cost. Derailment is one of railway accidents leading to fatalities and a high corrective maintenance cost. On plain line, derailment may occur when a train travels along a poor condition track. Track inspections and maintenances should be carried out to maintain track condition. Traffic control such as speed restriction cooperates with track maintenance to decrease accident frequencies or reduce accident consequences. Track maintenances cost a lot of money and traffic controls always reduce line availability. System risk metrics, railway line availability and management cost are required to decide when and how to maintain the track and when to perform speed restriction to get fewer accidents with higher availability and lower cost.

1.1 *Track quality and its modeling*

According to derailment investigations, around 74% of derailments occur due to track problems; in the track issues, track geometry fault (i.e. gauge spread, twist, cyclic top and buckle) is the major contribution to derailment. Wheels on one side may climbs the rail flange and wheels on the other side drop down the rails due to track faults (Lupton 2003).

Since the track faults are unrevealed, track condition data is collected for the one-eighth mile section by inspection methods (GC/RT 5021 2011) (GC/RT 5010 1998). Track faults can be described using track deterioration models. In the literature, deterministic model and stochastic model are used to model track degradation. Deterministic methods focus on the factors related to track quality, these factors can be materials, loads, speed and so on (Zwanenburg 2008) (Westgeest, Dekker, & Fischer 2012) (Sadeghi & Askarinejad 2010). However, track deterioration varies at different time, that is important to be considered in maintenance decision making, so stochastic models are introduced to describe these variations (Meier-Hirmer, Riboulet, Sourget, & Roussignol 2009) (Quiroga & Schnieder 2011).

This paper focus on gauge spread and assumes it is a stochastic process. Gauge spread is defined as the tendency of the maintained track gauge to become greater. It occurs due to poor fastening system or poor sleepering condition, such as

baseplate shuffle, chair shuffle, rotten sleepers and chair screws losing their grip in the sleepers, these events might be identified by visual inspection and fixed by refastening (Ellis 2006). Track gauge is classified to be static and dynamic regarding to the loading on track. The standard static track gauge is 1430 mm, the allowed maximum dynamic gauge is 1480 mm. The static gauge can be measured by visual inspection; once the static gauge exceeds 1450 mm, dynamic gauge should be measured by train recording vehicle. If static gauge is over 1430 and below 1450 mm, gauge spread can be controlled by speed restriction or tie-bar. If the gauge exceeds 1450 mm and below 1480 mm, speed restriction and tie bar should be carried out at the same time. If the gauge spread is high (the loaded gauge is over 1480 mm), the line should be closed until re-sleepering restores track gauge (GC/RT 5021 2011).

A multi-stage deterioration model is adopted to describe the process of gauge spread. Corresponding repairs are carried out for each observed deterioration stages. In this paper the component deterioration and the corresponding maintenance and control methods are assumed as shown in Table 1.

1.2 *Railway risk model*

Risk analysis is required to evaluate the accident frequency and consequences. In railway industry, Safety Risk Model (SRM) is used to estimate system risk, SRM consists of Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Fault tree estimates accident frequency considering system failure logic (Muttram 2002). It calculates top event frequency or probability using minimal cut sets. Basic events in fault tree describe the component failures; they can model revealed repairable failure, revealed unrepairable failure and unrevealed repairable failure with periodic inspection (Andrews & Moss 2002). The above failure models for basic event are not enough to consider the effects of maintenances on risk as these models cannot describe multi-level repairsor inspections in details.

Petri nets are used in the railway risk model due to their capability to describe concurrent events in accident scenarios (Zheng, Mueller, Slovak, & Schnieder 2009). Furthermore Petri nets can describe the combined process of stochastic deterioration and maintenance in details (Andrews 2012) (Prescott & Andrews 2013). Petri nets estimate accident frequency or probability by thousands of Monte Carlo simulations. Colored Petri nets are a kind of high level Petri nets. They introduce colored set into the Petri nets, so it is possible to build an object-oriented Petri net model for complex systems.

A railway block section is chosen in this paper which is a railway plain line segment including 8 track components, an entry signal and an exit signal. The section is open for the waiting trains if there is no inspection, no maintenance and no train in the section. A derailment is assumed to occur once a train is passing along a track which exceeds dynamic gauge limitation (1480 mm). Train speed restriction might be carried out to control the corresponding stage of failure. Train speed in this section is informed by the entry signal and train will pass the whole section with the permissible speed. This paper presents a hierarchical CPN model for a railway block section to estimate the railway system derailment frequency due to gauge spread.

1.2.1 *Colored Petri Nets*

A Colored Petri net consists of places, transitions, arcs, color sets, variables, color set functions, guard, arc expression function and initialization functions. A CPN is defined as:

$$CPN_t = (P, T, A, \Sigma, V, C, G, E, I) \tag{1}$$

CPN_t is a timed CPN, P is the set of places, T is the set of transitions, A is the set of arcs, Σ is the set of colored set, V represents the set of variables. G is the set of guard functions, I is the initial marking of the net, C is the set of colored set functions and E is the set of the arc expression functions (Jensen, Kristensen, & Wells 2007).

Table 1. Repair assumption for different component states.

Component state	Inspection	Repair	Effect	Waiting time	Duration
Level 1	–	N/A	–	–	–
Level 2	VI	Refastening	Level 1	τ_{f2}	μ_{f2}
Level 3	VI	Tie bar	Level 2	τ_{f3}	μ_{f3}
Level 4	VI/TRV	Tie bar & speed restriction	Level 3 (TSR)	τ_{f4}	μ_{f4}
Level 5	TRV	Re-sleepering	Level 1	τ_{f5}	μ_{f5}
Accident	–	Renewal	Level 1	τ_{f6}	μ_A

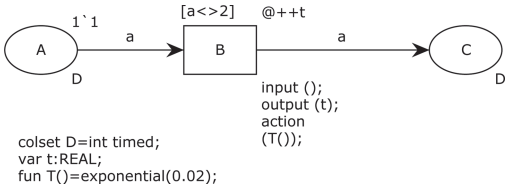


Figure 1. Colored Petri Net concept.

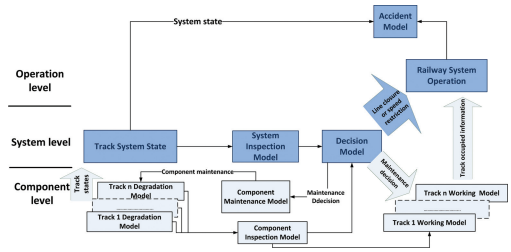


Figure 2. Modeling framework.

Figure 1 shows a simple timed CPN example, 'D' is defined to be colored set, colored set can be defined to be any data type, for example, in this figure, colored set D is defined to be integer type. Place A and Place C belong to coloredset D. Transition B transfers variable *a* from place 'A' to place 'C'. Function $T()$ defines a stochastic function and assigns the value to variable *t*. It means variable 'a' is transferred from place 'A' to place 'C' at time 0, the token in place 'C' is valid at time *t*. At place 'A', '1' 1' is the initial token.

For a complex system, it is impractical to build a CPN model as a single net. Therefore, a hierarchical CPN model introduces the concept of modules and the interfaces. A module is related to a substitution transition, which is represented by a rectangularbox with double line borders. There are input and output places in the substitution transition to connect different modules. A complex system can be modeled in a modular manner thus we can work at different abstraction levels and use component models repeatedly.

2 MODELING FRAMEWORK & ASSUMPTIONS

A modeling framework for the chosen section is proposed to combine risk modeling and track deterioration modeling. The framework can be described as shown in Figure 2, including three levels: Component level, System level and Operation level.

The component level describes track component deterioration and component working status. Inspection is needed to detect the unrevealed track degradation, then maintenance activities are carried out for the defective components. At component level, component working status contains: being inspected, being maintained, occupied by train, available.

The system level consists of the system state, the system inspection and the decision model. System state depends on track component deterioration and system structure. Any component failure will lead to system failure state, thus system is considered to be a series system. A system inspection is carried out for the entire chosen section, then the decision making model decides maintenance activities according to system and component inspection results.

Operation level contains the system operation model and the accident model. Operation model describes two system statuses: available and unavailable. When there is a train, an inspection or a repair, the system is unavailable for a waiting train; otherwise it is available. Accident model describes possible event sequences which might lead to derailment.

2.1 *Component modeling*

In this framework, the model of maintained component is shown in Figure 3. The component degradation process is divided into k stages, this process is shown in the grey rectangle area in Figure 3. The time distribution of each level is assumed to be an exponential distribution with rate λ_i, when the component deteriorates to level k, it may cause an accident.

Each level can be identified by inspections *INSPi*, then the component state is observed and a corresponding repair *Mi* controls the observed deterioration. Unfortunately, the repair arrives in a delay time and the component keeps degrading when this defective component is waiting for the repairs, hence the arriving repair may not fix the defects. Figure 4 shows an example of these situations. Level 5 is assumed to be the failure state in this example. When level 3 arrives and it is identified by the *i*-th inspection, there is a waiting time for the repairs R_i. Before the *i*-th repair R_i arrives, the level 3 defect may degrade to be level 5, in this case, a derailment accident may happen. If R_i arrives between T_{l4} and T_{l5}, level 4 may be observed. Therefore, the dash arrows from 'observed deterioration level 3' in Figure 3 show the possible situations that the repair waiting time exceeds deterioration time to the other stages.

The component working model is used to model a component having the different working states. In the chosen section, track component working states

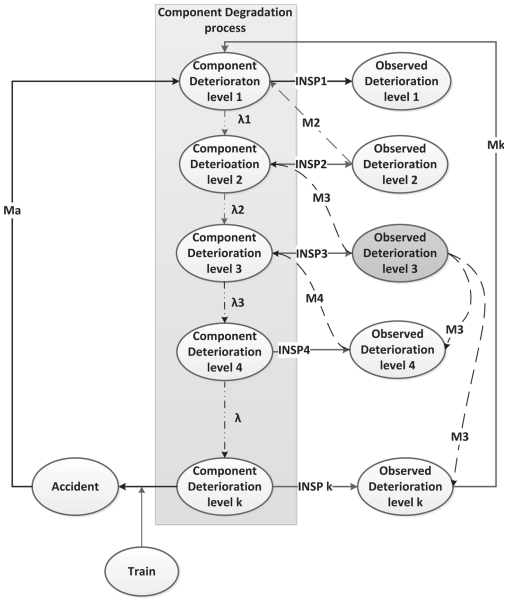


Figure 3. The maintained component model.

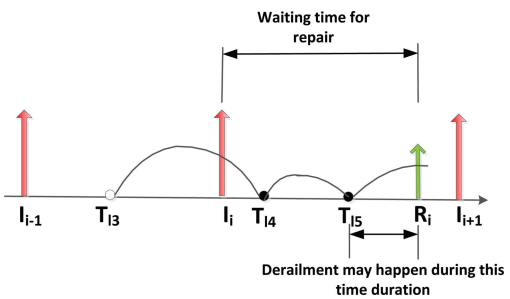


Figure 4. Repair waiting time exceeds deterioration time.

include 'available', 'being inspected', 'being maintained' and 'occupied by train'. Figure 5 shows the relationship of these working states. For example the track is being inspected if an inspection arrives when the track is available and track becomes available once inspection leaves.

2.2 *System operation and accident model*

System operation model describes railway section behaviors. There are two operation modes for the chosen section. Normally, trains may pass the section with normal speed; if there is a defect, train may be required to pass the section with a speed restriction; if there is an identified failure, an inspection or a maintenance, the railway

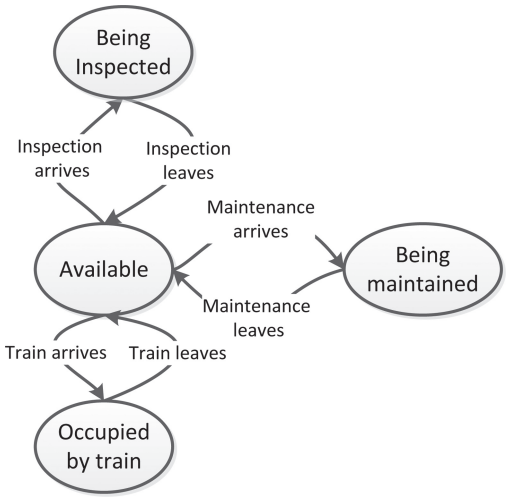


Figure 5. Track component working status model.

line is closed. An accident will occurs when a train passes a poor condition track with normal speed or speed restriction.

3 CPN MODEL FOR THE RAILWAY SECTION

A plain line block section is modeled in this paper to evaluate inspection and maintenance strategies. According to the above modeling framework, a hierarchical CPN model is built to estimate derailment frequency, system availability and maintenance cost. The CPN model contains several parts: component deterioration model, component working model, operation and accident model.

The CPN model evaluates two inspection schemes:

- Visual inspection and Train Recording Vehicle for gauge spread are taken periodically;
- Visual inspection is carried out periodically, Train Recording Vehicle has a maximum planned interval but its interval decreases if the number of identified defects increases.

3.1 *Component CPN model*

The component CPN model contains the CPN model of component working states and the CPN model of inspection and maintenance.

3.1.1 *Component deterioration CPN model*

According to the deterioration process in Figure 3, a component deterioration model is built as shown in Figure 6.

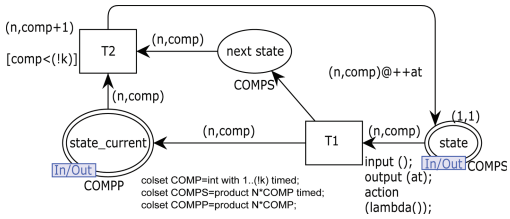


Figure 6. CPN component deterioration model for track component 1.

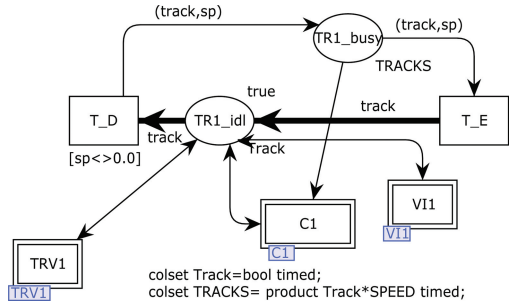


Figure 7. CPN component working model for track 1.

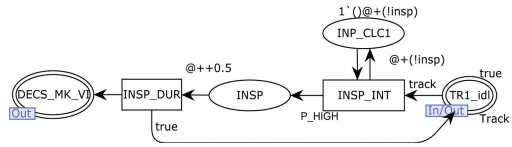


Figure 8. Visual inspection model.

Place 'state' represents the initial state, place 'state_current' represents the current track state. Variable *comp* represents the defect level, there are *k* component deterioration levels. Transition T1 samples deterioration time to next state by function *lambda*() and it assigns the deterioration time to 'next state' by variable *at* in arc inscription, place 'next state' records the next state arriving time in its token time stamp. Once the token in 'next state' is valid, transition T2 fires, the component state degrades.

3.1.2 *Component working CPN model*

Figure 7 shows the CPN model, which describes the component working process.

The working model considers existence of train, inspection and maintenance. The place *TR*1*_busy* represents a track occupied by train, the place *TR*1*_idl* represents the component being available. Transition *T_D* means that a train enters this track component. *T_E* represents train leaving. Substitution transitions *TRV*1 and *VI*1 represent the inspection arrivals. Substitution transition *C*1 combines the component deteriorations and the maintenances.

3.1.3 *Component inspection CPN model*

Visual inspection is considered to be the component level inspection in this paper, it is assumed to be taken periodically.

The substitution transition 'VI1' in Figure 7 is extended as shown in Figure 8. When a track is available (the token in Place 'TR1_idl' is valid) and the cycled inspection time arrives (token in place 'INP_CLC1' is valid), a visual inspection takes place (transition *INP_INT* fires). In Figure 7 there may be the conflicts among substitution transition TRV1, C1 and VI1 if they are enabled at the same time. In this paper the inspections are assumed tohave a higher priority, therefore the priority of transition 'INSP_INT' is set to be 'P_HIGH' (high priority). The inspection lasts 0.5 unit time and the transition INSP_DUR assigns the inspection duration and represents a finished inspection; then a decision is made (the place 'DECS_MK_VI') and the track becomes available (TR1_idl).

3.1.4 *Component maintenance CPN model*

Maintenances are carried out according to the visual inspection result. Table 1 lists the repair activities for the identified component degradation levels, these degradation levels are defined by global reference values *!j* = 2, *!m* = 3, *!l* = 4 and *!k* = 5. There are four repair activities for identified track gauge spread: refastening, tie bar, re-sleepering and renewal. These repair processes for level '!k','!l' and '!m' are described in substitution transition *C*1.

Figure 9 illustrates the repair CPN model for the observed component deterioration level *!j*. Substitution transition deterioration describes the deterioration process, which is shown in Figure 6. Token in place DECS_MK_VI is valid when visual inspection is completed at time *t*, at this moment, the value of the token in place 'state_current' is level *j*, according to this state, transition 'Tmm_D' fires. After 'rdelay2' time, the token in place 'WTmm' is valid, whichmeans the planned repair arrives. Transition Tmm fires which means repair for level *!j* is carried out, according to the maintained model in Figure 3, if the current state is the same as the observed state, repair maintains track state to be '*comp*—1 in place 'state', the repair takes '!mu2' unit time; if the current state degrades to be the failure state *!k*, a token is put in place 'WTMM' which means waiting for maintenance for level *!k*. If the current state is *!l* or *!m*, a token is put in place 'WTMm' and the track component will wait for another level repair (repair for level *!l* and *!m*).

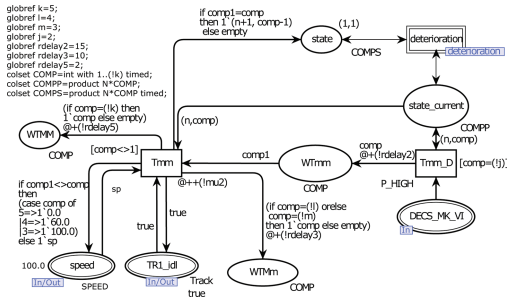


Figure 9. Repair model of observed level '!j' for track component 1.

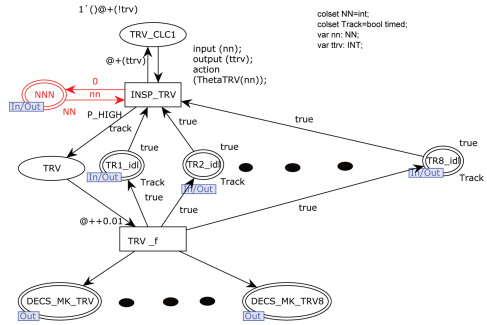


Figure 10. Train recording car inspection model.

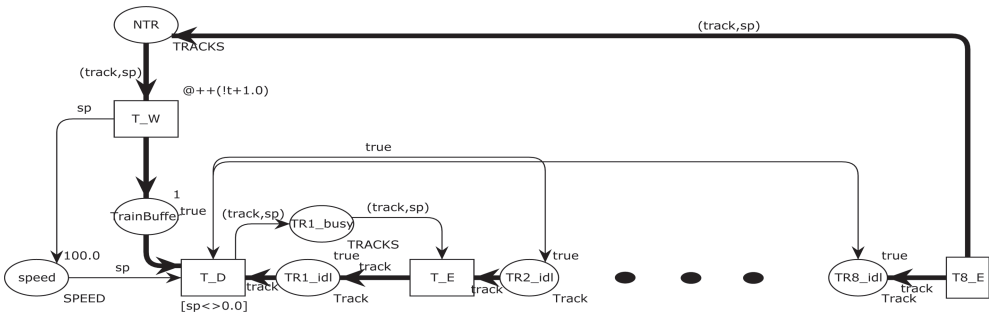


Figure 11. System operation model.

3.2 *System inspection CPN model*

Train Recording Vehicle can be carried out once there is no train, no maintenance and visual inspections in the section.

A CPN model of the Train recording car is shown in Figure 10. If all of the places 'TR*i*_idl' have a token when it is time for TRV (a token at place 'TRV_CLC1' is enabled), transition 'INSP_TRV' fires and a token arrives at place 'TRV' and the decisions for track components (places 'DECS_MK_TRVi') are made.

The TRV CPN can model two inspection schemes using function *ThetaTRV*(*nn*). Function *ThetaTRV*(*nn*) controls the interval of train recording car by variables *ttrv*. If TRV is periodic, function *ThetaTRV*(*nn*) = *!trv*, where *!trv* is defined as the planned maximum TRV interval. If TRV depends on the number of observed defects, place NNN collects the number of defects in the section, then function *ThetaTRV* defines 'ttrv' according to 'nn'.

3.3 *System operation and accident CPN model*

The track system operation model is shown in Figure 11. Place TrainBuffer represents a waiting train at the entry of the section. Place 'Speed' controls train operation modes due to the track

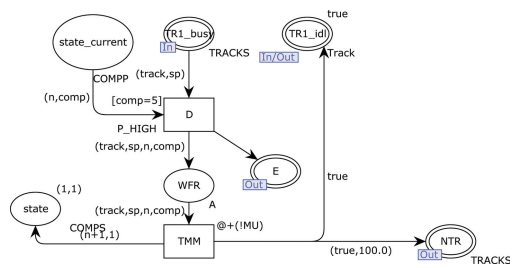


Figure 12. Accident model at track component 1.

gauge spread. Train can pass the section normally with speed 100, or in a degraded mode with speed 60; if the extreme failure exists, traffic must be stopped (speed is 0). Transition 'T_D' describes a train entering the section; it fires if all of the places 'TR*i*_idl' have tokens and variable *sp* of place 'Speed' is not zero. 'T_D' fires and it takes token from place 'TR*i*_idl' to 'TR*i*_busy', which means that track component is occupied by train, thus 'T_D' is not enabled and another train is not allowed to enter.

Figure 12 shows the derailment model: a derailment happens (transition D fires) when train is

passing along the component (the place 'TRi_busy' has a token), where a track failure exists (place 'state current' has a value 5). After the accident, a renewal ('TMM' fires) is carried out and the track is restored (the variable *track* is 1 in place 'state') in '!MU' time (μ_A in Table 1).

4 SIMULATION RESULTS

The CPN model can be used to evaluate different inspection policies of the two inspection schemes. Four inspection policies are assumed in this paper:

- Policy 1: Two level periodical inspections, Visual Inspection interval $\theta_{vi} = 40$ units;
- Policy 2: Visual Inspection interval is $\theta_{vi} = 40$ units while Train Recording cars interval depends on the number of defects.
- Policy 3: Two level periodical inspections, Visual Inspection interval $\theta_{vi} = 50$ units;
- Policy 4: Visual inspection interval is $\theta_{vi} = 50$ units while Train Recording cars interval depends on the number of defects.

For these inspection policies, the planned Train Recording car interval ranges from 5 to 2000 units. The parameters for maintenance in Table 1 are assumed to be: $\tau_{f2} = 15$, $\mu_{f2} = 1$, $\tau_{f3} = 10$, $\mu_{f3} = 4$, $\tau_{f4} = 5$, $\mu_{f4} = 4$, $\tau_{f5} = 2$, $\mu_{f5} = 10$, $\tau_{f6} = 0$, $\mu_A = 70$.

The system performance index 'Scheduled line availability A_{sch}', 'Line availability A_{uns}', 'Line Scheduled cost C_{sch}', 'Total cost C_{uns}' and 'The number of availability $N_{derilment}$' are used to compare these four inspection policies.

$N_{derilment}$ is counted by monitoring transition D in Accident model. The scheduled availability A_{sch} and the line availability A_{uns} are obtained by monitoring transition T_D and T_i_E according to Equation 2 and Equation 3. $T_{avilable}$ is the line available time, T_{total} is the total time, DT_{uns} is the unscheduled down time.

$$A_{sch} = \frac{T_{available}}{T_{total} - DT_{uns}} \tag{2}$$

$$A_{uns} = \frac{T_{available}}{T_{total}} \tag{3}$$

C_{sch} and C_{uns} are calculated by Equation 4 and 5. C_M is maintenance cost, C_{trv} is the cost of each Train Recording car, C_{vi} is the cost of each visual inspection and $C_{Accident}$ is the cost of each accident. The number of Train Recording cars N_{trv}, the number of Visual Inspections N_{vi} are counted by monitoring the transition *INSP_TRV* and transition *INSP_INT*. The number of maintenances N_M are obtained by monitoring transition *Tmms*(refastening), *TMms* (tie bar) and *TMMs* (re-sleepering) in the CPN model.

$$C_{sch} = C_M N_M + C_{trv} N_{trv} + C_{vi} N_{vi} \tag{4}$$

$$C_{uns} = C_{sch} + C_{Accident} N_{derailment} \tag{5}$$

20000 simulations are carried out to check how many simulations are required to observe a convergence in the results. A plot of the average line availability against the number of simulations is shown in Figure 13. The middle curve is the average availability result, the curve below it and above it are the 99% confidence results. It shows the simulation converges at around 2000 simulations. If the number of simulations is less than 2000, the results have larger deviations. Therefore, at least 2000 simulations are needed to get the solution of CPN model.

Figure 14 shows the normalized number of derailments against TRV interval per year. The derailment frequency increases when either Visual Inspection interval or Train recording Vehicle interval increases.

If the Train Recording car interval increases, the scheduled availability increases as shown in Figure 15. However, the line availability decreases if TRV interval increases as shown in Figure 16.

The scheduled cost and unscheduled cost are shown in Figures 17 and 18. All of the inspection policies have the minimum total cost as shown in Figure 18. For policy 1 and policy 3, the minimum maintenance cost can be obtained for a Train Recording vehicle interval of 65 units. For policy 2 and policy 4, the minimum total cost can be obtained if the train recording car interval is 125 units.

In the plot of derailment, if TRV interval ranges from 0 to 300 units, policy 2 and 4 exhibit fewer

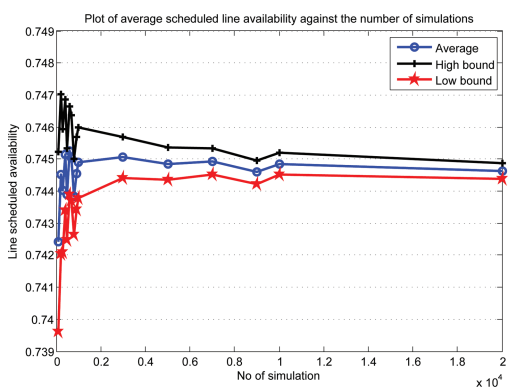


Figure 13. The number of simulation against the availability.

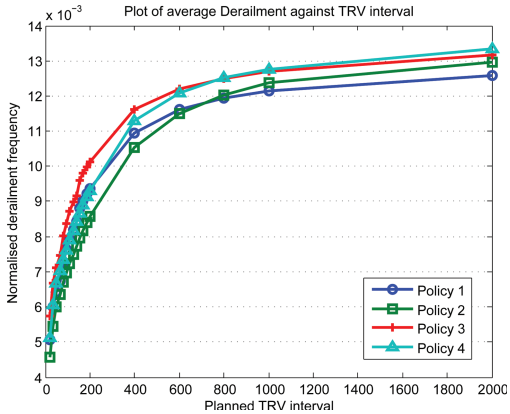


Figure 14. The number of derailment against TRV interval in one year.

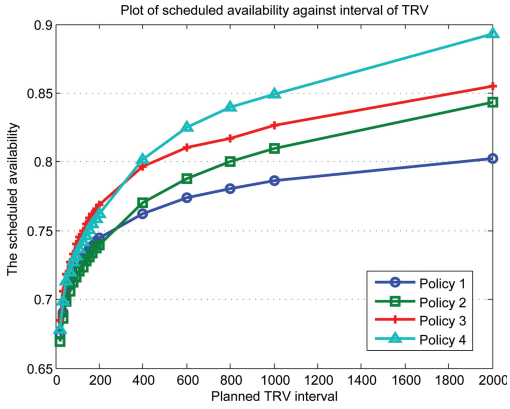


Figure 15. Scheduled availabilities against TRV intervals.

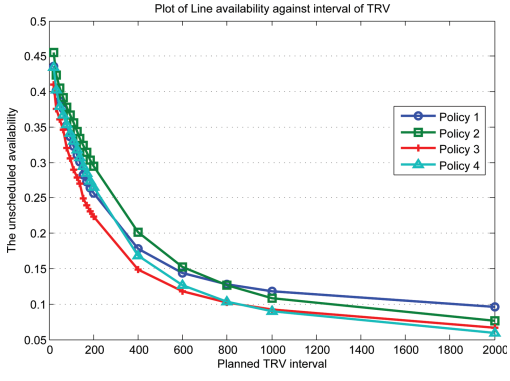


Figure 16. Unscheduled availabilities against TRV intervals.

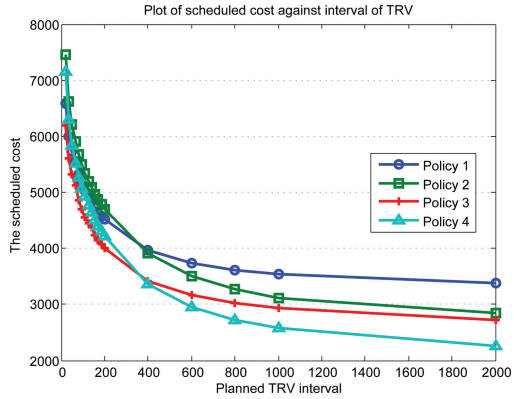


Figure 17. Scheduled cost against TRV intervals.

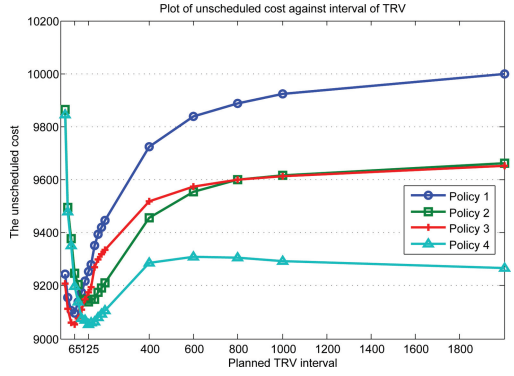


Figure 18. Total cost against TRV intervals.

derailments and a shorter visual inspection interval can lead to a lower number of derailments. If TRV interval is within range from 300 units to 700 units, policy 1 and policy 2 are better than policy 3 and policy 4, policy 2 has a lower number of derailments than policy 1; if TRV interval exceeds 700 units, policy 1 is better than policy 2.

5 CONCLUSIONS

A modeling framework is presented for a track block section. System degradation and system operation are taken into account for the system performance evaluation. A hierarchical CPN model is built according to this framework, which consists of component working model, deterioration model, inspection model and maintenance model. Monte Carlo simulations are carried out to obtain the solutions.

CPN is a flexible modeling tool due to the concept of color set, for example, the track deg-

radation states are defined by color set COMP as shown in Figure 6, the preventive maintenance thresholds (the parameter 'k', 'l' and 'm' in Fig. 9) are defined by global references. In addition, function *ThetaTRV* can be defined as an input of the CPN model to combine the different inspection schemes.

The model can be used to evaluate the strategies for risk-based maintenance and cost-effective maintenance. It can also evaluate the performance measures according to the practical inspection requirements, that requires visual inspection to be 168 hours and the maximum train recording car interval to be 3 months.

REFERENCES

Andrews, J. (2012). A modelling approach to railway track asset management. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 227*(1), 56–73.

Andrews, J. & T.R. Moss (2002). Fault Tree Analysis. In *reliability and risk assessment* (2nd Editio ed.)., pp. 201–300. London: Wiley-Blackwell.

Ellis, I. (2006). *Ellis' British Railway Engineering Encyclopaedia* (2nd Editio ed.). London: Lulu Enterprises, UK Ltd.

GC/RT 5010 (1998). *Track Standards Manual—Section 7: Track System*. (issue 2 ed.). London: Rail Safety and Standards Board.

GC/RT 5021 (2011). *Track System Requirements*. (issue 5 ed.). London: Railway Safety and Standard Board.

Jensen, K., L.M. Kristensen, & L. Wells (2007, March). Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer 9*(3–4), 213–254.

Lupton, J. (2003). Derailment mitigation-categorisation of past derailments. Technical report, Railway Safety and Standard Board, London.

Meier-Hirmer, C., G. Riboulet, F. Sourget, & M. Roussignol (2009, September). Maintenance optimization for a system with a gamma deterioration process and intervention delay: application to track maintenance. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 223*(3), 189–198.

Muttram, R.I. (2002, January). Railway Safety's Safety Risk Model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 216*(2), 71–79.

Prescott, D. & J. Andrews (2013, April). A track ballast maintenance and inspection model for a rail network. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 227*(3), 251–266.

Quiroga, L.M. & E. Schnieder (2011, December). Monte Carlo simulation of railway track geometry deterioration and restoration. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 226*(3), 274–282.

Sadeghi, J. & H. Askarinejad (2010, December). Development of improved railway track degradation models. *Structure and Infrastructure Engineering 6*(6), 675–688.

Westgeest, F.P., R. Dekker, & R.H. Fischer (2012). Predicting rail geometry deterioration by regression models. *Risk Management*, 926–933.

Zheng, W., J.R. Mueller, R. Slovak, & E. Schnieder (2009). Estimation of traffic risk of level crossing based on stochastic petri nets models and social economic data. In *2009 International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2009*, Volume 3, School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China, pp. 518–521.

Zwanenburg, W.-J. (2008, August). A model for the life expectancy of railway switches and crossings for maintenance and renewal planning in asset management systems. *Computers in Railways XI 103*, 765–773.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Analysis of the process of unloading containers at the inland container terminal

M. Zając & J. Świeboda
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: Intermodal transport is a complicated way of transportation, where there is usually over a dozen means of transportation and many modes of transportation. As can be easily seen cargo is subjected redoubled number of transshipments in comparison to the number of vehicles, which is transported. Very popular transport relation Asia—Europe shipping takes around 25 days, while terminal operations take up 17% of the time transferring cargo container. In all decisive importance to the planning of operations to plan the operation of machinery—planning is affected by the resulting time. The purpose of this article is to demonstrate the direct impact duration elements of the service on the total time of the process.

1 INTRODUCTION

After the difficult years of 2008–2010 container transport becomes stronger. In Poland it is visible seeing more and more new container handling transshipment points. Currently, the total container turnover in the market of intermodal transport is estimated by the owners of intermodal companies over 2.5 million TEUs per year (for comparison, in 2007, there are approximately 1.7 million TEU).

Modern combined transport terminal is more than a simple transshipment point. It develops in the creation of centers freight with a wide range of services (Braekers, 2011 and Jakubowski, 2009). Sea terminals are to be run in such a way as to reduce to a minimum residence time of the loading units within the terminal. Using sophisticated technology, handling, such as full automation of the process can substantially reduce the time of cargo handling, eliminate errors, increase the level of safety and reliability (*Ambrosino & Caballini & Siri, 2013 and* Boysen & Fliedner & Jaehn, 2011 and Gambardella & Rizzoli & Zaffalon, 1998). Problems of vulnerability was mentioned also in (Vališ & Koucký & Žák, 2012 and Vališ & Pietrucha-Urbanik, 2014). These technologies are extremely expensive and are not widely used. In smaller ports, high throughput is achieved by streamlining operations. The inland terminals link transport and storage functions. Problem in intermodal transshipment hubs is linked with choosing appropriate method of container warehousing (Zajac, 2011a and 2011b). Very often it is necessary to move container several times from one point to another during process of storage. The results are more expensive container service and probability that containers can't be easy available then are needed.

The increase in intermodal transport is a natural phenomenon in the face of the *White Paper on Transport* recommendations. Nevertheless, intermodal transport as a logistics process requires scientific work and research, the effect of which is to strengthen the competitiveness of intermodal transport to the traditional road to the carriage of highly processed goods.

Intermodal technology functioning is mainly based on experience in Poland. Over the years, intermodal transport was underrated way of transporting goods. Its principal advantage lies in combining functionality with the ability to cargo transport and storing in intermodal transshipment point. Intermodal transport technologies are shown in (Nowakowski & Kwaśniowski & Zając, 2008). Design rules container terminals are presented in the (Steenken & Voss & Stahlbock, 2004). Both publications are land-based container terminal.

Both the technology and design rules terminals do not show know how to manage the movement of cargo units inside the terminal. However, the functioning of the inland container terminals is far different from the typical container ports on which there is a lot of information in foreign literature (Vatanabe, 2005).

Sea terminals are to be run in such a way as to reduce to a minimum residence time of the loading units within the terminal [8]. This is due to the need for high bandwidth as a result of the conditions established infrastructure and container turnover. Using sophisticated technology, handling, such as full automation of the process can substantially reduce the time cargo handling, eliminate errors, increase the level of safety of the process. These technologies are extremely expensive and are not

widely used. In smaller ports, high throughput is achieved by streamlining operations. One of the solution is increasing tariff for storage of cargo at the port (Vis & Koster, 2003).

Intermodal technology is mainly based on experience in Poland. Over the years, intermodal transport was underrated way of transporting goods. Its principal advantage lies in combining functionality with the ability to cargo transport and storage in intermodal transshipment point. Intermodal transport technologies are shown for example in the development of (Nowakowski & Kwaśniowski & Zając, 2008).

Both the technology and design rules terminals do not show know how to manage the movement of cargo units inside the terminal. However, the functioning of the inland container terminals is far different from the typical container ports on which there is a lot of information in literature (Braekers, 2011). There are some element of terminal operation management and reliability (Nowakowski & Werbinska-Wojciechowska, 2012). There are also some technical aspects described in (Vališ & Vintr & Malach, 2012 and Vališ & Žak & Pokora, 2014).

Sea terminals are to be run in such a way as to reduce to a minimum residence time of the loading units within the terminal. This is due to the need for high bandwidth as a result of the conditions established infrastructure and container turnover. Using sophisticated technology, handling, such as full automation of the process can substantially reduce the time cargo handling, eliminate errors, increase the level of safety of the process. These technologies are extremely expensive and are not widely used. In smaller ports, high throughput is achieved by streamlining operations. One of the solution is increasing tariff for storage of cargo at the port.

The inland terminals, as mentioned previously, links Transport and storage functions. In this case, the tariff for the storage of empty containers or loaded is decreasing. Both types of containers are stored within a storage space. Problem in intermodal transhipment hubs to adopt an appropriate method of storage of intermodal units, the implementation process container depots, so that there was no need of their translocation to another storage location. In reality Polish intermodal hubs, stacking containers and large volume of financial and intuitive decision-making, such situations often occur. This is the reason for the formation of additional costs and sometimes even necessary, adjusting the container several times.

In the international literature, little space is devoted to the theme of inland terminals. Generally it is a showcase of new technologies intermodal attempt to analyze their applicability, detailed technical solutions. There is no literature on the process of storage. There have been no analysis of the arguments has to be taken into account when storing. Do not analyzed the information contained in the transport documents for their use in the management of places components in intermodal transshipment node. We can say that this area of knowledge is not recognized, and the practice sets the rules in force here. The article presents the characteristics of unloading operations of containers in relation rail wagon—yard. Presented times perform the duties of the components and their impact on the whole process.

2 PROCEDURES CHARACTERISTICS

The inland terminals storage containers usually up to three layers to four layers vain. The storage yard in a terminal is usually divided into rectangular regions called storage blocks or blocks. Each row typically Consists of over twenty 20 -ft container stacks stored lengthwise end to end. For storing a 40 -ft container stack, two 20 -ft stack spaces are used. Load distribution and hence the allocation of storage is done by machine operators. This is done on the basis of their experience and relying on the information derived from public goods. Basic information to be taken when allocating loads are:

- whether the container is empty, loaded, refrigerated, tank, ADR/RID;
- the size of the container,
- the expected storage time charge on the terminal,
- the recipient,
- the gross mass,
- operator.

The essential part of machine operator's work is to memorize and consistently putting in a storage container so as not to turn the download does not require adjustment of the upper layers of containers. This task is difficult and involves unreliability. This problem increases the lack of information from one of the main customers of schedule downloads terminal at the time of arrival of containers by rail to unload the cargo units. As a result, the containers are unloaded in free space components (cached), and after being informed of the date of delivery segregated and placed in the correct order.

Schedules cargo operations are difficult to define because they vary depending on the sender or recipient, traffic conditions, etc., although this time the service should be as short as possible. Therefore, previous planning manual handling is often very difficult, if not impossible, due to random factors beyond the control of the operator terminal. To transfer the containers in the number

of hours between scheduled transport services large batches, the temporary storage of containers is essential. Meets the buffer function terminals. Unfortunately, the container terminal is limited capacity and technology used transport units, thus piling up more layers to increase capacity. This increases the number of containers in the landfill, but very often difficult to locate the container, and the effective execution of transhipment operations on it. As the number of handled cargo units, there are new problems. With little turnover of the cargo container to find the company was not a problem for those involved in the physical handling of cargo. Today, however, the terminal supports more load and hence there is a possibility of a problem to locate the container that is to be assigned. During the deployment analyze intermodal cargo transshipment node can watch two indicators:

- rotation ratio,
- the intensity of use of the component.

Rotation ratio is the number of operations performed per unit time with respect to one component of the terminal. This means that the residence time of the free—space component may be relatively short, but the number of containers in a given location may be large. This means that the area is heavily used, but due to the large rotation load. Achieving high turnover ratio is desirable for marine terminals, where it counts the technical efficiency of the transport process and land-based terminals, where the number of occupied seats begins to cause complications in the implementation of the basic functions of transport. The intensity of the storage is a busy time of the landfill by the same unit load per unit of time. The smaller the value of this ratio the greater the rotation of the loading unit is characterized by a terminal.

3 CHARACTERISTICS OF THE STUDY AREA

The observations were done in 2014 on one of container terminals in Poland. Observations treat handling relation wagon-yard at the container terminal. Containers were taken from the first or second rail track, then put at the free space on the storage yard in one of the 4 levels. The aim of the research was to characterize the relationships binding site to download and postpone load. Observations were including duration of operation and the distance moved both with load and without.

Figure 1 presents transshipment cycle.

It was assumed that the unloading of the container from the train starts from the application to the operating system needs to perform an operation. Then crane begins the process of setting the drive.

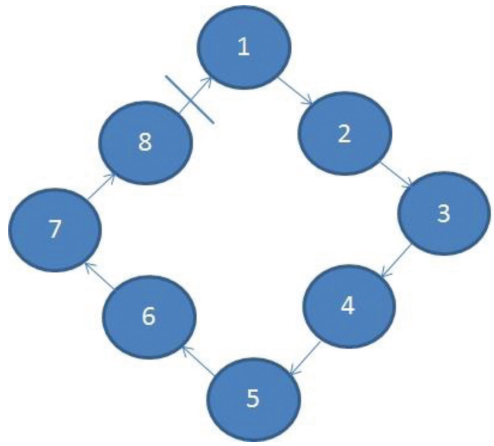


Figure 1. Container transhshipment cycle. 1—setting up the dribe, 2—drive, 3—setting to catch, 4—lifting the container, 5—settitng up the drive, 6—drive, 7—setting for unloading, 8—unloading.

After arriving at the wagon with maneuvering to capture the correct container. Then retrieves the container, and when set to begin driving transport to postpone. The final step is to set aside container at the storage location.

4 THE RESULTS

During the more than 800 observations the distance of transportation was measured and time recorded. Table 1 shows summary information for the group of observations.

As can be seen from the data presented in Table 1 most of the time during the execution of the discharge cycle takes a ride with the cargo, immediately after driving without a load. The total cycle takes an average 133 s reloading while driving is more than 62 s. It can be seen here that one of the fundamental option of shortening the cycle is shortened drive to and with the container. Reloading cycle-times differ depending on the relationship of handling. The Table 2 and Table 3 present results for handling relationships and track—first floor, and track—the fourth floor.

In relationships I track—I floor the average operating time was 123 s. Like the collective results are also driving time was the largest (total 55 s). Due to the experience of the operators turned out to be a very short time—away containers. Due to the visibility of the container, and no need for very precise withdrawal of the unit load on the already standing—another—this time was the shortest of all possible relationships.

Table 1. The overall results of the observation.

Operation	Mean value	Std deviation	Variance
Setting up the drive [s]	17.98	8.48	71.94
Drive [s]	28.45	20.49	419.87
Distance (without) [m]	54.04	38.37	1472.23
Setting to download and download [s]	15.57	6.00	36.02
Setting up the drive [s]	18.57	10.34	106.90
Drive [s]	33.64	17.24	297.12
Distance (with) [m]	65.45	39.82	1585.83
The setting for unloading and unloading [s]	19.00	11.00	121.08

Table 2. Results of the unloading in relation I track—I floor.

Operation	Mean value	Std deviation	Variance
Setting up the drive [s]	16.76	8.86	78.44
Drive [s]	25.29	20.18	407.22
Distance (without load) [m]	45.47	31.99	1023.14
Setting to download and download [s]	14.71	5.16	26.60
Setting up the drive [s]	20.88	17.20	295.74
Drive [s]	30.12	18.98	360.11
Distance (with load) [m]	62.00	42.39	1796.50
The setting for unloading and unloading [s]	15.29	7.74	59.97

Table 3. Results of the unloading in relation I track—IV floor.

Operation	Mean value
Setting up the drive [s]	22.00
Drive [s]	31.50
Distance (without load) [m]	50.00
Setting to download and download [s]	11.00
Setting up the drive [s]	14.00
Drive [s]	26.50
Distance (with load) [m]	20.00
The setting for unloading and unloading [s]	45.50

Unloading on the fourth floor proved to be far more time-consuming. The average duration of the operation was over 150 s., in this case, almost one third the time it took defer the load on a high level. Driving time with load were similar to those obtained with the unloading of the first floor: a little over 55 s. Table 4 contains the time and speed of the crane with load. The observations can be noted that the experience led operators overcome the greatest distance putting the container on the third layer. Regardless of the level of deposition of the load, the speed obtained without charge are—as expected—higher than the load.

Table 4. Time and distance with and without load.

Without load	Time		Distance	
Floor	I track	II track	I track	II track
1	30.12	21.25	62.00	32.50
2	34.45	26.67	71.68	43.33
3	40.64	26.83	71.18	46.50
4	26.50	26.00	20.00	30.60

The studies lead to the following general conclusions:

- If taking account time of operations it does not matter whether the container is deposited on level 1 or level 2.
- Postpone the level 3 lasts longer than half the level of 1–2.

  Putting container on level 4 in comparison to the level 1 is three times longer.
- The difference between putting on levels 1–2 and level 3 allows for passing around 5–10 m.
- The difference between putting on levels 1–2 and level 4 allows the passing of about 50–60 m.

5 SUMMARY

As practice shows decision problem applies to most containers. In addition, during the work simulation should pay attention not only to the time of transhipment single container, but also groups: there may be a situation where it is worth to lose a few seconds for one to gain even a few minutes in subsequent operations.

Implementation of the described research is related to the development of effective methods of reducing the operative time for the container terminal cranes. The result, which seeks to provide the following effects:

- reducing the number of meter hours by shortening cycles of loading.
- reducing the number of operations by 10%.

It is worth noting that the assumption that the cycle will be shorter loading only 1 minute obtain savings in the form of one review per year (terminal, where the project is implemented annually performs about 150 thousand cycles). When reducing the number of operations by 5% we obtain a reduction of another review annually. By reducing the cycle of 1 minute and reduction cycles by 10% saving on fuel inspections and within five years will amount to nearly EUR 550 000.

ACKNOWLEDGEMENTS

The results presented in this paper have been obtained within the project "The model of operations in intermodal terminal" (contract no. POIG.01.03.01-02-068/12 with the Polish Ministry of Science and Higher Education) in the framework of the Innovative Economy Operational Programme 2007–2013.

REFERENCES

Ambrosino, D., Caballini, C., Siri, S., 2013. A mathematical model to evaluate different train loading and stacking policies in a container terminal. Maritime Economics & Logistics (2013) 15, 292–308.

Boysen, N., Fliedner, M., Jaehn, F. 2011. A Survey on Container Processing in Railway Yards. Transportation Science, Volume: 47 Issue: 3 Pages: 312–329.

Braekers, K. 2011. Optimization of empty container movements in intermodal transport. 4or-A Quarterly Journal Of Operations Research (2011) Volume: 11.

Gambardella, L.M., Rizzoli A.E., Zaffalon M. 1998. Simulation and planning of an intermodal container terminal. Simulation 71. 1998.

Jakubowski, L. 2009. Handling operation technology (in polish). Warsaw University of Technology, Warszawa.

Nowakowski, T., Kwasniowski, S., Zajac M. 2008. Intermodal transport in logistics chains (in polish). Of Wyd. PWr, Wroclaw, 2008.

Nowakowski, T., Werbinska-Wojciechowska, S. 2012. Means of transport maintenance processes performance. Decision support system. Carpathian Logistics Congress, CLC' 2012: congress proceedings, Jesenik, Czech Republic, November 7th–9th 2012. Ostrava: Tanger, cop. 2012.

Olivo, A., Di Francesco, M., Zuddas P. 2013. An optimization model for the inland repositioning of empty containers. Maritime Economics & Logistics (2013) Volume: 15.

Steenken, D., Voss, S., Stahlbock R. 2004. Container terminal operation and operations research—a classification and literature review, OR Spectrum 26/2004.

Vatanabe, I. 2005. Contaier terminal Planning. Theoretical approach. WCN Pubishing.

Vis, I.F.A., de Koster, R. 2003. Transshipment of containers at a container terminal. An overview, European Journal of Operational Research 147/2003.

Vališ, D., Koucký, M., Žák, L. 2012. On approaches for non-direct determination of system deterioration. Maintenance and Reliability, vol. 14, no. 1, p. 33–41.

Vališ, D., Vintr, Z., Malach, J. 2012. Selected aspects of physical structures vulnerability—state-of-the-art. Maintenance and Reliability, vol. 14, no. 3, p. 189–194.

Vališ, D., Pietrucha-Urbanik, K. 2014. Utilization of diffusion processes and fuzzy logic for vulnerability assessment. Mainteance and Reliability, vol. 16, no. 1, p. 48–55.

Vališ, D., Žak, L., Pokora, O. 2014. Engine residual technical life estimation based on tribo data. Maintenance and Reliability 16(2): 203–210.

Zajac, P. 2011a. Can the raising of energy consumption of information interchange be a factor that reduces the total energy consumption of logistic warehouse system? Production engineering innovations and technologies of the future, Edward Chlebus (ed.), 2011. s. 79–89, International Conference "Production Engineering 2011", Wroclaw, 30 June–1 July 2011.

Zajac P. 2011b. The choice of parameters of logistic warehouse system, with taking the energy into consideration. Selected logistics problems and solutions. Publishing House of Poznan University of Technology, 2011. s. 107–120.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability based model of the cost effective product reusing policy

A. Jodejko-Pietruczuk & M. Plewa
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: Recently it has been a remarkable growth of interest in processes that supports recapturing value from used goods, waste and objects moving in the opposite direction of the supply chain. Minimization of waste production has become an important element of the smart economy. Reusing of products has become a factor of competitiveness for modern companies. This will accelerate the change of the linear production model to circular one where demand can be partially satisfied with new items manufacture or returned products recovery. Reuse of products can bring direct advantages because company uses recycled materials instead of expensive raw materials. The main goal of this paper is to create a reliability based model of the cost effective product reusing policy.

1 INTRODUCTION

Recently it has been a remarkable growth of interest in processes that supports recapturing value from used goods, waste and objects moving in the opposite direction of the supply chain. Minimization of waste production has become an important element of the smart economy. Reusing of products has become a factor of competitiveness for modern companies. This will accelerate the change of the linear production model to circular one where demand can be partially satisfied with new items manufacture or returned products recovery. Reuse of products can bring direct advantages because company uses recycled materials instead of expensive raw materials. The first part of the article contains literature survey, which is a summary of work that has been done around the theme of research.

Based on the studied literature [e.g. Dekker et al. 2004, Fleischmann et al. 1997, Rogers & Tibben-Lembke 1999, Thierry et al. 1995] it is possible to define the area of interest, which includes the following products:

– returns of raw materials, intermediates and final products from the production phase (surplus raw materials, defective products rejected by quality control, by-products and wastes generated in the production process);
– product returns and packaging from the phase of distribution (products damaged during transport, reusable packaging, excess inventory, unsold products);
– decommissioned objects (products returned because of changing the purchasing decision or a qualitative defect, parts replaced during the maintenance process, products that fail during warranty period which repair was impossible and other and waste).

Based on the classification presented in [Thierry et al. 1995] it is possible to specify the following types of recovery:

– direct reuse/resale,
– repair,
– refurbish,
– remanufacturing,
– cannibalization,
– recycling.

Description of the different recovery options was presented in (Fleischmann et al. 1997, Guide 2000, Rogers & Tibben-Lembke 1999, Thierry et al. 1995). Cannibalism has been described in (Fisher et al. 1986, Fisher, 1990, Hirsch et al. 1968, Hochberg 1973, Ormon & Cassady 2004, Simon 1972).

The problem of the design of products suitable for the recovery has been widely discussed in the literature, for example in the following articles (Hoffmann 2001, Ijomah 2007, Jiang 2000, Kang & Jung 2001). Design of recovery-oriented includes avoiding the creation of irregular shaped objects, which are more easily damaged in the distribution phase and the reduction and standardization of connectors to facilitate the process of removal.

Forecasting the number of returns is also an important part of planning the production process and recovery. In papers [Murayama & Shu 2001, Murayama et al. 2004, Murayama et al. 2005, Murayama et al. 2006] authors present a model of planning the production process, which is in predicting the number of returns based on reliability theory. In the present model, the demand for new products does not depend on the number of returned products. The authors describe the method on the example of a

product consisting of components forming serial reliability structure. The analyzed product can be taken out of service if any component fails or the user finds the product's useless. Object withdrawn from service is disassembled. Components that are suitable for reuse, are sent to the manufacturer of the product.

In the literature one can also find the other models describing the planning and implementation of production and the recovery processes (eg, [Clegg et al. 1995, Dekker et al. 2004, Guide et al. 1997, Guide 1996, Gupta & Taleb 1994]). Review of the literature relating to production planning systems that use remanufacturing as the method of recovery are shown in [Kennedy et al. 2002].

In the literature on is also possible to identify other areas of interest of scientists. In [Zikopoulos & Tagaras 2007] the authors analyze the impact of the quality of the returned products on the costs of recovery processes. In [Kimura et al. 1998] the authors convince the reader of the benefits of shortening product life cycle. They believe that products with short life cycles, such as Single Use Cameras can be easily re-used, because their components do not undergo aging process.

Literature review that have been done so far allowed to define the main shortages of existing reverse logistics models:

- most of models assume single-component product,
- they usually are based on the assumption that recovered products are as good as new ones,
- very few articles optimize the threshold age of returns, but none of them gives any guidelines what kind of recovery technology or method should be applied.

On the base of literature overview the aims of the paper were established. It proposes the model that use reliability theory to optimize manufacturing policy parameters for the case when:

- a new, multi-component object is produced from the mix of new and reused components,
- reused elements are not good as new,
- depending on the age of returns and its reliability characteristics, various actions may be undertaken:
- a direct reusing of the component,
- an element repair, which allows to improve its condition with additional cost, disposal.

2 MODEL OF REUSING POLICY

The model that is presented in the paper is based on the following assumptions:

- A company produces an object composed of two elements (A and B) being in the series reliability structure, so the object fails after any components failure.
- A failure of components occurs independently.
- If the product fails during the warranty period, it is returned to the manufacturer and he has to pay some penalty cost (e.g. the cost of a new product).
- The components may be reused in a new production if are upstate after return and were not reused before (twice reusing is allowable). Thus, every component returned, capable to further work may be:
  - reused without any activities,
  - recovered in order to improve its condition with an additional cost,
  - disposed.

To indicate if the returns should be reused, a producer should estimate the expected profit resulting from using mix of new and old elements instead of the new ones:

$$P(T,\Delta T,T_W) = C_B - C_R(T,\Delta T) - C_M - C_O(T,\Delta T,T_W) \quad (1)$$

$$C_O(T,\Delta T,T_W) = c_o\left[F_1(T,\Delta T,T_W) - F_2(T_W)\right] \quad (2)$$

where: $P(T, \Delta T, T_W)$ = the total expected profit resulting from the components' reusing, T = age of a returned element, ΔT = the period by which the item will be rejuvenated by additional recovery operations, T_W = the warranty period of the object, C_B = the cost of a new element B, C_R = the total cost of all activities including additional recovery operations: decomposition, cleaning, preparing of the returned B element to reusing in a new production, C_M = the cost of element indication before reusing, C_O = the expected cost of claims resulting from lower reliability of the product in the warranty period, c_O = the unit cost of a product failure during warranty period, $F_1(t)$ = unreliability function of the product with a reused component, $F_2(t)$ = unreliability function of the object comprised of all new elements.

The cost model of the reusing policy (Eq. 1) includes potential savings and losses of a producer. The savings are the effect of a lower cost of returned element than a new one but the price difference has to cover all the costs necessary to reuse product components: cost of elements identification, recovery activities and cost of lower reliability of a reused element in a warranty period. A manufacturer may consider four basic options:

- to make a new product from new elements,
- to produce the new object from the mix of new and old components,
- to manufacture the product composed of "old" elements but offered as "new" one at the market,

– to manufacture the product composed of "old" elements and offer it with another warranty or pricing conditions than the new product at the market.

Moreover, in some cases a producer deciding to reuse returns may take some additional operations "changing" the age of a returned component understood as the age from the reliability point of view. Usually, these operations generate some additional costs which should be included when one consider the profitability of the reusing policy.

Following the assumptions presented at the start of the chapter, when a product with reused components has the series reliability structure, its unreliability functions $F_1(t)$, $F_2(t)$ should be expressed:

– for the case when both elements installed in a product are new:

$$F_2(T,T_W) = 1 - R_B(T_W) \cdot R_A(T_W) \tag{3}$$

– for the case when single element (B) is reused without any rejuvenation operations after return:

$$F_1(T,T_W) = 1 - \frac{R_B(T+T_W)}{R_B(T)} \cdot R_A(T_W) \tag{4}$$

– for the case when A and B elements are reused without any rejuvenation operations after return:

$$F_1(T,T_W) = 1 - \frac{R_B(T+T_W)}{R_B(T)} \cdot \frac{R_A(T+T_W)}{R_A(T)} \tag{5}$$

– for the case when returned and reused element B has been rejuvenated for ΔT:

$$F_1(T,\Delta T,T_W) = 1 - \frac{R_B(T-\Delta T+T_W)}{R_B(T-\Delta T)} \cdot R_A(T_W) \tag{6}$$

– for the case when both (A and B) returned and reused elements have been rejuvenated for ΔT:

$$F_1(T,\Delta T,T_W) = 1 - \frac{R_B(T-\Delta T+T_W)}{R_B(T-\Delta T)} \cdot \frac{R_A(T-\Delta T+T_W)}{R_A(T-\Delta T)} \tag{7}$$

where: $R_A(t)$ = reliability function of the element A, $R_B(t)$ = reliability function of the element B.

The formulas 3–7 describe all the production possibilities: new components, mix of new-old, old components used in a new product. If a producer has sufficient data required to estimate the reliability functions of product elements, the calculations of potential profit from the reusing policy should not be very difficult for a given cost components and the length of a warranty period.

The issue that may raise objections is an estimation of the returns' age T, whose value must be assumed in calculations. The age of returned element T in equations 3–7 may be approximated by its expected value, according to the following formula:

$$E(T_B) = \int_0^{T_W} t \cdot f_A(t) \cdot R_B(t) \cdot dt \tag{8}$$

where: $E(T_B)$ = the expected age of returned B elements, $f_A(t)$ = probability density function of the time to failure of the A element.

The probability of the return of a reusable B component during a warranty period is equal zero for products, whose lifetime is longer than the warranty (element B is not returned) as well as for products returned because of a failure of B element (element B is downstate and cannot be reused). For this reason in some cases the better estimation of the expected age of a reusable component is given by equation:

$$E(T_B) = \frac{\int_0^{T_W} t \cdot f_A(t) \cdot R_B(t) \cdot dt}{\int_0^{T_W} f_A(t) \cdot R_B(t) \cdot dt} \tag{9}$$

3 THE AGE OF REUSABLE COMPONENTS

The cost model presented in the previous part of the paper may be applied in the profitability analysis of various options of the reusing policy, nevertheless it requires to know or assume all the parameters of the policy Most of them are decision variables of a producer or depends on market environment, e.g. warranty period length, cost components, etc. and may be determined more or less precisely. The hardest to estimate are parameters pertaining to reliability characteristics of manufactured product components. Moreover, in combination with warranty features, they have direct impact on the number and the age of reusable returns and thus—on the efficiency of the reusing policy.

Undoubtedly the fact whether reusable components appear in a manufacturing system is the key factor for potential of a reusing policy application. The aim of this chapter is to present the most significant factors of the reusing policy, which determine the ability of a production system to reuse elements, i.e.: the length of a warranty period, reliability characteristics of co-components and resulting from the both: the expected age of reusable returns.

The influence of a warranty period length on the expected age of a reusable component appearing in a production system may be observable in Figures 1–2. The longer warranty period causes growing probability of return as well as the growing age of elements which may be reused. The Figure 1 also depicts the relationship between the expected age and the mean time to failure of the element which may be reused (MTTFB), whereas the

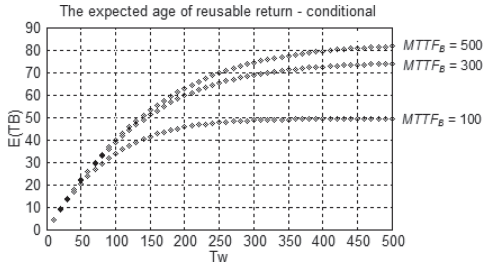


Figure 1. The expected age of a reusable element B (Eq. 9) for various warranty periods (T_W) and mean time to failure ($MTTF_B$) of the element ($MTTF_A = 100$).

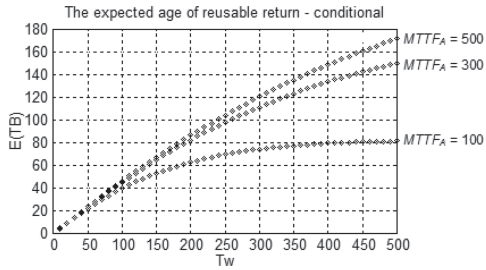


Figure 2. The expected age of a reusable element B (Eq. 9) for various warranty periods (T_W) and mean time to failure of its co-component ($MTTF_A$), ($MTTF_B = 500$).

Figure 2—between the age and the mean time to failure of its co-component (MTTFA). It may be clearly seen that MTTFA is the main determinant of the expected age of returns (E(TB)) for the same warranty conditions: an element may be reused in a new production only if it returns from a market because of a failure of an another component according the assumption of the series reliability structure. The same result was observed while study of relationship of the expected age of a reusable element and its failure rate as well as a failure rate of a co-components. A change of a failure rate of co-component A caused more rapid changes in the number and the age of reusable elements than similar changes in reusable element B.

The second study conducted in this part of the paper pertains the better estimation of the expected age of reusable returns elements which may be used in profitability model of the reusing policy (Eq. 1–7). The equation 8 describes the expected age of returned elements unconditionally, whilst equation 9 determine the expected age of elements conditionally, considering only those which are returned. For the majority of cases the conditional way (Eq. 9) gives much higher results than the another. In order to assess usefulness of the both approaches in the analysis of the reusing policy profitability, simple Monte Carlo simulation has been done and convergence of obtained results was tested for a chosen set of numerical experiments.

The figures below present the residual reliability of a reusable component B, understood as the conditional reliability of the reused element during the next warranty period. Figures 3 and 4 depict two cases characteristic for the all research results: the unconditional expected age of the reused element is more adequate to predict reliability of product containing "old" elements. The fact has been confirmed for constant failure rate of product components, independently on their MTTF or the warranty length (Fig. 3). The conditional expected age of a return (eq. 9) is better to use (Fig. 4, TW < 150) when one wants to predict the residual reliability of the mixed product comprised of elements under the two conditions:

– elements have a rising failure rate,
– reusable element has a comparable or lower MTTF than its co-components.

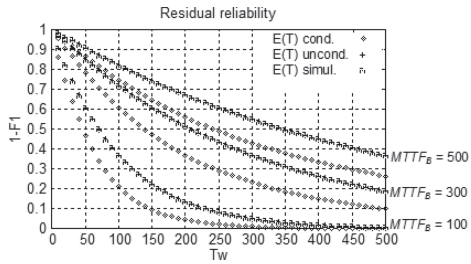


Figure 3. The expected age of a reusable element B obtained according to Eq. 9 (E(T) cond.), Eq. 8 (E(T) uncond.) and from Monte Carlo simulation (E(T) simul.) for constant failure rate of both co-components ($MTTF_A = 100$).

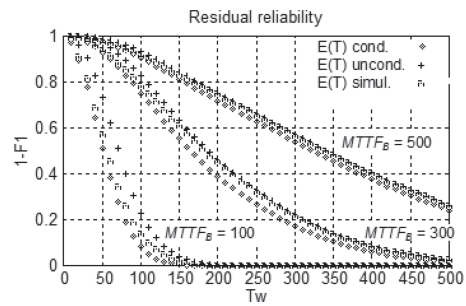


Figure 4. The expected age of a reusable element B obtained according to Eq. 9 (E(T) cond.), Eq. 8 (E(T) uncond.) and from Monte Carlo simulation (E(T) simul.) for rising failure rate of both co-components ($MTTF_A = 100$).

4 DIFFERENT RECOVERY OPTIONS

The conclusions drown in the previous chapter may be applied when a producer considers various recovery options of returned element. One of them is to mix new and old components in a product and offer it in the market as if it was the new one. In this part of the paper some results of such strategy will be shown.

The cost model of the reusing policy (Eq. 1) assumes the two cost components directly combined with recovery options of reusable returns: the cost of recovery operations and the expected cost of increased product unreliability during the next warranty period of a product. The relationship between them is inversely proportional, but not necessarily linear and continuous. The first cost component depends only on the range of recovery operations and is some function of the period by which the item will may be rejuvenated (ΔT). The second—the cost of increased reliability depends on the same factor (ΔT), the age of retuned component and a length of a warranty period. On the foundation given in the previous chapter, the age of reusable element may be estimated as a function of the length of a warranty period, thus the recovery options may be quite easily analyzed. If one considers any rejuvenating operations, should calculate the following costs' relation:

$$P_R(\Delta T, T_W) = \left[F_1(\Delta T, T_W) - F_2(T_W) \cdot c_o - C_R(\Delta T) \right] \tag{10}$$

where: P_R = the profitability of element recovery.

If the above coefficient (PR) is positive for any value of ΔT, recovery operations should be taken when it comes to cost minimization. Figures 5, 6 present the profitability analysis for exemplary cases of recovery actions which may be applied in the case of reusable return installed in a new product. The Figure 5 shows profitability for the element rejuvenation reused in a product, composed of two series elements, while Figure 6 depict the same rejuvenation possibilities but for the element, which is single in a new one-element product. Because the warranty period for the both analyzed cases is chosen to be very long (TW = 200, MTTFA = 100, MTTFB = 500), the profitability of recovery is very high when B element is installed in as an one-element product (Fig. 6), whereas there is almost no point in recovering element in the two-component, series system (Fig. 5). Neither restoring activities will be useful because of the low reliability of the co-component during a warranty period, thus it is extremely important to study the potential of the reusability policy considering its comprehensive influence on the production results.

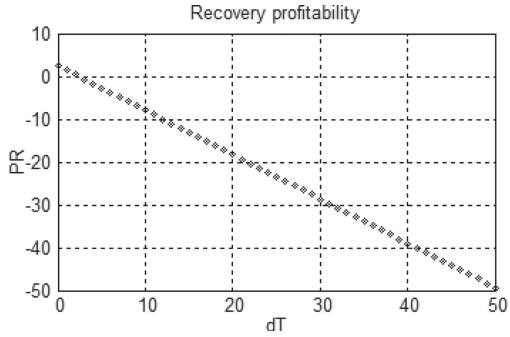


Figure 5. The profitability of rejuvenation of returned B component (of dT period) in a product composed of the mix of new and old elements.

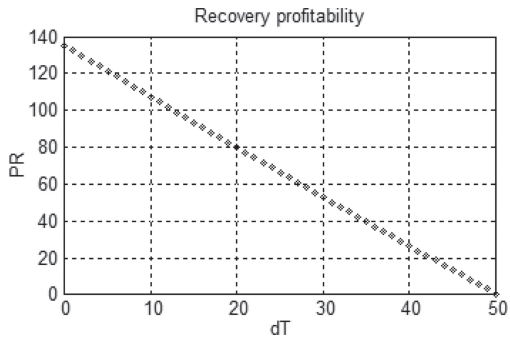


Figure 6. The profitability of rejuvenation of returned component (of *dT* period) in one—element product (assumed unit costs: $c_o = 1000$, $c_r = 1$ dT).

5 SUMMARY

The cost model has been presented and developed to the cases of various production options (Eq. 1–7).

In the next step the analysis of the expected age of reusable returns has been proposed. On this foundation two alternative estimations of the age have been formulated and used in the subsequent part of the paper. The paper ends up with the proposition on how to assess the profitability of various recovery options and the exemplary results of the assessment.

REFERENCES

Clegg A.J. & Williams D.J., 1995, *Production planning for companies with remanufacturing capability*, Proceedings of the 1995 IEEE International Symposium on Electronics and the Environment, Orlando FL, s. 186–191.

Dekker R. & Fleischmann M. & Inderfurth K. & Van Wassenhove L.N., 2004, *Reverse Logistics, Quantitative Models for Closed-Loop Supply Chains*, Springer-Verlag, Belin Heidelberg.

Fisher W.W. & Brennan J.J., 1986, The Performance of Cannibalization Policies in a Maintenance System with Spares, Repair, and Resource Constraints, Naval Research Logistics Quarterly, Vol. 33, s. 1–15.

Fisher W.W., 1990, *Markov Process Modeling of a Maintenance System with Spares, Repair, Cannibalization and Manpower Constraints*, Mathematical and Computer Modelling, Vol. 13, No. 7, s. 119–125.

Fleischmann M. & Bloemhof-Ruwaard J.M. & Dekker R. & van der Laan E. & van Nunen J.A.E.E. & van Wassenhove L.N., 1997, *Quantitative models for reverse logistics: A review*, European Journal of Operational Research, Vol. 103, s. 1–17.

Guide Jr. V.D.R. & Kraus M.E. & Srivastava R., 1997, *Scheduling policies for remanufacturing*, International Journal of Production Economics, Vol. 48, s. 187–204.

Guide Jr. V.D.R., 2000, *Production planning and control for remanufacturing: industry practice and research needs*, Journal of Operations Management, Vol. 18, s. 476–483.

Guide Jr. V.D.R., 1996, *Scheduling using drum-buffer-rope in a remanufacturing environment*, International Journal of Production Research, Vol. 34, s. 1081–1091.

Gupta S.M. & Taleb K.M., 1994, *Scheduling disassembly*, International Journal of Production Research, Vol. 32, No. 8, s. 1857–1866.

Hirsch W.M. & Meisner M. & Boll C., 1968, *Cannibalization in Multi-component System and the Theory of Reliability*, Naval Research Logistics Quarterly, Vol. 15, s. 331–359.

Hochberg M., 1973, *Generalized Multi-component System under Cannibalization*, Naval Research Logistics Quaterly, Vol. 20, s. 585–605.

Hoffmann B. & Kopacek B. & Kopacek P. & Knoth R., 2001, *Design for Re-use Disassembly*, Proceedings of the 2nd International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'01), Tokyo, Japan, s. 378–381.

Ijomah W.L. & McMahon A. & Hammond P. & Newman S.T., 2007, *Development of design remanufacturing guidelines to support sustainable manufacturing*, Robotics and Computer-Integrated Manufacturing, Vol. 23, s. 712–719.

Jiang Z.H. & Shu L.H. & Benhabib B., 2000, *Reliability Analysis of Non-Constant-Size Part Populations in Design for Remanufacture*, Transactions of the ASME Journal of Mechanical Design, Vol. 122, No. 2, s. 172–178.

Kang H.Y. & Jung J.W., 2001, *Recycling Oriented Design—A Case Study on House Appliances Using the Software ATROiD*, Proceedings of the 2nd International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'01), Tokyo, Japan, s. 309–314.

Kennedy W.J. & Patterson J.W. & Fredendall L.D., 2002, *An overview of recent literature on spare parts inventories*, International Journal of Productions Economics, Vol. 76, s. 201–215.

Kimura F. & Hata T. & Suzuki H., 1998, *Product Quality Evaluation Based on Behavior Simulation of Used Products*, Annals of the CIRP, Vol. 47, No. 1, s. 119–122.

Murayama T. & Shu L.H., 2001, *Treatment of Reliability for Reuse and Remanufacture*, Proceedings of the 2nd International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'01), Tokyo, Japan, s. 287–292.

Murayama T. & Yamamoto S. & Oba F., 2004, *Mathematical Model of Reusability*, Proceedings of the 12th IEEE International Symposium on Electronics and the Environment (ISEE), Scottsdale AZ, USA, s. 183–188.

Murayama T. & Yoda M. & Eguchi T. & Oba F., 2005, *Adaptive Production Planning by Information Sharing for Reverse supply Chain*, Proceedings of the 4th International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'05), Tokyo, Japan, s. 326–331.

Murayama T. & Yoda M., Eguchi T. & Oba F., 2006, *Production Planning and Simulation for Reverse Supply Chain*, Japan Society Mechanical Engineering International Journal, Series C, Vol. 49, No. 2, s. 281–286.

Ormon S.W. & Cassady C.R., 2004, *Cannibalization Policies for a Set of Parallel Machines,* RAMS, s. 540–545.

Rogers D.S. & Tibben-Lembke R.S., 1999, *Going backwards: Reverse Logistics Trends and Practices*, Reverse Logistics Executive Council, Pittsburgh, PA.

Simon R.M., 1972, *The Reliability of Multi-component System Subject to Cannibalization*, Naval Research Logistics Quarterly, Vol. 19, s. 1–14.

Thierry M.C. & Salomon M. & Van Nunen J. & Van Wassenhove L., 1995, *Strategic Issues in Product Recovery Management*, California Management Review, Vol. 37, No. 2, s. 114–135.

Zikopoulos C. & Tagaras G., 2007, Impact of uncertainty in the quality of returns on the profitability of a single-period refurbishing operation, European Journal of Operational Research, Vol. 182, s. 205–225.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Asset maintenance optimization: The case-study of an offshore wind farm

Y. Bot & D. Azoulay
BQR Reliability Engineering, Israel

ABSTRACT: Offshore wind farms are very expensive assets, not only to design and build, but also to operate and maintain. Their remote location, coupled with weather's constraints and harsh marine environment, and the lack of adapted access equipment, make their maintenance complicated and expensive due to high repair costs, high transportations costs and painful production losses due to high downtime.

More generally, the offshore wind technology is in a stage of development where its economic worthiness has still to be fully demonstrated, and numerous projects are largely supported by governmental subsidies (European 2011). This lack of maturity is evident, for example, through the numerous reliability problems of wind turbines components.

This article aim is to explain this industry challenges and a new technology that can help to reduce maintenance cost.

1 INTRODUCTION

1.1 *Summary*

Offshore Wind Farms are very expensive assets, not only to design and build, but also to operate and maintain. Their remote location, coupled with weather's constraints and harsh marine environment, and the lack of adapted access equipment, make their maintenance complicated and expensive due to high repair costs, high transportations costs and painful production losses due to high downtime.

More generally, the offshore wind technology is in a stage of development where its economic worthiness has still to be fully demonstrated, and numerous projects are largely supported by governmental subsidies (European 2011). This lack of maturity is evident, for example, through the numerous reliability problems of wind turbines components.

Both the inherent aspects of the offshore wind industry and the reliability problems it is facing contribute to the high Operation and Maintenance (O&M) costs and eventually hinder its competitiveness compared to other sources of energy. It is commonly assumed that up to 25% of the cost of energy produced by offshore wind turbines is due to O&M activities, which is twice as expensive as onshore installations (Sonderkar 2013).

This paper describes a methodology to optimize the maintenance strategy of offshore wind farms in order to minimize life cycle costs and maximize availability and performance. The ApmOptimizer, developed by BQR Reliability Engineering (BQR) is the software tool used for modelling, reliability analysis, cost and performance estimations and maintenance optimization.

For the purpose of the demonstration, a case study of a typical wind farm is defined. A detailed model is built that accounts for numerous operational, cost and maintenance parameters. The ApmOptimizer optimization modules are then implemented for optimizing the preventive maintenance, periodical inspections, condition-based maintenance, and spares levels. Starting from a baseline scenario, several optimization steps are investigated, following a typical RAM/LCC analysis assessment procedure: Operational Availability, Operational Downtime, Lifecycle O&M Costs and produced Energy are used as the main metrics. The optimal maintenance strategy is obtained from an exact optimization process and not from Monte Carlo simulations that can provide only an approximate assessment for a user-inputted strategy.

The study shows that by following several optimization steps, the wind farm performances can be significantly increased, to a level that makes the cost of produced energy more competitive. The influence of modelling parameters like failure distribution and degradation process is also investigated.

1.2 *Background on the apmOptimizer*

The apmOptimizer is a Modelling, Analysis and Optimization tool designed to bring Asset

maintenance to an optimal state, maximize Availability and minimize Cost of Ownership over lifetime. Optimization algorithms are implemented to find the optimal solution among all possible outcomes, according to the problem constraints and targets. The apmOptimizer is not based on Monte Carlo method whose results accuracy is function of the number of calculated simulations and dependent on user's best guess, but instead performs exact analytical computations from the input data, including failure rate distribution and reliability model (serial, parallel, standby redundancy, K out of N). The optimization process itself is not user-driven since the space of possible solutions is built from these exact computations. This guarantees that even non-evident solutions can be found out.

In this work, the ApmOptimizer is used to build the model of a typical wind farm and calculate its Reliability Availability Maintainability (RAM) parameters, as well as Lifecycle Costs (LCC). The Energetic Performance of the wind farm is also computed and the cost of energy extracted. The apmOptimizer model can integrate the most specific features of a wind farm and of its maintenance operations: accessibility limitations, weather variability, high cost of downtime, planned and unplanned maintenance etc. Although this is not done in the present work, operational data from actual wind farm (maintenance records, log book, sensors readings) can also be used for a better assessment of failure distribution.

After defining and characterizing a baseline model, several scenarios have been created that successively investigate the influence of the preventive inspections, preventive replacements, and inventory level. Each of these scenarios is provided to the ApmOptimizer for optimization and RAM/LCC and Performance Metrics are compared.

2 DESCRIPTION OF MODEL

A complete description of the input parameters being out of the scope of this paper, only a brief review of the main elements is provided here. The authors would like to highlight the fact that data used in this work was obtained from publicly available sources and unavailable data was assessed by engineering judgment.

2.1 *Wind farm elements*

The considered system is a 240 MW wind farm composed of 80 generic wind turbines each one having a rated power of 3 MW, one offshore substation and submarine cables. Turbines are grouped in 8 clusters (radials) that each contains 10 WT and cables. The farm is located at a medium distance of 30 km from shore. The Wind Farm (WF) is operating on a 24/7 basis, with an expected lifetime of 20 years. Since this paper is focused on evaluating the costs related to O&M activities only, it is assumed that the WF is completely operational from year 1 and that commissioning and decommissioning phases are not considered for cost analysis.

It is assumed that each 3 MW wind turbine is pitch-regulated, variable speed, with gearbox installed and is modelled by a breakdown structure—see Figure 1, adapted from the Reliawind project (Relia 2010). For the sake of simplicity, the breakdown tree is limited to assembly level and sub-assemblies and components are not modelled.

2.2 *Failure and reliability parameters*

The global WT failure rate was assumed to be 3.8 failures/turbine/year, based on an initial onshore value of 1.5 and conversion coefficients K1 = 1.75 and K2 = 1.447 for environmental stress and near shore location respectively (Karyotakis 2011). The components contribution to total wind turbine failure rate was then obtained from (Reliawind 2010), where exponential distribution is assumed.

In accordance with (Maples 2013) approach, we define for each element of the wind turbine several generic Failure Modes (FM) and for each failure mode a Failure Ratio (FR). For example, the Gear Box (GB) has 3 failure modes defined as shown in Table 1.

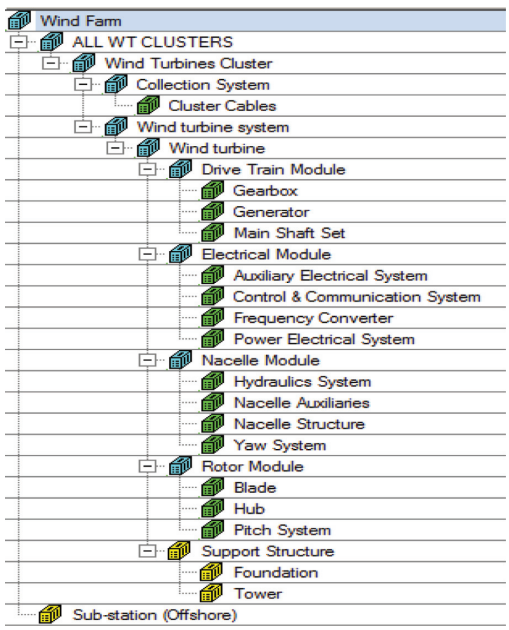


Figure 1. Wind farm breakdown (screenshot).

Table 1. Gearbox failure modes.

Name	FR	Detectability	Type	Degradation to failure, hrs	Deviation
GB-1	0.45	Evident	–		
GB-2	0.45	Hidden	Gradual	20000	+/–50%
GB-3	0.1	Evident	–		

The failure modes having some inspection tasks are defined as hidden (others are evident failure modes), meaning the failure cannot be detected until an inspection is performed. Failures detected by condition monitoring equipment are considered as evident. Additionally, the degradation process of hidden failure modes is modelled by defining a "mean time from degradation start to failure", as well as a "deviation" parameter representing the uncertainty on the degradation process.

2.3 *Maintenance tasks and resources*

The failure modes are assigned some maintenance tasks and maintenance resources required to restore the equipment in accordance with (Maples 2013).

The costs of personnel, support equipment, materials and other resources are defined in libraries and allocated to maintenance tasks. The wind farm is maintained by 20 Maintenance technicians that work 12 hr per day, 350 days a year with a cost of 70€/hour. Operations personnel (located in a control room) is composed of 3 teams of 3 operators (8-hr shift) with a cost of 50 Euros/hr.

2.4 *Maintenance locations*

Most of the maintenance tasks are performed on-site and only the heaviest repair tasks like blade or gearbox repair are performed at an on-shore maintenance facility. Spare parts are also stored in this facility, where they arrive from different suppliers or after repair. Spares procurement is "on-demand" and a time delay that accounts for production and/or administrative delays are defined for every replaceable item. For example, the blades procurement delay is 6 days. The maintenance locations and transportation between them are defined in the ApmOptimizer through the maintenance map shown in Figure 2.

Between the wind farm and the maintenance facility, several access vessels are defined:

– A cable laying vessel is used for cables,
– A Jack-up vessel for large parts
– A workboat access vessel for transporting personnel
– Diving support vessel for inspecting foundations

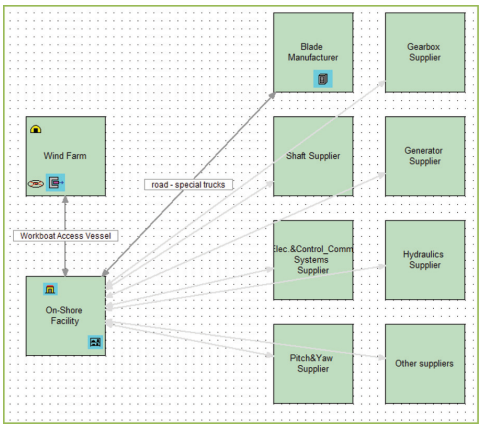


Figure 2. Maintenance synoptic map (screenshot).

Wind turbines are equipped with an internal crane that can handle small parts, while larger parts require use of the Jack-up vessel.

Supply of spare parts to maintenance facility is assured by regular truck with an average transportation time of 20 hours except for the blades where a special truck is assumed with a time of 120 hours.

2.5 *Environmental parameters*

The Wind variability is the most influential factor on the energy production. Its variation is mostly seasonal and largely studied in the literature (Morgan 2011). In the present case study, wind speed variability is accounted on a yearly basis in the energy production module by assuming a wind speed density function of Weibull type, with scale parameter $A = 8.09$, and shape parameter $k = 1.96$ (Redemakers 2002) and a rated power output curve of the Vestas V90 3 MW WT, as shown in Figure 3. By combining this data with the reliability metrics of the Wind farm components, the total produced energy at wind farm level and its cost can be extracted.

An Initial performance computation yields an ideal (no failures) annual energy production of 960096 MWh.

The second major impact of the wind variability is its delaying of maintenance operations. This is

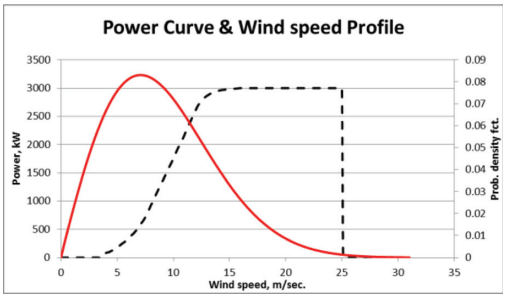


Figure 3. Assumed WT power curve and wind speed distribution.

accounted in our study by additional mean transportation time delays depending on the transportation vessels.

3 BASELINE SCENARIO

3.1 *Initial maintenance strategy*

The basic assumptions of the initial maintenance strategy are described hereunder:

- Inspections of all components are performed once a year for all components.
- When an inspected item has a too high degradation or has failed, a spare is ordered from stock.
- If spare is available in stock, it is sent to wind farm with required maintenance resources by using the appropriate vessel; if not, it is ordered from supplier.
- Stock delay due to administrative constraints is assumed to be 24 hrs.
- Suppliers delays are item dependent (several days in all cases)

Transportation delays incorporate: mobilization time, transportation time, positioning time, and an assumed weather variability delay:

- When spare arrives at the wind farm, item is removed and replaced by the new one
- Failed item is taken back onshore for repair at repair facility according to defined tasks. A repair delay (for administrative procedures) of 2 days is assumed in addition to repair time.
- Repaired item is made available in stock.
- Some items have repair condemnation, meaning they can be repaired only a limited number of times, before they are disposed of. In that case, a new spare is ordered.

3.2 *Analysis results*

Computations are performed to extract the main characteristics of the wind turbine: Reliability metrics, Performance Metrics and Cost Metrics. Figures 4 and 5 show the contribution of each component to the total failure rate and to the total computed downtime.

The pitch and yaw systems are clearly the main contributors to the downtime, along with the generator and gearbox. This is mostly due to a relatively high failure rate combined with a high turnaround time: when a part has to be replaced, the time for the jack-up vessel to be available and to reach the wind farm is very high and in the meantime, the wind turbine is not operational. On the other side, components with similar failure rates like frequency converter contribute much less to the downtime since spare parts are brought to site by faster workboat vessels. In addition, the limited number of spares in stock is also a cause for downtime since more spares may be necessary for repair than available at stock, thus creating a spare waiting time. The spares problem is addressed in §4.3.

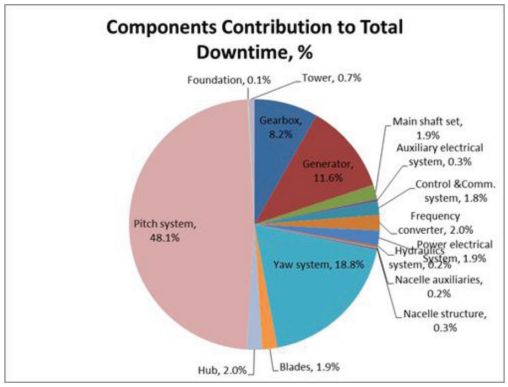


Figure 4. Components contribution to total failure rate.

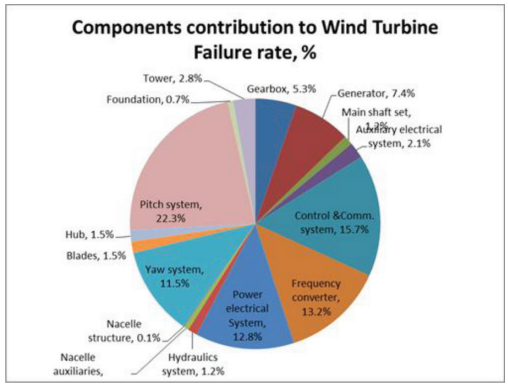


Figure 5. Components contribution to total downtime.

Table 2. Summary of baseline and optimized scenarios results.

Scenario	Availability	Number of inspections per turbine	Energy produced, MWh	Capacity factor, %	O&M costs, M€	CM costs, M€	PM costs, M€	Revenue losses, M€	Cost of energy, €/MWh
1	80.0	20	763697	36.3	23.4	20.0	2.0	18.6	31
2	87.3	115	833426	39.6	16.9	14.7	0.9	12.0	20
3	91.4	79	880117	41.9	13.4	10.9	0.9	7.59	15
4	93.6	79	889666	42.3	12.3	9.8	0.9	6.7	14

The resulting WT availability is 80%, and the energy produced by the whole Wind Farm is 763697 MWh/year at a cost of 23.4 M€ (O&M only). The resulting cost of energy is 31€/MWh produced, and the capacity factor of the wind farm is 36.3%. See Scenario 1 in Table 2.

4 OPTIMIZATION SCENARIOS

4.1 *Inspections optimization*

The inspection schedule of the baseline scenario gives an identical weight to each WT component. While this approach is not unusual in existing installations, it is somewhat unjustified. An adapted inspection schedule should be able to improve the system availability by accounting for the different reliability rates and degradation process. The Inspection Optimization module of the ApmOptimizer is used for performing the optimization, where optimization objective is the minimization of total costs, i.e. maintenance costs, failure damage costs and downtime costs (revenue losses). Optionally, it is possible to define minimal required availability or reliability at component or system level. Since inspections are planned in advance, required spares can also be ordered in advance and provided on time.

The optimization results in the optimal inspections schedule shown in Table 3.

The interval unit is weeks, such that for example the optimization recommends performing inspection on the yaw system every 30 weeks. User is free to accept these recommendations or not, according to its own judgment. When possible, inspections are grouped in order to reduce cost. After accepting the recommendations, the resulting RAM/LCC and Production parameters are computed, see scenario 2 in Table 2. Optimization yields very significant results: the WT availability increases by 7.3 points, which translates in a 9% increase in energy production. From the cost perspective, the effect is even more evident through a 26.5% reduction in corrective maintenance costs, as well as a reduction in preventive maintenance costs due to better oriented inspections although much more inspections are performed (inspections cost depends on equipment). Overall, the cost of produced energy is reduced by about 30%.

Table 3. Optimal inspections schedule.

Inspections Schedule

Inspection interval (in PMU)	Interval in operation hours	Inspection session name
14	2352	Pitch System
30	5040	Yaw System
35	5880	Control & Communication System
40	6720	Frequency Converter
45	7560	Generator, Power Electrical System
63	10584	Gearbox
200	33600	Tower
210	35280	Blade, Hub
270	45360	Main Shaft Set
300	50400	Auxiliary Electrical System
540	90720	Nacelle Structure
600	100800	Nacelle Auxiliaries

The advantage of performing an optimization through an optimization algorithm, versus using Monte Carlo type simulations is clearly seen by looking at the proposed inspections schedule. Optimization algorithm is powerful enough to yield original solutions that provide the strongest cost reductions and performance improvements.

4.2 *Condition monitoring system scenario—preventive maintenance optimization*

The effectiveness of implementing a CMS system is investigated here. CMS systems are useful in the case of offshore farms since they provide operator failure detection and identification, and enable to schedule a repair/replacement with much more precision. However, these systems are still expensive and do not always give a clear picture on what is really happening in the turbine.

In the present scenario, we assume that a CMS is installed on the following items: gearbox, pitch system and yaw system (the main downtime drivers) and that their degradation is continuously measured. Coupled with an assumed prediction model, they enable to predict the Time-To-Failure

(TTF) density distribution at a given time, and from then decide for an optimal maintenance planning that best accounts for maintenance costs and other maintenance tasks.

In our model, we assume that the monitored equipment now have a normally distributed failure time (instead of exponential) with an unchanged mean value, thus reflecting the results of the condition monitoring and prediction analysis. The previously defined inspections for the 3 items are cancelled and the Preventive Maintenance Optimization module is now used to find the best schedule to perform preventive replacement.

Again, the optimization objective is a minimization of the total lifecycle costs. Inspections optimization is then updated to adapt the new maintenance schedule. The preventive replacement and updated inspections schedule recommended by the apmOptimizer are shown in Tables 4 and 5.

The three instrumented systems are now subject to replacement only, and it can be observed that the inspections schedule has been adjusted to account for these replacements.

The resulting reliability, performance and cost metrics are summarized in scenario 3 of Table 2.

For the sake of comparison, an average investment cost of 1200€ per CMS system (total CMS cost of 288000€) has been included in the cost computations. Even with this additional cost, the implementation of CMS remains worthwhile and brings a reduction in O&M costs of more than 3.5 M€ per year compared to the previous scenario. However, this improvement has to be tempered by the fact that:

– The introduction of the CMS systems in the wind turbine does affect its reliability, since the CMS may fail as well,

Table 4. Optimal preventive maintenance schedule.

Preventive Maintenance Schedule

	Interval in PMU	Interval in calendar hours	Interval in operation hours	PM session name
	21	3528	3528	Pitch System
	50	8400	8400	Yaw System
	70	11760	11760	Gearbox

Table 5. Updated inspections schedule.

Inspections Schedule

	Inspection interval (in PMU)	Interval in calendar hours	Interval in operation hours	Inspection session name
	32	5376	5376	Control & Communication System
	40	6720	6720	Frequency Converter, Power Electrical S
	42	7056	7056	Generator
	160	26880	26880	Tower
	210	35280	35280	Blade, Hub
	270	45360	45360	Main Shaft Set, Hydraulics System
	300	50400	50400	Auxiliary Electrical System
	540	90720	90720	Nacelle Structure
	600	100800	100800	Nacelle Auxiliaries

– It was assumed here that 100% of the degradations are clearly detected, though there are cases where signals cannot be clearly interpreted, or not sufficient to draw conclusions.

4.3 *Spares level optimization*

Optimizing the inventory level of spare parts is an important stage in order to reduce downtime, especially for parts that have very long lead or turnaround time. After the inspections and preventive maintenance have been optimized, the requirement for spares is modified and should be also optimized. For that purpose, we use the spares optimization module of the ApmOptimizer. The optimization algorithm objective is to minimize the total costs and damage. The program provides the optimal initial spares quantity as well as the required spares that must be ordered during lifetime in order to replenish stocks of condemned parts.

As a result of the spare optimization, availability increases to 93.6%, as well as the energy produced. The reduction in corrective maintenance costs reflects a decrease in revenue losses due to downtime. The cost of energy produced decreases a little more to 14€/MWh. See scenario 4 in Table 2.

5 CONCLUSIONS AND FUTURE WORK

This case study has demonstrated the capabilities of the ApmOptimizer to efficiently model an offshore wind farm, and propose original maintenance configurations to bring significant downtime and O&M cost reductions. Starting from a hypothetical though representative baseline model, the inspection, preventive maintenance and spares modules have successively reduced the downtime and improved the total energy produced. It has been shown that the knowledge of the failure modes of each component, and especially of the associated degradation process enables to define the optimal inspection schedule and reduce the overall downtime.

The interest of using Condition monitoring systems in order to detect as early as possible the degradation process has been highlighted, and was proven to be worth the investment. Moreover, the use of failure distributions extracted from on-site measurements has been proven to be profitable for optimization of preventive replacements.

In a future work, more detailed model of the wind turbine components, as well as field data from real wind farms installations will be used to extract accurate reliability figures. This field data will be used to evaluate real failure distributions for all components instead of the usual assumptions.

REFERENCES

BQR Reliability Engineering Ltd, http://www.bqr.com.

European Wind Energy Association (EWEA) (2011), Wind in Our Sails.

Karyotakis, Alexander, (2011), On the Optimization of Operation and Maintenance Strategies for Offshore Wind Farms, Department of Mechanical Engineering University College London.

Maples, B. & Saur, G. & Hand M. & Van de Pietermen R. & Obdam T.—NREL (2013), Installation, Operation, and Maintenance Strategies to Reduce the Cost of Offshore Wind Energy.

Morgan Eugene C., Lackner Matthew, Vogel Richard M., Laurie Baise G., (2011), Probability distributions for offshore wind speeds, Energy Conversion and Management Journal, No 52, pp 15–26.

Rademakers L.W.M.M., H. Braam, (2002), O&M Aspects of the 500 MW Offshore Wind Farm at NL7, DOWEC project.

ReliaWind Deliverable D 6.7—(2010), Report.

Recommendations from the ReliaWind Consortium for the Standardization for the Wind Industry of Wind Turbine Reliability Taxonomy, Terminology and Data Collection.

Reliawind Deliverable D.1.3 (2010), Report on Wind Turbine Reliability Profiles.

Sonderkar Nielsen, Jannie PhD (2013), Risk-Based Operation and Maintenance of Offshore Wind Turbines, Aalborg University.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Maintenance planning for drum shearer machine based on its reliability characteristics and economical sensitivity analysis

S.H. Hoseinie, B. Ghodrati & U. Kumar
Division of Operation, Maintenance and Acoustics, Luleå University of Technology, Luleå, Sweden

ABSTRACT: Cutting arms are the main productive units of coal shearer machine that contact directly with coal seam. More importantly, the cutting arms operate under a high stress environment. In this paper, in order to suggest an optimum maintenance plan for the subsystem of shearer machine, firstly, we conducted a failure and reliability analysis using the data acquired from the Parvadeh coal mine Iran over the last two years. In doing so, we applied estimated distribution functions and calculated cost parameters to identify the cost-based optimum preventive maintenance interval. The analysis shows that the Power Law Process model provides a good fit to the failure data. Accordingly, the preventive maintenance operation can improve the reliability of the system by 53.5%. Furthermore, we conducted a sensitivity analysis of the studied machine and identified that if we consider the variation of the world price of the raw coal then the maintenance plan is sensitive to the price, however the effects of this change on reliability improvement is almost zero.

NOTATIONS

C_C:	Cost of the consequence of failure or production loos
C_{CM}:	Cost of corrective maintenance
C_{CMi}:	Cost of failure when the preventive maintenance is used
C_i:	Cost of inspection
CM:	Corrective Maintenance
C_{PM}:	Cost of a pre-planned preventive maintenance
C_{pm}:	Cost of preventive maintenance can be carried out in the scheduled intervals during inspections
C_{PMi}:	Expected cost of inspection and preventive maintenance
C_R:	Cost of repair
k:	Number of events
MCSPPM:	Mean cost of spare parts for preventive maintenance
MCSPR:	Cost of spare part during the inspection operation
MTTR:	Mean time to repair
MTBF:	Mean time between failures
NHPP:	Non-Homogeneous Poisson Process
N_t:	Cumulative number of failures up to time t
PLP:	Power Law Process
P_e:	Probability that inspection will indicate the potential failure
P_f:	Probability of the failure occurring
Pp:	Probability of the failure being detected
PM:	Preventive Maintenance
RP:	Renewal Process
R(t):	Reliability function
TBF:	Time between failures
t_k:	Total running time
t_i:	Running time of the ith event
T_{PM}:	Optimal preventive maintenance interval
β:	Shape parameters
θ:	Scale parameters

1 INTRODUCTION

The high productivity and lean operation are critical factors which should be addressed in the management and production strategies of mines. In this regard, longwall mining is one of the special mining methods that use high technology, high mechanization and automation process. The basic types of equipment that are used in modern longwall mining are: coal cutting machine (drum shearer), armored face conveyor and powered supports (Stefanko 1983, Ramani 1981, Mandal & Banik 1996). A mine production system demands a sequential operation of the equipment that can be used in cutting-loading and transport operations. Therefore, it is important that each subsystem should perform well during the time of requirement, likewise achieve the goal production during subsystem failures (Bhatacharaya et al., 1991).

As explained above, shearer is the first component of production chain in longwall face; therefore

its operational characteristics can seriously affect the rest of production process as well as mine productivity. The reliable and efficient performance of this machine can lead the system to achieve the target production effectively.

Similarly, cutting head (cutting system) is one of the important and critical subsystems of longwall shearers. It plays direct role in coal cutting and production and has a close relation to other subsystems such as electrical, water and hydraulic systems. Any failure to this unit directly affects the drum performance and leads to immediate stoppage of the machine. Therefore, the reliability study of this subsystem of shearers is essential to prevent the machine from unpredictable break downs.

In this paper, we analyze the reliability of cutting arms of drum shearer and furthermore, we calculate the optimum preventive maintenance planning based on cost parameters and reliability characteristics. Finally, we discuss the effects of the international coal price on maintenance planning of machine and amount of reliability improvement.

2 RELIABILITY ANALYSIS

Common occurrence of failures in the repairable systems is the result of discrete events that happens over time. These processes are often called stochastic point processes (Modarres, 2006). The stochastic point process is used to model reliability of the repairable systems. The analysis in this process includes renewal process, homogeneous Poison process, and non-homogeneous Poison process.

Before any reliability analysis is started, tests for trends and serial correlations must be performed to evaluate the type of the available TBF data and to select the best analysis method. If there is a trend in the dataset, this means that the data are not identically distributed. The presence of serial correlation shows that the data are not independent. In the case of no trend and no serial correlation, data are called iid (independent and identically distributed) and the RP method is the best method for reliability analysis, while in the case of having trend and serial correlation, the NHPP method is used for modelling.

The PLP is a well-known NHPP model used to study the reliability of the repairable systems. Duane (1964) was the first to report that the cumulative number of failures of such systems up to time t, N_t, often have a "power-law" growth pattern. Then, Crow (1974) formulated the corresponding model as a nonhomogeneous Poisson process model. The reliability function at time t are defined by the following equation:

$$R(t) = \exp\left[-\left(\frac{t}{\theta}\right)^{\beta}\right] \tag{1}$$

The θ and β parameters can be estimated by the following expressions as suggested by Crow (1974);

$$\hat{\beta} = \frac{k}{\sum_{i=1}^{k-1} \ln(t_k / t_i)} \tag{2}$$

$$\hat{\theta} = \frac{t_k}{k^{1/\beta}} \tag{3}$$

A simple graphical method for testing the goodness-of-fit is to simply plot $\ln(N(t))$ against $\ln(t)$ on a square graph paper. If a straight line is observed, it means the power law process model is a suitable model for reliability analysis (Klefsjö & Kumar, 1992, Crow, 1974).

3 MAINTENANCE PLANNING AND OPTIMIZATION

There are two primary types of maintenance actions: PM and CM. When the system is in a wear-out condition that is represented by increasing failure rate, in many cases, the preventive maintenance may be a suitable policy for improving the operational condition of machine.

The important goal of this study is to find the optimal preventive maintenance policies that can minimize the total cost of operation, at the same time, improve the reliability of the cutting arms of shearer. In this paper, we will use the analytical method for estimation of optimal overhaul intervals. The suggested method will minimize the long-run cost per unit of operation time given the system is modeled by the power law process.

In this case, the cost per unit of time can be calculated by Equation 4:

$$C(T) = \frac{(C_{CM} + C_{PM})\left(\frac{T}{\theta}\right)^{\beta} + C_{PM}}{T} \tag{4}$$

The Equation 4 has minimum value at T_{PM}, where;

$$T_{PM} = \theta\left(\frac{C_{PM}}{(C_{CM} + C_{PM})(\beta - 1)}\right)^{\frac{1}{\beta}} \tag{5}$$

Therefore, one possibility of estimating the optimal time interval T_{PM} between complete overhauls

is to use Equation 6 where $\hat{\beta}$ and $\hat{\theta}$ are estimates of β and θ.

$$\hat{T_{PM}} = \hat{\theta}\left(\frac{C_{PM}}{(C_{CM}+C_{PM})(\hat{\beta}-1)}\right)^{\frac{1}{\hat{\beta}}} \quad (6)$$

If a component/subsystem runs to failure, the expected cost of CM over a given time interval includes the product of P_f and $(C_C + C_R)$ (Barabady & Kumar, 2007):

$$C_{CM} = (C_C + C_R) \times P_f \quad (7)$$

The expected cost of maintenance over a given time interval includes two main parts (Barabady & Kumar, 2007):

a. C_{CMi}: It is not possible to remove all failures by using PM, but the number of failure could be decreased. The C_{CMi} applied in this case, can be calculated as follows:

$$C_{CMi} = (C_C + C_R) \times P_f \times (1 - P_p) \quad (8)$$

b. C_{PMi}: The C_{PMi} can be calculated by using the Equation 8.

$$C_{PMi} = C_i + (C_{pm} \times P_f \times P_p) + (C_{pm} \times (1 - P_f) \times P_e) \quad (9)$$

Finally, the C_{PM} is the sum of Equation 8 and 9:

$$C_{PM} = C_{CMi} + C_{PMi} \quad (10)$$

4 CASE STUDY: PARVADEH COAL MINE, IRAN

In this paper, the shearer machine of Parvadeh coal mine in the central Iran was selected for case study and data collection. The extracted coal seam of this mine has 1.8 m thicknesses and is mined by retreat longwall method using a double-drum shearer (Fig. 1).

As shown in Figure 1, each side of studied shearer machine has a ranging arm and a cutting drum. The arm is fixed to drive unit and electric system block by means of the articulated joint and pins. The arm can be lifted and lowered down in steeples way, and maintained at desired height by means of hydraulic servo.

4.1 *Failure data analysis*

The required data for this research was collected from operation and maintenance reports and direct field observations over a period of two years. Many of the desired information, such as failure occurrence times, reasons of failure, types of repair actions and time to repair were available in mine database, therefore only TBFs values were calculated. All needed calculations related to data analysis and reliability modeling were carried out using Easy*fit* and Microsoft Excel software.

According to the results of trend and serial correlation tests, a trend was noticed as interpreted from the convexity of the curve. The test for the serial correlation showed no correlation in general. Therefore, non-homogeneous Poison process it the best way for reliability analysis. In this research, the

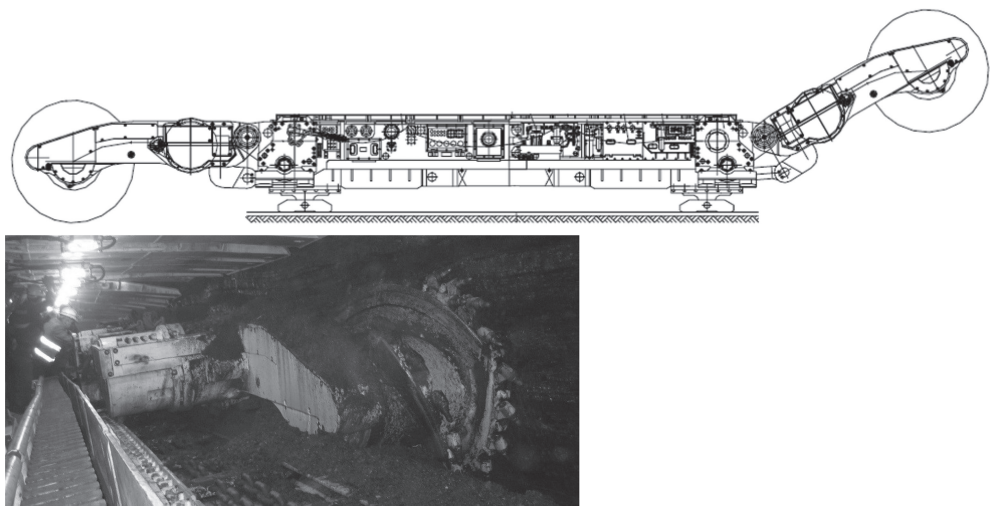


Figure 1. Drum shearer of Parvadeh coal mine.

power law process, as a certain form of nonhomogeneous Poisson process, was tested and selected for analyzing the reliability of cutting system of drum shearer.

4.2 *Reliability analysis*

After validation of the PLP assumption, the parameters of the PLP model were estimated analytically using the Equation 2 and 3. The calculations showed that β is 1.58 and θ is 443.8. According to achieved reliability model, the reliability curve was plotted as shown in Figure 2. The plot shows that the reliability of cutting arms of drum shearer reaches the zero after about 1300 hours of operation. There are 80% and 50% chance that this system can work without any failure after 170 hour and 350 hour respectively.

Since β is greater than one, the cutting arms of shearer machine have increasing failure rate. Therefore, this system needs a preventive maintenance operation to prevent the system from reaching the high failure rates and serious breakdown.

4.3 *Maintenance planning and reliability improvement*

As depicted in Equation 4, calculation of the costs of corrective and preventive maintenances is essential to find the optimum maintenance interval of a system. The cost parameters which were presented in Equations 4 to 9 are calculated as follows:

C_C: To calculate this parameter, statistical analysis was done on the available data so that we can find the average production hour per shift and average cutting rate (advance speed) of drum shearer. The results showed that, the shearer of Parvadeh mine works 2.71 hours per shift in average, likewise the average cutting rate of machine in working condition was 1.16 m/min. Considering the all available information and the density of 1.6 g/t for extracted coal, the total production per minute was 2.67 tons in average. If we assume that the raw coal price is 55$/t in average then the value of the produced coal per minute will be 146.85$/min. It means any breakdowns in the production can cost around 146.85$/min in Tabs coal mine. Using this information, if we know MTTR of the cutting arms of shearer, we can calculate the C_C by multiplying 146.85$ with the MTTR. Therefore, in the Parvadeh mine case, first, the MTTR of the system was calculated, and then the C_C of the system was calculated.

C_R: To calculate the cost of repair, two main costs were considered:

a. MCSPR: the cost of spare parts and tools is directly depending on the type of subsystem and maintenance operation. According to the available financial data and spare part usage reports of the Parvadeh mine, an average value was considered for the cutting arms of the subsystem. The considered value is presented in Table 1.
b. Labor cost: this cost represents all human works done on machine during the maintenance operation. The labor cost for the maintenance operation in Parvadeh mine is ≈0.23$/min according to the salary and working hours for each worker per day. These values can be used to calculate the labor cost, supposing the MTTR of system is given, by multiplying the 0.23 with MTTR.

Finally, the above cost can be added to calculate the C_R. Calculated value of C_R is presented in Table 1.

P_f: To calculate this parameter, we need to consider initial intervals for maintenance operations and then calculate the failure probability based on cumulative failure distribution function (F(x)), which is the outcome of TBF data analysis. In his paper, MTBF was used as an initial maintenance intervals; therefore using the MTBF value the

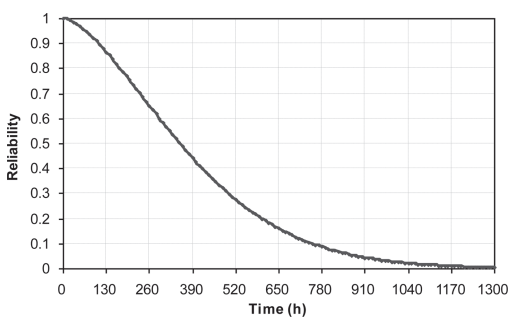


Figure 2. Reliability plot of cutting arms of drum shearer.

Table 1. Cost parameters of cutting arms of drum shearer of Parvadeh coal mine.

Parameters	Values
MTTR (min)	42.5
C_C ($)	6247.3
MCSPR ($)	150
C_R ($)	165.3
P_f	2.35%
P_e	30%
C_i ($)	5.4
MCSPPM ($)	65
C_{pm} ($)	78.5
C_{PMi} ($)	29.7
C_{CM} ($)	150.7
C_{PM} ($)	74.9

failure probability was calculated. The result is presented in Table 1.

C_i: the rate of inspection consists of two main costs: labor costs and tool/test costs. Parvadeh mine, usually, conduct visual inspection because of the specific working condition, for instance limited space and light and low accessibility to machine parts. Therefore the cost of tools and tests was negligible. The calculated labor cost in Parvadeh mine was 0.125$/min. Using this cost, if we know the mean time of inspection then we can calculate the labor cost. The inspections usually take in average 25 minutes for cutting arms. As a result, the inspection cost calculated for this system is 3.125$.

C_{pm}: the preventive maintenance can be carried out in the scheduled intervals during inspections. In this study, the scheduled PM is considered for the cost estimation. Therefore, PM is done in real operation and uses real duration and tasks. To calculate the total of PM, we used two costs: MCSPPM and labor cost. The final value of C_{pm} is calculated by adding these two costs. The result is presented in Table 1.

P_e and P_p: maintenance operation has special difficulties in mining. The operation is also seriously affected by the environment. Cutting arms had so many mechanical parts which are not easily visible. Therefore, 30% has been assigned to the probability that inspection will falsely indicate the potential failure of cutting arms. Thus, the probability that the failure can be detected by inspections (P_p) is 70%.

With regard to previous explanations, the input data for calculating the C_{PM} and C_{CM} of the cutting arms of the drum shearer of Parvadeh coal mine is shown in Table 1.

According to the cost parameters as presented in Table 1, Equation 6 can be used for calculating the optimum preventive maintenance interval of cutting arms of drum shearer as shown below:

$$\hat{T}_{PM} = 443.8\left(\frac{74.9}{(150.7+74.9)(1.58-1)}\right)^{\frac{1}{1.58}} \approx 289 \tag{11}$$

Therefore, preventive maintenance tasks should be done in intervals equal to $T_{PM} = 289$ hours.

5 SENSITIVITY ANALYSIS OF MAINTENANCE PLAN

All the time most of the mining companies are afraid of the effects of raw material price on operation and benefits of their mines. As can be seen in Table 1, the highest cost of maintenance is related to the C_c which represents the cost of production loss. This value directly depends on the price of raw coal in international market.

In this study, the basic price of raw coal was assumed 55$/ton in average. For sensitivity analysis, the whole calculations have been repeated by 40, 50, 60 and 70 $/ton. The result of the calculations is shown in Figure 3. As can be seen in Figure 3, the T_{PM} is very little affected by raw coal price. It means that, 35$ change in coal price changes the T_{PM} only by 6 hours.

Figure 4 shows the improved reliability plots for different T_{PM}. As can be see, due to very little

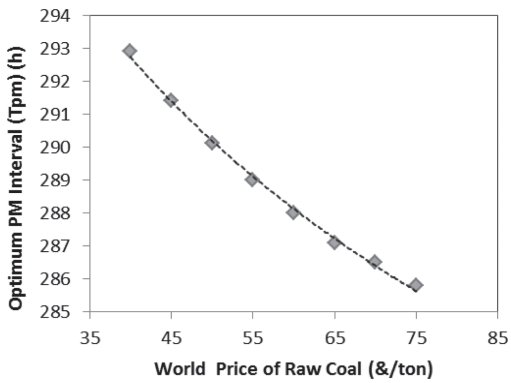


Figure 3. Effect of world price of raw coal on optimum maintenance interval (TPM).

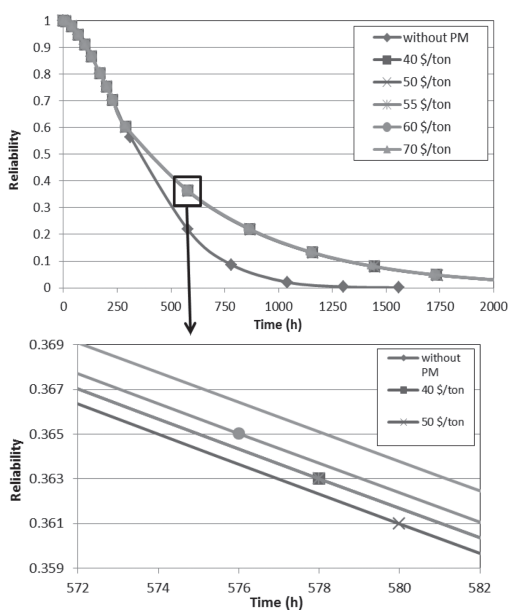


Figure 4. Effect of world price of raw coal on improved reliability plots resulted from PM.

differences in optimum maintenance intervals, the reliability of machine is not much sensitive to raw coal price and all the reliability plots are lay in a same way. The zoomed out part of plots are clearly shows that, the difference among the reliability plots are negligible. Therefore, as a clear result, the mine managers and planners should not be afraid of the world price of coal and its effects on their maintenance plan and operation.

The sensitivity analysis of maintenance plan showed that the big changes in world price of raw coal are not so effective on maintenance plan of the drum shearer, especially on cutting arms of the machine. This matter can be checked in other subsystems of machine and also other equipment of longwall mining. Then, we can come to an exact statement about the operational effects of unstable international market of coal on longwall operation.

6 CONCLUSION

According to the results of trend analysis and test for the serial correlation, it is clear that the assumption of iid is normally not valid for the TBFs of the cutting arms of the drum shearer machine. The assumption that the power law process adequately describes the TBFs of this system was validated and confirmed by graphical method. Since the failure rate of this system is increasing, the preventive maintenance is suitable strategy for this system.

The cost parameters that have been calculated based on case study data were used for calculating the optimal preventive maintenance interval for this system. The calculation showed that approximately 289 hour is optimum value for PM intervals. It is predicted that if we conduct the preventive maintenances in 289 intervals then the reliability of cutting arms of drum shearer will improve by minimum 53.5%, which is a noticeable positive change in operational and economical condition of machine performance.

The sensitivity analysis showed that by changing the world price of coal from 40$ to 75$/ton, the optimal maintenance interval can decrease from 293 hours to 286 hours. In this case, however, the difference is not so significant. One of the reasons for this little difference can be that with the increase of the coal price, the C_C also increase, which in turns leads to C_{CM} increase, consequently, that leads to T_{PM} decrease. In practice it means that, when the coal price is high, we are more concerned about our machine because any unpredictable failure can result in a higher revenue loss (or higher production loss). Therefore to reduce the probability of breakdown occurrence, the preventive maintenance in a shorter period is advised. However, in this particular case of mine, there was no significant difference between the PM intervals of various coal prices. On the other hand, the reductive trend was obvious (Fig. 3).

Because of the low changes in T_{PM}, the amounts of reliability improvements in different intervals were very low or almost negligible. The implication of the result to the Parvadeh coal mine is that the international coal prices don't have any serious effect on maintenance program of the coal shearer machine, and may not be the real risk factor.

ACKNOWLEDGEMENT

The authors are grateful to employees and managers of Parvade Coal Complex in Iran for their kind cooperation during data collection. The financial support of the Center for Advanced Mining and Metallurgy (CAMM) of Lulea University of Technology is also acknowledged.

REFERENCES

Barabady, J. & Kumar, U. 2007. Reliability characteristics based maintenance scheduling: a case study of a crushing plant, *International Journal of Performability Engineering* 3(3), pp. 319–328.

Bhatacharaya, J., Murthy A.S.R. & Ray S.C. 1991. A methodology for forecasting and performance evaluation of mining systems. *International Journal of Mining, Reclamation and Environment* 5(3), pp. 129–133.

Crow, L.H. 1974. Reliability analysis for complex repairable systems. F. Proschan & R.J. Serfling (eds). *Reliability and Biometry*, Philadelphia: SIAM. pp. 379–410.

Duane, J.T. 1964. Learning curve approach to reliability monitoring, *IEEE Transactions on Aerospace* AS-2, pp. 563–566.

Klefsjö, B. & Kumar, U. 1992. Goodness-of-fit tests for the power-law process based on the TTT-plot, *IEEE Transactions on Reliability* 41, pp. 593–598.

Mandal, S.K. & Banik, P.K. 1996. Evaluation of Reliability Index of Longwall Equipment Systems, *Mining Technology* 78, pp. 138–140.

Modarres, M. 2006. *Risk Analysis in Engineering: Techniques, Tools, and Trends*. New York: Taylor & Francis.

Ramani, R.V. 1981. *Longwall-Shortwall Mining, State-of-the-Arts*. New York: Society of Mining Engineers (SME).

Rausand, M. & Høyland, A. 2004. *System Reliability Theory: Models, Statistical Methods and Applications*. Hoboken: John Wiley & Sons.

Stefanko, R. 1983. *Coal Mining Technology, Theory and Practice*. New York: Society of Mining Engineers (SME).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A guide for Block Inspection Policy implementation

A. Jodejko-Pietruczuk & S. Werbińska-Wojciechowska
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: In the presented paper, authors focus on the investigation of Block-Inspection (BI) policy implementation possibilities. They provide the synthetic approach to the results on BI policy research which gives the possibility to define guidelines for determining its use. Thus, there is provided a comprehensive literature review covering the issues on inspection policy parameters modelling and optimization or implementation. This gives the possibility to present the approach for maintenance inspection selection problem from engineering point of view. The research work is aimed at summarizing some authors developments in the analysed research area.

1 INTRODUCTION

The main maintenance problems which face maintenance managers mostly regard to the definition of a problem/disruption occurred in the area of operational processes performance, and identification of its nature, locations and possible maintenance actions (Valis and Vintr 2006). Following this, maintenance problems of technical systems have been of significant importance for the past fifty years, especially because of the applications in industry, aviation, transportation systems, or medicine (see e.g. (Babiarz 2006, Bajda et al. 2011, Kierzkowski 2010, Kierzkowski et al. 2012, Kierzkowski and Zając 2012)). During that time, there have been developed many conceptions and models in the area of technical objects maintenance performance, which are aimed at maintenance tasks scheduling and optimization, taking into account economical and reliability criteria (Nowakowski and Werbińka 2009).

Moreover, the two approaches have evolved from performing maintenance actions. First, there are known models in which a system or its components fail and there are no visible symptoms about the forthcoming failure (assuming that it is a sudden failure). The majority of the maintenance modelling concepts, being discussed in the literature since the early 1960s, regards to this kind of a problem investigation. For more information we recommend reading e.g. (Młyńczak et al. 2014, Nowakowski and Werbińka 2009, Werbińska-Wojciechowska 2014).

The second approach involves the modelling problems of systems/its components, when assuming that it is not a sudden failure. In this approach, before a component breaks down, there will be some sings of reduced performance or abnormalities. The time between the first identification of abnormalities (called initial point) and the actual failure time (failure point) will vary depending on the deterioration rate of the component. This concept (delay time concept), which provides useful means of modelling the effect of periodic inspections on the failure rate of repairable technical systems, was developed by Christer et al., see e.g. (Christer 1987, Christer 1982, Christer & Waller 1987, 1984a, 1984b, Christer & Whitelaw 1983).

However, the identification of the best maintenance strategy and its parameters for real-life systems is a complex problem. On the one side, there is a problem to define if and what kind of signal of forthcoming failure may occur. On the other, some signals about system defects cannot strictly indicate what kind of problem occur in the system.

For example, the squealing of vehicle belt during its operation process performance indicates the need for its preventive replacement. However, the occurred noise during operation processes performance of construction machines (e.g. wheel loader) will only indicate a problem in the drive system, which may regard to e.g. differential problems or transmission problems (e.g. propeller shaft).

One of the examples, which serves to illustrate the difficulty and complexity of proper maintenance action definition my regard to the problem, which occurred during operational processes performance by a loader which worked at different surfaces. In the analysed case, at a speed of 17.5 km/h, the construction machine fall in the resonance which even make its correct operation impossible. After a long search for the cause of the problem (e.g. assessment of the potential damage to the front axle and rear), it turned out that the tires have been wrongly selected what caused such the problems.

Taking one step further, even the preventive maintenance policy selection (e.g. Block Replacement Policy) for exploitation or operational materials may be complicated and determined e.g. by changeable

working conditions. An example here would be the replacement of teeth in a loader's bucket. The time between successive replacements will depend on the class of abrasion of excavated materials.

Another problem is that some inspection (diagnostic) actions may be performed only during planned maintenance actions performance. A good example here is the planned replacement of engine oil in construction machines. During this maintenance operation performance, one can use a sample of used oil and examined it for the content of metallic elements. The increased level of their content may attest to the usage of certain engine system components, such as wear out of cylinders, piston rings or bearings.

There is also possible continuous control of some signals which indicate for defects. The example here may be the control process of temperature or pressure of engine oil, transmission oil or axles oil. This control allows for ongoing assessment if there appears in the system too high friction or leakage.

The given example indicate the need for research work in the area of maintenance decision process support tools development and definition of methods of maintenance strategy and its parameters selection.

Following the above considerations, authors focus on the investigation of given Block-Inspection (BI) Policy implementation possibilities. They provide the synthetic approach to the results on BI policy research which gives the possibility to define guidelines for determining its use and setting out the questions to be answered:

- When to use the BIP policy?
- What kind of data to estimate?
- How to choose the optimal period T?

Thus, in the next Section, there is provided a comprehensive literature review covering the issues on inspection policy parameters modelling and optimization as well as its implementation. This gives the possibility to present the approach for maintenance inspection selection problem from engineering point of view. The research work is the continuation of investigations presented e.g. in (Jodejko-Pietruczuk et al. 2013a, Jodejko-Pietruczuk and Werbińska-Wojciechowska 2014b, 2012a, 2012b) and is aimed at summarizing some authors developments in the analysed research area. The work ends up with summary and directions for further research.

2 INSPECTION POLICY MODELLING— LITERATURE REVIEW

Ones of the first works dedicated to the inspection problems literature review are (Barlow et al. 1963), where authors investigated the issues of periodic inspections, and (Sherif 1982), where author reviewed about 818 international papers aimed at optimal inspection and maintenance schedules of failing systems. More related studies on optimal inspection issues can be found e.g. in (Abdel-Hameed 1995, Cui et al. 2004, Kaio and Osaki 1988, Luss 1983, Onoufriou and Frangopol 2002).

In the recent literature, one can find models of inspection frequency optimization with the use e.g. simulation processes (see e.g. (Alfares 1999, Vaghefi and Sarhangian 2009)), probability analysis (see e.g. (Baohe 2002)), Bayes or quasi-Bayes approach (see e.g. (Durango-Cohen and Madanat 2008, Jones et al. 2010)), or Markov processes (see e.g. (Kenzin and Frostig 2009)). Moreover, the analysed problems include e.g. the periodic inspection optimization for systems with failure interaction (see e.g. (Golmakani and Moakedi 2012, Zequeira and Berenguer 2005)), or the introduction of imperfect inspection (see e.g. (Berrade et al. 2013, Zhao et al. 2007)).

There are also many papers dedicated to inspection policy implementation e.g. in the area of industrial systems performance (see e.g. (Duffaa and El-Ga'aly 2013, Yun and Nakagawa 2010)), railway systems maintenance (see e.g. (Podofillini et al. 2006)), or cargo container reliability analysis (see e.g. (Ramirez-Marquez 2008)).

The basic inspection models are extended by using a technique called Delay Time Analysis (DTA), which has been developed for modelling the consequences of an inspection policy for any systems (Christer 1982). A literature review, in which delay-time models are investigated along with other PM models are given e.g. in (Dekker & Scarf 1998, Mazzuchi et al. 2007, Ozekici 1996, Thomas 1986, Valdez-Flores & Feldman 1989). The state of art works, dedicated strictly to DT modelling are given in e.g. (Alzubaidi 1993, Baker & Christer 1994, Christer 2002, 1999, Christer & Redmond 1992, 1990, Lee 1999, Nowakowski & Werbińska-Wojciechowska 2012, Redmond 1997, Wang 2012).

In the case of a repairable component, it is possible to model the reliability, operating cost and availability functions when pdf $f_h(h)$ and $g(u)$ are known.

The basic multi-component system delay-time model is given in e.g. (Christer & Redmond 1992, Christer & Waller 1984a, 1984c, Wang 2003). The basic assumptions include perfect inspection case, independent system components, the number of defects arising over T following a HPP with a constant rate λ per unit time, known pdf $f_h(h)$, regular inspection actions performance which requires a constant time d. Following these assumptions, probability of defect arising as a failure $P_b(T)$ and downtime per unit time $E_D(T)$ may be estimated.

The basic extensions for analysed delay time model regard to the non-perfect inspection case (see

e.g. (Christer 1999, Wang 2009)), multiple nested inspections case (see e.g. (Wang 2000, Wang et al. 2012)), imperfect inspections performance (see e.g. (Cai & Zhu 2011, Wang 2010)), or NHPP defect arrival process (see e.g. (Christer 1999, Christer & Wang 1995)).

The presented above maintenance models regard to PM policy consideration. The implementation of condition monitoring policy in delay-time models for complex systems is given e.g. in (Chilcott & Christer 1991, Jalani Naini et al. 2009, Wang 1992).

Delay time modelling applied to industrial maintenance problems can be traced back to (Christer 1982). Since then, there has been developed a lot of maintenance models that use the delay-time concept. Many works have been carried out on the DT modelling to production plants (e.g. (Akbarov et al. 2008, Jones et al. 2009)). Other works include the application to gearbox failure process (see e.g. (Leung & Kit-leung 1996)), modelling PM for a vehicle fleet (see e.g. (Christer & Waller 1984b, Desa & Christer 2001, Jardine & Hassounah 1990, Scarf & Bouamra 1995)), PM process for a coal face machinery (Chillcott & Christer 1991), wind turbine maintenance optimization (see e.g. (Andrawus et al. 2007)), modelling maintenance of fishing vessel equipment (see e.g. (Pillay et al. 2001)), medical equipment (see e.g. (Christer & Scarf 1994)), or application to concrete structures (see e.g. (Redmond 1997)). Moreover, well known models base on time-based PM or condition-based maintenance (e.g. (Chilcott & Christer 1991, Jalani Naini et al. 2009, Wang 1992)). Additionally, Cui in his work (Cui 2002) provides a semi-automated DTM tool, which is based on models developed till the 2002 and enables engineers to themselves undertake e.g. model based decision making.

All the presented works give the model of optimal period between inspections estimation. However, they do not address the issues of selection of the type of maintenance strategy which should be use depending on the analysed technical system and its operational process. These issues are one of the scope of maintenance management systems or decision support systems developed in the analysed research area. For more information we recommend reading e.g. (Bojda et al. 2014, Laskowski and Bylak 2013, Vintr and Valis 2012).

3 MAINTENANCE MODELLING METHODOLOGY FOR TECHNICAL SYSTEMS

3.1 *Block Inspection policy*

The analysed methodology of DT concept use in maintenance modelling of technical systems is developed for implementation of Block Inspection Policy. This maintenance policy assumes, that inspections take place at regular time intervals of T, and each requires a constant time. Usually components are prone to become defective independently of each other when the system is in operating. All defects which may have arisen in the system, deteriorate over an operating time. Later, all elements with identified defects will be replaced within the inspection period. However, the inspection actions may be perfect or imperfect ones what affect the optimization process.

3.2 *Developed methodology*

There is no simple decision rule which maintenance policy should be taken to provide the best effectiveness of technical systems during their life span. While developing the methodology for modelling the processes of technical systems maintenance, taking into account the DT concept, it should be noted that the purpose of the model is usually to minimize the expected duration of system downstate $E_d(T)$, the expected maintenance costs $C(T)$, or maximize the system availability function $A(T)$. At the same time, the impact of their components failures on its environment is also important. The level of this impact can be expressed by the function of the expected failure consequences costs $C_C(T)$. On the other hand, further considerations omit the possibility of performing a multi-criteria analysis.

Following this, the algorithm for the determination of the optimal period between the inspection actions performance T should contain the following steps (Fig. 1) (Cunningham et al. 2011, Jones et al. 2009, Wang and Christer 2003):

- understanding the process of maintaining the selected system (e.g. determining the type of the involved maintenance operation, the relationship between the system's components, definition of the types of obtainable data),
- identifying the problems in the selected system exploitation process (e.g. long-term repair operations, frequent damage),
- analysis if there is a possibility of expected delay time $E(h)$ or characteristics of initial point u estimation,
- data collection and analysis—based on using subjective and objective methods;
- determining the assumptions of the model—based on the data and knowledge about the operation processes in effect (e.g. single-/multi-element system),
- estimating the basic parameters of the model—for example, functions $f_h(h)$ and $F_h(h)$ for the time delay parameter h, selecting the probability distribution for the time between failures or the repair time,

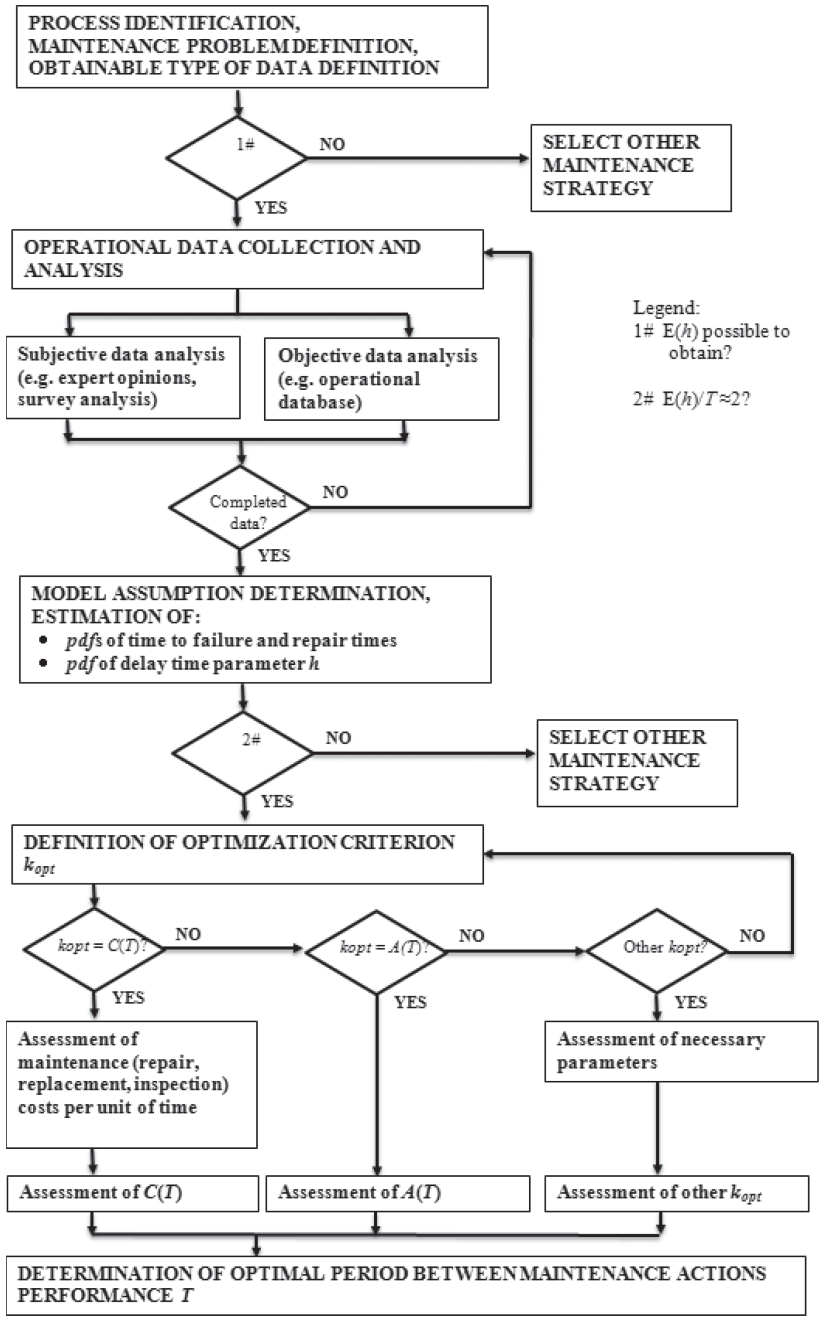


Figure 1. The algorithm for assessment of optimal period T using the concept of DT.

- determining the relationship between the expected value of the time delay parameter h and the optimal period T—in order to determine whether the DT concept allows for optimum solution obtainment (more info e.g. in (Jodejko-Pietruczuk and Werbińska-Wojciechowska 2012a, 2012b)),
- defining optimization criteria—depending on the available operational data and model assumptions,

- estimating the function of the optimization criterion, designating the optimal period T.

3.3 *The main guidelines for optimal period T assessment with the use of BI policy*

The previous authors' research works was aimed at investigation of BI policy modelling and implementation for technical systems performing in various reliability structures (see e.g. (Jodejko-Pietruczuk and Werbińska-Wojciechowska 2014a, 2014b, 2012a, 2012b). Thus, there were developed some rules for definition of the principal relations between the system performance under given PM policy and chosen PM policy parameters.

3.3.1 *Perfect inspection case*

Let's consider the system comprised of 3 identical elements, in a k-out-of-n reliability structure, working independently under the same conditions. The performance of the investigated system, being illustrated in Figure 2, is also defined by the additional assumptions:

- the system is a three state system where, over its service life, it can be either operating, operating acceptably or down for necessary repair or planned maintenance,
- maintenance actions restores system to as good as new condition,
- the system can remain functioning in an acceptable manner until breakdown (despite having defects),
- the breakdown will be assumed to have been caused by two of the defects which has deteriorated sufficiently to affect the operating performance of the system as a whole,

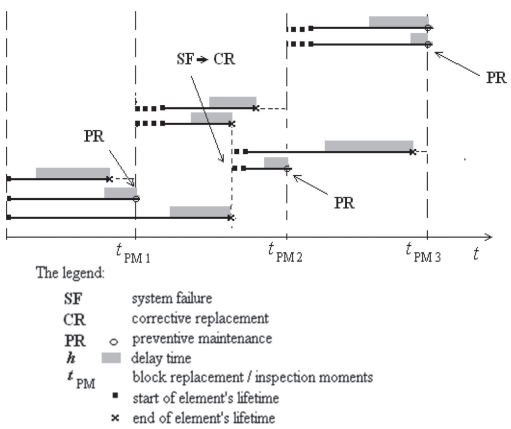


Figure 2. Block inspection policy for the investigated system (2-out-of-3 reliability structure).

- failures of the system are identified immediately, and repairs or replacements are made as soon as possible,
- system incurs costs of: new elements, when they are replaced, inspection costs, and some additional, consequence costs, when system fails,
- time of defects occurrence defined by u is a random variable described by its probability distribution functions $g(u)$ and $G(u)$
- elements' lifetime, repair time, replacement time and the length of the delay time before element's failure are random and their probability distributions are known.

The performance of the chosen system is modelled with the use of simulation processes. The modelling process was based on the use of *GNU* Octave software. More information can be found e.g. in (Jodejko-Pietruczuk and Werbinska-Wojciechowska 2012a, 2012b). The modelled system parameters are given in Table 1.

Following the carried out research analyses results, some decision rules on when to use BI policy can be defined for technical systems performing in various reliability structures.

Observation of the modeled operating process' simple scheme (Fig. 2) leads to believe that the main variables affecting the BI maintenance policy performance are: an element's time to failure (T_p) and a delay time (h). Thus, according

Table 1. Modelled system parameters.

Notation	Description	Tested values
n	Number of elements of the system	3
k	Minimal number of up-stated elements for having system in an operational state	1, 2, 3
c_r	The cost of new element	1
c_i	The cost of an inspection	1
c_f	The cost of a system failure	10 000
T_i	The time required for inspection	0
$F(t)$	C.d.f. of elements' lifetime	$F(t) = 1 - e^{-(t/100)^{3,5}}$
$G_r(t)$	C.d.f. of single elements' repair time (resulting from a system failure)	$G_r(t) = 1 - e^{-(t/100)^{2,3}}$
$G_p(t)$	C.d.f of single element's replacement time (resulting from preventive replacement)	$G_p(t) = 1 - e^{-(t/10)^{2,3}}$
$F_h(h)$	C.d.f. of elements' delay time	$F_h(h) = 1 - e^{-(h/35)^{3,5}}$

to the research works (Jodejko-Pietruczuk and Werbińska-Wojciechowska 2012a, 2012b), which investigated the BIP policy in multi-unit systems performance implementation, there is possible to determine the relationship between time T and the expected value of the variable h in systems with serial reliability structure, which is obtained for the lowest maintenance cost and highest system availability:

$$\frac{E(h)}{T} \approx 2 \tag{1}$$

$$4 \le \frac{T_p}{T} \le 6 \tag{2}$$

where: T—the period between inspections, T_p—the $MTTF$ of system elements, h—the mean delay time value.

System with parallel reliability structure may be inspected even at longer time intervals because of its higher resistance to single element failures ($E(h)/T \approx 1$).

Figure 3 shows the example of the economic results of analysed system depending on the expected value $E(h)$ and the length of the period T. The presented analysis results for "*1- out-of t 3*" reliability structure (the parallel reliability structure) are indicated as bright markers and for "*3*-out-of-*3*" reliability structure (serial reliability structure)—as dark markers. The relationship given by Eq. (1) is presented in Figure 3 as an additional line, near which are the best solutions for the economic and availability criteria and analysed expected values $E(h)$.

The results presented in the Figure show that "nearly optimal" period between inspections of the series system performed according to BIP strategy should be determined on the basis of information about the expected value of the delay time. The expected maintenance costs of system C_{BI} reaches a minimum at the values of the $E(h)/T \approx 2$ for technical system performing in series reliability structure. The optimal values of costs C_{BI} for the system operating in parallel reliability structure are observed for the smaller value of the relationship $E(h)/T$. In the case, where $E(h)/T >> 2$, maintenance costs are still low what is connected with the "safe" maintenance variant including frequent system elements inspections performance.

For more information we recommend reading e.g. ((Jodejko-Pietruczuk and Werbińska-Wojciechowska 2014a, 2014b, 2012a, 2012b).

3.3.2 *Imperfect inspection case*

To complete the research analysis, there should be investigated case of imperfect inspection performance. For this purpose, *Inspection precision* is understood as the ability of system to detect (and correctly interpret) its elements' defects during inspection if their symptoms may be observable. This ability is given by p factor describing the probability that an element defect will not be noticed by maintenance service. The greater value of p means more difficult diagnosis of a real state of system during Inspection (Jodejko-Pietruczuk and Werbińska-Wojciechowska 2012c).

To analyze how the expressions (1) and (2) should be changed when inspection becomes less precise, additional assumption has been made to the system. Any component's defect, which occurred in the system till the moment of inspection, will be unnoticed with probability p or correctly identified with probability 1-p. All elements with identified defects will be replaced within the inspection period. The performance of the investigated system with additional assumptions, is illustrated in Figure 4.

The system in the Figure 4 is inspected at t_{PM} moments. Diagnosis of defect symptoms is imperfect thus elements 2 and 7 are allowed to further work although their defects might be noticed. Because of the fact, during one of following periods between inspections (t_{PM1}–t_{PM2}) two consecutive

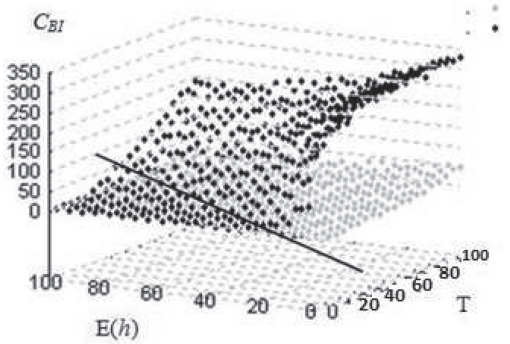


Figure 3. The total cost C_{BI} for various relations $E(h)/T$ (for $c_c = 10\,000$).

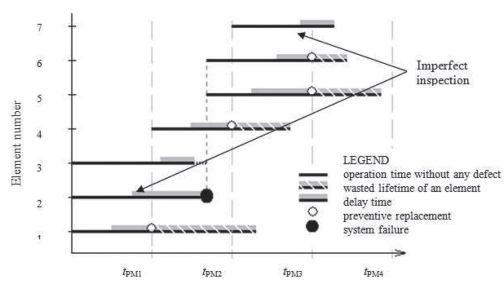


Figure 4. Idea of the block inspection policy with imperfect inspection (2-out-of-3 reliability structure).

elements fail what causes a system failure. On the other hand, some elements' defects are properly diagnosed at the first possible inspection (elements: 1,4,5,6) and the components are preventively replaced but their potential lifetime is wasted.

Figures 5 and 6 present chosen BI results obtained for various levels of inspection imprecision p and various lengths of period T in relation to mean element's lifetime (T_p/T) and to mean delay time (h/T), presented for two system's reliability structures. To save the space of the paper, the outcomes are presented at the same time as the function of p, T_p/T, h/T.

Presented in Figure 6 cost results are unequivocal for the analyzed series reliability structured system—the period between inspections set according to Eq. (1) and (2) generates low system costs when inspection is perfect. When diagnosis becomes less reliable (higher p value) the system should be inspected much more often ($T_p/T > 4$, $h/T > 2$) but explicit optimum T cannot be specified for any level of p. The result is the effect of significant role of the system failure consequence cost in the total cost of the maintained system and makes profitable

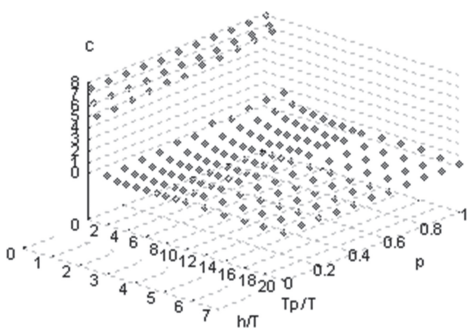


Figure 5. The total costs of the parallel system for various levels of inspection precision p, relations T_p/T and h/T.

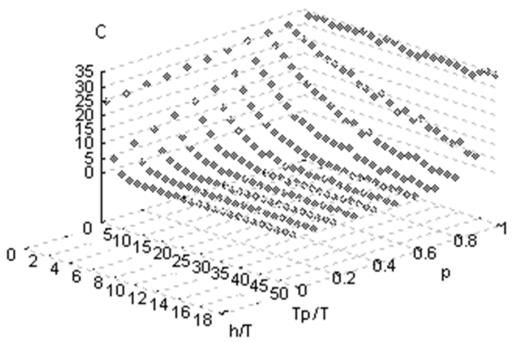


Figure 6. The total costs of the series system for various levels of inspection precision p, relations T_p/T and h/T.

every maintenance strategy with no system failure. The same effect of higher (but comparable) profitability of shorter periods T, is observable in *1-out-of-3* system (parallel) but for lower values of T_p/T and h/T. Thus one cannot to precisely determine explicit optimum relation of period T to elements' lifetime or delay time.

For more information we recommend reading (Jodejko-Pietruczuk et al. 2013b, Jodejko-Pietruczuk and Werbińska-Wojciechowska 2012c), where also the optimization analysis, bases on simulation model use, was made.

3.4 *Optimization of T parameter*

To provide a comprehensive optimization of time period T, the analytical model was developed (for the case of perfect inspection). Taking into account the additional assumption, that inspection action performance begins the new maintenance cycle for the analyzed system, the expected costs of n-element system maintenance in one inspection cycle are defined (Jodejko-Pietruczuk and Werbińska-Wojciechowska, in press):

$$C(T_i) = C(t_{i-1}, t_i) = \frac{c_f F(t_i) + c_r\left(1 - F(t_i)\right)\left(\sum_{j=1}^{n} G_j(t_i)\right) + c_i\left(1 - F(t_i)\right)}{\prod_{j=1}^{n}\left(1 - G_j(t_{i-1})\right)} \tag{3}$$

The formulae may be used under the condition that all the system elements were as good as new at the beginning of the cycle. When system performs in a series reliability structure, there is a possibility to define the *C.d.f.* of time to failure, $F(x)$, as the convolution of u and h such that $u + h \leq x$ (Jodejko-Pietruczuk and Werbińska-Wojciechowska, in press):

$$F(x) = 1 - \prod_{j=1}^{n}\left[1 - \int_{u=0}^{x} g_j(u) F_{h_j}(x-u)du\right] \tag{4}$$

When the system elements work in a parallel reliability structure, the *C.d.f.* of time to failure, $F(x)$, given by the formulae (4) may be estimated as (Jodejko-Pietruczuk and Werbińska-Wojciechowska, in press):

$$F(x) = \prod_{j=1}^{n}\int_{u=0}^{x} g_j(u) F_{h_j}(x-u)du \tag{5}$$

The strong convergence of simulation and analytical results of the presented maintenance model was investigated in (Jodejko-Pietruczuk and Werbińska-Wojciechowska, in press). Both the models, simulation and analytical one yield the

same results, what may be the foundation to confirm their correctness. This conclusion gives the possibility to define the optimum (or at list good) period between two consecutive system inspections, which may be determined on the base of minimization of the difference of the failure and elements' replacement costs:

$$K = CF - CE \tag{6}$$

The plot of the K value in the function of period between inspections (T) for various *k-out-of-n* systems is presented in the Figure 7.

The results presented in the Figure 7 shows different optimum periods between inspections for *k-out-of-n* system, dependently on the k value. When system is liable to every component failures (3-*out-of-* 3), it should be inspected much more often than systems being more resistant for elements' unreliability ($k < 3$). The presented effect exemplifies the usability of the analytical maintenance model for the general case of system with *k-out-of-n* reliability structure.

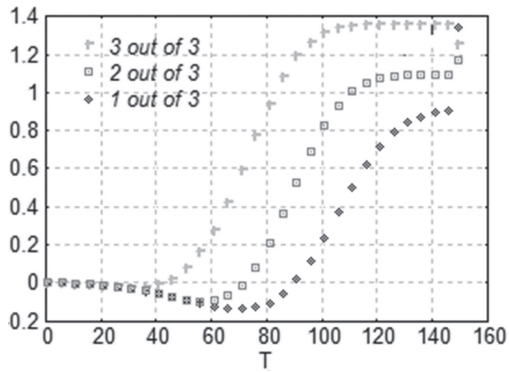


Figure 7. Function K according to Eq. (6) (for the case: $c_r = 5$, $c_i = 1$, and $c_f = 100$).

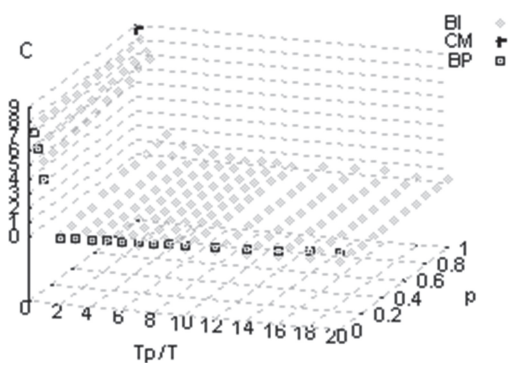


Figure 8. The total costs of the parallel system for BI, CM, BP maintenance policies.

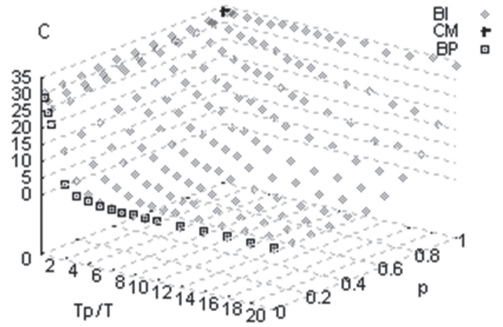


Figure 9. The total costs of the series system for BI, CM, BP maintenance policies.

4 CONCLUSIONS

The discussed issues give the possibility to obtain some rules for definition of the principal relations between the system performance under given PM policy with perfect/imperfect maintenance and chosen PM policy parameters.

The obtained analysis results indicate that the cost-effectiveness of maintenance policy implementation depends on the lengths of T time period and delay time period h. Taking into account these facts together and earlier performed analyses, there can be stated a conclusion that the best results of the BI maintenance policy may be achieved when the period between inspections T is shorter than the system elements' $MTTF$ and their mean delay time h.

To summarize the presented research work, there could be made answer the question if the BI maintenance policy is more profitable in comparison to other maintenance policies when its inspection precision drops. For this reason the system has been tested assuming BI policy, corrective maintenance policy (CM) ($T \to \infty$) and BP policy ($h_i = T_{pi}$, $p = 0$). The chosen results are presented in Figures 8 and 9.

As one can see, the results show some general rules valid for the modelled system:

- the corrective maintenance policy is the worst of all the analysed policies.
- cost results of the BP policy obtained in the research are better than BI effects (or mostly the same) for every tested case of inspection precision. Such a situation happens because preventive replacement of all system elements ensures the lowest consequence cost, which is the dominant cost component. Another relation of new element and system failure costs may make the BI policy more profitable in comparison to the BP policy.

REFERENCES

Abdel-Hameed, M. (1995). Inspection, maintenance and replacement model. *Computers and Operations Research* 22(4): 435–441.

Akbarov, A., Christer, A.H., Wang, W. (2008). Problem identification in maintenance modelling: a case study. *International Journal of Production Research* 46(4): 1031–1046.

Alfares, H. (1999). A simulation model for determining inspection frequency. *Computers and Industrial Engineering* 36: 685–696.

Alzubaidi, H.J. (1993). *Maintenance modelling of a major hospital complex*. PhD thesis, University of Salford, Salford.

Andrawus, J.A., Watson, J., Kishk, M. (2007). Wind turbine maintenance optimization: principles of quantitative maintenance optimization. *International Journal of Wind Engineering* 31(2): 101–110.

Babiarz, B. (2006). An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping* 83(4): 230–235.

Bajda, A., Wrażeń, M., Laskowski, D. (2011). Diagnostics the quality of data transfer in the management of crisis situation. *Electrical Review* 87(9 A): 72–78.

Baker, R.D., Christer, A.H. (1994). Review of delay-time OR modelling of engineering aspects of maintenance. *European Journal of Operational Research* 73: 407–422.

Baohe, S. (2002). An optimal inspection and diagnosis policy for a multi-mode system. *Reliability Engineering and System Safety* 76: 181–188.

Barlow, R.E., Hunter, L., Proschan, F. (1963). Optimum checking procedures. *Journal of the Operational Research Society* 47(8): 1037–1045.

Barrade, M.D., Scarf, P.A., Cavalcante, C.A.V., Dwight, R.A. (2013). Imperfect inspection and replacement of a system with a defective state: A cost and reliability analysis. *Reliability Engineering and System Safety* 120: 80–87.

Bojda, K., Dziaduch, I., Nowakowski, T., Werbińska-Wojciechowska, S. (2014). Decision support system for means of transport maintenance processes performance: a case study of rail buses. *Safety, reliability and risk analysis: beyond the horizon: proc. of the European Safety and Reliability Conference, ESREL 2013, Amsterdam, The Netherlands, 29 September–2 October 2013.* Leiden: CRC Press/Balkema: 909–919.

Cai, J., Zhu, L. (2011). A delay-time model with imperfect inspection for aircraft structure subject to a finite time horizon. *Proc. of IEEE International Conference on Grey Systems and Intelligent Services 2011. 15–8 Sept. 2011, Nanjing, China*.

Chilcott, J.B., Christer, A.H. (1991). Modelling of condition based maintenance at the coal face. *International Journal of Production Economics* 22: 1–11.

Christer, A.H. (2002). A Review of Delay Time Analysis for Modelling Plant Maintenance. in: *Stochastic Models in Reliability and Maintenance*, Osaki S. (ed.), Springer.

Christer, A.H. (1999). Developments in delay time analysis for modelling plant maintenance. *Journal of the Operational Research Society* 50: 1120–1137.

Christer, A.H. (1987). Delay-time model of reliability of equipment subject to inspection monitoring. *Journal of the Operational Research Society* 38(4): 329–334.

Christer, A.H. (1982). Modelling inspection policies for building maintenance. *Journal of the Operational Research Society* 33: 723–732.

Christer, A.H., Redmond, D.F. (1992). Revising models of maintenance and inspection. *International Journal of Production Economics* 24: 227–234.

Christer, A.H., Redmond, D.F. (1990). A recent mathematical development in maintenance theory. *IMA Journal of Mathematics Applied in Business and Industry* 2: 97–108.

Christer, A.H., Scarf, P.A. (1994). A robust replacement model with applications to medical equipment. *Journal of the Operational Research Society* 45(3): 261–275.

Christer, A.H., Waller, W.M. (1987). A Descriptive model of capital plant replacement, *Journal of the Operational Research Society* 38, 6: 473–477.

Christer, A.H., Waller, W.M. (1984a). Reducing production downtime using delay-time analysis. *Journal of the Operational Research Society* 35(6): 499–512.

Christer, A.H., Waller, W.M. (1984b). Delay Time Models of Industrial Inspection Maintenance Problems. *Journal of the Operational Research Society* 35(5): 401–406.

Christer, A.H., Waller, W.M. (1984c). Reducing production downtime using delay-time analysis. *Journal of the Operational Research Society* 35(6): 499–512.

Christer, A.H., Wang, W. (1995). A delay-time-based maintenance model of a multi-component system. *IMA Journal of Mathematics Applied in Business & Industry* 6: 205–222.

Christer, A.H., Whitelaw, J. (1983). An operational research approach to breakdown maintenance: problem recognition. *Journal of the Operational Research Society* 34(11): 1041–1052.

Cui, X. (2002). *Delay time modeling and software development*. PhD thesis, University of Salford, Salford.

Cui, L., Xie, M., Han-Tong L. (2004). Inspection schemes for general systems. *IEE Transactions* 36: 817–825.

Cunningham, A., Wang, W., Zio, E., Allanson, D., Wal, l.A., Wang, J. (2011). Application of Delay-time Analysis via Monte Carlo Simulation. *Journal of Marine Engineering and Technology* 10(3): 57–72.

Dekker, R., Scarf, P.A. (1998). On the impact of optimisation models in maintenance decision making: the state of the art. *Reliability Engineering and System Safety* 60: 111–119.

Desa, M.I., Christer, A.H. (2001). Modelling in the absence of data: a case study of fleet maintenance in a developing country. *Journal of the Operational Research Society* 52: 247–260.

Duffuaa, S.O., El-Ga'aly, A. (2013). A multi-objective mathematical optimization model for process targeting using 100% inspection policy. *Applied Mathematical Modelling* 37: 1545–1552.

Durango-Cohen, P.L., Madanat, S.M. (2008). Optimization of inspection and maintenance decisions for infrastructure facilities under performance model uncertainty: A quasi-Bayes approach. *Transportation Research Part A* 42: 1074–1085.

Golmakani, H.R., Moakedi, H. (2012). Periodic inspection optimization model for a two-component repairable system with failure interaction. *Computers and Industrial Engineering* 63(3): 540–545.

Hassounah, M.I. (1990). An optimal vehicle fleet inspection schedule. *Journal of Operational Research Society* 41(9): 791–799.

Jalali Naini, S.G., Aryanezhad, M.B., Jabbarzadeh, A., Babei, H. (2009). Condition based maintenance for two-component systems with reliability and cost considerations. *International Journal of Industrial Engineering & Production Research* 20(3): 107–116.

Jardine, A.K.S., Hassounah, M.I. (1990). An optimal vehicle-fleet inspection schedule. *Journal of the Operational Research Society* 41(9): 791–799.

Jodejko-Pietruczuk, A., Nowakowski, T., Werbińska-Wojciechowska, S. (2013a). Time between inspections optimization for technical object with time delay. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* vol. 4, nr 1: 35–41.

Jodejko-Pietruczuk, A., Nowakowski, T., Werbińska-Wojciechowska, S. (2013b). Block inspection policy model with imperfect inspections for multi-unit systems. *Reliability: Theory & Applications* 8(3): 75–86.

Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. (in press). Expected maintenance costs model for time-delayed technical systems in various reliability structures. Article accepted for publication in Proc. of The Probabilistic Safety Assessment & Management conference PSAM 12, 22–27 June 2014, Honolulu, Hawaii, USA.

Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. (2014a). Analysis of maintenance models' parameters estimation for technical systems with delay time. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 16(2): 288–294.

Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. (2014b). Block Inspection policy for non-series technical objects. *Proc. of the European Safety and Reliability Conference, ESREL 2013, Amsterdam*, *The Netherlands, 29 September–2 October 2013*. Leiden: CRC Press/Balkema: 889–898.

Jodejko-Pietruczuk, A. & Werbińska-Wojciechowska, S. (2012a). Economical effectiveness of Delay Time approach using in Time-Based maintenance modelling. *Proc. of PSAM 11 & ESREL 2012 Conference,* 25–29 *June 2012, Helsinki, Finland*.

Jodejko-Pietruczuk A. & Werbińska-Wojciechowska, S. (2012b). Analysis of Block-Inspection Policy parameters from economical and availability point of view. *Proc. of PSAM 11 & ESREL 2012 Conference, 25–29 June 2012, Helsinki, Finland*.

Jodejko-Pietruczuk A. & Werbińska-Wojciechowska, S. (2012c). A delay-time model with imperfect inspections for multi-unit systems. *Journal of KONBiN* 3: 157–172.

Jones, B., Jenkinson, I., Yang, Z., Wang, J. (2010). The use of Bayesian network modelling for maintenance planning in a manufacturing industry. *Reliability Engineering and System Safety* 95: 267–277.

Jones, B., Jenkinson, I., Wang, J. (2009). Methodology of using delay-time analysis for a manufacturing industry. *Reliability Engineering and System Safety* 94: 111–124.

Kaio, N., Osaki, S. (1988). Inspection policies: comparisons and modifications. *Revue Francaise d'Automatique, d'Informatique et de Recherche Operationnelle. Recherche Operationnelle* 22(4): 387–400.

Kenzin, M., Frostig, E. (2009). M out of n inspected systems subject to shocks in random *environment. Reliability Engineering and System Safety* 94: 1322–1330.

Kierzkowski, A. (2010). Reliability models of transportation system of low cost airlines. *Reliability, risk and safety: back to the future.* eds. Ale, B.J.M., Papazoglou, J.A., Zio E., Raton, B.: CRC Press: 1325–1329.

Kierzkowski, A., Kowalski, M., Magott, J., Nowakowski, T. (2012). Maintenance process optimization for low-cost airlines. *Proc. of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, Helsinki, Finland, 25–29 June 2012*.

Kierzkowski, A., Zajac, M. (2012). Analysis of the reliability discrepancy in container transshipment. *Proc. of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012,* PSAM11 ESREL 2012, Helsinki, Finland, 25–29 June 2012.

Laskowski, D., Bylak, M. (2013). Efficient diagnostics encoding mechanism for wireless networks. *Electrical Review* 89(9): 133–138.

Lee, Ch. (1999). *Applications of Delay Time Theory to Maintenance Practice of Complex Plant*. PhD thesis, University of Salford, Salford.

Leung, F., Kit-leung, M. (1996). Using delay-time analysis to study the maintenance problem of gearboxes. *International Journal of Operations & Production Management* 16(12): 98–105.

Luss, H. (1983). An inspection policy model for production facilities. *Management Science* 29(9): 1102–1109.

Mazzuchi, T.A., van Noortwijk, J.M., Kallen, M.J. (2007). *Maintenance optimization,* Technical Report, TR-2007-9.

Młyńczak M., Nowakowski, T., Werbińska-Wojciechowska, S. (2014). Technical systems maintenance models classification (in Polish). *Proc. of XLII Winter School of Reliability, 12–18 January, 2014,* Szczyrk, Poland.

Nowakowski, T., Werbińska-Wojciechowska, S. (2012). Developments of time dependencies modeling concepts, Advances in safety, reliability and risk management. *Proc. of the European Safety and Reliability Conference, ESREL 2011*, Troyes, France, 18–22 September 2011. eds. Bérenguer Ch., Grall A., Guedes Soares C., Leiden: CRC Press/Balkema: 832–838.

Nowakowski, T., Werbińka, S. (2009). On problems of multicomponent system maintenance modeling. *International Journal of Automation and Computing* 6(4): 364–378.

Onoufriou, T., Frangopol, D.M. (2002). Reliability-based inspection optimization of complex structures: a brief retrospective. *Computers an Structures* 80: 1133–1144.

Ozekici, S. (ed.). (1996). *Reliability and Maintenance of Complex Systems*. NATO ASI Series, Series F: Computer and Systems Sciences, Vol. 154, Springer.

Pillay, A., Wang, J., Wall, A.D., Ruxton, T. (2001). A maintenance study of fishing vessel equipment using delay-time analysis. *Journal of Quality in Maintenance Engineering* 7(2): 118–127.

Podofillini, L., Zio, E., Vatn, J. (2006). Risk-informed optimization of railway tracks inspection and maintenance procedures. *Reliability Engineering and System Safety* 91: 20–35.

Ramirez-Marquez, J.E. (2008). Port-of-entry safety via the reliability optimization of container inspection strategy through an evolutionary approach. *Reliability Engineering and System Safety* 93: 1698–1709.

Redmond, D.F. (1997). *Delay Time Analysis in Maintenance*. PhD thesis, University of Salford, Salford.

Scarf, P.A., Bouamra, O. (1995). On the application of a capital replacement model for a mixed fleet. *IMA Journal of Mathematics Applied in Business & Industry* 6: 39–52.

Sherif, Y.S. (1982). Reliability analysis: optimal inspection and maintenance schedules of failing systems. *Microelectronics Reliability* 22(1):59–115.

Thomas, L.C. (1986). A survey of maintenance and replacement models for maintainability and reliability of multi-item systems. *Reliability Engineering* 16: 297–309.

Vaghefi, A., Sarhangian, V. (2009). Contribution of simulation to the optimization of inspection plans for multistage manufacturing systems. *Computers and Industrial Engineering* 57: 1226–1234.

Valdez-Flores, C., Feldman, R. (1989). A survey of preventive maintenance models for stochastically deteriorating single-unit systems. *Naval Research Logistics* 36: 419–446.

Valis, D., Vintr, Z. (2006). Vehicle Maintenance Process Optimisation Using Life Cycle Costs Data and Reliability-Centred Maintenance. In: *Proceedings of the First International Conference on Maintenance Engineering. Beijing*: Science Press, 2006.

Vintr, Z., Valis, D. (2012). A Tool for Decision Making in k-out-of-n System Maintenance. In: *Applied Mechanics and Materials* Vol.: 110–116: 5257–5264.

Wang, W. (2012). An overview of the recent advances in delay-time-based maintenance modelling. *Reliability Engineering and System Safety*106: 165–178.

Wang, W. (2010). Modeling planned maintenance with non-homogeneous defect arrivals and variable probability of defect identification. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 2: 73–78.

Wang, W. (2009). *Delay time modelling for optimized inspection intervals of production plant*. In: Handbook of Maintenance Management and Engineering. Ben-Daya, M., Duffuaa, S.O., Raouf, A., Knezevic, J., Ait-Kadi, D. (eds.). Springer, London.

Wang, W. (2003). A delay time based approach for risk analysis of maintenance activities. *The Journal of the Safety and Reliability Society* 23(1): 103–113.

Wang, W. (2000). A model of multiple nested inspections at different intervals. *Computers & Operations Research* 27: 539–558.

Wang, W. (1992). *Modelling condition monitoring inspection using the delay-time concept*. PhD thesis. Univ. of Salford, U.K.

Wang, W., Carr, M.J., Chow, T.W.S. (2012). A two-level inspection model with technological insertions. *IEEE Transactions on Reliability* 61(2): 479–490.

Wang, W., Christer, A.H. (2003). Solution algorithms for a nonhomogeneous multi-component inspection model. *Computers & Operations Research* 30: 19–34.

Werbińska-Wojciechowska, S. (2014). Maintenance models of multi-element technical systems—state of art (in Polish). *Proc. of XLII Winter School of Reliability, 12–18 January, 2014*, Szczyrk, Poland.

Yun, W.Y., Nakagawa, T. (2010). Replacement and inspection policies for products with random life cycle. *Reliability Engineering and System Safety* 95: 161–165.

Zequeira, R.I., Berenguer, Ch. (2005). On the inspection policy of a two-component parallel system with failure interaction. *Reliability Engineering and System Safety* 88: 99–107.

Zhao, J., Chan, A.H.C., Roberts, C., Madelin, K.B. (2007). Reliability evaluation and optimization of imperfect inspections for a component with multi-defect. *Reliability Engineering and System Safety* 92: 65–73.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Availability model of technical objects—block inspection policy implementation

A. Jodejko-Pietruczuk & S. Werbińska-Wojciechowska
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: In the presented paper, authors focus on development of mathematical delay-time model for single-unit technical systems liable to costly failure. Failure is taken here to mean a breakdown or catastrophic event, after which the system is unusable until repaired or replaced. Thus, the briefly literature review in the area of delay-time modelling is provided. Later the analytical model of expected system availability is investigated. Authors also discuss the sensitivity analysis of given simulation model. The directions for further research work are defined.

1 INTRODUCTION

One of the basic targets of maintenance services is to ensure the proper and uninterrupted performance of technical systems. This is of particular importance because any unforeseeable and unreasonable disruption of a technical system performance may entail huge costs associated with e.g. the interruption of production or the occurrence of catastrophic events (see e.g. (Babiarz 2006, Kierzkowski 2010, Kierzkowski et al. 2012, Kierzkowski and Zając 2012)). Unplanned downtime can be prevented through the use of appropriate maintenance strategies or diagnostics. Tasks are designed to forecasting upcoming moments of repair or replacement of wearing parts during their operation and to shorten the duration of taken maintenance processes (Valis and Vintr 2006, Vintr and Valis 2012).

The technical objects performance is strictly connected with aging process. The wear processes are the most common cause of damage (about 70–80% of all the occurred failures) in mechanical devices (Boda 1999, Ickiewicz and Ickiewicz 1998, Laskowski and Bylak 2013). One of the possible solutions aimed at improving operational processes is inspection policies applying. Moreover, authors focus on investigation of technique called delay time analysis, which has been developed for modeling the consequences of an inspection policy implementation for any systems (Christer 2002).

Most of the known in literature delay-time models regard to single-unit systems performance optimization issues (Frostig 2003, Valdez-Florez and Feldman 1989, Wang 2002). Moreover, widely investigated inspection models are dedicated for new elements maintenance performance (Jodejko-Pietruczuk et al. 2013). However, when assuming that the working element is not defected at the point of inspection maintenance time, the optimization model for time between next inspections performance is not investigated.

Following the above considerations, authors focus on the development of analytical maintenance model of single-unit technical objects with taking into account availability criteria. Thus, in the next Section, there is provided a briefly literature review in the investigated research area. This gives the possibility to present the maintenance model for the case of one-component system. Following this, in the next step, authors examine the sensitivity analysis of obtained model. The work ends up with summary and directions for further research.

In conclusion, this article is to be the continuation of consideration about mathematical modelling of technical objects with time delay maintenance. The analytical model with cost constraints is given in (Jodejko-Pietruczuk et al. 2013), the cases of multi-unit systems performing in different reliability structures are investigated in (Jodejko-Pietruczuk and Werbińska-Wojciechowska, in prep.).

2 BLOCK INSPECTION POLICY MODELLING—LITERATURE REVIEW

The delay-time concept is widely known in the literature since the 70 s. of XX century (Christer 2002). The literature review works strictly dedicated to the issues of DT modelling and implementations are given mostly in (Alzubaidi 1993, Baker and Christer 1994, Christer 2002, 1999, Christer and Redmond 1992, 1990, Lee 1999, Nowakowski and Werbińska-Wojciechowska 2012, Wang and Christer 2003, Wang 2012). There should be also

underlined the state of art work, in which delay-time models are presented along with other PM models (see e.g. (Cho and Parlar 1991, Dekker and Scarf 1998, Mazzuchi et al. 2007, Ozekici 2006, Thomas 1986, Valdez-Flores and Feldman, 1989)).

The known technical systems maintenance models which base on delay-time concept implementation can be divided into two main groups (Jodejko-Pietruczuk et al. 2013, Wang 2008):

- inspection models for single-unit or complex systems;
- inspection models for multi-unit systems.

The issues on maintenance modelling of single-unit and complex systems were reviewed e.g. in (Jodejko-Pietruczuk et al. 2013). The main problem investigated in this area regard to e.g. replacement decisions (see e.g. (Christer and Waller 1987)), or model parameter estimation issues (see e.g. (Baker and Wang 1992)). Moreover, there can also be found maintenance models for single-component systems under condition based maintenance (see e.g. (Christer and Wang 1992, Okumura 1997, Okumura et al. 1996)), and models dedicated to risk analysis implementation (see e.g. (Wang 2003)) or safety issues investigation (see e.g. (Wang and Christer 1997)).

3 DELAY-TIME MODEL FOR SINGLE-UNIT SYSTEM

In this Section, there is considered a delay-time model for a single-unit system. The performed maintenance policy bases on Block Inspection policy (*BI*) which assumes, that inspections take place at regular time intervals of T, and each requires a constant time. The inspections are assumed to be perfect. Thus, component defect which occurs in the system till the moment of inspection will be identified and replaced within the inspection period.

In the analysed system may be performed one of the two maintenance operations: failure repair or inspection together with replacement of element with defect. Moreover, the performance of the investigated system is also defined by the additional assumptions and notation:

- the system is a three state system where, over its service life, it can be either operating or down for necessary repair or planned maintenance,
- the system is renewed at either a failure repair or at a repair done at an inspection if a defect is identified,
- after either a failure renewal or inspection renewal the inspection process restarts,
- maintenance actions restores maintained components to as good as new condition,
- failures of the system are identified immediately and repairs or replacements are made as soon as possible,
- failure replacement, inspection replacement and inspection replacement require d_f, d_r and d_i time units respectively,
- time of defects occurrence defined by u is a random variable described by its probability distribution functions $g(u)$ and $G(u)$,
- the length of the delay time before element's failure is random and its probability distributions are given by $f_h(h)$ and $F_h(h)$.

Moreover, there is a possibility to define the *c.d.f.* of time to failure, $F(x)$, as the convolution of u and h such that $u + h \leq x$ (Redmond 1997):

$$F(x) = \int_{u=0}^{x} g(u)F_h(x-u)du \tag{1}$$

And the reliability, $R(x) = 1 - F(x)$.

For the presented above assumptions, in accordance with the literature concept of the delay time, known models assume that an inspected element is newly replaced at the beginning of the inspection period, e.g. the previous inspection exposed a defect of the element and caused a maintenance action.

Following this, there can be estimated e.g. the expected cost over each cycle $C(T)$, or expected downtime $E_d(T)$ of an inspection cycle of length T (see e.g. (Christer 1999). The examples of such the model implementation are given e.g. in (Redmond 1997, Wang 2008).

The cost and availability models given in the literature (see e.g. (Jodejko-Pietruczuk et al. 2013)) describes the first inspection cycle results, i.e. when a new element is run to work at the beginning of the cycle. On this base, one can choose the length of the cycle T, and thus—the moment of the first inspection, which yields the minimum expected costs per the cycle. However, not in every situation there is a possibility to define maintenance costs. Sometimes, more important is to optimize maintenance strategy parameters taking into account dependability constraints. Thus, the model for system availability ratio is investigated.

3.1 *Availability model of single unit system with delay time*

The availability results of a system with delay time, which is inspected periodically, depends upon the relations of basic time components, like system up time, time of inspection activities performance, preventive replacements and failure time. To estimate such the relation, one

needs to express the expected values of these time variables.

In the curse of the first inspection cycle the expected lifetime of the system may be expressed:

$$T_M(t_1) = \int_0^{t_1} x \int_0^x g(u) f_h(x-u)\, du dx + t_1 \cdot \int_{u=0}^{t_1} g(u)(1 - F_h(t_1 - u)) du \quad (2)$$

where:
$T_M(t_1)$—the expected lifetime of the system in the first inspection cycle,
t_1—the moment when the first inspection cycle ends.

The first component of the sum in the formulae (2) expresses possible moments of system failures, while the second part of the expression takes into consideration the probability that the system defect is observed in the time of the first inspection performance.

However, if we assume that an element may operate longer than to the first inspection, because the system does not reveal any symptoms of defects, the expected system lifetime should be expressed as follows:

$$T_M(t_{i+1}) = \left[\int_{t_i}^{t_{i+1}} x \int_0^x g(u) f_h(x-u) du dx + t_i \cdot \int_{u=0}^{t_i} g(u)(1 - F_h(t_i - u)) du \right] (1 - G(t_i)) \quad (3)$$

where:
$T_M(t_i)$—the expected lifetime of the system to the end of the i-th inspection cycle,
t_i—the moment when the i-th inspection ends.

The probability of a system failure in the inspection cycle between moments (t_i, t_{i+1}) depends on the fact that the previous inspection have not revealed any defect symptoms. Thus, the expected lifetime length has to be lowered by the probability of this fact $(1 - G(t_i))$.

The total expected length of the system up time in the curse of a single renew cycle (the time elapsing between two consecutive system replacements, independently on the replacement premise) may be estimated as the sum of expected lifetimes resulting from the sequence of inspection periods, when $t_i \to \infty$:

$$T_M(t_i) = T_M(t_1) + \sum_{i=2}^{\infty} T_M(t_i) \quad (4)$$

In practice, when we consider one-component system, the sum from equation (4) converges, when t is three times longer than the expected system lifetime, for the situation when there is no preventive action taken.

When one wants to estimate the expected time of inspection actions performance in a single renew cycle, the formulae (5) may be applied:

$$T_I(t_i) = d_i \cdot \sum_{i=1}^{\infty} (1 - G(t_{i-1}))(1 - F(t_i)) \quad (5)$$

where:
$T_I(t_i)$—the expected time of inspections carried out in the system during a single renew period,
d_i—the time of a single inspection actions.

A next inspection (i-th) may be taken depending on the probability of the two facts: that a previous inspection has not revealed defect occurrence and at the end of $(i-1)$-th inspection period the system is still reliable.

The estimation of the expected time of preventive replacement of the system in the course of a single renew period should base on the probability of defect occurrence at the end of an inspection cycle and lack of this defect at the moment of the previous inspection performance. The time should be calculated separately for every single inspection period and the sum of them expresses the total expected replacement time.

$$T_R(t_{i+1}) = d_r \cdot \sum_{i=1}^{\infty} (1 - G(t_i)) \left[\int_{u=0}^{t_i} g(u)(1 - F_h(t_i - u)) du \right] \quad (6)$$

where:
$T_R(t_i)$—the expected preventive replacement time of the system to the end of the i-th inspection cycle,
d_r—the time of a preventive replacement of the system.

The last time component, which should be estimated to assess the system availability ratio, is the expected failure time in a single renew cycle. The time depends on the failure probability in a given inspection period, assuming that at the moment of a previous inspection performance any defect has not been detected. It lays the foundation to define the following equation:

$$T_F(t_{i+1}) = d_f \cdot \sum_{i=1}^{\infty} \left(1 - G(t_i)\right)\left(F(t_{i+1}) - F(t_i)\right) \quad (7)$$

where:
$T_F(t_i)$—the expected failure replacement time of the system to the end of the i-th inspection cycle,
d_f—the time of a corrective replacement of the system.

The calculated time values of: inspections, preventive and corrective replacement in the curse of a single renew period $(t_i \to \infty)$ allows to estimate

the availability ratio for the cycle, according to the well know formulae:

$$A = \frac{T_{M(t_i)}}{T_{M(t_i)} + T_{I(t_i)} + T_{F(t_i)} + T_{R(t_i)}} \tag{8}$$

where:
A—the availability ratio of the system for a single renew period.

3.2 *Sensitivity analysis of developed availability model for single-unit case*

In this Section, there is presented the short sensitivity analysis of the model developed above. The objective of given analysis was to investigate what is the influence of given model basic time components on the system availability ratio level. To provide the analysis, there have been assumed main model parameters (Table 1).

First, the Figure 1 depicts the expected time components in a single renew cycle for the chosen range of T (length of a single inspection cycle). It presents the relation between expected times and the length of the inspection period T. The mean time to failure of the tested system has been c.a. $MTTF \approx 100$ (units of time), thus the range of T has been set based on this system parameter estimation.

Table 1. The parameters of the tested availability model.

Parameter	Value
d_i	1
d_r	10
d_f	100
$G(u)$	Weibull distribution with $\alpha = 3.5$, $\beta = 65$
$F_h(x)$	Weibull distribution with $\alpha = 3.5$, $\beta = 35$

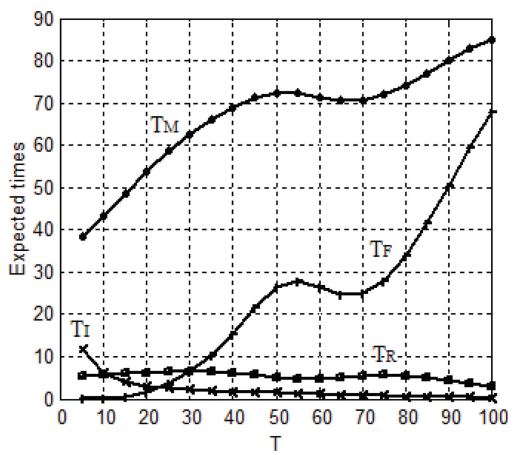


Figure 1. Expected system lifetime and times of inspection, preventive and corrective replacements per a single renew cycle.

During the analysis of results presented in the Figure 1, one might notice that the longer periods between inspections (T), the longer system lifetime (T_M) and failure time (T_F). On the other hand, when the inspection period approaches to the mean time to the defect occurrence (mean time to defect occurrence $MTTD \approx 67$), the expected lifetime as well as the failure time drops for some segment of the tested range of T. This interesting effect results from the fact, that during inspection action performance a defect may be noticed, and the system is preventively replaced. Thus, its lifetime is usually limited to the value of the length of the inspection period and the system is not allowed to start work in a next inspection cycle. The same observable effect in the Figure 1 pertains to the failure time. When the defect is revealed in the time of an inspection, element is preventively replaced, new element starts its lifetime and the probability of a system failure decreases.

On the other hand, when one examines the expected time of preventive replacements, the minimum values are visible at the segment of the tested range of T, lower than $MTTD$ ($T \in (50, 65)$). The same values of T yield the local maximum of the expected failure time T_F. When an inspection action is performed just a moment before a defect will occur, the system is allowed to start a new inspection cycle and the probability of failure occurrence the next inspection cycle increases.

Basing on the presented calculations, the system availability ratio has been estimated and presented in the Figure 2.

The availability ratio reaches its maximum values ($A \approx 0{,}8$) for $T \approx 30$ [units of time]. The location

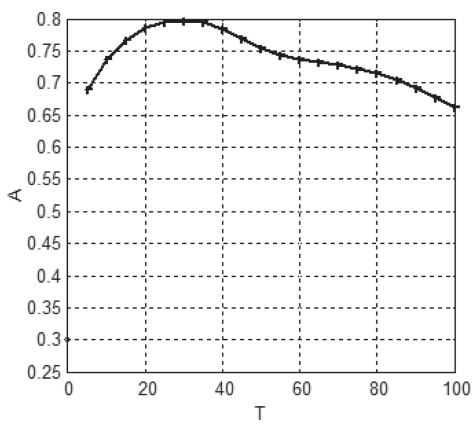


Figure 2. System availability ratio for a single renew cycle.

of the maximum value of the availability ratio may result from the relation of T and $MTTD$ ($MTTD/T \approx 2$) or from the mean time since defect occurs to a failure moment $T \approx (MTTF - MTTD)$. The results obtained for another parameter values of the system are presented in the Figures 3 and 4.

The results, illustrated in the Figure 3, has been obtained for failure replacement times (d_f) extended ten times in comparison to the one, presented in the Table 1. The availability ratio has been reduced for the whole range of the tested values of T and the optimum point has also shifted toward lower values of inspection lengths (T). When failure consequences becomes more severe, one try to reduce the consequence probability. Thus, the system should be inspected more often in order to reveal the defect as soon as it may be visible.

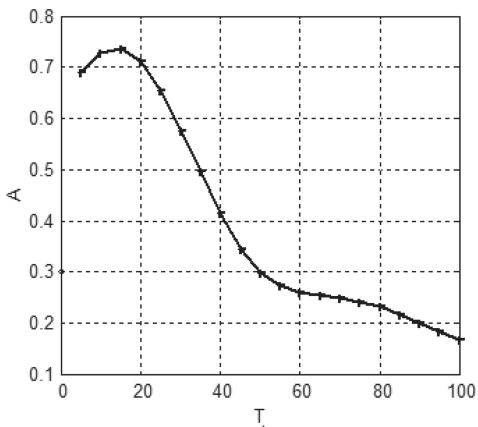


Figure 3. System availability ratio for a single renew cycle and $d_f = 1000$.

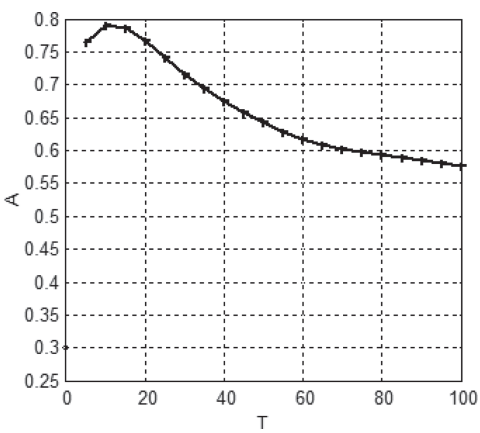


Figure 4. System availability ratio for a single renew cycle and $T \approx MTTF - MTTD \approx 15$.

Figure 4 depicts the availability ratio obtained for the situation, when the mean time of defect occurrence has been reduced ($MTTF - MTTD \approx 15$). It means that the periods of system up time without any defect signals are relatively much longer than the period when the signal may be noticed. Inspections have to be done more frequently in order to complete preventive actions as often as possible. Due to the availability level of the system with delay time, the most profitable solution is to choose the inspection cycle length very closed to the value of $T \approx (MTTF - MTTD)$, the time between the moments of defect and failure occurrence $\approx (MTTF - MTTD)$.

4 CONCLUSIONS

In the area of technical systems maintenance modelling with the use of DT concept, the main task is to optimize the length of time between successive inspection actions performance. In the presented article, this problem is solved by developing an analytical model of the expected availability ratio for single-component case. The authors are continuing their research on the mathematical modeling with the use of DT approach for technical systems presented e.g. in (Jodejko-Pietruczuk and Werbińska-Wojciechowska 2014, Jodejko-Pietruczuk et al. 2013).

Following this, in the next step, authors plan to develop the availability model for the case of multi-element system with delay time. This will complete the research work of authors connected with maintenance analytical modelling for technical systems with time delay.

REFERENCES

Alzubaidi, H.J. 1993. *Maintenance modelling of a major hospital complex*. PhD thesis, University of Salford, Salford.

Babiarz, B. 2006. An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping* 83(4): 230–235.

Baker, R.D., Christer, A.H. 1994. Review of delay-time OR modelling of engineering aspects of maintenance. *European Journal of Operational Research* 73: 407–422.

Baker, R.D., Wang, W. 1992. Estimating the delay-time distribution of faults in repairable machinery from failure data. *IMA Journal of Mathematics Applied in Business & Industry* 3: 259–281.

Boda, A. 1999. Forecasting of failures occurrence for technical object with wearing process (in Polish). *Proc. of XXVII Winter School of Reliability,* vol. 2, Szczyrk.

Cho, I.D., Parlar, M. 1991. A survey of maintenance models for multi-unit systems. *European Journal of Operational Research* 51: 1–23.

Christer, A.H. 2002. A Review of Delay Time Analysis for Modelling Plant Maintenance. in: *Stochastic Models in Reliability and Maintenance*, Osaki S. (ed.), Springer.

Christer, A.H. 1999. Developments in delay time analysis for modelling plant maintenance. *Journal of the Operational Research Society* 50: 1120–1137.

Christer, A.H., Redmond, D.F. 1992. Revising models of maintenance and inspection. *International Journal of Production Economics* 24: 227–234.

Christer, A.H., Redmond, D.F. 1990. A recent mathematical development in maintenance theory. *IMA Journal of Mathematics Applied in Business and Industry* 2: 97–108.

Christer, A.H., Waller, W.M. 1987. A Descriptive model of capital plant replacement, *Journal of the Operational Research Society* 38, 6: 473–477.

Christer, A.H., Wang, W. 1992. A model of condition monitoring of a production plant. *International Journal of Production Research* 30, 9: 2199–2211.

Dekker, R., Scarf, P.A. 1998. On the impact of optimisation models in maintenance decision making: the state of the art. *Reliability Engineering and System Safety* 60: 111–119.

Frostig, E. 2003. Comparison of maintenance policies with monotone failure rate distributions. *Applied Stochastic Models in Business and Industry* 19: 51–65.

Ickiewicz, J, Ickiewicz, I. 1998. Hydraulic sensitivity to contamination of hydraulic fluids (in Polish). *Proc. of XXVI Winter School of Reliability*, Szczyrk.

Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. in prep. Expected maintenance costs model for time-delayed technical systems in various reliability structures. Article accepted for publication in *Proc. of Probabilistic Safety and Assessment and Management PSAM 12, 22–27 June, 2014, Honolulu, Hawaii, USA*.

Jodejko-Pietruczuk, A., Werbińska-Wojciechowska, S. 2014. *Model of expected maintenance costs for multi-unit systems with time delay* (in Polish). Proc. of XLII Winter School of Reliability, Szczyrk, 12–18 January 2014. Warsaw: Warsaw University of Technology.

Jodejko-Pietruczuk, A., Nowakowski, T., Werbińska-Wojciechowska, S. 2013. Time between inspections optimization for technical object with time delay. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* vol. 4, nr 1: 35–41.

Kierzkowski, A. 2010. Reliability models of transportation system of low cost airlines. *Reliability, risk and safety: back to the future.* eds. Ale, B.J.M., Papazoglou, J.A., Zio E., Raton, B.: CRC Press: 1325–1329.

Kierzkowski, A., Kowalski, M., Magott, J., Nowakowski, T. 2012. Maintenance process optimization for low-cost airlines. *Proc. of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, Helsinki, Finland, 25–29 June 2012.*

Kierzkowski, A., Zajac, M. 2012. Analysis of the reliability discrepancy in container transshipment. *Proc. of 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, Helsinki, Finland, 25–29 June 2012.*

Laskowski, D., Bylak, M. 2013. Efficient diagnostics encoding mechanism for wireless networks. *Electrical Review* 89(9): 133–138.

Lee, Ch. 1999. *Applications of Delay Time Theory to Maintenance Practice of Complex Plant.* PhD thesis, University of Salford, Salford.

Mazzuchi, T.A., van Noortwijk, J.M., Kallen, M.J. 2007. *Maintenance optimization,* Technical Report, TR-2007-9.

Nowakowski, T., Werbińska-Wojciechowska, S. 2012. Developments of time dependencies modelling concepts, Advances in safety, reliability and risk management. *Proc. of the European Safety and Reliability Conference, ESREL 2011*, Troyes, France, 18–22 September 2011/ eds. Bérenguer Ch., Grall A., Guedes Soares C., Leiden: CRC Press/Balkema: 832–838.

Okumura, S. 1997. An Inspection Policy for Deteriorating Processes Using Delay-Time Concept. *International Transactions in Operational Research* 4, 5–6: 365–375.

Okumura, S., Jardine, A.K.S., Yamashina, H. 1996. An inspection policy for a deteriorating single-unit system characterized by a delay-time model. *International Journal of Production Research* 34, 9: 2441–2460.

Ozekici, S. (ed.). 1996. *Reliability and Maintenance of Complex Systems*. NATO ASI Series, Series F: Computer and Systems Sciences, Vol. 154, Springer.

Redmond, D.F. 1997. *Delay Time Analysis in Maintenance*. PhD thesis, University of Salford, Salford.

Thomas, L.C. 1986. A survey of maintenance and replacement models for maintainability and reliability of multi-item systems. *Reliability Engineering* 16: 297–309.

Valdez-Flores, C., Feldman, R. 1989. A survey of preventive maintenance models for stochastically deteriorating single-unit systems. *Naval Research Logistics* 36: 419–446.

Valis, D., Vintr, Z. (2006). Vehicle Maintenance Process Optimisation Using Life Cycle Costs Data and Reliability-Centred Maintenance. In: *Proceedings of the First International Conference on Maintenance Engineering. Beijing*: Science Press, 2006.

Vintr, Z., Valis, D. (2012). A Tool for Decision Making in k-out-of-n System Maintenance. In: *Applied Mechanics and Materials* Vol.: 110–116: 5257–5264.

Wang, W. 2012. An overview of the recent advances in delay-time-based maintenance modelling. *Reliability Engineering and System Safety* 106: 165–178.

Wang, W. 2008. Delay time modelling. In: *Complex system maintenance handbook*. Kobbacy, k. A.H. & Prabhakar Murthy, D.N. (eds.). Springer.

Wang, W. 2003. A delay time based approach for risk analysis of maintenance activities. *Journal of the Safety and Reliability Society* 23, 1: 103–113.

Wang, H. 2002. A survey of maintenance policies of deteriorating systems. *European Journal of Operational Research* 139: 469–489.

Wang, W., Christer, A.H. 2003. Solution algorithms for a nonhomogeneous multi-component inspection model. *Computers & Operations Research* 30: 19–34.

Wang, W., Christer, A.H. 1997. A modelling procedure to optimize component safety inspection over a finite time horizon. *International Quality and Reliability Engineering* 13: 217–224.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Condition-based maintenance policies for multi-component systems with Lévy copulas dependence

Heping Li, Laurence Dieulle & Estelle Deloux
Charles Delaunay Institute, University of Technology of Troyes, Troyes, France

ABSTRACT: The maintenance planning of systems has become more and more complex over the last decades due to the fact that systems consist of more components which depend on each other. Stochastic dependencies exist in industry due to a common environment or to the fact that components share the same stress while economic dependencies arise when grouping maintenance activities can save setup cost. Interactions between components make the modeling and optimization of maintenance tricky. However dependencies between components have to be taken into account in order to optimize the maintenance activities but the way of modeling stochastic dependencies remains to explore. Copulas are widely used to model the dependence structure of random variables and they separate dependence structure from marginal properties. Kallsen & Tankov (2006) extended the Sklar's Theorem for Lévy measure and they defined a new copula for Lévy processes so called Lévy copulas. Based on marginal Gamma processes, we use Clayton-Lévy copula to model the dependent stochastic degradation of components. This model of dependence is different from previous literatures as Lévy copula provides a means of modeling stochastic dependence which can be from independence to complete dependence and it is easily simulated. By considering economic dependence, we propose a condition-based maintenance policy with a new decision rule allowing grouping opportunities and we compare the performance with classic maintenance strategies.

1 INTRODUCTION

In order to ensure the productivity, the safety and to save the cost, maintenance policies have been widely studied since the last century. Nevertheless, the nowadays systems contain more and more components resulting in more complex structures. As a result, the research of maintenance policies focusing on the single-unit systems is not suitable any more. For a multi-component system, interactions between components have to be taken into consideration. According to Thomas (1986), generally interactions between components in a multi-component system are classified into three types: economic dependence, stochastic dependence and structural dependence. In this paper, we consider economic and stochastic dependence. Stochastic dependence arises in industry due to the common environment or to the fact that components share the same stress. Hong, Zhou, Zhang, & Ye (2014) shows that maintenance optimization will be affected by dependent degradation. Golmakani & Moakedi (2012) propose a periodic inspection optimization model for a two-component repairable system with failure interactions, Mercier & Pham (2012) model dependence by a bivariate wear subordinator with Gamma marginal distributions. However, these models of dependence can only represent a few range of possible dependence. Moreover, when the system contains a large number of components, it seems that the dependence are hardly to be builded in the system level. In other hands, copulas are widely used to model the dependence structure of random variables as they separate dependence structure from marginal properties. Hong, Zhou, Zhang, & Ye (2014) model the dependence structure of stochastically deteriorating components by the ordinary copula which has several drawbacks when applied to Lévy processes and pointed out by Cont & Tankov (2004). To overcome these drawbacks, they extended the Sklar's Theorem for Lévy measure and they defined a new copula for Lévy processes so called Lévy copulas. Kallsen & Tankov (2006) enrich the properties of Lévy copulas. Based-on marginal Gamma processes, we use Clayton-Lévy copula to model the dependent stochastic degradation of components. This model of dependence is different from previous literatures as Lévy copula provides a means of modeling stochastic dependence which can befrom independence to total dependence and it is easily simulated. Economic dependence offers opportunities to group maintenance actions so as to save set-up cost. Including the economic dependence,

we implement several maintenance policies. The main contribution of this paper is to propose a new adaptive maintenance decision rule considering not just the currently-inspected component, but also the available information about the other components. The paper is arranged as follows. In section 2 we recall some basic information about Lévy copulas and Gamma processes. Section 3 describes our proposal of maintenance decision rule and proposes classic maintenance strategies to implement for the purpose of comparison. In section 4, numerical results are presented. Conclusions and perspectives are given in section 5.

2 STOCHASTIC DEGRADATION MODELS

To simplify the model and the calculations, we firstly consider a system which consists of two components in parallel. The state of the system is characterised by the individual deterioration level of each component. The deterioration level of each component can be represented by a scalar variable X_t^i (i = 1, 2). All of components in the system are new at the beginning. When the deterioration level of component i exceeds its own failure threshold L_i, it is considered as failed.

2.1 *Stochastic degradation modeling of component*

As we assume that the deterioration of the component can be summarized by a scalar variable X_t^i (i = 1, 2), $(X_t^i)_{t\geq 0}$ is supposed to be modeled by a stationary Gamma process with shape parameter α_i and scale parameter β_i ($i = 1,2$) with following properties:

- $X_0^i = 0$
- $(X_t^i)_{t\geq 0}$ has independent increments
- For $t > 0$ and $h > 0$, $X_{t+h}^i - X_h^i$ follows a Gamma distribution with shape parameter $\alpha_i t$ and scale parameter β_i and the probability density function of $(X_{t+h}^i - X_h^i)$ is given by:

$$f(x|\alpha_i t, \beta_i) = \beta_i^{\alpha_i t} x^{\alpha_i t - 1} exp(-\beta_i x)/\Gamma(\alpha_i t) \qquad (1)$$

Such a process means that the mean and variance of X_t^i are $\alpha_i t/\beta_i$ and $\alpha_i t/ \beta_i^2$. Parameters α_i et β_i allow us to model different deterioration behaviours of components in the system. Note that the Gamma process is a positive process with independent increments, hence it is sensible to use this process to describe the deterioration (Noortwijk (2009)). Another interest of the Gamma process is the existence of an explicit probability distribution function, which permits feasible mathematical developments.

2.2 *Stochastic dependence modeling with Lévy copula*

Since the components in the same system share a common stress, it is reasonable to assume that the deterioration of components are dependent. In this paper, we use Lévy copula to model the dependence between components for a wide range of dependence. To introduce Lévy copula, we firstly recall that according to the Sklar's Theorem, for F_1, ..., F_n univariate continuous cumulative distribution function and H a multivariate joint cumulative distribution function there exists a unique function C such that

$$\begin{aligned} H(x_1, x_2, ..., x_n) &= C(F_1(x_1), F_2(x_2), ..., F_n(x_n)) \\ &= C(u_1, u_2, ..., u_n) \end{aligned}$$

This is that $H(x_1, x_2, ..., x_n)$ has the same dependence structure with $C(u_1, u_2, ..., u_n)$ regardless its marginal functions. Hence, copulas allow to separate the univariate margins and the multivariate dependence structure in the continuous multivariate distribution functions. To model the dependence structure for stochastic processes, Cont & Tankov (2004) define the dependence structure of Lévy measure by Lévy copula. Thus Lévy copula retains the dependence information of a Lévy measure. Let $X = (X^1, ..., X^d)$ be a Lévy process. Then there exists a Lévy copula C_L such that the tail integral of X satisfies:

$$U(x_1, ..., x_d) = C_L(U_1(x_1), ..., U_d(x_d)) \qquad (2)$$

with for the joint measure: $U(x_1, \ldots, x_d) = \int_{x_1}^{\infty} ... \int_{x_d}^{\infty} \nu(dx_1 ... dx_d)$ and for the marginal measure: $U_1(x_1) = \int_{x_1}^{\infty} ... \int_0^{\infty} \nu(dx_1 ... dx_d)$. Similar to ordinary copulas, there are also several families of Lévy copulas. For our two-component system with marginal Gamma processes, we choose Clayton-Lévy copula where dependence structure C is defined as follows:

$$C(u,v) = (u^{-\theta} + v^{-\theta})^{-1/\theta} \qquad (3)$$

When $\theta \to 0$, u and v are independent; when $\theta \to \infty$, u and v are completely dependent. What's more, when u and v are independent, $C(u,v) = u1_{v=\infty} + v1_{u=\infty}$.

As a consequence, our model of stochastic dependence is obtained by following steps:

1. For a Gamma process with shape parameter α and scale parameter β, the Lévy measure $\nu(dx) = \{\alpha \exp(-\beta x)/x\}dx$. So we have

$$U(x) = \alpha E_1(\beta x) \qquad (4)$$

where E_1 is exponential integral and the inverse is

$$U^{-1}(x) = E_1^{-1}(x/\alpha)/\beta \tag{5}$$

2. When the dependence Lévy copula is in Clayton family, according to equation (3) the conditional distribution function take a form:

$$C(v,u) = \partial C_\theta(u,v)/\partial u = \left\{1 + (u/v)^\theta\right\}^{-1-1/\theta} \tag{6}$$

and can be easily inverted:

$$v = C^{(-1)}(y \mid u) = u(y^{-\theta(1+\theta)} - 1)^{-1/\theta} \tag{7}$$

where y is a random variable uniformly distributed on [0,1].

3. Since a Gamma process $(X_t)_{t\geq 0}$ can be represented in law by series representations $(\tilde{X}_t)_{t\geq 0}$ where

$$\tilde{X}_t = \sum_{i=1}^{\infty} U^{(-1)}(\Gamma_i)1_{[0,t]}(v_i) \tag{8}$$

with $\{\Gamma_i\}$ a sequence of jumping times of a standard Poisson process and $\{V_i\}$ an independent sequence of independent random variables, uniformly distributed on [0,1] (Rosinski (2001)). Furthermore, a two-dimensional Gamma process (X_t, Y_t) with Lévy copula dependence can be represented as follows (Cont & Tankov (2004)):

$$X_t = \sum_{i=1}^{\infty} U_x^{(-1)}(\Gamma_i)1_{[0,t]}(v_i) \tag{9}$$

$$Y_t = \sum_{i=1}^{\infty} U_y^{(-1)}(C^{(-1)}(w_i \mid \Gamma_i))1_{[0,t]}(v_i) \tag{10}$$

Finally, according to equation (5), equation (7), equation (9) and equation (10), a two-dimensional Gamma process (X_t, Y_t) can be represented by

$$X_t = \sum_{i=1}^{\infty} E_1^{-1}(\Gamma_i/\alpha_1)1_{[0,t]}(v_i)/\beta_1$$

$$Y_t = \sum_{i=1}^{\infty} E_1^{-1}(\Gamma_i(w_i^{-\theta(1+\theta)} - 1)^{-1/\theta}/\alpha_2)1_{[0,t]}(v_i)/\beta_2$$

where $(w_i)_{i\in\mathbb{N}}$ and $(v_i)_{i\in\mathbb{N}}$ are independent random variables which have uniform distribution on [0,1] and $(\Gamma_i)_{i\in\mathbb{N}}$ is an independent sequence of jump times of a standard Poisson process. In next section, we propose an adaptive maintenance decision rule aiming at taking full advantage of the dependence between components by increasing the possibilities of grouping maintenance tasks.

3 MAINTENANCE POLICIES

In this section, we detail our proposal for taking full advantage of grouping opportunities with respect to the current available information. In order to compare the performance of such a decision rule, we propose to implement classical maintenance strategies. For all considered maintenance policies, we make following assumptions:

- In order to avoid failures, a preventive maintenance takes place when X_t^i exceeds corrective threshold M_i (with $0 \leq M_i \leq L, i = 1,2$). Both preventive and corrective replacements are assumed to be perfect and instantaneous.
- The deterioration level of component can be obtained only by inspection. Besides, if the component fails, it remains unavailable until the next inspection and then it is repaired. We assume that each inspection reveals the real state of component perfectly.
- Considering the economic dependence, we assume that the costs of preventive replacement ($c_p^i, i = 1,2$) and of corrective replacement ($c_c^i, i = 1,2$) are composed of two parts: the set-up cost (c_r) and the individual cost. If one component fails but the other one still works, it will have a penalty cost per time unit (c_u); if both of components fail, the system is failed and it will have a down-time unitary cost per time unit (c_d). Of course, we have a inspection cost (c_{insp}) for every inspection.

To evaluate maintenance policies, we use the criterion of expected cost of system per time unit: $\overline{C} = \lim_{t\to\infty} E_0(c(t))/t$. The cumulative cost of system $c(t)$ depends on the number of preventive and corrective replacements ($N_p^i(t)$, $N_c^i(t)$), the number of inspections ($N_i^i(t)$), the cumulative failed time of components ($U_i(t)$) and the cumulative down-time of system ($D(t)$). Therefore $c(t)$ can be represented by

$$c(t) = \sum_{i=1}^{2} (c_p^i N_p^i(t) + c_c^i N_c^i(t) + c_{insp} N_i^i(t) + U_i c_u(t)) + c_d D(t)$$

and the Monte-Carlo simulation method is employed for the computation. In industry, combining the maintenance activities is often cheaper than maintaining the components separately because of the scale effect, the set-up cost or taking full advantage of downtime (Nicolai & Dekker (2008)). In this study, we mainly consider the case of set-up cost (c_r). When the maintenance actions of two component take place at the same time, we save a set-up cost. Therefore, with economic dependence, the expected cost of system per time

unit is modified by the number of group ($N_g(t)$) as follows:

$$c(t) = \sum_{i=1}^{2} (c_p^i N_p^i(t) + c_c^i N_c^i(t) + c_{insp} N_i^i(t) + U_i c_u(t)) + c_d D(t) - c_r N_g(t)$$

3.1 *A new condition-based maintenance policy with grouping opportunities (policy 0)*

The component 1 and 2 are inspected every ΔT_1 and ΔT_2 time unit respectively. Applied at each inspection time, we propose an advanced maintenance decision rule allowing to postpone or to preempt a maintenance task (according to aprobabilistic criterion) in order to take full advantage of the cost saving induced by replacements that are simultaneously performed. Suppose that at time $n\Delta T_1$, the deterioration level of component 1 ($X^1_{n\Delta T_1}$) exceeds the preventive replacement threshold ($M_1 < X^1_{n\Delta T_1} < L_1$) hence the component needs to be preventively replaced. Simultaneous replacement of both components is thus feasible. Two cases are considered according to the available information: postponing or preempting. As component 2 is not observed at time $n\Delta T_1$, the last known deterioration level of component 2 is $X^2_{m\Delta T_2}$ ($m\Delta T_2 < n\Delta T_1 < (m+1)\Delta T_2$) (see Fig. 1) is used as follows:

1. Set $p_a = P(X^2_{n\Delta T_1} > M_2 \mid X^2_{m\Delta T_2})$ be the probability that component 2 would need to be preventively replaced at time $n\Delta T_1$, if $p_a \to 1$, then the component 2 will probably be replaced soon ($(m+1)\Delta T_2$). In this case which is called preempting case, we can preempt the replacement of component 2 in order to save a set-up cost as well as to avoid the failure of component 2 before the next inspection. However such an action may replace the component 2 too early and lead to an increase of preventive maintenance cost. Parameter p_a depends only on the last known deterioration level of component 2 and is computed as follows:

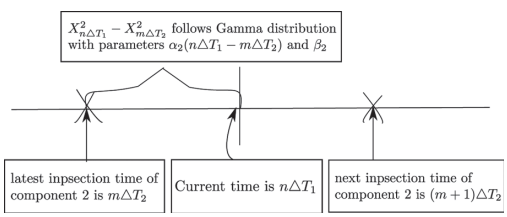


Figure 1. Sketch of inspection time.

$$p_a = P(X^2_{n\Delta T_1} > M_2 \mid X^2_{m\Delta T_2}) = P(X^2_{n\Delta T_1 - m\Delta T_2} > M_2 - X^2_{m\Delta T_2})$$

Since the random variable $X^2_{n\Delta T_1}$ knowing that $X^2_{m\Delta T_2}$ follows Gamma distribution with parameter $(n\Delta T_1 - m\Delta T_2)\alpha_2$ and β_2, therefore $p_a = \overline{F}_{(n\Delta T_1 - m\Delta T_2)\alpha_2, \beta_2}(M_2 - X^2_{m\Delta T_2})$ where $\overline{F}_{(n\Delta T_1 - m\Delta T_2)\alpha_2, \beta_2}(x) = \int_x^{+\infty} f_{(n\Delta T_1 - m\Delta T_2)\alpha_2, \beta_2}(u)du$

2. set $p_p = P(X^1_{(m+1)\Delta T_2} > L \mid X^2_{m\Delta T_2})$ be the probability that component 1 will be failed at the inspection time of component 2, if $p_p \to 0$, then the component 1 will almost impossibly fail before the next inspection time of component 2 ($(m+1)\Delta T_2$). In this case which is called postponing case, the replacement of component 1 can be postponed to the next inspection period of component 2 in order to save a set-up cost also to extend the working hours of component 1. However such an action may take the risk that component 1 fails before it is replaced and furthermore the cost of corrective replacement is more expensive than that of preventive replacement. Similar to case 1,

$$p_p = \overline{F}_{((m+1)\Delta T_2 - n\Delta T_1)\alpha_1, \beta_1}(L - X^1_{n\Delta T_1})$$

For general case,

$$p_a = \overline{F}_{(n\Delta T_i - m\Delta T_j)\alpha_j, \beta_j}(M_j - X^j_{m\Delta T_j}) \quad (11)$$

$$p_p = \overline{F}_{((m+1)\Delta T_j - n\Delta T_i)\alpha_i, \beta_i}(L - X^i_{n\Delta T_i}) \quad (12)$$

where current inspection time is $n\Delta T_i$ and $M_i < X^i_{n\Delta T_i}$.

In order to decide which is more benefit between postponing or preempting, a priority is given to the first condition. Let us note that condition $p_a \to 1$ is checked first because if p_a is small then it would be useless to postpone the replacement of component 1 because component 2 will be hardly replaced at next inspection period. As a result, we give priority to the condition of $p_a \to 1$ and we define our decision rule in Figure 2. Pay attention to that the replacement of component 1 can not be postponed if $X^1_{n\Delta T_1} > L_1$. Condition 1 is met if p_a is greater than an input threshold PA whereas condition 2 is met when p_p is greater than another input threshold PP (see Fig. 2). PA and PP are chosen in order to optimize the cost criterion. When PA is small, condition 1 will be often met leading to many grouped maintenance tasks. When both PA and PP are small then condition 2 is often met and at $n\Delta T_1$, preempting the replacement of component 2 is preferable to postponing replacement of component 1.

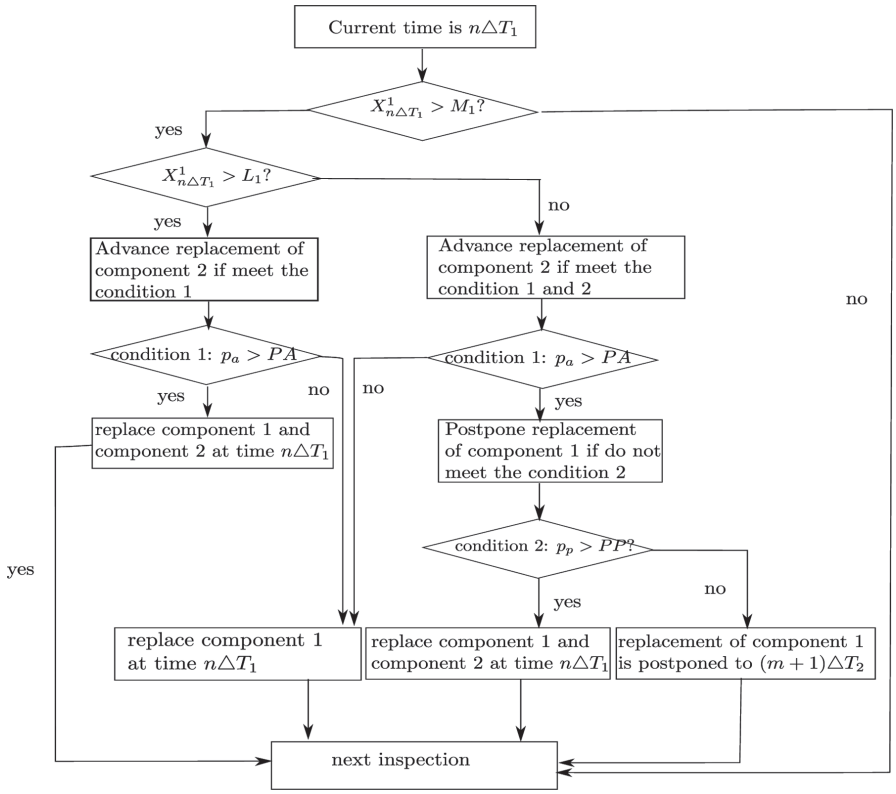


Figure 2. Sketch of decision rule for example of component 1 inspected at time $n\Delta T_1$.

3.2 *Classic maintenance strategies*

3.2.1 *Condition-based maintenance policy not considering the economic dependence (policy 1)*

Firstly we consider a basic condition-based maintenance policy. We inspect the components every ΔT_1 time unit for component 1 and ΔT_2 for component 2. At every inspection time $n\Delta T_i$ $(n \in \mathbb{N}, i = 1,2)$, the deterioration level of component i ($X^i_{n\Delta T_i}$) is revealed. When $X^i_{n\Delta T_i}$ exceeds its own corrective replacement threshold L_i, a corrective replacement takes place; when $X^i_{n\Delta T_i}$ exceeds its preventive replacement threshold M_i, a preventive replacement is carried out; otherwise the inspection to be continued. Obviously, to minimise the expected cost of system per time unit, we have to find the optimal values of ΔT_i and M_i $(i = 1,2)$.

3.2.2 *Condition-based maintenance policy considering the economic dependence (policy 2)*

The maintenance decision rule is the same as the policy 1. The only difference is the account of a set-up cost c_r. As described in the introduction of this section, the set-up cost modifies the expression of $c(t)$ and impacts the optimal values of ΔT_i and M_i $(i = 1,2)$. This maintenance policy is noted Policy 2.

3.2.3 *Condition-based maintenance policy with a unique inspection period and a unique replacement threshold considering the economic dependence (policy 3)*

When the set-up cost accounts a large part, grouping more maintenance activities is more economic. Hence we propose a condition-based maintenance policy where components 1 and 2 share the same inspection period ΔT and the same preventive replacement threshold M. Such a maintenance policy provides more grouping opportunities since maintenance actions take place only at inspection time.

3.2.4 *Block-based maintenance policy considering the economic dependence (policy 4)*

Finally, we propose a block-based maintenance policy. The component i $(i = 1,2)$ is replaced every

ΔTB_i time units, independently of its failure history.

4 NUMERICAL EXAMPLE

Numerical examples are presented and the performance of our new adaptive maintenance decision rule is compared with classic maintenance strategies detailed in section 3.2. Moreover, the sensibility of cost criterion to the set-up cost is studied.

4.1 *Input data*

We consider a two-component parallel system. The degradation parameters of components, as described in detail in section 2, are given in Table 1. Component 2 deteriorates more rapidly in average with the average degradation rate is 9. When the parameter of the Lévy copula θ is set equal to 10, there is a strong dependence between the two components. The characteristic parameters of the various implemented maintenance policies are described in Table 2.

4.2 *Analysis of maintenance policies with different set-up cost*

In order to compare the performance of our maintenance policy with classic strategies, we vary the set-up cost (c_r) from 0 to 5. Optimal inspection periods for Policy 1 are calculated using numerical evaluation of the stationary law as in Dieulle, Bérenguer, Grall, & Roussignol (2003). The simulation results are presented in Table 3, Table 4, Table 5, Table 6, Table 7 and Figure 3 where we note life cycle of component 1 as LC_1 and life cycle of component 2 as LC_2.

From a general point of view, the maintenance policies attempt to balance the life cycle of two components and replace them earlier when set-up cost is higher. When stronger economic dependence exists, the expected global cost of system is more reduced.

Policy 1 (no set-up cost is considered for Policy 1) is always the worst case unless the set-up cost is very small (0 or 1). In this case, Policy 3 (a unique inspection period and preventive threshold for Policy 2) with a unique inspection period cannot take advantage of grouping. Comparing

Table 1. Component degradation parameters.

	α	β	θ	L
Component 1:	7/5	1/5	10	180
Component 2:	9/5	1/5	10	180

Table 2. Cost parameters.

c_p^i $(i = 1, 2)$	c_c^i $(i = 1, 2)$	c_{insp}	c_u	c_d
20	100	1	5	10

Table 3. Optimal values of policy 0.

c_r	$\bar{C}$	$\Delta T_1/\Delta T_2$	M_1/M_2	PA/PP	LC_1/LC_2
0	2,8218	6/4	116/122	0.6/0.1	19.87/15.89
1	2,8047	6/4	116/122	0.5/0.1	19.85/15.92
2	2,7928	6/4	116/122	0.5/0.1	19.85/15.92
3	2,7143	18/4	90/126	0.1/0.1	16.43/16.40
5	2,5975	18/4	90/126	0.1/0.1	16.43/16.40

Table 4. Optimal values of policy 1.

$\bar{C}$	ΔT_1	ΔT_2	M_1	M_2	LC_1/LC_2
2,8313	6	4	116	122	19.96/15.86

Table 5. Optimal values of policy 2.

Set-up cost	$\bar{C}$	ΔT_1	ΔT_2	M_1	M_2	*Lifecycle* 1/2
0	2,8313	6	4	116	122	19.96/15.86
1	2,8225	6	4	116	122	19.96/15.86
2	2,8136	6	4	116	122	19.96/15.86
3	2,8057	5	5	120	110	19.96/15.86
5	2,7651	15	15	40	40	15.02/15.00

Table 6. Optimal values of policy 3.

Set-up cost	$\bar{C}$	ΔT	M	*Lifecycle* 1	*Lifecycle* 2
0	2,8558	5	118	19.73	15.90
1	2,8412	5	118	19.73	15.90
2	2,8228	5	118	19.73	15.90
3	2,8051	5	118	19.73	15.90
5	2,7651	15	50	15.02	15.00

Table 7. Optimal values of policy 4.

Set-up cost	$\bar{C}$	ΔTB_1	ΔTB_2	*Lifecycle* 1/2
0	2,8040	18	14	18/14
1	2,7936	18	14	18/14
2	2,7897	18	14	18/14
3	2,7773	18	14	18/14
5	2,6427	15	15	15/15

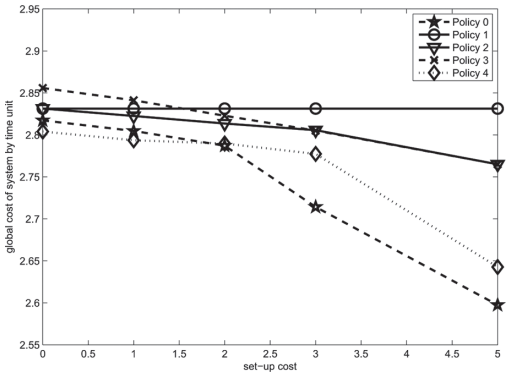


Figure 3. Optimal values of $\bar{C}$ for policy 0, policy 1, policy 2, policy 3 and policy 4 with $c_r = 0$, $c_r = 1$, $c_r = 2$, $c_r = 3$, $c_r = 5$.

Policy 2 (two different inspection periods and preventive thresholds for Policy 2) with Policy 3, Policy 3 is less efficient when the set-up cost is small, because component 1 and component 2 have two different deterioration rate therefore it is better to have various periods and thresholds. However when set-up cost increase to 2, Policy 2 and Policy 3 come up with close optimal values and tends to be equal when set-up cost continue to increase, since the higher set-up cost leads to the same inspection period because the strong economic dependence plays a important role. Furthermore, when the set-up cost passes to 5, Policy 2 and Policy 3 tend to a systematic replacement policy as Policy 4 (block-based maintenance policy). This is because the set-up cost is relatively too high comparing with the preventive replacement cost is 20 and it gains a lot by replacing two components together. However, when set-up cost equals to 5, in spite of the similar optimal values of decision parameters for Policy 2, Policy 3 and Policy 4, the cost of Policy 2 and Policy 3 are greater than that of Policy 4 because of additional monitoring cost. In fact we define a system where components deteriorate so slowly that it is not profitable to apply a condition-based maintenance policy in this case where inspection cost equals to 1. As a result, Policy 4 is always better than Policy 2 et Policy 3. Nevertheless, by applying our new decision rule detailed in section 3.1, Policy 0 (advanced policy with decision rule) can overcome this drawback. The optimal values of PA and PP search the better date for replacing two components together. It is obviousthat PA is smaller with a higher set-up cost and PP can not be too high. In fact, postponing preventive replacement may let the component fail and it would be too expensive. Hence the case of postponing should be strictly controlled. Although Policy 2, Policy 3 and Policy 4 also try to search the better date of grouping, the decision rule offers a broader scope. For example, when $c_r = 5$, in order to have more groups, Policy 2, Policy 3, and Policy 4 only can group at a multiple of ΔT_1 and ΔT_2 (say 15, 30, 45 ...); however, Policy 0 allows the ability to group more often (15, 18, 20, 25, 30, 35, 36 ...) taking advantage of two different inspection periods. The key point of our decision rule is that it includes the available information about all the components at each inspection time so that it achieves to decrease the total cost as well as to increase the life cycle of components.

4.3 *Conclusion and future work*

The objective of this paper was to propose maintenance policies for multi-component system considering the economic and stochastic dependence. As a result, we have shown that our advanced condition-based maintenance policy (Policy 0) can improve results of classic block-based strategy which is known to be well adapted to slowly degrading systems by overcoming the inspection cost drawback by taking full advantage of grouping opportunities.

The decision rule of maintenance is easy to apply and to calculate. It is efficient to find suitable dates of grouping maintenance by including the latest deterioration of components. When we want to extend our model to multi-component system with a largenumber of components, there are not parameter to add in the part of decision rule and we just have PA and PP to optimise. Consequently, our policy will be more efficient for a system which has more components. Nevertheless, for applying our decision rule, it should be convenient to change the maintenance plan.

The investigation of set-up cost shows that grouping maintenance activities is important to reduce the global maintenance cost where it is better to search the opportunities of grouping as possible. As well as the economic dependence, the stochastic dependence has to be taken into consideration for optimising the maintenance schedule. Future work will be on investigating the influence of stochastic dependence which is modeled by Lévy copula on the optimization of maintenance schedule.

REFERENCES

Cont, R. & P. Tankov (2004). Financial modelling with jump processes.

Dieulle, L., C. Bérenguer, A. Grall, & M. Roussignol (2003). Sequential condition-based maintenance scheduling for a deteriorating system. *European Journal of Operational Research 150*(2), 451–461.

Golmakani, H.R. & H. Moakedi (2012). Periodic inspection optimization model for a two-component repairable system with failure interaction. *Computers & Industrial Engineering 63*(3), 540–545. Energy Management and Economics.

Hong, H., W. Zhou, S. Zhang, & W. Ye (2014). Optimal condition-based maintenance decisions for systems with dependent stochastic degradation of components. *Reliability Engineering & System Safety 121*(0), 276–288.

Kallsen, J. & P. Tankov (2006, August). Characterization of dependence of multidimensional lévy processes using lévy copulas. *J. Multivar. Anal. 97*(7), 1551–1572.

Mercier, S. & H.H. Pham (2012). A preventive maintenance policy for a continuously monitored system with correlated wear indicators. *European Journal of Operational Research 222*(2), 263–272.

Nicolai, R. & R. Dekker (2008). Optimal maintenance of multi-component systems: A review. In *Complex System Maintenance Handbook*, Springer Series in Reliability Engineering, pp. 263–286. Springer London.

Noortwijk, J.V. (2009). A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety 94*(1), 2–21. Maintenance Modeling and Application.

Rosinski, J. (2001). Series representations of lévy processes from the perspective of point processes. In O. Barndorff-Nielsen, S. Resnick, and T. Mikosch (Eds.), *Lévy Processes*, pp. 401–415. Birkhauser Boston.

Thomas, L. (1986). A survey of maintenance and replacement models for maintainability and reliability of multi-item systems. *Reliability Engineering 16*(4), 297–309.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Application of standards in reliability prognosis of braking system of moving walks

E. Rogova, G. Lodewijks & Y. Pang
TU Delft, Delft, The Netherlands

ABSTRACT: The reliability of braking systems in people transportation equipment is very important. There are however only a few researchers that developed a maintenance and inspection method for such systems based on accident analysis. These methods are without correspondence to an appropriate Safety Integrity Level (SIL). The international standards IEC 61508 and ISO 22201-2 have special requirements with respect to a SIL. All systems and subsystems of moving walks should correspond to the required level of SIL. In this paper method of reliability prognosis for braking system of moving walks is presented based on the reliability degradation of system components and the requirements of related standards. This method enables the determination of a regular maintenance schedule. It also enables the development of an intelligent system for preventing failures in braking systems of moving walks. This allows keeping the required safety level from the beginning to the end of its technical lifetime.

1 INTRODUCTION

The first task of people transportation equipment is to move people. The second task and equally important is to do this safely. The first and the second task cannot exist separately. Safety is one of the most important property of any device that used by a human. There are many safety standards that regulate norms of construction, exploitation and functional safety of equipment in different engineering fields. These standards have requirements, recommendations, methods and tools for reliability analysis. Although safety and reliability are different properties and a system can be reliable but unsafe and vice versa (Leveson 2011), surely, safety and reliability are closely related. For moving walks it is assumed in this study that unreliable subsystems cannot be safe. That is why the system has to be reliable and to meet requirements of related standards and norms. Reliability is defined as "ability of a functional unit to perform a required function under given conditions for a given time interval". "The term used in IEV 191-02-06 is "reliability performance" and the definition is the same with additional notes" (ISO/IEC 2382-14 1997). Prediction of the reliability value not only for a specified time period, but also for all the exploitation period of a system is called reliability prognosis.

The role of a reliability prognosis cannot be overestimated. Reliability prognosis plays a serious role in maintenance management of a machine. "The ability to forecast machinery failure is vital to reducing maintenance cost, operation downtime or operation risk" (Sun & Jia 2011). Reliability prognosis of the machine consists of several parameters: 1) to predict time of failure of the machine; 2) to estimate money costs for future repair; 3) to conduct appropriate repair or replacement of equipment to reduce the cost of major repairs. Such prognosis allows to reduce probability of accidents and money expenditure for repair of equipment. Reliability prognosis is used in different engineering fields such as nuclear, chemical, aerospace, civil and other fields. This research is focused on implementation of reliability prognosis in mechanical engineering. Reliability prognosis of a braking system of moving walks is considered in this paper.

In most cases reliability prognosis is executed because of reliability degradation of parts of the system. It means that the reliability of a system at the start differs from reliability after some time. In literature four main groups of prognostic approaches for degradation systems are described: experience-based, model-based, knowledge-based and data-driven (Gojian et al. 2009). In practice, reliability prognosis of complex systems doesn't only use one method: sometimes engineers apply even a few approaches. The type of reliability prognosis depends on nature of degradation. For instance, some components such as controllers almost don't have degradation during exploitation period. They have an approximately constant failure rate. But others (mechanical components) have strong degradation of reliability parameters.

Reliability degradation of a braking system of moving walks is caused by wear of mechanical and hydraulic components. Combination of experience-based, SIL-based approach and application of international standards are used in this paper for the reliability prognosis of a braking system of moving walks. This combined method enables not only estimation of the overall reliability of a system, it also creates an intelligent system that will announce not appropriate safety integrity level in advance.

The method described here for the reliability analysis and prognosis is SIL-based which means using the SIL concept—the central concept of functional safety, described in the standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems". The Safety Integrity Level (SIL) is defined as "a discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems" (IEC 61511-1 2004). The standard ISO 22201-2 "Programmable Electronic Systems in Safety Related Applications—Part 2: Escalators and moving walks (PESSRAE)" specifies general requirements of IEC 61508 for escalators and moving walks. These and other standards establish requirements for functional safety of moving walks. However, SIL-based reliability analysis and prognosis of a braking system of moving walks were not considered in research until now. Meanwhile this approach does not only allow meeting all requirements of related standards, it also allows creating a suitable tool for engineers, constructors and audit companies. The target of this paper is demonstration of application of related standards in different stages of reliability prognosis of a braking system of moving walks. The calculations presented in this paper are for illustration purposes only and cannot be considered as direct engineering calculations for any type of braking system.

The focus of this paper is moving walks, an example of transportation equipment. There are two types of brakes recommended by the standard EN 115-1: an operational and an auxiliary (EN 115-1 2010). Auxiliary brakes are optional for the majority of moving walks and required only for inclined moving walks with special conditions. Literature describes two main types of operational brakes: hydraulic and electromagnetic (Al-Sharif 2006). For this paper the estimation of reliability for hydraulic operational braking system of moving walks was chosen, cause hydraulic brakes are more amenable to proportional control, than electromagnetic (Al-Sharif 2006). Statistics of accidents on escalators and moving walks in big malls and metro proves necessity of the present research, because the main part of all deaths on these machines is caused by people falling (Mccann 2006). Possible causes of falling are crowdedness, wrong behavior of elderly people and children, and overspeed. A moving walk has to be stopped immediately in these cases. If brakes are faulty, it can lead to serious injuries or even death.

The structure of the paper is organized as follows. Section 2 describes safety standards applicable for a braking system of moving walks. Section 3 contains risk assessment and SIL requirements for a braking system. Section 4 is about the reliability analysis of a braking system of moving walks in accordance to the SIL requirements. Section 5 describes SIL-based reliability prognosis for a braking system of moving walks. Section 6 is a brief conclusion and discussion of future work.

2 INTERACTION OF STANDARDS

There are several safety standards for consideration of safety questions of moving walks. They can be divided into four groups: 1) standards of functional safety (IEC 61508, IEC 62061, ISO 22201-2, ISO 13849-1); 2) reliability analysis tools (IEC 60300-3-1, IEC 61649, IEC 61078, IEC 61165 etc.); 3) risk assessment (ISO 14798, ISO 12100, ISO/TR 14121-2); 4) mechanical safety standards for the sector application (EN115-1+A1, ISO 18738-2). A diagram of the standards interaction is shown on Figure 1. All four groups of standards are correlated to each other and used for reliability prognosis of moving walks. Moreover, all these standards should be studied in complex reliability analysis of a braking system of moving walks.

Safety standards such as IEC 61508 from the first group of standards are an important source of information for development of safety-critical systems in many engineering fields, including transport engineering. IEC 61508 has become a foundation of international standards for safety-related systems such as airborne systems, railway, nuclear

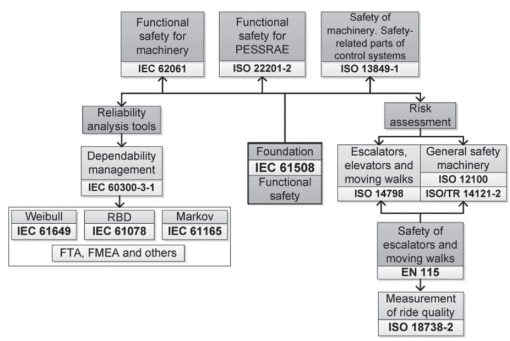


Figure 1. Diagram of standards.

power plants, medical equipment, energy and process systems, machinery, furnaces and automobiles (Azianti 2013). IEC 61508 defines general safety integrity requirements for safety functions allocated to the E/E/PE safety-related systems: SIL1 is the lowest level, SIL4 is the highest. However, IEC 61508 "does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards" (IEC 61508-1 2010). This standard doesn't provide engineers with specific requirements and recommendations for development of transport equipment. That is why three standards of functional safety of machinery were developed: IEC 62061, ISO 22201-2, and ISO 13849-1. IEC 62061 provides a machine sector specific framework for functional safety of machines in general (IEC 62061 2005). ISO 22201-2 has been developed "in order that consistent technical and performance requirements and rational be specified for Programmable Electronic System in Safety-Related Application for Escalators and moving walks (PESSRAE)" (ISO 22201-2 2013). This standard is based on IEC 61508, IEC 62061, and EN 115-1, and is considered as an "application sector standard" (IEC 61508-1 2010). However, ISO 22201-2 defines risk classes by means of the table with correspondence between frequency of accidents and risk consequences. There are no guidelines or rules in this standard how to transfer from risk classes to SILs that makes this a topic of future research. The standard defines the highest (SIL3) and the lowest (SIL1) possible safety integrity levels for moving walks. ISO 13849-1 from the first group of standards provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems of machinery (ISO 13849-1 2008).

The second group of standards is used for reliability analysis. The standard IEC 60300-3-1 "describes the usual methodologies, their advantages and disadvantages, data input and other conditions for using various techniques" (IEC 60300-3-1 2003). Standards IEC 61649 (Weibull analysis), IEC 61078 (Analysis techniques for dependability—Reliability block diagram and boolean methods), IEC 61165 (Application of Markov techniques) and others describe in details specific methods and techniques (mentioned in IEC 60300-3-1), that can be applied for reliability analysis and prognosis of a braking system of moving walks, separately.

The third group of standards is divided into two subgroups: general risk assessment for safety machinery and risk assessment for escalators, elevators and moving walks. The standard ISO 14798 "Lifts (elevators), escalators and moving walks—Risk assessment and reduction methodology" describes examples of hazards, consequence of steps of risk assessment for elevators, escalators and moving walks (ISO 14798 2009). The standard ISO 12100 (Safety of machinery—General principles for design—Risk assessment and risk reduction) is basic safety standard "giving basic concepts, principles for design and general aspects that can be applied to machinery" (ISO 12100 2010). This standard describes procedures for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or the provision of sufficient risk reduction. "The practical use of a number of methods for each stage of risk assessment is described in ISO/TR 14121-2" (ISO 12100 2010). The technical report ISO/TR 22100-2 describes how ISO 12100 relates to ISO 13849-1 from the first group of standards. "For the correct application of ISO 13849-1, basic input information resulting from the application of the overall risk assessment and risk reduction process for the particular machine design is necessary. Based on this input information, the safety-related parts of the control system can be appropriately designed according to ISO 13849-1. Information resulting from a detailed design of safety-related parts of the control system relevant for its integration into the machine design has then to be considered in the overall risk assessment and risk reduction process according to ISO 12100" (ISO/TR 22100-2 2013).

The standards from the fourth group contain mechanical data for safety limitations. EN 115-1+A1 comprises all types of hazards, allowable distances, speed and load limitations etc. ISO 18738-2 provides readers with information about ride quality of escalators and moving walks, it focused mainly on vibration and noise.

It is important to say that these groups of standards are used in different stages of reliability prognosis, as it will be described in this paper. The standards from the third group can be used mainly in the determination of safety requirements stage. The standards from the second group are used in the stage of reliability analysis in accordance to safety requirements. The fourth group provides information for development additional safety devices, diagnostic systems and redundancy architecture on the stage of reliability improvement. The first group provides general requirements and recommendations for a functional safety concept. Standards from this group are used in all the stages of analysis as a main guideline.

Application of safety standards and using SIL-based methodology, described in these standards, simplifies not only the work of audit companies.

Using an unified method also helps engineer-constructors, project managers at the design and maintenance stages. Safety integrity levels of all the safety functions should be defined in accordance to IEC 61508. Depending on the complexity of a system, there are one, two, three or many subsystems, which execute safety functions. Equipment for these subsystems should correspond to appropriate safety requirements. Knowledge of SIL for a safety function allows to calculate SIL of equipment which performs this safety function. It gives a possibility to find suitable equipment at the design stage of moving walks. It means that a project manager has to buy, for example, 5 devices with SIL2, SIL3, SIL2, SIL3 and SIL2 respectively to provide a safety function of SIL2.

However, the methodology described in standards is general and does not clear up the picture of the process: from risk assessment and determination of the SIL requirements till reliability analysis and reliability improvement. The next sections will show an application of safety standards for different stages of reliability prognosis of braking system of moving walks, using a SIL-based approach.

3 RISK ASSESSMENT AND SIL REQUIREMENTS SPECIFIED FOR MOVING WALKS

The determination of SIL requirements should be started from the determination of accident consequence levels in accordance to standards IEC 61508 and ISO 22201-2. IEC 61508-5 as well as ISO 22201-2 defines four categories of accident consequences: "catastrophic, critical, marginal, negligible" (IEC 61508-5 2010). At the same time ISO 22201-2 also calls accident consequences as "high, medium, low, negligible". Using different terminology inside one standard sometimes creates misunderstanding. The same categorization is suggested by ISO 14798. Unfortunately, these standards do not explain how to define the category of accident consequences. Table 1 suggests correspondence between the consequences of an accident (in injuries and deaths) and the duration of brakes unavailability for determination of an accident consequences category. This table is an interpretation of the table 'Quantitative consequence categories' from the manual for APCS engineers "Risk analysis of technological system in Interlock system for ITER" (Rogova 2012). The table is interpreted and adopted for moving walks in accordance to severity levels description given by ISO 14798 and ISO 22201-2.

Consequences of an accident and brakes unavailability were estimated based on reports, newspaper and scientific papers (Mccann 2006, Scott Tyson 2010). It is important to mention that this table suggests an example of determination accident consequences for moving walks. It is a general idea and it can be varied depending on the transport sector or type of transport equipment.

Table 1. Accident consequences.

	Brakes unavailability				
Consequences of an accident	<1 hour	<1 day	<2 days	<1 week	<1 month
No injuries	Mi	Se	Se	Se	Se
No significant injuries	Se	Se	Se	Ma	Ma
5 severe injuries	Ma	Ma	Ma	Ma	Ca
>5 and <10 severe injuries	Ma	Ma	Ma	Ca	Ca
>=1 death and/or multiple severe injuries	Ca	Ca	Ca	Ca	Ca

where Mi—minor, Ma—major, Se—severe, Ca—catastrophic.

The next significant step in risk assessment procedure is to define occurrence probability. ISO 22201-2 already developed this table for moving walks (Table 2). There are six categories of frequency: frequent, probable, occasional, remote, improbable and negligible. The same categorization is suggested by ISO 14798.

Table 3 demonstrates estimation and evaluation of risk that are described in ISO 14798 and ISO 22201-2. Intersection of "event probability" column and "accident consequences" row gives a risk class: I, II, III, IV (A, B, C, D, E, F).

In this paper for determination of risk mitigation measures it was assumed that consequences of an accident is *No significant injuries* and duration of brakes unavailability is *less than 1 day*. Thereby Table 1 gives a consequences category *Severe*. If an accident happens about 1 time per year, taking into account a mean value for total (2000) population per year, Table 2 gives a frequency category: *Occasional*. Intersection of column *Severe* and row *Occasional* of Table 3 gives risk class *IIIC*, that means "review and determine if any further mitigation is technically practicable" (ISO 22201-2 2013). However further explanation of determination of SIL is absent in ISO 22201-2. IEC 61508-5 provides information on the concepts of risk and the relationship of risk to safety integrity. As one of possible ways, the standard recommends a risk graph method which "has been used extensively within the machinery sector, see ISO 14121-2 and Annex A of ISO 13849-1" (IEC 61508-5 2010). This method was used for determination the safety integrity level

Table 2. Occurrence probability in events per year (ISO 22201-2 2013).

Category	Potential frequency for effect F	Mean value per year per unit moving walk	Mean value for total (2000) population per year
Frequent	$F \geq 0{,}01$	0,01	20
Probable	$0{,}001 \leq F < 0{,}01$	0,005	10
Occasional	$0{,}0001 \leq F < 0{,}001$	0,0005	1
Remote	$0{,}00001 \leq F < 0{,}0001$	0,00005	0,1
Improbable	$0{,}000001 \leq F < 0{,}00001$	0,000005	0,01
Negligible	$F < 0{,}000001$	$4{,}16667 \times 10^{-7}$	0,000833

Table 3. Risk estimation and evaluation (ISO 14798 2009).

Event probability	Accident consequences			
	Catastrophic	Major	Severe	Minor
Frequent	IA	IIA	IIIA	IVA
Probable	IB	IIB	IIIB	IVB
Occasional	IC	IIC	IIIC	IVC
Remote	ID	IID	IIID	IVD
Improbable	IE	IIE	IIIE	IVE
Negligible	IF	IIF	IIIF	IVF

for the safety function *Stop machine* in this paper. By means of application of the risk graph method, SIL was defined as SIL2. Input parameters for the risk graph method were calibrated in accordance to Tables 1–3. Description of the applied method is not the target of this paper and it will not be described here in details. The standards ISO 22201-2 and EN 115-1 confirm the defined SIL for a safety function related to stopping device. ISO 22201-2 defines SIL2 for the safety function "Check Stop switch in inspection controls" (ISO 22201-2 2013). EN 115-1 also defines SIL2 for the safety function "Stopping of an escalator or moving walk …" (EN 115-1 2010). It is important to mention that the brake is a final actuator in case of any type of accident situation. Thus reliability analysis and prognosis will be conducted for a braking system, which performs the safety function *Stop machine*.

4 RELIABILITY ANALYSIS

Equipment of a safety system has to meet the SIL requirements. In the previous section it was estimated that SIL for the safety function *Stop machine* is SIL2. It means that the overall safety integrity level of a braking system, which performs the safety function *Stop machine*, has to correspond to SIL2.

There are many reliability technics described in IEC 61508-6 and IEC 60300-3-1. However, all of them are divided into two main groups: qualitative and quantitative. Qualitative reliability analysis methods are used for analysis the functional system structure, determination "system and component fault modes, failure mechanisms, causes, effects and consequences of failures" (IEC 60300-3-1 2003). But qualitative methods cannot estimate numerical value of reliability. For quantitative analysis there are three most widely used methods: Fault Tree Analysis (FTA), Reliability Block Diagram (RBD) and Markov Analysis (MA). They are used in different situations. All of these methods are recommended by IEC 61508, but the right of choice is on behalf of an engineer.

Markov analysis considers all possible states of a system and this method is mainly used for systems with constant failure rates (IEC 60300-3-1 2003). But braking system contains components with constant and non-constant failure rates. Thus MA is not appropriate for an overall reliability analysis of a braking system of moving walks or can be applied partially to some subsystems. FTA as well as RBD relate to one of the top-down methods. These methods are able to account for effects arising from a combination of faults (IEC 60300-3-1 2003). However, RBD seems to be more suitable for the calculation of the braking system reliability because of its block structure. A braking system of moving walks consists of electrical/electronic parts with constant failure rates and mechanical and hydraulic parts with non-constant failure rate. RBD consists of blocks with known reliability parameters. As IEC 60300-3-1 states, this method is applicable, for systems "where independent blocks can be assumed" (IEC 60300-3-1 2003). It means that this method is good for those systems where reliability for every block of the system is defined or can be estimated at any period of time. In this paper for a braking system whose structure is presented on Figure 2, RBD was chosen as a suitable method for reliability analysis. RBD is not used for repairable systems. However approximation was done in this paper for reliability estimation of a braking system, because time of repair of a braking system is small in percentage ratio as compared with time of exploitation.

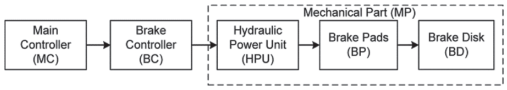


Figure 2. RBD of a braking system.

In this paper a BS (Braking System) is divided into a MC (Main Controller) part, a BC (Brake Controller) part with constant failure rates and a MP (Mechanical Part) with non-constant failure rates. A braking system is considered as high demand (executing in a continuous mode) because an interlock event of the BS is supposed to happen more than once a year. That is why estimation of the reliability for the system is conducted in this section by RBD method using Probability of dangerous Failure per Hour (PFH).

The general equation for the calculation of PFH for the system consisting of serial blocks of RBD is (IEC 61508-6 2010):

$$PFH_S \approx \sum_{i=1}^{N} PFH_i \tag{1}$$

where i is the number of blocks.

The Equation 2 for the reliability of a braking system was obtained by means of Equation 1 and RBD of braking system, demonstrated on Figure 2.

$$PFH_{BS} = PFH_{MC} + PFH_{BC} + PFH_{MP} \tag{2}$$

PFH values of the main and the brake controllers are estimated based on basic configuration of modules. In this paper configuration of main and brake controllers is assumed identical and consists of CPU, digital input/output modules, IM interfaces and Profinet:

$$PFH_{MC} = PFH_{BC} = PFH_{CPU} + PFH_{DI} + PFH_{DO} + PFH_{Profinet} + PFH_{IM} \tag{3}$$

A cumulative distribution function for the estimation of the reliability of a Mechanical Part (MP) with non-constant failure rate is obtained by means of Weibull distribution:

$$F_i^w(t) = 1 - e^{-\left(\frac{t}{\eta_i}\right)^{\beta_i}} \quad \text{(IEC 61649 2008)} \tag{4}$$

where
η is the characteristic life or scale parameter;
β is the shape parameter.

Weibull distribution is experience-based approach as it was mentioned in the Introduction. The standard IEC 61649 considers also other than the Weibull distribution and makes a conclusion that, for example, lognormal distribution is "the second choice for life data analysis" after the Weibull (IEC 61649 2008). Parameters of Weibull distribution characterize nine main mechanical components of a braking system: cylinder, motor DC, solenoid valve, pump, check valve, relief valve, springs, braking disk and pads. Values of the shape parameter and the characteristic life for these components are found in the book "Machinery failure analysis and troubleshooting" (Bloch & Geitner 1994) and free database of Barringer & Associates, Inc. (Weibull Database 2010). It is important to mention that Weibull parameters are not used for specific engineering calculations in this paper. The task of calculations presented here is to reveal a trend and basic regularities for such systems as a braking system of moving walks. Because of current lack of real data for estimation of Weibull parameters authors use data obtained from books and Internet databases presented "for educational purposes" (Weibull Database 2010). Values of the Weibull cumulative distribution function are transferred to PFH values using Equation 4 by replacement of the time value t. Operation time t is the time of use of a braking system in hours per day. In other words, t is time when the brake is used for braking. For example, PFH for motor DC can be obtained in accordance to Equation 4 using Weibull parameters $\beta = 1$, 2 and $\eta = 50000$ hours.

A general time-dependent Equation 5 of PFH calculation for a monosystem (system with 1oo1 architecture) was obtained based on Equations 2–4:

$$PFH_{1oo1}(t) = \sum_{i=1}^{n=9} F_i^w(t) + PFH_{MC} + PFH_{BC} \tag{5}$$

In accordance to Equation 5 PFH values for a monosystem were obtained for seven periods of time (from 1 month till 5 years of exploitation) and demonstrated on Table 4.

The estimation of PFH values of a braking system for 7 periods of time shows degradation of the system in terms of reliability. Comparing with PFH values of SILs given by IEC 61508-1, it is concluded, that after three months SIL of the system is equal 1, while in accordance to SIL requirements, SIL has to be equal to 2. This is not appropriate and means that reliability improvement has to be conducted.

As it was defined by the standard IEC 61508, in case of inadequate level of reliability corrective actions are required. There are a few methods of reliability improvement. The application of redundancy and diagnostics are among of them.

Table 4. PFH values of a braking system.

	Values (for a monosystem)	Values (after applying redundancy)
$PFH_{BS}^{1\,month}$	4,1914e-007	1,1303e-007
$PFH_{BS}^{6\,months}$	2,1421e-006	5,8967e-007
$PFH_{BS}^{1\,year}$	4,3938e-006	1,2702e-006
$PFH_{BS}^{2\,years}$	9,0241e-006	2,8749e-006
$PFH_{BS}^{3\,years}$	1,3805e-005	4,8217e-006
$PFH_{BS}^{4\,years}$	1,8689e-005	7,1146e-006
$PFH_{BS}^{5\,years}$	2,3653e-005	9,7596e-006

IEC 61508-6 considers main types of redundancy architecture. The standard also suggests options of voting logic with and without diagnostics: so-called k-out-of-n (KooN) architecture.

Reliability of a braking system can be improved by means of applying 1oo2D redundancy architecture. The architecture is organized as two identical channels. These channels are supplemented with a diagnostics (based on data from an incremental sensor), and a brake controller. Two brake disks are installed on the same shaft. Data obtained from incremental sensors have to be identical. By means of comparison of data from two sensors these sensors can be verified. Two brakes (main and redundant) have to work in turn that allows verification of their operability permanently. Calculation of the redundant scheme is not the target of this paper and it will not be described here in details. However, all calculations were conducted in accordance to formulas of PFH calculation for 1oo2D architecture (IEC 61508-6 2010). These formulas were converted to time-dependent Equations 6–7:

$$t_{CE}'(t) = \frac{\lambda_{DU}(t)\left(\frac{T_1}{2} + MRT\right) + \left(\lambda_{DD}(t) + \lambda_{SD}(t)\right)MTTR}{\lambda_{DU}(t) + \lambda_{DD}(t) + \lambda_{SD}(t)} \quad (6)$$

$$PFH_{1oo2D}(t) = 2(1-\beta)\lambda_{DU}(t)((1-\beta)\lambda_{DU}(t) + (1-\beta_D)\lambda_{DD}(t) + \lambda_{SD}(t))t_{CE}'(t) + 2(1-K)\lambda_{DD}(t) + \beta\lambda_{DU}(t) \quad (7)$$

Based on Equations 6–7, taking into account $\lambda_{DU}(t) = PFH_{1oo1}(t)$ (Fedorov 2008) and recommendations of ISO 13849-1 for estimation of diagnostic coverage, time-dependent PFH equation for 1oo2D system was obtained. The PFH values for seven periods of time for a system after application of 1oo2D redundancy architecture are shown on Table 4.

5 RELIABILITY PROGNOSIS

After having passed through all the stages of the analysis of a braking system of moving walks (defining of SIL requirements, reliability analysis and reliability improvement) PFH functions required for SIL-based reliability prognosis were obtained. Figure 3 demonstrates two lines of PFH: for a monosystem and for a system with redundancy. These lines present two functions: $PFH_{1oo1}(t)$ and $PFH_{1oo2D}(t)$.

The upper part of the graph shows "SIL zones" for a monosystem, the bottom part shows "SIL zones" for a system with applied redundancy architecture. Division into SIL zones demonstrates the necessity of redundancy of a braking system of moving walks. When divided into SIL zones, the reliability graph can be a prototype of a reliability trend for SCADA systems, which are used for the control of transport systems.

Kuo et al. also consider reliability prognosis. The authors do this for an aircraft engine as an example (Kuo et al. 2001). They developed three criteria for determination the replacement age of a critical item for a maintained system: 1) minimum replacement cost-rate, 2) maximum availability, and 3) lower bound on mission reliability. "Four methods are used to obtain solutions for multiple criteria decision making" (Kuo et al. 2001). However these methods do not take into account SIL requirements, which are mandatory and defined by international standards as mentioned above. The time of replacement of an element is defined by decision-making technic. Suggested in this paper reliability prognosis method allows to

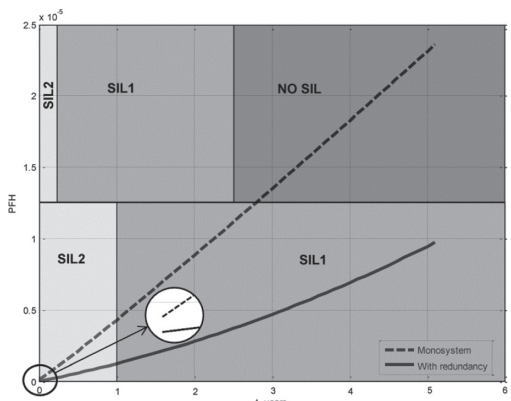


Figure 3. PFH dependence on time.

define the time of replacement or repair of a braking system component by means of an estimation of SIL requirements for a system and degradation of SIL during the exploitation period.

SIL-based approach uses obtained time-dependent PFH functions for a monosystem and for a system with applied redundancy architecture to calculate the corresponded safety integrity level at any period of time. This approach can be implemented in an intelligent system that will periodically recalculate PFH value of a system and related SIL. An intelligent system will notify an operator about a close border between SILs. In addition, based on introduced method, it can be suggested two modes of maintenance for a braking system of moving walks: full and economical. In a full maintenance mode the system has to be completely recovered till the initial value of reliability. In an economical mode SIL will be kept on the required level, but the system will be recovered partially by means of replacement/repair of the elements with the worst reliability characteristics. Time of periodical maintenance t_{per} is different in these two modes. In case of full mode t_{per} is constant. In case of economical mode, this time is reduced every maintenance period.

6 CONCLUSIONS

The described SIL-based method of reliability prognosis is based on a combination and interaction of requirements and recommendations of safety standards. This method meets requirements of related standards required for studying of safety of braking system of moving walks. These standards are compared, classified and divided into several groups.

Time-dependent PFH functions for a monosystem ($PFH_{1oo1}(t)$) and for a system with redundancy ($PFH_{1oo2D}(t)$) were obtained and demonstrated on Figure 3. The area of this graph was divided into several areas with different SIL for the system with and without redundancy. The graph demonstrates reliability improvement after applying redundancy. This approach allowed introducing an intelligent system that will recalculate reliability values during the exploitation period and compare them with appropriate SIL requirements. The intelligent system can predict possible failures by means of detecting close SIL border between two areas which means increase of PFH value (Fig. 3). The decision about replacement or repair of equipment is made by means of a calculation of the system reliability. If this value doesn't meet the SIL requirements, the system notifies an operator about the necessity to plan maintenance.

Maintenance procedure, used now on moving walks, can be simplified by means of this approach. The method also allows creating a suitable tool for engineers, constructors and audit companies to check safety of people transportation equipment in buildings, supermarkets, metro and other objects of civil engineering. The developed method can be applied not only for braking systems of moving walks, but also for other technical systems with degradation of their reliability parameters over time.

The future work relates to the verification, the validation of the described methods, and further development of the intelligent system. The application of this intelligent system will allow correction of Weibull parameters in online mode based on braking time. Subsequent study also will be focused on mathematical justification of the correspondence between risk classes and SILs for elevators, escalators and moving walks, which can be summarize in a table. Such a table of correspondence could be a suitable tool for engineer-constructors, project managers, audit companies, and important supplement to the existing sector application standards.

ACKNOWLEDGEMENTS

This research is financially supported by LiftInstituut, Amsterdam.

REFERENCES

Al-Sharif, L. 2006. Intelligent Braking Systems for Public Service Escalators, Lift-report 4.

Azianti, I. & Won, J. 2013. Research Trends in Automotive Functional Safety, 2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering QR2MSE; Proc. intern. conf., Emeishan, Sichuan, China, 15–18 July 2013. IEEE.

Bloch, H.P. & Geitner, F.K. 1994. Machinery failure analysis and troubleshooting. 3rd ed. Houston, Texas: Gulf Publishing Company.

EN 115-1+A1. 2010. Safety of escalators and moving walks—Part1: Construction and installation.

Fedorov, Y.N. 2008. APCS Engineering Handbook: design and development. Moscow: Infra-Ingeneriya. Russian.

Gojian, N. et al. 2009. A review on degradation models in reliability analysis, the 4th World Congress on engineering asset management; Proc. intern. congr. Athens, Greece 28–30 September 2009. Springer.

IEC 60300-3-1. 2003. Dependability management Part 3-1: Application guide—Analysis techniques for dependability—Guide on methodology.

IEC 61511-1. 2004. Functional safety—Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements.

IEC 61649. 2008. Weibull analysis.
IEC 61508-1. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.
IEC 61508-2. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-5. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels.
IEC 61508-6. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.
ISO/IEC 2382-14. 1997. Information technology—Vocabulary-Part 14: Reliability, maintainability and availability.
ISO 13849-1. 2008. Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design.
ISO 14798. 2009. Lifts elevators, escalators and moving walks—Risk assessment and reduction methodology.
ISO 12100. 2010. Safety of machinery—General principles for design—Risk assessment and risk reduction.
ISO/TR 14121-2. 2012. Safety of machinery—Risk assessment—Part 2: Practical guidance and examples of methods.
ISO/TR 22100-2. 2013. Safety of machinery-Relationship with ISO 12100—Part 2: How ISO 12100 relates to ISO 13849-1.
ISO 22201-2. 2013. Lifts elevators, escalators and moving walks—Programmable electronic systems in safety related applications—Part 2: Escalators and moving walks PESSRAE.
Kuo, W. et al. 2001. Optimal reliability design. Fundamentals and applications. Cambridge: Cambridge University Press.
Leveson, N.G. 2011. Engineering a safer world. Cambridge, Massachusetts: The MIT Press.
Mccann, M & Zaleski, N. 2006. Deaths and injuries involving elevators and escalators. Deaths and injuries involving elevators or escalators 3rd ed. The Center to Protect Workers' Rights Report. 2006 Dec, p.12.
Rogova, E.S. 2012. Risk analysis of technological system in Interlock system conception for ITER. Manual for APCS engineers. Moscow: Typography NRNU MEPhI. Russian.
Scott Tyson, A. 2010. Metro escalator brake, maintenance problems widespread. The Washington post. 2010 Nov 14.
Sun, L. & Jia, Y. 2011. Research of equipment reliability prognosis model based on SVR. 2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering ICQR2MSE; Proc. intern. conf., Xi'an, China, 17–19 June 2011. IEEE.
Weibull Database [Internet]. Humble TX: Barringer & Associates, Inc. c 2010—[cited 2014 Feb 17]. Available from: http://www.barringer1.com/wdbase.htm.

This page intentionally left blank

Occupational safety

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A Bayesian population variability analysis for estimation of the work time loss distributions due to occupational accidents

M.C. Moura, R. Azevedo & E.L. Droguett
CEERMA, UFPE, Brazil

L. Rego & W. Jorge
UFPE, Brazil

R. Vilela
CHESF, Brazil

ABSTRACT: Occupational accidents pose several negative consequences to employees, employers, environment and people surrounding the local where the accident takes place. Thus, this paper proposes a Bayesian population variability analysis-based method for the prediction of work time loss distributions due to occupational accidents. The use of Bayesian analysis aims at investigating future trends regarding occupational accidents in the workplace as well as enabling a better management of the labor force. In fact, the key performance indicators here estimated are the expected unavailability of the labor force and also the expected recovery time from an accident which will be computed by a Markov-based model. Finally, the paper presents a practical example by using available data on occupational accidents from a hydroelectric power company in Brazil to predict the work time losses and their respective distributions.

1 INTRODUCTION

Occupational accidents pose several negative consequences to employees, employers, environment and people surrounding the local where the accident takes place (Marcoulaki et al. 2012). Therefore, it is imperative to develop adequate safety policies and operational procedures that minimize the probability of occurrence of occupational accidents. To do that, it is required to predict measures such as the expected work time loss.

As in failures analysis this process consists of two main steps: (i) inference of reliability quantities that explain the stochastic mechanism that originate the accident/recovery process such as accidents and recovery rates and (ii) characterization of accidental behavior by applying stochastic process analysis methods (e.g. Markov process).

A lot of research has been done on the quantitative analysis of occupational accident data. This includes modeling of occupational accident frequency (Marcoulaki et al. 2012, Marcoulaki et al. 2011, Meel et al. 2007) and work time losses (Marcoulaki et al. 2012, Blanch et al. 2009). Several authors have used descriptive statistics and factor analysis, as Babu & Nayak (2003). From the 90's, Bayesian inference methods have long been used for the analysis of accident databases (Hora & Iman, 1990) to model uncertainties and enable future predictions but very few studies deal with prediction of work time loss (Marcoulaki et al. 2012).

For Meel et al. (2007), the use of advanced Bayesian prediction methods is more suitable due to the scarcity and censorship of accident data. Meel & Seider (2006) and Meel et al. (2007) developed a Bayesian approach for the assessment of accident frequency in petrochemical industries in Europe. Marcoulaki et al. (2012) extended the Meel's model by including analysis on work time loss and unavailable due occupational accidents.

Marcoulaki et al. (2012) assumed that all workers have the same accident and recovery rates. Thus, the authors used data from all workers together and treated them as homogenous in order to formulate the likelihood function of the Bayesian model. However, due to the existence of subjective and individual characteristics it is expected that a same class of employees have a unique accident and recovery rates even though they have similar functions in the workplace or are allocated in the same occupational environment as other employees. Therefore, a population variability assessment over the rates is more appropriate for accidents analysis.

Thus, this paper proposes a Bayesian population variability analysis-based method for this

problem. Bayesian population variability analysis is an estimation procedure for the assessment of the variability of reliability measures among a group of similar systems/employees. Moreover, a Markov-based model is proposed for investigating future trends regarding occupational accidents in the workplace as well as enabling a better management of the labor force from the results of the population variability analysis. In fact, the key performance indicators here estimated by the Bayesian models will be the expected unavailability of the labor force and, consequently, the expected recovery time from an accident which will be computed by a Markov-based model. Thus, the Markov-based model will work as a simulation algorithm to generate the accident and recovery times for the workers. To do that the numerical method proposed by Moura & Droguett (2009) will be used because it is efficient to estimate the expected unavailability curve and associated uncertainty.

The remainder of this paper is organized as follows. Section 2 presents the theoretical background about the Bayesian Population Variability Analysis. Section 3 presents the proposed model, while Section 4 discusses the numerical results using evidence from a real accident database of a hydroelectric power company in Brazil. Finally, section 5 presents concluding remarks.

2 THEORETICAL BACKGROUND

2.1 *Bayesian population variability assessment for accident analysis*

The failure and repair rates of a system are often used to characterize our expectations regarding the system's ability to perform its intended function. Likewise, we can use these measures to represent our prospects about the workers safety making the accident an expression of our personal uncertainty about the workers accidental behavior (Singpurwalla, 1988).

Thus, let ρ be a random variable that defines the accident or recovery rate of an employee and $\varphi(\rho) = (\rho/\theta_1, \ldots, \theta_r)$ denote the parametric variability distribution model. Then, a probability distribution $\pi(\theta_1, \ldots, \theta_r)$ over the parameters $\theta_1, \ldots, \theta_r$ of the model can be used to describe the uncertainty about the population variability distribution. The estimated population variability density is taken as

$$\hat{p}(\rho) = \int \ldots \int_{\theta_1, \ldots, \theta_r} \varphi(\rho \mid \theta_1, \ldots, \theta_r) \cdot \pi(\theta_1, \ldots, \theta_r) \cdot d\theta_1 \ldots d\theta_r \quad (1)$$

Therefore, the estimated density function consists of a weighted mix of distributions of the chosen model. This is opposed to estimation methods as the Maximum Likelihood Estimators which is based in a single 'best' distribution chosen from the set of distributions.

The Bayesian population variability analysis of ρ assumes that the distribution $\pi(\theta_1, \ldots, \theta_r)$ is uncertain and a Bayesian method is applied to infer it. For this, in addition to the collected accident data is necessary to have prior information about the population variability. Let E_0 be prior evidence that provides information about the π distribution, i.e. E_0 is the prior knowledge over π without considering data recorded (e.g. the expert's estimates about the probability distributions of $(\theta_1, \ldots, \theta_r)$. Then, $\pi_0(\theta_1, \ldots, \theta_r) = \pi(\theta_1, \ldots, \theta_r \mid E_0)$ is the prior probability distribution of the population variability distribution parameters $(\theta_1, \ldots, \theta_r)$ and $\hat{p}_0(\rho \mid E_0) = \int \ldots \int \theta_1, \ldots, \theta_r \, \varphi(\rho \mid \theta_1, \ldots, \theta_r) \times \pi_0(\theta_1, \ldots, \theta_r) \cdot d\theta_1 \ldots d\theta_r$ is the prior population variability distribution of ρ.

Let the evidence E_1 include the information about the accidents database i.e. the information obtained from accidents records. Then, the employees' population distribution over ρ, conditional on E_0 and E_1 is given by

$$\hat{p}_1(\rho \mid E_0, E_1) = \frac{P(E_1 \mid \rho, E_0) \cdot \int_{\underline{\theta}} \varphi(\rho \mid \underline{\theta}) \cdot \pi_0(\underline{\theta}) \cdot d\underline{\theta}}{\int_{\rho} P(E_1 \mid \rho, E_0) \cdot d\rho \cdot \int_{\underline{\theta}} \varphi(\rho \mid \underline{\theta}) \cdot \pi_0(\underline{\theta}) \cdot d\underline{\theta}} \quad (2)$$

where $\underline{\theta} = \{\theta_1, \ldots, \theta_r\}$ and $P(E_1 \mid \rho, E_0)$ is the likelihood of the evidence E_1. The posterior distribution of the population variability parameters based on information types E_0 and E_1 is developed by applying the Bayes' theorem:

$$\pi_1(\underline{\theta} \mid E_0, E_1) = \frac{P(E_1 \mid \underline{\theta}, E_0) \cdot \pi_0(\underline{\theta})}{\int_{\underline{\theta}} P(E_1 \mid \underline{\theta}, E_0) \cdot \pi_0(\underline{\theta}) \cdot d\underline{\theta}} \quad (3)$$

Therefore, it's possible to evaluate the posterior population variability distribution of the accident or recovery rate by making $\hat{p}_1(\rho \mid E_0, E_1) = \int_{\underline{\theta}} \varphi(\rho \mid \underline{\theta}) \times \pi_1(\underline{\theta} \mid E_0, E_1) . d\underline{\theta}$ (Kaplan 1983, Deely & Lindley, 1981).

Assuming that the accidents occurring in each employee are independent, the likelihood function of the exposure data becomes

$$P(E_1 \mid \underline{\theta}, E_0) = \prod_{i=1}^{n} P(E_{1i} \mid \underline{\theta}, E_0) \quad (4)$$

where $P(E_{1i} \mid \underline{\theta}, E_0)$ is the probability of observing evidence E_{1i} for the i-th out of n employees. Note that the accident measure for the i-th worker, ρ_i, is not known exactly and therefore $P(E_{1i} \mid \underline{\theta}, E_0)$ is given as a function of ρ_i ($P(E_{1i} \mid \underline{\theta}, E_0, \rho_i)$). We know

that ρ_i is one of possibly many values of variable ρ. Moreover, according to our model, ρ is distributed according to $\varphi(\rho|\underline{\theta})$, and $\underline{\theta}$ is also unknown. Therefore, we calculate the probability of observing the information E_{1i} by allowing the accident measure to assume all possible values i.e. by averaging ($P(E_{1i}|\underline{\theta},E_0,\rho)$ over the distribution of ρ:

$$P(E_{1i}|\underline{\theta},E_0)=\int_{\rho}P(E_{1i}|\underline{\theta},E_0,\rho)\cdot\varphi(\rho|\underline{\theta})\cdot d\rho \quad (5)$$

3 A POPULATION VARIABILITY AND MARKOV-BASED INTEGRATED MODEL

3.1 *The timeline of the worker*

The assessment of the likelihood function (4) is mainly based on the exposure data i.e. the number of accidents or recoveries by the operational time of a worker (runtime data). In general, the employment time is not necessarily the same for all workers. Therefore, only knowing the number of accidents suffered in an observation period is not sufficient. The observation of the timeline for each worker allows obtaining exposure data (Marcoulaki et al. 2012).

Then, consider that any occupational accident is reported and recorded. Typically, the registration and reporting forms of occupational accidents contains the accident date and the duration of the recovery period following the accident. This information, in addition the admission and dismissal dates, sets the timeline for each work as illustrated in Figure 1.

Figure 1 shows the timeline for a workplace with 12 workers during a period of observation starting at time T_S and terminating at T_F, where $T_{Si} \geq T_S$ and $T_{Fi} \leq T_F$ are, respectively, the starting and finishing times of i-th worker. If $T_{Si} > T_S$ then the worker was admitted after the initial observation period and, similarly, if $T_{Fi} < T_F$ then the worker was fired before the final observation period. In the interval $[T_{Si}; T_{Fi}]$ the worker is involved in K_i accidents. The working time of worker n between k_{n-1} and k_n ($k_n = 1, 2, \ldots, K_n$) is denoted by t_{n,K_n}. The respective recovery time is denoted by r_{n,K_n}. The time range between the recovery from the last accident, K_n, and T_{Fn} is denoted by s_n.

The staring times T_{S1}, T_{S2}, T_{S3}, T_{S6}, T_{S7}, T_{S9}, T_{S10} and T_{S11} coincide with T_S; this means these workers were hired before or at T_S. The finishing times T_{F1}, T_{F2}, T_{F3}, T_{F4}, T_{F5}, T_{F7}, T_{F10} and T_{F11} coincide with T_F i.e. the workers 1, 2, 3, 4, 5, 7, 10 and 11 remained working after T_F. Only workers 1, 2, 3, 7, 10 and 11 are employed over the whole exposure time, while the others work only for a fraction of this time. Workers 3, 5, 8 and 11 have no accidents, so $s_3 = T_{F3} - T_{S3}$, $s_5 = T_{F5} - T_{S5}$, $s_8 = T_{F8} - T_{S8}$ and $s_{11} = T_{F11} - T_{S11}$. The contract of worker 9 expires when he recovers from his last accident, thus $s_9 = 0$ (it is noteworthy that some regulations protect workers from this type of situations, giving him a labor warranty for a specified period after the recovery from an accident. However, this example is useful for illustration). Ultimately, the finish time (T_F) occurs before the worker 10 back to work, therefore the recovery time $r_{10,1}$ is said to be censored and there is no s_{10}.

Note that $T_n = \left(\sum_{i=1}^{K_n} t_{n,k_i}\right) + s_n = T_{Fn} - T_{Sn} - R_n$ (where $R_n = \sum_{i=1}^{K_n} r_{n,k_i}$) represents the total time for which the worker n was submitted to the risks of occupational accidents. Thus, we can determine the exposure data of each work by the pair (K_n, T_n). Similarly we can determine the exposure data for the recovery data by the pair (K_{Rn}, R_n), where K_{Rn} is the number of recoveries of the worker n. Thus, it is possible to use the censored data found in the database available. Table 1 illustrates the exposure data extracted from in Figure 1. The information in Table 1 provides a clear view of the E_1 evidence needed for the likelihood function construction in the population variability model ($E_{1\lambda}$ corresponds to E_1 type evidence for the accidents rate analysis and $E_{1\mu}$ corresponds to E_1 type evidence for the recovery rate analysis).

3.2 *The population variability analysis construction*

3.2.1 *Mixed likelihood model*

In order to perform a population variability analysis of accident or recovery rate we need to specify an appropriate probability distribution to describe the underlying variability of the measure of interest, $\varphi(\rho|\underline{\theta})$, as well as construct the likelihood function $P(E_1|\underline{\theta},E_0)$. The specification of the probability distribution describing the variability may be guided by the nature of the accident measure. According to Droguett et al. (2004), the use of the Gamma or Lognormal distribution is suitable for representing the variability in the number of failure of the various systems with different failure rates. Thus, let us consider the population variability of the accident measure is given by a lognormal distribution i.e.

$$\varphi(\rho|v,\tau)=\frac{1}{\sqrt{2\pi}\rho\tau}e^{-\frac{1}{2}\left(\frac{\ln\rho-v}{\tau}\right)^2} \quad (6)$$

where v and τ are the parameters (mean and standard deviation). The Lognormal distribution can be

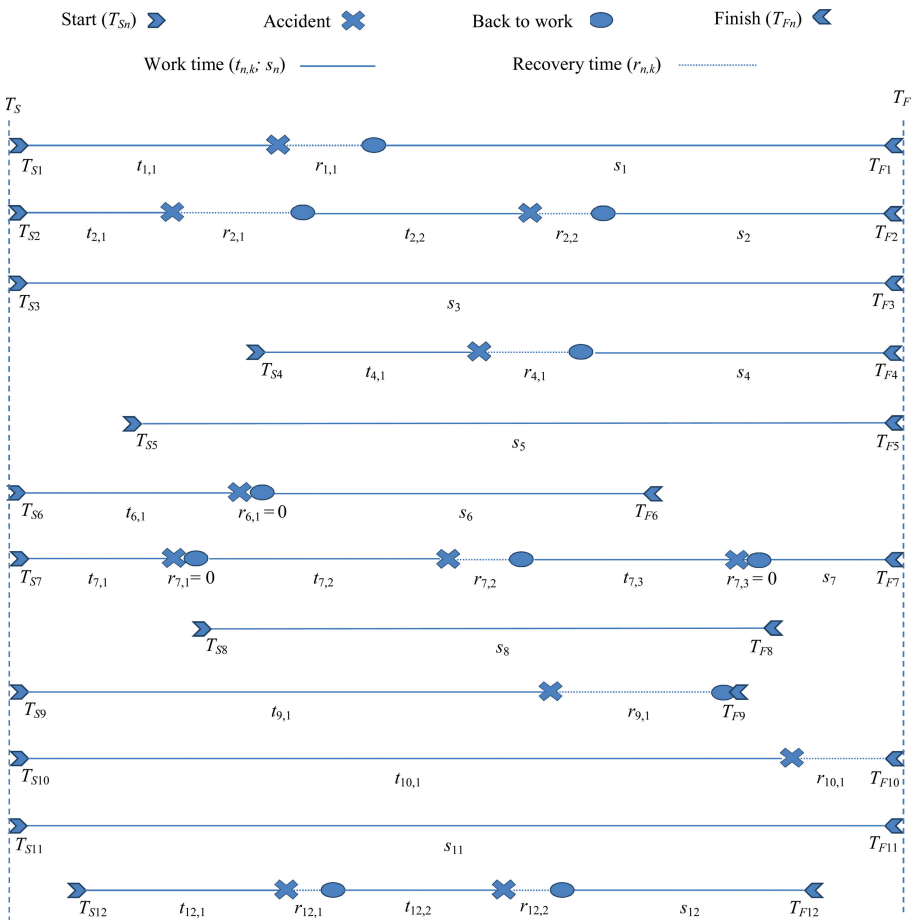


Figure 1. Timelines for a workplace with 12 workers. Source: Adapted from Marcoulaki et al (2012).

Table 1. Exposure data (E_1 evidence) for Figure 1 example.

	$E_{1\lambda}$		$E_{1\mu}$	
Worker (i)	K_i	T_i	K_{Rn}	R_n
1	1	$t_{1,1}+s_1$	1	$r_{1,1}$
2	2	$t_{2,1}+t_{2,2}+s_2$	2	$r_{2,1}+r_{2,2}$
3	0	s_3	–	–
4	1	$t_{4,1}+s_4$	1	$r_{4,1}$
5	0	s_5	–	–
6	1	$t_{6,1}+s_6$	1	$r_{6,1}$
7	3	$t_{7,1}+t_{7,2}+t_{7,3}+s_7$	3	$r_{7,1}+r_{7,2}+r_{7,3}$
8	0	s_8	–	–
9	1	$t_{9,1}$	1	$r_{9,1}$
10	1	$t_{10,1}$	0	$r_{10,1}$
11	0	s_{11}	–	–
12	2	$t_{12,1}+t_{12,2}+s_{12}$	2	$r_{12,1}+r_{12,2}$

written in terms of median (ρ_{50}) and error factor ($EF\rho$) of the distribution by making the following changes: $\rho_{50}=e^{\nu}$ and $EF\rho=e^{1.645\tau}$, as illustrated in Equation

$$\varphi(\rho\,|\,\rho_{50},EF\rho)=\frac{1}{\sqrt{2\pi}\cdot\rho\cdot\dfrac{\ln EF\rho}{1.645}}e^{-\frac{1}{2}\left(\frac{\ln\rho-\ln\rho 50}{\ln EF\rho/1.645}\right)^2} \tag{7}$$

The posterior of the variability distribution parameters in Equation

$$\pi_1(\underline{\theta}\,|\,E_0,E_1)=\frac{P(E_1\,|\,\underline{\theta},E_0)\cdot\pi_0(\underline{\theta})}{\int_{\underline{\theta}}P(E_1\,|\,\underline{\theta},E_0)\cdot\pi_0(\underline{\theta})\cdot d\underline{\theta}} \tag{3}$$

can be written as Equation

$$\pi_1(\rho_{50}, EF_\rho \mid E_0, E_1) = \frac{P(E_1 \mid \rho_{50}, EF_\rho, E_0) \cdot \pi_0(\rho_{50}, EF_\rho)}{\int_{\rho_{50}} \int_{EF_\rho} P(E_1 \mid \rho_{50}, EF_\rho, E_0) \cdot \pi_0(\rho_{50}, EF_\rho) \cdot dEF_\rho \cdot d\rho_{50}} \quad (8)$$

$$\varphi(\rho \mid \rho_{50}, EF\rho) = \frac{1}{\sqrt{2\pi} \cdot \rho \cdot \frac{\ln EF\rho}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho - \ln\rho 50}{\ln EF\rho/1.645}\right)^2} \quad (7)$$

$$\pi_1(\rho_{50}, EF_\rho \mid E_0, E_1) = \frac{P(E_1 \mid \rho_{50}, EF_\rho, E_0) \cdot \pi_0(\rho_{50}, EF_\rho)}{\int_{\rho_{50}} \int_{EF_\rho} P(E_1 \mid \rho_{50}, EF_\rho, E_0) \cdot \pi_0(\rho_{50}, EF_\rho) \cdot dEF_\rho \cdot d\rho_{50}} \quad (8)$$

The likelihood construction is an evidence-driven process i.e. it is dependent on the type of the available evidence E_1. In the analysis of accidents is difficult to obtain expert estimates on the accidents rate of each worker individually. In general, the exposure data (as in Table 1) are the only available evidences. Moreover, due to non-homogeneity among workers (as discussed in Section 2), it is not representative to obtain such estimates directly from the accidents databases.

In this way, the likelihood can be constructed. If we know the accident rate $\lambda_i = \lambda$ or the recovery rate $\mu_i = \mu$ of each employee (ρ represents both rates), we can use the Poisson distribution to estimate the likelihood of observing q_i events (K_i accidents or K_{Ri} recoveries) in the time w_i (T_i or R_i):

$$P(q_i \mid w_i, \rho, E_0) = \frac{(\rho \cdot w_i)^{q_i} \cdot e^{-\rho \cdot w_i}}{\Gamma(q_i + 1)} \quad (9)$$

As we only know that ρ is one of the possible values of the rate represented by its population variability distribution $\varphi(\rho \mid \rho_{50}, EF\rho)$, we average the likelihood given by Equation

$$P(E_{1i} \mid \underline{\theta}, E_0) = \int_\rho P(E_{1i} \mid \underline{\theta}, E_0, \rho) \cdot \varphi(\rho \mid \underline{\theta}) \cdot d\rho \quad (5)$$

over all possible values of ρ in order to calculate the probability of the data unconditional on the unknown value of ρ:

$$P(q_i, w_i \mid \rho_{50}, EF_\rho, E_0) = P_i = \int_\rho P(q_i, w_i \mid \rho, E_0) \cdot \varphi(\rho \mid \rho_{50}, EF_\rho) \cdot d\rho \quad (10)$$

Replacing Equations

$$\varphi(\rho \mid \rho_{50}, EF\rho) = \frac{1}{\sqrt{2\pi} \cdot \rho \cdot \frac{\ln EF\rho}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho - \ln\rho 50}{\ln EF\rho/1.645}\right)^2} \quad (7)$$

and

$$P(q_i \mid w_i, \rho, E_0) = \frac{(\rho \cdot w_i)^{q_i} \cdot e^{-\rho \cdot w_i}}{\Gamma(q_i + 1)} \quad (9)$$

into Equation

$$P(q_i, w_i \mid \rho_{50}, EF_\rho, E_0) = P_i = \int_\rho P(q_i, w_i \mid \rho, E_0) \cdot \varphi(\rho \mid \rho_{50}, EF_\rho) \cdot d\rho \quad (10)$$

$$P_i = \int_\rho \frac{(\rho \cdot w_i)^{q_i} \cdot e^{-\rho \cdot w_i}}{\Gamma(q_{i+1})} \cdot \frac{1}{\sqrt{2\pi} \cdot \rho \cdot \frac{\ln EF\rho}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho - \ln\rho 50}{\ln EF\rho/1.645}\right)^2} d\rho \quad (11)$$

The total likelihood is then obtained by replacing Equation

$$P_i = \int_\rho \frac{(\rho \cdot w_i)^{q_i} \cdot e^{-\rho \cdot w_i}}{\Gamma(q_{i+1})} \cdot \frac{1}{\sqrt{2\pi} \cdot \rho \cdot \frac{\ln EF\rho}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho - \ln\rho 50}{\ln EF\rho/1.645}\right)^2} d\rho \quad (11)$$

into Equation

$$P(E_1 \mid \underline{\theta}, E_0) = \prod_{i=1}^{n} P(E_{1i} \mid \underline{\theta}, E_0) \quad (4)$$

$$P(E_1 \mid \underline{\theta}, E_0) = \prod_{i=1}^{n} \int_\rho \frac{(\rho \cdot w_i) q_i \cdot e^{-\rho \cdot w_i}}{\Gamma(q_{i+1})} \cdot \frac{1}{\sqrt{2\pi} \cdot \rho \cdot \frac{\ln EF\rho}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho - \ln\rho 50}{\ln EF\rho/1.645}\right)^2} d\rho \quad (12)$$

3.2.2 *A prior distribution specification*

Application of population variability analysis requires specifying the prior distribution defined over the parameter space of the chosen variability model, representing the prior belief about the variability distribution before the evidence (accident database) becomes available. Some authors propose that the prior be specified in the form of a

discrete prior distribution (Kaplan 1983, Pickard et al. 1985).

The algorithm here adopted involves the specification of an informed continuous prior over the parameter space of the variability model. The analyst is required to provide initial estimates in terms of a central value (median) and the extent of variability (error factor) in the population variability distribution. As discussed in Droguett et al. (2004), these estimates take the form of Lognormal distributions. If the parameters v and τ of the population variability distribution of ρ are distributed as a Lognormal distribution, then the distributions of $\rho_{50} = e^{v}$ and $EF\rho = e^{1.645\tau}$ take the forms

$$f(\rho_{50}) = \frac{1}{\sqrt{2\pi}\cdot\rho_{50}\cdot\dfrac{\ln\varepsilon_{\rho_{50}}}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln\rho_{50}-\ln\gamma_{\rho_{50}}}{\ln\varepsilon_{\rho_{50}}/1.645}\right)^2} \quad (13)$$

and

$$f(EF_{\rho}) = \frac{1}{\sqrt{2\pi}\cdot EF_{\rho}\cdot\dfrac{\ln\varepsilon_{EF_{\rho}}}{1.645}} e^{-\frac{1}{2}\left(\frac{\ln EF_{\rho}-\ln\gamma_{EF_{\rho}}}{\ln\varepsilon_{EF_{\rho}}/1.645}\right)^2} \quad (14)$$

where γ_x and ε_x are the median and error factor of the distribution of x (where x can represents both the median and error factor of ρ). Considering the independence between v and τ then the prior distribution of variability model is $\pi_0(\rho_{50}, EF\rho) = f(\rho_{50}) \times f(EF\rho)$. The definition of prior distributions consists in to determine the values $\gamma_{\rho 50}$, $\varepsilon_{\rho 50}$, $\gamma_{EF\rho}$ and $\varepsilon_{EF\rho}$ (e.g. by specialist's opinions):

$$\pi_0(\rho_{50}, EF_{\rho}) = f(\rho_{50}\,|\,\gamma_{\rho_{50}}, \varepsilon_{\rho_{50}})\cdot f(EF_{\rho}\,|\,\gamma_{EF_{\rho}}, \varepsilon_{EF_{\rho}}) \quad (15)$$

So the set $\{\gamma_{\lambda 50}, \varepsilon_{\lambda 50}, \gamma_{EF\lambda}, \varepsilon_{EF\lambda}\}$ corresponds to the E_0 evidence for accident rate analysis and the set $\{\gamma_{\mu 50}, \varepsilon_{\mu 50}, \gamma_{EF\mu}, \varepsilon_{EF\mu}\}$ is the E_0 evidence for recovery rate analysis.

3.2.3 *Variability measures*

The likelihood functions and prior distributions have been incorporated in a Bayesian inference procedure in which the posterior density $\pi_1(\underline{\theta}\,|\,E)$ is computed. The Bayesian inference is performed by using a Markov Chain Monte Carlo Method (MCMC), which allows samples to be generated from a continuous unnormalized density (Chiband & Greenberg, 1995). The MCMC method, which is frequently applied to Bayesian Inference problems (Gilks et al. 1996), results in a m-samples set $S = \{\underline{\theta}_1, \ldots, \underline{\theta}_m\}$, representing the posterior density over the parameters of the variability distribution model $\varphi(\rho\,|\,\underline{\theta})$. Given S, the estimated population variability density is computed as

$$\hat{p}(\rho) = \frac{1}{m}\sum_{i=1}^{m}\varphi(\rho\,|\,\underline{\theta}_i) \quad (16)$$

The corresponding mean and variance are computed as

$$\hat{\mu}_{\rho} = \frac{1}{m}\sum_{i=1}^{m}\mu(\underline{\theta}_i) \quad (17)$$

$$\hat{\sigma}_{\rho}^{\,2} = \frac{1}{m}\sum_{i=1}^{m}\sigma^2(\underline{\theta}_i) \quad (18)$$

where $\mu(\underline{\theta})$ and $\sigma^2(\underline{\theta})$ are the mean and variance of $\varphi(\rho\,|\,\underline{\theta})$.

Furthermore, the generated results include uncertainty bounds of the cumulative variability density $P(\rho) = \int_{x=0}^{\rho} p(x)dx$ in the form of zth percentiles $P_z(\rho)$, defined as $\Pr(P(\rho) < P_z) = z/100$. The zth percentiles are determined by finding the value $\hat{P}_Z(\rho)$ for which for a fraction z/100 of the samples $\underline{\theta}_i \in$ S:

$$\int_{x=0}^{\rho}\varphi(x\,|\,\underline{\theta}_i)\cdot dx < \hat{P}_z(\rho) \quad (19)$$

These bounds provide the analyst with a basis to assess the uncertainty associated with the estimated population variability distribution related to accidents or recovery rates.

3.3 *Estimation of the work time loss distributions by Markov-based model*

As discussed in Section 2 it is assumed that each employee has a unique accident rate even that they have functions similar or be allocated in the same occupational environment as the other employees. This assumption is due to the existence of idiosyncrasies that make every worker particular.

The random behavior, which leads to occupational accidents, and the corresponding recovery of the worker, can be represented by a Markov-based stochastic process as shown in Figure 2. Workers who are in the first state are performing their function normally (they are available for work), while those in the second state are recovering from an accident (on medical leave). Random mechanisms, which lead the worker i to an accident, occur with rate λ_i, so that if the worker was available (State 1) he becomes unavailable (state 2). Another random mechanism recovers the victim to the available

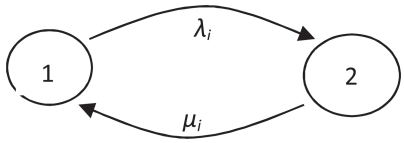


Figure 2. Markov diagram of the stochastic process.

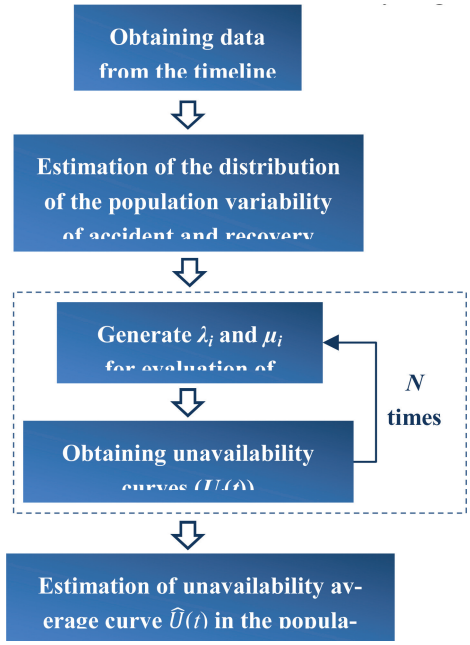


Figure 3. Proposed model.

status with rate μ_i. It is assumed that the two rates, λ_i and μ_i, are independent.

If we know the accident rate λ_i and the recovery rate μ_i we can determine the unavailability curve of the worker by applying some method of solution of the Markov diagram (numerical methods, analytical treatment, simulation, etc.). However, we only know that λ_i and μ_i are one of possibly many values of the variables λ and μ, distributed as $p(\lambda)$ and $p(\mu)$ respectively. $p(\lambda)$ and $p(\mu)$ are estimated by $\hat{p}_1(\lambda|E_{0\lambda},E_{1\lambda})$ and $\hat{p}_1(\mu|E_{0\mu},E_{1\mu})$ from the Bayesian model presented in Section 3.2.

Of course, if workers have different accident and recovery rates, they have different unavailability curves. We can simulate the stochastic process linked to accidental behavior of a worker by generating the values λ_i and μ_i from $\hat{p}_1(\lambda|E_{0\lambda},E_{1\lambda})$ and $\hat{p}_1(\mu|E_{0\mu},E_{1\mu})$. By doing this, we obtain the unavailability curve by solving the Markov process. However, we can't determine the worker for which this result is valid. Repeating this process N times (N must be large enough to ensure the representativeness of the simulation), we obtain an N-samples set where each sample contains one curve of unavailability. Thus, we estimate the average unavailable curve ($\hat{U}(t)$) as

$$\hat{U}(t) = \frac{1}{N}\sum_{i=1}^{N} U_i(t) \tag{20}$$

where $U_i(t)$ corresponds to the curve of the unavailability resulting from the i-th iteration of Markov process.

It is acceptable to assume that $\hat{U}(t)$ represents the fraction of man-hour loss due to occupational accidents. Also, it is possible to define the uncertainty associated with this estimate by the zth percentiles of the set $\{U_1(t), \ldots, U_N(t)\}$.

In this paper, we use the numerical treatment based on transition frequency densities by Moura & Dorguett (2009) to infer unavailability curves. The Population Variability and Markov-based integrated model can then be resumed by Figure 3.

4 EXAMPLE APPLICATION

In this section, we illustrate and discuss the use of the Bayesian Population Variability analysis and Markov-based models by means of an example. We start by supposing that we are interested in assessing the average distribution of work time loss due to occupational accidents for workers of a hydroelectric power company in Brazil. Runtime data were collected from the timeline of operation employees between 01/01/2005 and 09/31/2012 in order to construct the likelihood function.

As discussed in Section 2.1 the Bayesian Population Variability Analysis must be used in a workers population subject to similar risk of accidents. So, in this section, the model is applied to employees with the same job and workplace. The administrators located in the operation sector of the company were analyzed. These workers suffered mainly two types of accidents: (1) accidents in commuting and (2) falls. It is expected that one worker has different accident and recovery rates for each type of accident. Therefore, the model was applied separately for analyzing the work time loss distributions due to accidents in commuting and falls.

4.1.1 *Results*

57 workers were analyzed in a total of 157,784 mendays of work. 27 accidents were recorded in the period, of which 13 are accidents in commuting and 14 are falls. Upon solving the Bayesian population variability and Markov-based integrated

model, the expected unavailability of the population of workers has a 5th and 95th percentiles of 0.00017 and 0.0043 due accidents in commuting an of 0.00025 and 0.008 due falls, respectively, with a mean of 0.0013 for accidents in commuting and of 0.0022 for falls.

If $T_L(t)$, $T_L^{5\%}(t)$ and $T_L^{95\%}(t)$ correspond to the mean and the 5th and 95th percentiles distributions of expected work time lost by one worker of population then the mean and the 5th and 95th percentiles distributions of expected work time lost in the population of workers ($T_P(t)$, $T_P^{5\%}(t)$ and $T_P^{95\%}(t)$) can be obtained by multiplying the $T_L(t)$, $T_L^{5\%}(t)$ and $T_L^{95\%}(t)$ by the number of workers in population. This means that the expected work time loss by workers located in the operation sector in one year is $0.46 \times 57 = 26.35$ men-days due to accidents in commuting and $0.81 \times 57 = 46.33$ men-days due to falls, amounting 72.68 men-days loss per year among the workers located in operation sector of the hydroelectric power company. The corresponding 5th and 95th percentiles are $0.063 \times 57 = 3.60$ and $1.58 \times 57 = 90.10$ for accidents in commuting and $0.09 \times 57 = 5.10$ and $2.9 \times 57 = 165.81$ for falls. Figures 4 and 5 illustrate the expected work time loss curves for accidents in commuting and for falls.

4.1.2 *Validation*

To validate the application of the model we generate the data from the results of the Bayesian population variability model in order to compare them with the actual data. The Bayesian model applied in the real case provides estimations for population variability distributions of accidents and recoveries rates. From these distributions we generate the accidents and recoveries data of workers. It is expected that these data can represent the accident-recovery process of this population of workers.

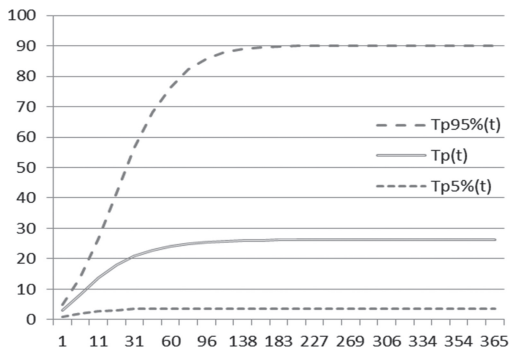


Figure 4. Work time loss distributions for accidents in commuting.

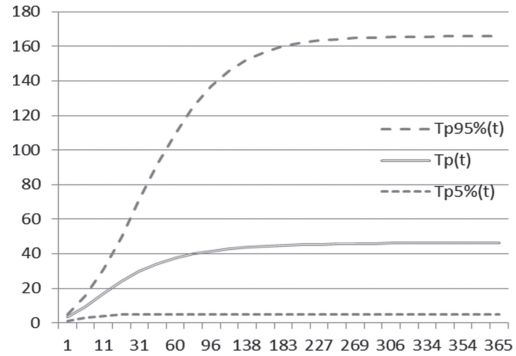


Figure 5. Work time loss distributions for falls.

Table 2. *p*-values of the hypothesis tests.

Test	Accidents in commuting	Falls
Time to accident	0.1871	0.125
Time to recovery	0.2606	0.1755
Unavailable	0.2606	0.1705

These data were compared with the actual data by application of the statistic Kruskal hypothesis test (Kruskal & Wallis, 1952) under the null hypothesis that the data follow the same distribution. Three tests were realized for each type of accident: (i) test on time to accident, (ii) test on time to recovery and (iii) test on unavailability, amounting six (6) hypothesis tests. Table 2 shows the *p*-values of each test.

All *p*-values are greater than 0.1, then we can say that there is no evidence to reject the null hypothesis. Furthermore, we can accept the null hypothesis to be true i.e. the simulated and actual data come from the same distribution since the *p*-values in Table are large. This result validates the proposed model in this paper because it proves the efficiency of the model to represent the real population.

5 CONCLUDING REMARKS

The model presented in this paper represents an extension of the Bayesian population variability assessment method in accidents analysis. A Markov-based model is used for estimation of the expected work time loss distributions due to occupational accidents. The Bayesian population variability assessment method allows the evaluating of population variability of accidents and recovery rates based on exposure data of workers submitted to same occupational risks and the Markov-based model is used to derive the worker unavailability

statistics to predict the amount of time that workers will be recovering from accidents and therefore won't be available to perform the job they are paid for. The use of the population variability analysis allows to assess the uncertainty presented on the results of the Markov-based model.

The models developed here can be informed using available databases of occupational accidents documented in the industries. Sufficient statistics to use the models include only the number of workdays, the workdays loss due to recovering from occupational accidents, and the number of occupational accidents over the period of observation for each worker.

The implementation of the extension used in the examples in Section 4 has shown that the numerical solution of the models is feasible and provides a good estimation for the expected work time loss distribution due to occupational accidents. Also, the comparison of simulated data, from the population variability distributions, with real data showed that the estimated population variability distributions of the accidents and recoveries rates can be used to represent the actual situation.

REFERENCES

Babu, B.V. & Nayak, A.N. 2003. Treatment costs and work time loss due to episodic adenolymphangitis in lymphatic filariasis patients in rural communities of Orissa, India. *Tropical Medicine & International Healt*, 8: 1102–1109.

Blanch, A., Torrelles, B. & Salinas, J.A. 2009. Age and lost working days as a result of an occupational accident: a study in a shift work rotation system. *Safety Science*, 47(10): 1359–1363.

Chiband, S. & Greenberg, E. 1995. Understanding the Metropolis-Hastings Algorithm. *The American Statistician*, 49(4): 327–335.

Deely, J.J. & Lindley, D.V. 1981. Bayes Empirical Bayes. *Journal of the American Statistical Association*, 76 (376): 833–841.

Droguett, E. et al 2004. The Combined Use of Data and Expert Estimates in Population Variability Analysis. *Reliability Engineering and System Safety*, 83: 311–321.

Gilks, W.R., Richardson, W.R. & Spiegelhalter, D.J. 1996. *Markov Chain Monte Carlo in Practice*. London: Chapman & Hall.

Hora, S.C. & Iman, R.L. 1990. Bayesian modeling of initiating event frequencies at nuclear power plants. *Risk Analysis*, 10(1): 103–109.

Kaplan, S. 1983. On a 'Two-Stage' Bayesian Procedure for Determining Failure Rates from Experimental Data. *IEEE Transactions on Power Apparatus and Systems*, 102(1):195–199.

Kruskal, W.H. & Wallis, W.A. 1952. Use of Ranks in One-Criterion Variance Analysis. *Journal of the American Statistical Association*, 47(260): 583–621.

Marcoulaki, E.C., Konstandinidou, M. & Papazoglou, I.A. 2011. Dynamic failure assessment of incidents reported in the Greek Petrochemical Industry. *Computer-Aided Chemical Engineering*, 29: 1055–1059.

Marcoulaki E.C. *et al* 2012. Prediction of occupational accident statistics and work time loss distributions using Bayesian analysis. *Journal of Loss Prevention in the Process Industries*, 25: 467–477.

Meel, A. & Seider, W.D. 2006. Plant-specific dynamic failure assessment using Bayesian theory. *Chemical Engineering Science*, 61: 7036–7056.

Meel, A. et al 2007. Operational risk assessment of chemical industries by exploiting incident databases. *Journal of Loss Prevention in the Process Industries*, 20: 113–127.

Moura, M.C. & Droguett, E.L. 2009. Mathematical formulation and numerical treatment based on transition frequency densities and quadrature methods for non-homogeneous semi-Markov processes. *Reliability Engineering & System Safety*, 94: 342–349.

Pickard, Lowe and Garrick, Inc., "Seabrook Station Risk Management and Emergency Planning Study," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0432, December 1985.

Singpurwalla, N.D. 1988. Foundational Issues in Reliability and Risk Analysis. *SIAM Review*, 30(2): 264–282.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Continuous monitoring of at-risk behaviours: A risk-based statistical control method

D. Masi & P. Trucco
Politecnico di Milano, Milan, Italy

ABSTRACT: An effective implementation of the behaviour-based safety approach requires a continuous monitoring of the performance of workers. However, this continuous monitoring is challenging for practitioners due to the great demand of time, cost, and professional skills needed for its implementation. This paper proposes a sustainable solution consisting in a method which combines the continuous safety sampling method, a statistical analysis of non-conforming observations, and a consistent experts' judgements elicitation process based on the analytic hierarchy process.

1 INTRODUCTION

Accidents at work continue to be one of the major work environment challenges facing legislators, enterprises, and workers worldwide. According to the Labour Force Survey (LFS), using data from 2007, the 3.2% of the workforce in the EU-27 reported an accident at work in the past 12 months. This corresponds to approximately 6.9 million persons. In line, data from the European Statistics on Accidents at Work (ESAW) showed that 2.9% of the workers had an accident at work with more than three days of sickness absence and 5580 workers died in a fatal accident in 2007 (Eurostat European Commission. 2010). The data clearly show that accidents at work place a considerable burden on individuals, society and enterprises.

Because of the relevance of the problem, several attempts have been made aiming at improving Occupational Safety and Health (OSH) conditions within enterprises. In particular, several studies focused on the causes of accidents, with the purpose of removing these causes by means of different kinds of interventions. In this regard, there is scientific evidence that unsafe behaviours are a major cause of accidents (see e.g. Heinrich, 1950 and Hide et al., 2003); as a consequence, many approaches aiming at modifying human unsafe behaviours have been proposed in the scientific literature.

Among these, the Behaviour-Based Safety (BBS) approach is gaining an increasing attention in the area of OHS. BBS aims at modifying human unsafe behaviours (Scott Geller, E., 2001) by adding antecedents and/or consequences to the situation to alter response probability (DePasquale & Geller, 2000). Examples of interventions creating antecedents and consequences are Goal Setting and Feedback (DePasquale & Geller, 2000; Cameron & Duff, 2007). A goal of compliance level to safety is an antecedent which alters workers' response: the desire to achieve the goal would motivate workers to make efforts in this direction. On the other hand, positive feedback, incentive or reward are consequences which reinforce workers' safe behaviours.

Over the years, BBS has been applied successfully by many researchers in various settings such as clinical medicine (Dickerson et al., 2010), manufacturing (Hermann et al., 2010), mining (Hickman & Geller, 2003) and institution office (Al-Hemoud & Al-Asfoor, 2006). Moreover, BBS was found to be a promising way to further prevent accidents. Many researchers analysed the OSH records of enterprises which implemented BBS and the results revealed a significant decrease in incidents across groups following the BBS implementation (see e.g. Krause et al., 1999).

Despite these successful implementations, BBS approach faces a critical difficulty in achieving persistent effects. Some studies have reported that behavioural safety performance declined (Johnston et al., 1994; Lingard & Rowlinson, 1998) or even went back to the baseline level (Komaki et al., 1978) after intervention was stopped.

Although many factors may affect the final outcomes of BBS approach, this difficulty is largely attributed to the intervention strategy itself. Basically, BBS intervention focuses on external antecedent and consequence for the reinforcement of safe behaviours (Cameron & Duff, 2007), thus creating OHS improvements with a sensitive dependence on external situations. When the external situation changes, the safety performance

is likely to deteriorate (DeJoy, 2005). As a consequence, a continuous monitoring of the external situation and of the performance of the workers is necessary.

However, this activity is challenging due to the great demand of time, cost and professional skills for its implementation. In the light of the relevance of this practitioners' challenge, this paper proposes a solution consisting in a method which combines three different techniques: the Continuous Safety Sampling Method (CCSM) (Quintana and Nair, 1997), a statistical analysis of non-conforming behaviours, and a consistent experts' judgements elicitation process based on the Analytic Hierarchy Process (AHP).

The paper is structured as follows. In paragraph 2, the CCSM is summarised, due to its relevance for the proposed model. In paragraph 3, the Risk-Based Statistical Control Method is presented, by means of its application in an Italian manufacturing enterprise. Finally, in paragraph 4 main conclusions are taken.

2 THE CONTINUOUS SAFETY SAMPLING METHODOLOGY

The CCSM (Quintana and Nair, 1997) represents a method for the continuous monitoring of the external situation and of the performance of the workers. The methodology aims at collecting information on the safety conditions in a statistically verifiable and economically viable manner by using the principles of work sampling and control charts. The hypothesis is that a random sample of a sufficiently large size, as in work sampling, reflects the state of the system being observed. Sampling aims at observing the occurrence of conditions that may become hazardous in a given system, called dendritics. On the other hand, by providing information regarding the tendency of a system, the control charts in CCSM indicate when systems tend to become hazardous, thus facilitating the implementation of corrective steps.

For the creation of CSSM five steps are necessary:

Step 1—Dendritic construction. This step consists in the identification of the core conditions leading to hazards in any given system. This analysis can be performed by means of a Preliminary Hazard Analysis.

Step 2—Random Sampling. The sampling can be performed in conjunction with other routine job functions, without additional allocation of resources.

Step 3—Control chart. A p-chart is constructed by plotting the daily value of $\overline{p}$ against the date. The $\overline{p}$ is the daily weighted average of all the proportion of non-conforming observation. The Upper Control Limit (UCL) and the Lower Control Limit (LCL) are given by formulas reported in Equation (1) and in Equation (2):

$$UCL = \overline{p} + 3 \cdot \sqrt{\frac{\overline{p} \cdot (1 - \overline{p})}{n}} \tag{1}$$

$$LCL = \overline{p} - 3 \cdot \sqrt{\frac{\overline{p} \cdot (1 - \overline{p})}{n}} \tag{2}$$

Step 4—The control chart observations are tested for "out of control conditions".

Step 5—If an out of control condition is detected, appropriate action is taken to eliminate or control these conditions and thus to maintain a desired safe system.

The application of the above stepwise procedure provides a cost effective way of keeping a continuous check on the safety status of the workplace under consideration.

However, CCSM, in the described formulation, is not adequate for the continuous monitoring of the external situation and of the performance of the workers in a Behaviour-Based Safety perspective. The main limitation is that the model does not provide an estimation of the risk related to the non-conforming behaviours. The method distinguishes between conforming and non-conforming behaviours, without any further clarification on the criticality or on the expected consequences of the behaviours themselves. In fact, different at-risk behaviours are characterized by different criticalities.

When the OHS performance of the whole enterprise is monitored, interventions can be introduced only when the risk related to the non-conforming behaviours is not acceptable, while it is not possible to intervene every time that behaviours are simply non-conforming. If interventions implemented without any estimation of the criticality of the related non-conforming behaviours, resources can be easily wasted in correcting behaviours which are not critical for the improvement of the OSH performance of the enterprise.

In the light of the above, modifications and integrations to the CCSM are necessary for the continuous monitoring of the external situation and of the performance of the workers in a Behaviour-Based Safety perspective. This paper proposes a risk-based statistical control method which is grounded on the original CCSM and which overcomes its mentioned limitations by combining CCSM with a statistical analysis of non-conforming behaviours, and with a consistent experts' judgements elicitation process based on the Analytic Hierarchy Process (AHP).

The risk-based statistical control method redefines some parameters proposed by CCSM, thus shifting the method from a simply non-conforming based method into a risk-based method. The method has been tested by means a pilot application in an Italian manufacturing company which produces tractors. The method, together with the results obtained during its empirical application, are presented in the following paragraph.

3 THE RISK-BASED STATISTICAL CONTROL METHOD

Coherently with the steps proposed by CCSM, for the creation of the model five steps are necessary, which consists in (1) Dendritic construction, (2) Random Sampling, (3) Control chart design (4) Test for "out of control conditions, and (5) Action.

Step 1—The dendritic construction consists in the identification of the core conditions leading to hazards in the system. A preliminary hazard analysis has been performed in the monitored enterprise, and a checklist of behaviours leading to hazards has been identified. The dendritics leading to hazards have been classified in different groups. These dendritics are reported in Table 1. Many of the identified dendritics are workers' behaviours; however, some dendritics more related to contextual aspects, such as obstacles not clearly indicated, have been included.

The contemporary assessment of behavioural and contextual conditions potentially determining accidents is one advantage of the model, which allows for an unique analysis of all the aspect that determine the OSH performance of the company. Each of the dendritics is assessed during the inspection, and 1 is used for the indication of non-conformity, while 0 is used to state conformity.

Step 2—The sampling can be performed in conjunction with other routine job functions, without additional allocation of resources. In the analysed enterprise, the sampling has been done by monitoring the safety conditions of the "Transmissions" department, during 19 work-shifts.

Step 3—Control chart. The main modification introduced in the model consists in the way in which the control chart is designed. Instead of the p-chart proposed by CCSM, the model uses a R-chart, which means Risk-chart. A R-chart is constructed by plotting the daily value of $\bar{R}$ against the date. $\bar{R}$ is the daily weighted average of all the proportion of non-conforming Risks. The Upper Control Limit (UCL) and the Lower Control Limit (LCL) are given by the formulas reported in Equation (3) and in Equation (4)

Table 1. Checklist of dendritics.

Machinery and tools
D1 Tools are not correctly used
D2 Tools are not adequate or in non-adequate conditions
D3 Heavy objects are not ergonomically stored
D4 Materials are not ergonomically stored in cart lifts
PPEs
D5 Workers do not use protective gloves necessary for the task
D6 Workers do not use protective glasses necessary for the task
Procedures
D7 Procedures are not adequate
D8 Procedures are not known or not understood
D9 Procedures are not followed
D10 Lifting carriages are not correctly used
D11 Suspended loads are not correctly harnessed
D12 Forklifts are not used according to the procedures
D13 Forklifts stop close to pedestrian crossings
D14 Safety belt is not used
D15 Use of music earphones
Working environment
D16 Obstacles are not clearly indicated
D17 Floor and corridors are not clean
D18 Materials and tools are not stored in the special containers
D19 Lack of indications for the use of the tools
D20 Waste containers are full
D21 Lifting carriages are not correctly functioning
D22 Forklifts stop in forbidden areas
D23 Lockout procedures are not correctly followed
D24 Safety devices are not correctly used
D25 Lack of indications for the shelves

$$UCL = \bar{R} + 3 \cdot \sqrt{\frac{\bar{R} \cdot (1 - \bar{R})}{n}} \tag{3}$$

$$LCL = \bar{R} - 3 \cdot \sqrt{\frac{\bar{R} \cdot (1 - \bar{R})}{n}} \tag{4}$$

Risk is defined as the product between the severity of consequences (D) and the probability of occurrence of the accident (E) and of its related causes C_k, as indicated in Equation (5).

$$R = D \cdot P(E, C_1, C_2, \ldots, C_n) \tag{5}$$

The probability of occurrence of the accident and of its related causes can be calculated by means of Bayesian marginalisation, i.e. the summation of the products between the probability of occurrence of the accident, conditional to the occurrence of the k-cause $P(E/C_k)$, and the prob-

ability of occurrence of the cause $P^*(C_k)$, as indicated in Equation (6).

$$P(E, C_1, C_2, \ldots, C_n) = \sum_{k=1}^{N} P(E/C_k) \cdot P^*(C_k) \quad (6)$$

It is important to underline that the first term $P(E/C_k)$ has to be estimated during the setting of the model, and it is kept constant in further observations, while the second term $P^*(C_k)$ is obtained by the daily observation of non-conforming dendritics.

The probability $P(E/C_k)$ can be easily estimated using the Bayes' theorem, as shown in Equation (7)

$$P(E/C_k) = \frac{P(C_k/E) \cdot P(E)}{P(C_k)} \quad (7)$$

In Equation (7), $P(C_k/E)$ indicates the probability that an accident occurs as the direct consequence of the occurrence of the k-cause; $P(E)$ indicates the probability of occurrence of the accident, and $P(C_k)$ indicates the prior estimation of the probability of occurrence of the k-cause. An estimation of these three terms is necessary.

The probability of occurrence of an accident $P(E)$ has to be estimated during the setting of the model, and kept constant in further observation. The historical value of $P(E)$ during the year t, called $P(E)_t$, can be estimated as ratio between the number of accidents happened during one year and the number of total worked hours. The actual value of $P(E)$ can be estimated by applying exponential smoothing to the historical values. In the analysed case, the historical values of the last three years have been used; these values are reported in Table 2. Exponential smoothing (Equation 8) has been applied to the historical values $P(E)_t$ reported in Table 2.

$$S_t = P(E)_t + (1 - \alpha) \cdot S_{t-1} \quad (8)$$

In Equation (8), the initial value of the S_1 has been calculated as value of the first year, and the parameter alpha has been set to 0,9 in order to give higher importance to the most recent data. Indeed, the interventions progressively implemented improve the OHS conditions of the enterprise, and it is possible to predict that this trend is ongoing. The final estimation, calculated with exponential smoothing, is $P(E) = 0{,}39$.

The initial estimation of the probability of occurrence of the k-cause $P(C_k)$ has been calculated as ratio between non-conforming observations and total observations during five working shifts. Some representative values of $P(C_k)$, with the relative number of non-conforming observation, are reported in Table 3.

$P(C_k/E)$, namely the probability that the k-cause will generate an accident, has been estimated by combining an estimation from historical data $P(C_k/E)_t$ and experts' judgments $P(C_k/E)_{AHP}$.

As for the estimation from historical data $P(C_k/E)_t$, coherently with the technique used for the estimation of $P(E)$, the data of the last three years have been used. $P(C_k/E)_t$ has been estimated as ratio between the occurrences of accidents generated by the k-cause $\#(E/C_k)_t$ of the considered year and the total number of accidents of the considered year $\#\ accidents_t$. This ratio is shown in equation (9).

$$P(C_k/E)_t = \frac{\#(E/C_k)_t}{\#\ accidents_t} \quad (9)$$

On the other hand, experts' judgments $P(C_k/E)_{AHP}$ has been obtained using the Analytic Hierarchy Process (Saaty, 2008). The Analytic Hierarchy Process (AHP) is a theory of measurement through pairwise comparisons and relies on the judgements of experts to derive priority scales. It is these scales that measure intangibles in relative terms. The comparisons are made using a scale of absolute judgements that represents, how much more, one element dominates another with respect to a given attribute. Five experts were interviewed: the production engineer, the technology development engineer, the safety engineer, the safety manager, and the responsible for workshop machining. The experts were asked to pairwise evaluate the k causes by means of the following question: "Which of the two causes has the higher probability of generating an accident?".

Table 2. P(E) calculated for the last three years.

Year	Accidents	$P(E)_t$
1	117	0,53
2	96	0,44
3	84	0,38

Table 3. Examples of values of $P(C_k)$.

Dedritics	Non-conf. obs.	Total obs.	$P(C_k)$
Tools are not correctly used	3	224	0,01
Tools are not adequate or in non-adequate conditions	6	224	0,03

The results consists in a set of weights related to the k-causes of accidents.

The estimation from experts' judgments $P(C_k/E)_{AHP}$ and the estimation from historical data $P(C_k/E)_t$ have been mediated when possible. Indeed, the historical data did not contain any reference to some of the k-causes. For these k-casues, the final estimation $P(C_k/E)$ is equal to the estimation collected through experts' judgments $P(C_k/E)_{AHP}$. Some examples of final estimations are reported in Table 4.

Having estimated all the terms necessary to the estimation of the probability $P(C_k/E)$, the last parameter estimated is the severity of consequences (D). Again, the historical value of D during the year t, called D_t, can be estimated as ratio between the number of work shifts lost because of accidents and the total number of working hours, multiplied by 1000, as reported in equation (10).

$$D_t = \frac{\#\,work\ shifts\ lost}{\#\,working\ hour} \cdot 1000 \tag{10}$$

The actual value of D can be estimated by applying exponential smoothing to the historical values. Also in this case, the simple exponential smoothing has been used with data of the last three years. Alpha has been set to 0,9 since the hypothesis is that OHS interventions implemented in the last years progressively reduce the number of injuries and that this positive trend will continue in the future. The historical values D_t are reported in Table 5.

The application of an exponential smoothing with alpha = 0,9 gives a final value of D equal at 0,97.

Table 4. Examples of estimation of $P(C_k/E)$.

Dedritics	$P(C_k/E)_{AHP}$	$P(C_k/E)_t$	$P(C_k/E)$
Tools are not correctly used	0,08	–	0,08
Tools are not adequate or in non-adequate conditions	0,09	0,07	0,08

Table 5. Data used for the estimation of D by exponential smoothing.

Year	D_t
1	1,03
2	1,06
3	0,96

Having estimated all the terms of Equation (7), it is now possible to calculate the criticality of the k-cause. The criticality is defined by Equation 11.

$$Criticality_k = D \cdot P(E/C_k) \tag{11}$$

The criticality calculated for some of the k-causes is reported in Table (6).

The criticality is used for weighting the estimations of $P^*(C_k)$ obtained by the day-by-day observed non-conforming dendritics.

Having estimated all the terms of Equation (5), it is possible to calculate the total Risk of a production department, unit or single workplace. Some examples of numerical values of Risk are reported in Table 7.

The internal elements of Table (7) are the estimations of $P^*(C_k)$ obtained as ratio between the number of non-conforming observations and the total number of observations at each sampling session. For instance, the value 0,003, obtained in the sampling session of the day 2 for the cause "Heavy objects are not ergonomically stored", has been obtained as ratio between the number of non-conforming observations for "Heavy objects are not ergonomically stored" in the sampling session of the Day 2 (1 non-conforming observation) and the total number of observation in that day 2 (341 total observations).

In order to create the control chart, it is finally necessary to estimate the average R (equation 12), the Upper Control Limit (UCL) (equation 13), and the Lower Control Limit (LCL). In order to simplify the model, the lower control limit has been set to zero.

$$\bar{R} = \sum_t \frac{R_t}{t} \tag{12}$$

$$LCS = \bar{R} + 3 \cdot \sqrt{\frac{\bar{R} \cdot (1 - \bar{R})}{n}} \tag{13}$$

In Equation (13) n is the number of observations at each sampling session whereas in Equation (12) t the number of periods.

Having estimated all the parameters, it is now possible to create the final control chart, as shown in Figure 1.

Step 4. The control chart shows that the risk level has been out of control in one case. An analysis of the out of control case showed that it was created by the synergic combination of different causes. In the analysed enterprise, the sampling has been done by monitoring the safety conditions of the "Transmissions" department, during 19 work-shifts.

Step 5. Interventions have been introduced to remove these causes.

Table 6. Criticality calculated for some of the k-causes.

Dedritics	P(Ck/E)	P(E)	P(Ck)	Criticality
D1 Tools are not correctly used	0,08	0,39	0,013	2,14
D2 Tools are not adequate or in non-adequate conditions	0,09	0,39	0,027	1,31
D3 Heavy objects are not ergonomically stored	0,05	0,39	0,009	1,94
D4 Materials are not ergonomically stored in cart lifts	0,04	0,39	0	0

Table 7. Risk of the department.

	D1	D2	D3	…	D24	
Critic.	2,14	1,31	1,94	…	0,00	Risk
Day 1	0	0	0	…	0	0,01587
Day 2	0	0	0,003	…	0	0,01507
Day 3	0	0	0	…	0	0,01456
Day 4	0	0	0	…	0	0,00482

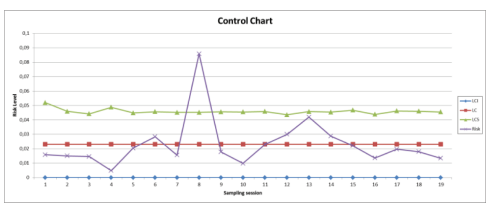


Figure 1. Control chart.

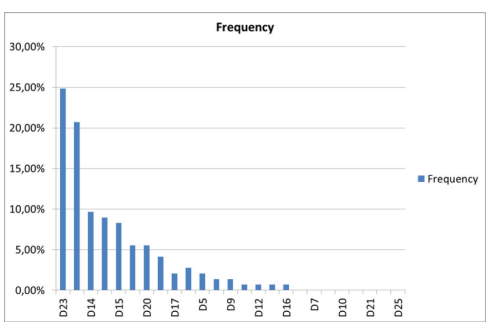


Figure 2. Frequency of occurrence of the k-causes.

Further analyses show that the department does not present particular criticalities. The non-conforming observations are mainly related to a restricted set of causes, with a prevalence of

– Lockout procedures not correctly followed (D23)
– Workers do not use protective glasses necessary for the task (D6)
– Safety belt is not used (D14)

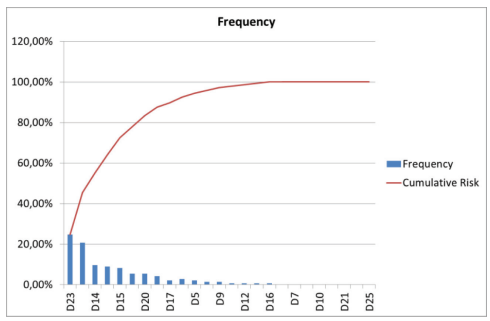


Figure 3. Cumulative risk curve.

– Forklifts stop in forbidden areas (D22)
– Use of music earphones (D15)

The frequency of occurrence of each single cause is reported in Figure 2, while the cumulative risk curve is reported in Figure 3.

4 CONCLUSIONS

The proposed method allows the continuous monitoring of OHS conditions in workplaces associated to workers' safety performance. The combination of a checklist of dendritics and a control chart seems to be an adequate and sustainable approach for this purpose. On the one hand, the checklist, developed by mean of a Preliminary Hazard Analysis, includes all the hazardous conditions of the company and in particular all the at-risk behaviours. On the other hand, the control chart allows identifying all the hazardous conditions that are critical for the employees.

This is a first innovative aspect respect to the simple CCSM method. While CCSM gives the same importance to all the detected non-conforming behaviours, our method introduces a distinction based on the criticality of the specific non-conforming observation. A second innovative aspect of the method is related to the possibility of combining historical data and experts' judgments in the estimation of the criticality. This aspect is of paramount importance, since the external conditions, which influence workers' behaviours, change

dynamically; experts' judgment is essential for a sound assessment of the dynamic evolution of the system.

Summing up, CCSM does not provide an estimation of the severity of the consequences related to the non-conforming behaviours, while traditional risk assessment does not allow continuous monitoring of working conditions and of the performance of the workers. The proposed method overcomes these limitations of CCSM and of risk assessment by combining their advantages. Being risk-based, the method allows for the estimation of the severity of consequences related to the non-conforming behaviours; on the other hand, thanks to statistical analysis of observed non-conformities, the method allows for the continuous monitoring of the external situation and of the performance of the workers, with an affordable demand of time, cost and professional skills for its implementation. Despite the implementation of our method requires an initial investment of resources that is higher than basic CCSM, the effort needed for its daily implementation is comparable. However, the former is substantially covered by the traditional risk assessment process (e.g. by using Job Safety Analysis or Facility Hazard Analysis), which is performed in each company (generally required by law).

The proposed method has some limitations, which open room for future improvements. The main limitation is related to the estimation of the severity factor (D). For the sake of simplicity, a single point severity value has been used for all the at-risk behaviours. However, a more robust estimation should consider different severities for different causes. Again, this estimation could be done by combining historical data, when available, with experts' judgments. A further limitation is related to the effectiveness of the model; it should be tested by means of a long term pilot implementation to check for any positive correlation between safety performance trends and the implementation maturity of the proposed method. This means that after the implementation of the method, a test should verify that the number of non-conforming behaviours as well as the related risk level reduced over time.

Finally, the model has been implemented at shop floor level (i.e. a Transmissions assembly department). Future researches could consider an extension of the method to be applied in other workplaces of a gneric industrial or service company. This requires a more flexible checklist as well as a clear definition of the sampling criteria that must be applied.

REFERENCES

Al-Hemoud, A.M. & Al-Asfoor, M.M. 2006. A behavior based safety approach at a Kuwait research institution. *Journal of safety research* 37(2): 201–206.

Cameron, I. & Duff, R. 2007. A critical review of safety initiatives using goal setting and feedback. *Construction Management and Economics* 25(5): 495–508.

DeJoy, D.M. 2005. Behavior change versus culture change: Divergent approaches to managing workplace safety. *Safety Science* 43(2): 105–129.

DePasquale, J.P. & Geller, E.S. 2000. Critical success factors for behavior-based safety: A study of twenty industry-wide applications. *Journal of Safety Research* 30(4): 237–249.

Dickerson, J.M., Koch, B.L., Adams, J.M., Goodfriend, M.A. & Donnelly, L.F. 2010. Safety coaches in radiology: decreasing human error and minimizing patient harm. *Pediatric radiology* 40(9): 1545–1551.

Eurostat European Commission 2010. *Health and safety at work in Europe (1999–2007)—A statistical portrait.*

Heinrich, H.W., Petersen, D. & Roos, N. 1950. *Industrial accident prevention*. New York: McGraw-Hill.

Hermann, J.A., Ibarra, G.V., & Hopkins, B.L. 2010. A safety program that integrated behavior-based safety and traditional safety methods and its effects on injury rates of manufacturing workers. *Journal of Organizational Behavior Management* 30(1): 6–25.

Hickman, J.S. & Geller, E.S. 2003. A safety self-management intervention for mining operations. *Journal of Safety Research* 34(3): 299–308.

Hide, S., Atkinson, S., Pavitt, T.C., Haslam, R., Gibb, A.G. & Gyi, D.E. 2003. *Causal factors in construction accidents*. Health and Safety Executive.

Johnston, J.J., Hendricks, S.A. & Fike, J.M. 1994. Effectiveness of behavioral safety belt interventions. *Accident Analysis & Prevention* 26(3): 315–323.

Komaki, J., Barwick, K.D. & Scott, L.R. 1978. A behavioral approach to occupational safety: pinpointing and reinforcing safe performance in a food manufacturing plant. *Journal of applied Psychology* 63(4): 434.

Krause, T.R., Seymour, K.J. & Sloat, K.C.M. 1999. Long-term evaluation of a behavior-based method for improving safety performance: a meta-analysis of 73 interrupted time-series replications. *Safety Science* 32(1): 1–18.

Lingard, H., & Rowlinson, S. 1998. Behavior-based safety management in Hong Kong's construction industry. Journal of Safety Research 28(4): 243–256.

Quintana, R., & Nair, A. (1996). Continuous Safety Sampling Methodology. *International journal of occupational safety and ergonomics: JOSE* 3(1–2): 3–14.

Saaty, T.L. 2008. Decision making with the analytic hierarchy process. *International journal of services sciences* 1(1): 83–98.

Scott Geller, E. 2001. Behavior-based safety in industry: Realizing the large-scale potential of psychology to promote human welfare. *Applied and Preventive Psychology* 10(2): 87–105.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Enhancing the implementation of Occupational Health and Safety interventions through a design of the socio-technical interaction

D. Masi & E. Cagno
Politecnico di Milano, Milan, Italy

P. Hasle
Aalborg University, Copenhagen, Denmark

S. Farnè
University of Pavia, Pavia, Italy

ABSTRACT: A multitude of Occupational Health and Safety (OHS) interventions have proven to be effective under controlled conditions, but their implementation in practice is often difficult and interventions may therefore not work as expected, especially when referring to Small and Medium sized Enterprises (SMEs). In order to solve this challenge, this paper proposes a model for the systematic design of OHS interventions which takes into account the underlying mechanisms and the contextual factors which can hamper or further the implementation of interventions.

1 INTRODUCTION

A multitude of Occupational Health and Safety (OHS) interventions have been proposed by researchers and practitioners. Even though the interventions as such have proven to be effective—normally under controlled conditions—implementation in practice is often difficult and interventions may therefore not work as expected. Therefore literature points out that the effects of interventions rarely are as strong as expected (see e.g. Kennedy et al., 2010). A number of researchers have tried to solve this problem by suggesting various models for the design of interventions which should secure a stronger implementation. Most of these models understand interventions as projects and they have adapted phase models from the industrial management literature (see e.g. Hare and Cameron, 2012).

However, even assisted by the phase-models, implementation of interventions is not necessarily effective, because the implementation is crucially dependent on the mechanisms promoting the social change and on the contextual factors which enable or disable these mechanisms (Pawson, 2002; Pedersen et al., 2012).

In order to consider the mechanisms and the contextual factors enabling the change process during the implementation of OHS interventions, Pedersen et al. (2012) have proposed a revised realistic evaluation model for the design and evaluation of OHS interventions. It includes factors such as role behaviour, leader and worker motivation, underreporting of injuries, production pressure, unplanned organisational change and accounting. More recently, Nielsen and Abildgaard (2013) presented an evaluation framework based on intervention research and process-oriented organization theory. The framework offers suggestions for which elements to include when evaluating organizational interventions. Within the framework, elements crucial to intervention evaluation are grouped into four overarching categories: the organizational "actors", the mental models of those actors, the context of the intervention, and intervention design and process.

Yet, these models are not fully exploitable by OHS practitioners during the design of OHS interventions because they do not guide practitioners into a systematic and structured fashion in the identification of the mechanisms and the contextual factors relevant for the particular OHS intervention. The models limit themselves to provide a generic definition of mechanisms and contextual factors, assuming that practitioners will be autonomously able to identify specific mechanisms and contextual factors on the basis of their skills and previous experience. The problem is that practitioners could be unable to properly identify specific mechanisms and contextual factors, since the practitioners' decision-making processes can at best be described as governed by bounded ration-

ality, in which heuristics and prior experience play a large role (Hasle and Sorensen, 2011). Moreover, several models assessing context and behavioural mechanisms in accident analysis (see, e.g., Chang and Mosleh, 2007), or human reliability analysis (see, e.g., Kim and Jung, 2003) demonstrate that the analysis of contextual factors and mechanisms is a complex task that needs to be supported by highly structured decision making models.

Practitioners can therefore be expected to face difficulties on the one hand in carrying out a sufficient in-depth analysis of context and mechanism, and on the other hand in keeping it sufficiently simple for utilisation in the practical situation.

This paper aims at providing a solution for this practitioners' challenge by proposing a model for the design of Occupational Safety and Health (OHS) interventions which takes into account the contextual factors and the behavioural mechanisms affecting the implementation of the intervention. The paper is structured as follows. In paragraph 2 (background), the literature related to implementation of interventions is briefly presented, with a focus on the realistic analysis and its limitations, which generated the research work. In paragraph 3, (the model), we present the model. In paragraph 4, the results of the test of the model in 20 Italian manufacturing firms are presented. Finally, in paragraph 5 some conclusions are taken.

2 BACKGROUND

The studies dealing with the implementation of OHS interventions have generally focused on a limited number of factors fostering or hindering the implementation of the interventions.

For instance, Whysall et al. (2006) explored the process of implementing interventions to tackle occupational ill-health, in particular the facilitators and barriers involved in implementing such interventions. The factors cited as key barriers and facilitators include the resistance of workers to changing their behaviour, gaining managerial commitment, and managers' general attitudes towards health and safety. Hale et al. (2010) describe the patterns of interventions distinguishing between successful and not successful projects and discuss the mechanisms lying behind them. They conclude that interventions that bring about constructive dialogue between shop-floor and line management, provide motivation to line managers and strengthen the monitoring and learning loops in the safety management system appeared more successful. There are other examples of studies which however share the same approaches, proposing one or more factors fostering or hindering the implementation of the interventions (see, e.g., Vedung, 2006; Nielsen and Randall, 2013). Thanks to their focus on behavioural characteristics and contextual factors affecting the performance of the workers, these studies help to explain the complex process necessary for the correct implementation of OHS interventions.

However, these studies cannot support practitioners in the design of more effective OHS interventions, because of a limited understanding of the role of the factors within the more general implementation process and of the way in which the factors interact. Existing studies propose factors that can actually play a key role in the implementation of interventions, such as the resistance of workers to change their behaviour or the managerial commitment and attitudes towards OHS. However, it is not clear how to promote the managerial commitment or how to overcome the resistance of workers to change their behaviour. In the same way, it is not clear whether these factors are equally important in different contextual conditions.

In order to effectively plan the implementation of OHS interventions, it is essential to have a clear understanding of the mechanisms promoting or overcoming some of the key factors listed in the literature, and it is essential to understand how these mechanisms and these factors are conditioned by the different contexts arising in different enterprises.

Realist analysis represents a valid theoretical approach for describing the mechanisms promoting or overcoming some key factors in the implementation of intervention and the interplay between those mechanisms and the context in which interventions take place (Pedersen et al., 2012). Realistic analysis was introduced by Pawson and Tilley (1997), and further developed in Pawson's later work (Pawson, 2002; Pawson et al., 2005). It is founded on the ontological position realism, and the key element is to identify what works for whom, under what circumstances, in what respects and how (Pawson and Tilley, 1997). The generative model of causality, which underpins realist enquiry, holds that to infer a causal outcome between two events, one needs to understand the underlying mechanisms that connects the events, and the context in which the relationship occurs (Pawson et al., 2005). The key elements are Context, Mechanism, and Output. Interventions are not presumed to have causal powers in themselves, instead context and mechanisms are seen as the factors which initiate or trigger the causal relationships; for instance motivation from the key actors is a necessary ingredient for the program to work. The actual outcome of the intervention will vary depending on the intervention, the context, the mechanisms, and the interplay between these, and can be categorized as positive or negative, expected

and unexpected. Realist analysis represents a valid alternative for describing the interplay between personal characteristics and contextual factors within safety interventions because it turns the chain of reasoning of workers into a comprehensive theory of the mechanisms through which the desired change should happen. In the same way, the chain of reasoning and reaction is influenced by some technical and organizational features of the company, and realist analysis represents these features of the company in terms of contextual factors affecting the mechanisms through which the interventions may enter the operator's mind.

Summing up, it is essential to have a clear understanding of the mechanisms and the role of the context in the implementation of OHS interventions, and realist analysis represents a valid theoretical approach in order to deal with these issues.

However, practitioners cannot use the realistic analysis yet for improving the implementation of OHS interventions. Indeed, in order to use realistic analysis in the industrial practice, practitioners need procedures which are simple, easy to use, systematic, but at the same time, comprehensive, valid and with a strong theoretical foundation. This aspect has not been adequately considered in the reviewed studies, which show two main limitations. Firstly, existing studies do not organize the analysed factors into a comprehensive model that can be used by practitioners in the design of OHS interventions. Each study focuses on a limited number of factors or on specific aspects, and a comprehensive view is missing. In order to properly design OHS interventions, practitioners dealing with the design of OHS interventions should identify all the relevant behavioural characteristics and contextual factors affecting the change process. Their knowledge as well as the amount of time and resources they can invest in the design of interventions is however limited. As a consequence they should be supported by a comprehensive taxonomy of contextual factors and behavioural characteristics that underlie the change process necessary for the implementation of OHS interventions. Some comprehensive taxonomies of contextual factors and behavioural mechanisms have been proposed in the accident analysis (see, e.g., Chang and Mosleh, 2007), and in the human reliability analysis (see, e.g., Kim and Jung, 2003) literature. Nevertheless, these models cannot be simply extended to OHS interventions, because they focus on specific actions in a short term temporal horizon, while the behaviour of the workers relevant for OHS interventions is made up of several different actions, that take place in a longer temporal horizon, and that are influenced by some intervention specific contextual factors. Secondly, practitioners need procedures which are simple, easy to use, and systematic. As a consequence, even if we have a clear theoretical understanding of the factors triggering the behavioural change of the workers, of the factors describing the context in which this behavioural change is embedded, and of the interplay between them, it is necessary to develop a procedure that drives practitioners in considering these factors during the design of the intervention. However, existing studies are mainly theoretical, and they do not propose any procedure that can be used by practitioners in their industrial practice.

In the light of the above limitations, in this paper we develop a model which supports practitioners in the use of the realistic analysis for an effective plan of the implementation of OHS interventions and which overcomes the abovementioned limitations.

3 THE MODEL

The model includes a taxonomy of mechanisms and contextual factors and a stepwise procedure which allows for a systematic analysis. Before developing the taxonomy, however, it has been necessary to develop a theoretical definition of mechanisms and contextual factors, presented in the following paragraph.

3.1 *Theoretical definition of mechanisms and contextual factors*

In order to produce a definition of mechanisms, we critically reviewed and combined previous definitions. Pedersen et al. (2012) defined mechanisms as "relevant personal characteristics of key actors or interpersonal relations between them". We picked the first part of this definition, and we focused on "relevant characteristics of key actors". In our model the mechanisms represent the thought that is instigated or "triggered" by the intervention and through which the workers' behaviour is changed. As a consequence, we narrowed the definition of Pedersen and his colleagues, and we assumed mechanisms as "mental state of key actors". Astbury and Leeuw (2010) discuss the concept of "mechanism'' and they attempt to elucidate what mechanisms are and what they are not. They conclude that there are three essential clues located in a "realist'' reading of mechanisms. These are that: 1) mechanisms are usually hidden; 2) mechanisms are sensitive to variations in context; and 3) mechanisms generate outcomes. We picked the last two definitions, since we are already assuming that mechanisms are hidden when we define them as mental states of key actors. In our case, the outcomes generated by mechanisms are the modifications in the performance or in the behaviour of the workers. Finally, Pawson and Tilley (1997)

point out how mechanisms are "triggered by a program". We included this aspect in our definition in order to clearly make a distinction between the personal characteristics of actors that are not varying and the ones that vary with the implementation of a particular intervention. For instance, while the motivation of the workers is a personal characteristic that varies on the basis of the particular intervention implemented, the experience of the workers is a cognitive state that cannot be modified by implementing a particular intervention, at least in the short term.

On the basis of the previous arguments, we define mechanism as "mental state of key actors that are triggered by a program, that vary with changes in the context, and that produce a change in the performance or in the behaviour of the workers". It is important to notice that the change in the mechanisms could enable or disable the desired change. The purpose of practitioners is to promote the mechanisms enabling the social change and to eliminate the mechanisms disabling the desired change.

As for contextual factors, we partially modified the definition of Pedersen et al. (2012) and we define contextual factors as "factors that are not directly related to the performance or to the behaviour of the workers, but that are expected to influence the performance or the behaviour substantially". Indeed, according to the proposed realist model, the mechanisms are directly related to the performance or to the behaviour of the workers, while the contextual factors create the conditions enabling or disabling mechanisms.

3.2 *Taxonomy of mechanisms and contextual factors*

Having developed a definition of mechanisms and contextual factors, we defined the criteria for the selection of mechanisms and contextual factors adequate for the purposes of the study. These criteria are listed below.

Criterion 1—Focus on the behaviour of the workers during the implementation of OHS interventions. The amount of factors which could potentially describe the context and the mechanisms influencing OHS interventions is huge. However, it is possible to select a limited number of relevant factors by focusing on the sole factors that are relevant for the behaviour of the workers during the implementation of OHS interventions. The behaviour of the workers during the implementation of OHS interventions indicates a complex set of specific actions, which all together influence the overall implementation of OHS interventions. A specific action is for instance a wrong movement of the operator, that could provoke an accident. Such an action is relevant in a model for accident analysis, but not so relevant in the more general optic of an OHS intervention. The hypothesis done is that an isolated action has not a relevant influence on the overall effectiveness of the intervention, and it's rather necessary to focus on a more general set of actions, and to consider a longer temporal perspective.

Criterion 2—Level of causality adequate for the assessment by SMEs' practitioners. The "level of causality" (Mohaghegh and Mosleh, 2009; Cagno et al., 2014) describes the position of the factors in the cause-to-effect chain. The choice of the level of causality answers questions such as: should the managerial decisions (hiring, training, etc.) be "bottom layer" factors, or should we move further up in the chain of causality, to top managers' strategic decisions, and do we need to include the regulators' impacts on interventions? In our model, we decided to set the level of causality considering the factors internal to the company that are able to affect the whole behaviour of the workers during the implementation of OHS interventions. This modelling choice is justified by the assumption that it is possible to describe the effect of external factors on the performance of the workers during the implementation of OHS interventions by means of some mediating factors that are internal to the company. For instance, the conditions of the financial markets, that are considered by Pedersen et al. (2012) as a relevant contextual factor, could be described by means of the Perception of available resources, the Trust in management and in the enterprise, and the Rewards. This modelling choice offers several advantages. For instance, the factors could be easily assessed by SMEs' practitioners. It is extremely difficult for OHS practitioners to assess the conditions of the financial markets and their influence on OHS interventions, while it is easy to assess the rewards available for the workers within the company.

Criterion 3—Level of detail adequate for the development of hypotheses on the overall intervention. The "level of detail" (Mohaghegh and Mosleh, 2009; Cagno et al., 2014) of factors depends on the importance attached to the different dimensions of the factors in terms of their impacts on the model output. For example, there are two possible approaches to make a cause-to-effect interaction between the "human resource system" and "safety climate". The modeller can consider these two factors as global factors. On the other hand, he/she can establish multiple relations between the "human resource system" and different dimensions of the "safety climate" (e.g., "perception of the reporting system", "perception of training", etc.). The latter is modelled with a higher level of details (Cagno et al., 2014). In our

model, we decided to set a level of detail optimal for the needs of the realist analysis, i.e. a level of detail allowing practitioners to develop hypotheses on the whole behaviour of the workers during the implementation of intervention. In order to understand this level, we reviewed some studies specifically developing hypotheses on the mechanisms underlying the behavioural change and the success during OHS interventions. On the basis of these studies, we identified a preliminary set of mechanisms and factors that has been used as a benchmark for the level of detail to be adopted in the taxonomy.

Criterion 4—Practicality. The factors should be used by ordinary field "safety persons", eventually of a SME, without the need for highly trained experts.

We did not find taxonomies in the literature which covered all the above aspects, neither for the mechanisms nor for the contextual factors. However, we found that some specific factors were able to satisfy all the mentioned criteria and that other factors were potentially suitable after a tailoring process. As a consequence, we performed a conceptualization work and we developed new taxonomies for mechanisms and contextual factors. In some cases, we simply picked factors from existing taxonomies, selecting some factors and excluding others for different reasons. Some factors mentioned in literature are split in different factors. Some were found to be overly broad and as such had to be modelled through other more narrowly defined sets of factors.

We focused on three kinds of studies. First, we reviewed the studies dealing with Human Error Analysis (HEA) or Human Reliability Analysis (HRA) in safety assessment. These studies represent the conditions that influence human performance by means of several 'context factors'. These context factors are referred to by different terms according to method: PSF (performance shaping factors), PIF (performance influencing factors), IF (influencing factors), PAF (performance affecting factors), EPC (error producing conditions), CPC (common performance conditions), and so on. Second, we reviewed the studies dealing with barriers and drivers to OHS interventions; barriers and drivers identify all those factors of context not directly involved in workplace safety intervention, but significantly affecting, respectively hindering and fostering, the outcome of interventions. Third, we reviewed studies dealing with realistic analysis of OHS interventions.

We combined the factors in order to obtain a taxonomy that is as comprehensive as possible. The taxonomy of mechanisms is reported in Table 1, while the taxonomy of contextual factors is reported in Table 2.

Table 1. Taxonomy of mechanisms, classified in classes.

Class	Mechanism
Temporary cognitive states	Memory of previous interventions
	Anticipation
	Autonomous identification of effective behaviours
	Perception of the importance of the intervention
	Perception of the consequences associated with the own behaviour
	Expectations of the workers
	Perception of familiarity with the situation
	Proper interpretation of the own role and responsibilities
	Perception of available resources
	Perception of the complexity of the intervention
	Emulation of behaviours of the working group
Psychological states	Motivation
	Morale
	Confidence in own behaviours
	Confidence in the chosen intervention
	Trust in management and in the enterprise
	Fear of failure
	Stress due to urgent requests
	Stress due to the conflict
	Frustration
	Uncertainty
	Attention

3.3 *Structure of the analysis*

In order to structure the analysis in a systematic and structured fashion we propose a stepwise procedure for the design of working environment programmes. The design procedure therefore adds some supplementary steps to the original procedure proposed by Hasle et al. (2012) and is made up of seven steps:

1. Define the OHS challenges of the target group.
2. Select methods and solutions that can improve the working environment by reducing the exposure and thereby producing the intended OHS outcome; for instance, the solution could consist in the introduction of Personal Protective Equipment (PPE), or in the modification of the tasks of the target group.
3. Define the change in the behaviour or in the performance of the workers necessary to the effectiveness of the OHS intervention; for instance, following the previous examples, the change in the behaviour of the workers consists in the first case in the fact that the workers use the PPE and

Table 2. Taxonomy of contextual factors, classified in classes and sub-classes.

Class	Sub-class	Factor
Operators	Physical factors	Fatigue
		Physical abilities
	Cognitive factors	Skills
		Knowledge
		Experience
		Training
Physical work environment, equipment and tools	Physical work environment	Illumination
		Noise
		Air quality
		Temperature and humidity
		Freedom of movement of workers
		Freedom of communication
		Layout of the plant
		Order and cleanliness
	Equipment and tools	Availability
		Quality
Organization factors	Management and policy	Plant Policy
		Work and task organization
		Level of supervision
		Production pressure
		Rewards
		Punishments
		Safety culture
	Tasks	Task related difficulties
		Other difficulties
	Procedures	Availability
		Quality
Team factors	Features of the team	Cohesiveness
		Coordination
		Composition
	Communication	Availability
		Quality
	Leadership	Leadership

in the second case in the fact that the workers accept and follow the new task.

4. Develop theories about mechanisms which can motivate the target group to initiate change, or which can hinder the change; in order to ensure the comprehensiveness of the analysis, the mechanisms should be selected from the taxonomy proposed in Table 1. For instance, following the previous examples, the mechanisms could be the "Motivation of the workers" and the "Fear of failure".
5. Analyse the influence of the context for each of the selected mechanisms; in this step, for each mechanism practitioners should select one or more contextual factors that "condition" the mechanism itself. For instance, the "Fear of failure" can be conditioned by the "punishments" adopted within the company, while the "Motivation of the workers" can be conditioned by the "rewards". In order to ensure the comprehensiveness of the analysis, the contextual factors should be selected from the taxonomy proposed in Table 2.
6. Assess the adequacy of the contextual factor in relation to the particular mechanism; for instance, practitioners should ask themselves question like: "Are the punishments adopted within my enterprise adequate in order to activate the fear of failure of the workers?" or "Are the rewards adopted within my enterprise adequate in order to activate the motivation of the workers?".
7. Develop design recommendations for the intervention which build on the results of the four preceding steps. For instance, on the basis of the previous assessment, the workers could decide to modify the reward or the punishment system.

4 TEST OF THE MODEL

4.1 *Methodology*

Between September 2013 and March 2014, twenty safety officers were interviewed, with the support of a questionnaire. The questionnaire was divided into three sections. In the first part, some enterprise characteristics (sector, turnover, etc.) were asked. In the second part, the safety officers used the model: the several steps of the procedure, as well as the preliminary steps necessary for the problem setting, were proposed to the practitioners by means of ten structured questions. In the third part, we asked to the practitioners to evaluate the performance of the model taking into account three main criteria: usefulness, completeness, and difficulty of use. The questions used for the evaluation of the performance are reported in Table 3.

The distribution of sample firms by industry sectors, turnover, and number or workers is summarised in Table 4. The Small- and Medium-sized Enterprises (SMEs)—as defined in the 2003/361/EC Recommendation (European Commission, 2003)—mainly belong to the most important manufacturing sectors of the Lombardy Region in Italy in terms of employees and turnover and they have been classified according to the International Standard Industrial Classification of All Economic Activities "ISIC rev.4", as reported in Table 5. As it can be argued from Table 4, the SMEs have been divided into four classes: Micro (MiEs, employees ≤ 10), the Small (SEs, 10 < employees ≤ 49), Medium (MEs, 50 < employees ≤ 99), and Medium-Large Enterprises (MLEs; 100 < employees ≤ 250).

Table 3. Questions used for the assessment of the performance of the model in the third part of the questionnaire.

Criterion	Questions
Usefulness	Was the model useful for the design of the intervention? Why? Did the model help to identify some factors that you did not identify? Did the model help you to better structure what you had in your mind?
	While setting the improvements of the intervention, was it helpful to consider the interaction between mechanisms and contextual factors? Why ? Were you able to identify—thanks to this interaction—some aspects of the contextual factors that you would have neglected without the model?
	Do the improvements introduced thanks to the model compensate the difficulty of use?
	Would you obtain the same results in the same time without the support of the model?
Completeness	Do you think that the list of mechanisms is complete?
	Do you think that the list of contextual factors is complete?
Difficulty of use	Which was the most difficult step performed during the use of the model? Why?

Table 4. Features of the companies in terms of turnover and employees.

Enterprise	Number of employees	Turnover [mln €]	Sector
1	20–49	5,9	C25
2	100–250	32,9	C25
3	20–49	3,67	C25
4	50–99	n.a.	C28
5	50–99	n.a	C10
6	100–250	n.a	Other
7	100–250	n.a	C22
8	100–250	60	C28
9	10–19	8	C22
10	20–49	5	C27
11	20–49	4,5	Other
12	20–49	12	C28
13	20–49	5	Other
14	50–99	10,5	C25
15	20–49	2,5	C25
16	10–19	3	C25
17	20–49	3	C25
18	10–19	3	C17
19	20–49	5	C22
20	50–99	10	C28

4.2 *Results*

All the twenty practitioners were able to correctly compile the second part of the questionnaire, in which they had to use the stepwise procedure and the taxonomies. The third part, in which we asked to the practitioners to evaluate the performance of the model taking into account the usefulness, the completeness, and the difficulty of use of the model was filled in by 19 of the 20 practitioners (excluded the practitioner of company 6).

In all the cases, the interviewees confirmed that the model was useful for the design of the intervention. The reasons reported by the interviewees include a higher effectiveness in the design of the solution, a better focus on the aspects that should be considered, the identification of aspects usually neglected, and a more organic and systematic way of structuring the data.

Table 5. Sectors of the companies.

Metal products, excluding machinery and equipment	C25
Machinery and equipment n.e.c.	C28
Food	C10
Paper and paper products	C17
Rubber and plastic products	C22
Electrical equipment and non-electric domestic appliances	C27

All the interviewees confirmed the usefulness of considering the interaction between mechanisms and contextual factors. The main reason was the identification of specific aspects of the contextual factors highlighted by the comparison with the mechanism. Other interviewees reported how the comparison between mechanisms and contextual factors improves the comprehensiveness of the analysis.

As for the improvements introduced compared to the difficulty of use, the answer to this question varied among the interviewees. In some cases, the interviewees reported that the improvements compensated the difficulty of use (company 1, 3, 5, 7, and 8, and 11–20); in other cases the interviewees reported that the improvements compensated the difficulty of use only partially (company 4, 9, and 10); and in one case the interviewee reported that the improvements did not compensate his difficulty of use (company 2).

As for the possibility of obtaining the same results in the same time without the support of the model, the interviewees provided different answers. In the majority of the cases, the interviewees reported that they would not obtain the same results in the same time without the support of the model (company 3, 5, 7, 8, and 9); in other cases, the interviewees were not able to answer to the question (company 1 and 4), and in other cases (company 2 and 10) the interviewees reported that they would obtain the same results in the same time without the support of the model, coherently with previous answers.

As for the completeness of the model, all the interviewees reported that the list of mechanisms and of contextual factors is complete.

There are three steps that seem to be critical. The first critical step is the selection of the mechanisms (company 3, 4, 7, 9, 11, 12, 13, 19, 20), because it is not easy to make a distinction between mechanisms "enabling" and mechanisms "disabling" a change in the behaviour of the workers (company 4) or because it is not easy to connect mechanisms with corresponding behaviours (company 9). In other cases (company 3 and 7) practitioners were not able to explain specifically the criticality of the step.

The second critical step is the combination between mechanisms and contextual factors (company 2, 10, 15, 16, 17 18), because, according to some interviewees, it requires a perfect knowledge of the context and of the workers involved in the intervention.

The third critical step is the development of the design recommendations (company 2 and 5), because, according to the two interviewees, it is difficult to identify solutions that are effective and, at the same time, realistic and feasible.

5 CONCLUSIONS

The test proved that the procedure and the proposed taxonomies can be easily used by "ordinary" safety practitioners. The practitioners identified several interesting combinations of mechanisms and contextual factors, which introduce novel insights also for the safety literature. For instance, the "Perception of familiarity with the situation" influenced by the "layout of the plant" has been identified as a mechanism disabling the desired performance. According to the authors' knowledge, the layout of the plant has never been related to the Perception of familiarity with the situation in previous safety literature.

The usefulness of the model seems to be clearly proved—although in a small sample—by the answers of the practitioners. The model does support practitioners during the design of the intervention, since it highlights specific aspects of contextual factors and mechanisms and it organizes the data in a more systematic and structured fashion. In the majority of the cases, the improvements introduced by the model compensated the difficulty of use and the model seems to be necessary for the introduction of these improvements.

The model seems to be complete, in sense that all the relevant factors and mechanisms determining the performance of the workers have been included in the taxonomies.

Some improvements could regard the difficulty of use. For instance, two critical steps are the selection of the mechanisms and combination between mechanisms and contextual factors; some practical examples could be helpful in these tasks. Examples can be progressively collected with the use of the model.

This test involved twenty companies and, as a consequence, the results can be considered as a preliminary validation of the model. Further researches will repeat the same test with a broader sample.

It is important to underline how the test analysed the outcome of the design process. After the design, the intervention should be actually imple-

mented and its effectiveness should be assessed. The improvement of the effectiveness of the intervention designed with the help of the model is the main objective of the model itself. This aspect will be investigated in further researches, also using the preliminary results of this test.

REFERENCES

Astbury, B. & Leeuw, F.L. 2010. Unpacking black boxes: mechanisms and theory building in evaluation. *American Journal of Evaluation* 31(3): 363–381.

Cagno, E., Micheli, G.J.L., Jacinto, C. & Masi, D. 2014. An interpretive model of occupational safety performance for Small-and Medium-sized Enterprises. *International Journal of Industrial Ergonomics* 44(1): 60–74.

Chang, Y.H.J. & Mosleh, A. 2007. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 2: IDAC performance influencing factors model. *Reliability Engineering & System Safety* 92(8): 1014–1040.

European Commission 2003. Commission recommendation of 6 May 2003 concerning the definition of micro-small and medium-size enterprises, 2003/361/ EC. 6th May ed.: Official Journal of the European Union.

Hale, A.R., Guldenmund, F.W., van Loenhout, P.L.C.H. & Oh, J.I.H. 2010. Evaluating safety management and culture interventions to improve safety: Effective intervention strategies. *Safety Science* 48(8): 1026–1035.

Hare, B. & Cameron, I. 2012. Health and safety gateways for construction project planning. *Engineering, Construction and Architectural Management* 19(2):192–204.

Hasle, P. & Sorensen, O.H. 2011. When health and safety interventions meet real-life challenges. *Policy and Practice in Health and Safety* 9(1): 3–16.

Hasle, P., Kvorning, L.V., Rasmussen, C.D., Smith, L.H., & Flyvholm, M.A. 2012. A Model for Design of Tailored Working Environment Intervention Programmes for Small Enterprises. *Safety and health at work* 3(3): 181–191.

Kennedy, C.A., Amick III, B.C., Dennerlein, J.T., Brewer, S., Catli, S., Williams, R., … & Rempel, D. 2010. Systematic review of the role of occupational health and safety interventions in the prevention of upper extremity musculoskeletal symptoms, signs, disorders, injuries, claims and lost time. *Journal of occupational rehabilitation* 20(2): 127–162.

Kim, J.W. & Jung, W. 2003. A taxonomy of performance influencing factors for human reliability analysis of emergency tasks. *Journal of Loss Prevention in the Process Industries* 16(6): 479–495.

Mohaghegh, Z., & Mosleh, A. (2009). Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations. *Safety Science* 47(8): 1139–1158.

Nielsen, K., & Randall, R. 2013. Opening the black box: Presenting a model for evaluating organizational-level interventions. *European Journal of Work and Organizational Psychology* 22(5): 601–617.

Nielsen, K. & Abildgaard, J.S. 2013. Organizational interventions: A research-based framework for the evaluation of both process and effects. *Work & Stress* 27(3): 278–297.

Pawson, R. & Tilley, N. 1997. *Realistic evaluation*. London: Sage.

Pawson, R. 2002. Evidence-based policy: The promise of realist synthesis. *Evaluation* 8(3): 340–358.

Pawson, R., Greenhalgh, T., Harvey, G., & Walshe, K. 2005. Realist review–a new method of systematic review designed for complex policy interventions. *Journal of health services research & policy* 10(1): 21–34.

Pedersen, L.M., Nielsen, K.J. & Kines, P. 2012. Realistic evaluation as a new way to design and evaluate occupational safety interventions. *Safety Science* 50(1): 48–54.

Vedung, E., 2006. *Process evaluation and implementation theory.* In E. Vedung (Ed.), Public policy and program evaluation (1st ed., pp. 209245). Piscataway, NJ: Transaction Publishers.

Whysall, Z., Haslam, C. & Haslam, R. 2006. Implementing health and safety interventions in the workplace: an exploratory study. *International Journal of Industrial Ergonomics* 36(9): 809–818.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A risk-based approach to manage the Occupational Hazards in the Arctic drilling waste handling practices

Y.Z. Ayele, A. Barabadi & J. Barabady
Department of Engineering and Safety, UiT The Arctic University of Norway, Tromsø, Norway

ABSTRACT: The paper proposes a risk-based approach to eliminate and manage occupational hazards, associated with the handling of drilling wastes in the cold and harsh operational condition. The proposed approach can help the user to investigate the occupational hazards, by recognizing, predicting and interpreting information about the potential hazard/risk influencing factors which are caused by the operating environment of the Arctic region. The approach can also help to identify and understand the peculiar occupational hazards, for the range of possible drilling waste handling technologies/solutions in cold Arctic regions. It also offers step-by-step risk reduction measures, by determining actions which are necessary to eliminate or reduce the occupational hazards identified as above acceptance criteria. By employing the proposed approach, an effective occupational hazard management plan—with suitable risk management and reduction measures can be selected and implemented.

1 INTRODUCTION

The oil and gas exploration results in the creation of drilling wastes that consist of a mix of drill-waste solids (cuttings) and non-recoverable drilling muds. These wastes can be contaminated with various chemicals which are added throughout the drilling process and in some cases with the hydrocarbons from the formation. In general, in the conventional waste handling practices, once the drill cuttings have passed through the solids control system, the cuttings collection and handling system takes the waste stream of cuttings with adhering drilling fluid and delivers it to the next stage of the disposal process (IPIECA and OGP, 2009). If discharge into the sea is the selected disposal option, handling requirements will be minimal and the occupational exposures to the waste will also be insignificant (IPIECA and OGP, 2009). However, for non-discharge options, some type of cuttings collection, processing, transport and disposal system will be required (Ayele et al., 2013, Paulsen et al., 2005, Veil, 2002). During those activities the workers involved faces occupational health and safety hazards (Holmér, 1999, Broni-Bediako and Amorin, 2010, Mearns et al., 2003, Robson et al., 2007, IPIECA and OGP, 2009). Moreover, the range of possible drilling waste handling technologies/solutions poses their own peculiar occupational hazards in terms of exposure routes (such as ingestion, inhalation, skin contact and skin absorption), frequency of exposure, and exposure duration.

Humans are "designed" to operate in very narrow temperature range and thus wind, icing and darkness reduce the operational effectiveness considerably and possibility of mistakes or being inaccurate increases (Barabadi and Markeset, 2011, Markeset, 2008, Gudmestad et al., 2007, Kumar et al., 2009). In other words the harsh and the cold operational environments of the Arctic have significant effect on the occupational performance of the workers, and these magnify the hazards associated with the waste handling practices. Thus, all influencing factors that affect the occupational performance must be recognized and quantified throughout the various phases of the waste handling streams properly. These identifications of the influencing factors can help to have an effective drilling waste handling practices with high level of safety in the harsh, remote and cold Arctic region. Moreover, it is also necessary to analyse the severity of each exposure routes from the occupational hazards point of view.

When deciding on the type of drilling waste handling technologies to use for work in cold Arctic environments, the operators need to conduct comprehensive occupational hazard assessments of the drilling waste streams. This is especially due to the negative impact of cold on human health and performance, as well as on work productivity, quality and safety (ISO 15743, 2008). The rigorous hazards assessment can be done by considering the HSE (health, safety, and environment) aspects, and by striking an appropriate balance between their potentially conflicting requirements (IPIECA and OGP, 2009). Moreover, an effective occupational hazards management plan need to comprise the assessment of potential job hazards, risks of

occupational injury, and health risks stemming from exposure to harsh environmental factors, such as cold, icing of work surfaces, ice falling from heights, darkness, etc. (Det Norske Veritas, 2009). Furthermore, identifying occupational hazards and assessing the level of risk associated with those hazards is the most important activity you perform every day, during handling and managing of the drilling wastes in cold regions (Public Services Health and Safety Association, 2011).

In order to investigate the workplace injuries in cold region, a number of occupational health and safety hazards assessment models have been developed (Giedraitytė, 2005, Holmér, 1999, Holmér, 1994, Broni-Bediako and Amorin, 2010, Risikko et al., 2003, Geller, 2005, Lindøe et al., 2006, Robson et al., 2007). ISO 15743:2008, Ergonomics of the thermal environment—Cold workplaces—Risk assessment and management, has been developed to describe the methods and practices for assessing and managing occupational health and performance risks in cold workplaces. In addition, occupational exposure limits for several types of drilling fluids are specified in IPIECA and OGP (2009) occupational health and safety regulations, and exposure should not exceed these levels.

However, the missing point in most of the occupational hazards assessment literature is that the effect of the operating environment of the cold region on the performance of workers during handling of drilling wastes has received less attention. This can have a significant impact during the planning of the waste handling process as well as during the execution of the intended work. As a result, in order to assure the operational performance and high level of safety in the cold Arctic region, occupational exposure assessment associated with the handling of drilling wastes should necessarily be risk-based.

Minimizing the overall hazards and risk profile and increasing safety and performance of the workers is the main objective of risk-based occupational hazard assessment in the drilling waste handling practices in the cold Arctic region. By analysing each drilling waste streams and identifying and quantifying the unique occupational hazards and risks involved, the oil and gas industry operating in the harsh and cold Arctic region, can take appropriate measures to mitigate those risks. Furthermore, taking appropriate mitigation measures can improve operational performance and reduces the consequences of unwanted events during the handling of the wastes. By employing a risk-based approach it is often easier and more effective to eliminate the occupational hazards before they are introduced into a drilling waste handling workplace by incorporating safety features at the design stage (Safe Work Australia, 2011).

Hence, the aim of this paper is to propose a risk-based approach to manage exposures to hazards during the handling of the drilling waste in the cold and harsh operational condition. The rest of the paper is organized as follows: Section 2 examines and summarizes the main occupational hazards associated with the handling drilling wastes in the harsh and the cold Arctic regions. Section 3 presents a risk-based approach. Section 4 proposes risk reduction and/or management measures and Section 5 provides the conclusion.

2 EXAMINATION AND SUMMARY OF THE MAIN OCCUPATIONAL HAZARDS

In general, an occupational hazard can be defined as a thing or situation with the potential to harm a worker (Ontario Ministry of Labour, 2013, Safe Work Australia, 2011). The occupational hazards can be divided into two categories: safety hazards that cause accidents that physically injure workers, and health hazards which result in the development of disease (Ontario Ministry of Labour, 2013). It is important to note that a "hazard" only represents a potential to cause harm. Whether it actually does cause harm will depend on circumstances, such as the toxicity of the drilling waste, exposure duration and amount, as well as the rate of recurrence of the exposure. Hazards can also be rated according to the severity of the harm they cause—a significant hazard being one with the potential to cause a critical injury or death (Ontario Ministry of Labour, 2013). Identifying hazards in the drilling waste handling and treatment workplace involves finding things and situations that could potentially cause harm to waste handling personnel's.

Some of health hazards due to exposure to cold environment during the drilling waste collection, processing, transporting as well as disposing are (Cameron, 2013): decreased blood circulation in the muscle tissue of the extremities (hands and feet) which can result in a reduction in waste handling staff's ability to function adequately; and exposure to the wind and draught can also compound the health issues by increasing ear and eye infections, which in turn can impair hearing and vision which may increase the risk of accidents.

Moreover, long-term exposure to cold environments can lead to a worsening of existing rheumatic conditions and occurrence of Raynaud's Syndrome, a vascular disease in which constricts blood vessels in the extremities such as the hands and feet, causing the blue colouring of the affected areas accompanied by on-going pain and discomfort and cold stress (Cameron, 2013). Furthermore, exposure to cold environments also increases the risk to persons with known asthma or cardiovascular disease.

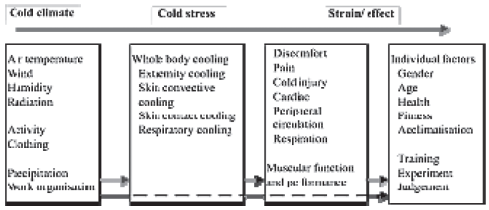


Figure 1. Relation between climate, stress, and strain, adapted from Holmér (1999).

Table 1. Example of common occupational hazards and their potential consequences.

Hazard	Consequences/potential harms
Extreme cold temperature*	: Cold injury such as hypothermia or frostbite.
	: Performance decrements due to cold hands, cold muscles or general cooling or due to hinders caused by protective clothing against cold such as weight, bulk, friction, etc.
Hazardous chemicals/dust inhalation**	: Chemicals (such as acids, hydrocarbons, heavy metals) and dusts (such as asbestos and silica) can cause respiratory illnesses, cancers or dermatitis.
Machinery and equipment*	: Being hit by moving vehicles, or being caught by moving parts of machinery can cause fractures, bruises, lacerations, dislocations, permanent injuries or death.
Gravity*	: Falling objects (such as icicles and falls) can cause fractures, bruises, lacerations, dislocations, concussion, permanent injuries or death.
Wind chill effect	: Extended period of exposure to the cold without adequate protection can lead to frostbite, hypothermia and freezing to death.
Psychological hazards	: The extended period of darkness leads to stress and depression.
Human error	: Lack of concentration, due to harsh and cold environment, during waste container lifting activities can causes fatal accidents.
	: Insufficient visibility due to darkness, heavy fog, rain, and snowfall increases the hazards during the handling of the waste containers.
Other hazards*	: Result from equipment or machine failures and misuse, chemical spills and structural failures may have many different occupational hazards.
	: Less frequently reported health effects are headache, nausea, eye irritation and coughing.

*Safe Work Australia (2011) and Giedraitytė (2005); **Safe Work Australia (2011) and US Department of Health and Human Services (1985).

The other significant contributor that magnifies the occupational hazards, in the cold Arctic region, is the wind chill effect. The wind chill effect can be defined as the perceived decrease in air temperature felt by the body on exposed skin due to the flow of air. The effect of the wind chill will even increase with high wind speed and in the worst case it can be expected to have outdoor working restrictions, for waste handling personnel, for some specified period.

Thus, when assessing occupational hazards in cold Arctic regions, the effect of the operating environment on the performance of the workers needs to be analysed thoroughly. Figure 1 shows the relationship between the various characteristics of the cold climate and its associated effect or strain.

Table 1 is an example of common types of occupational (workplace) hazards during handling wastes in the cold Arctic region. These hazards are for waste handling workers including those who work directly on top of uncovered waste sites, for workers collecting drilling wastes as well as for workers transporting the drilling wastes.

3 THE RISK-BASED APPROACH

Risk can be defined as the possibility that harm (death, injury or illness) might occur when exposed to a hazard (Safe Work Australia, 2011). Figure 2 shows the proposed risk-based approach for eliminating and/or managing the occupational hazards associated with the handling of drilling wastes in the harsh, remote and sensitive Arctic environment. The proposed risk-based approach

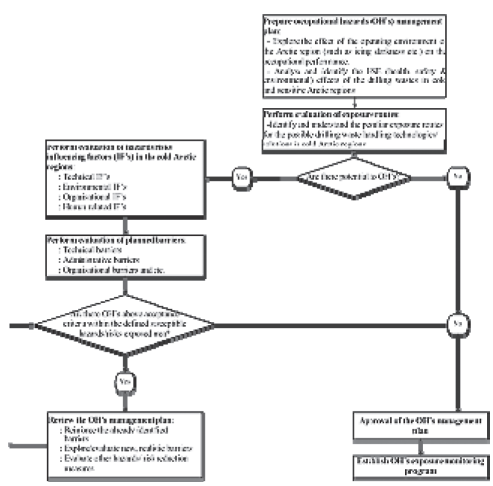


Figure 2. A risk-based approach to eliminate and/or manage the Occupational Hazards (OH's) in drilling waste handling practices in the cold Arctic region.

starts with preparing the Occupational Hazards (OH's) management plan. The plan needs to explore the overall effect of the physical operating environment of the Arctic region on the performance of the workers, the drilling waste handling tasks and how they are performed as well as the type of equipment, materials and drilling substances used.

During preparation of the plan, the HSE effects of the drilling mud and the associated drilling wastes in the cold Arctic regions needs to be identified and recognised. In addition, some types of hazards prevention and/or reduction barriers needs to be planned. A barrier is defined as a measure which is put in to prevent the release of a hazard or to prevent the occurrence of a top event once the hazard is released, and barriers may be physical or non-physical (Veerasingam, 2011). These prevention measures or barriers can be actions aimed at eliminating or minimizing the impact of the hazard or the top event (the incident that occurs when a hazard is realized). Successful prevention of occupational hazards depends upon: knowledge of causation or exposure routes, identification of risk factors, availability of early detection measures, and continuous evaluation of and development of new and timely prevention procedures (Robson et al., 2007).

Subsequently, the evaluation of the main exposure routes (such as ingestion, inhalation, skin contact and absorption) needs to be performed. This evaluation needs to include the understanding as well as identifying of the peculiar exposure routes for the range of possible drilling waste handling technologies/solutions to be deployed in cold and harsh Arctic environment. The analysis of the most commonly observed health effects of drilling wastes, such as skin irritation and contact dermatitis, in waste handling workers, needs to be part of the evaluation. In addition, the physico-chemical properties of the drilling wastes and the inherent properties of drilling mud needs to be evaluated.

In the next stage the assessment of the potential Occupational Hazards (OH's) need to be carried out. At this evaluation stage, it is crucial to identify and recognise all possible OH's related to the handling of drilling wastes in the cold Arctic region. There are several techniques for identifying and analysing occupational hazards associated with handling of drilling wastes, such as checklist analysis, what-if analysis, and Hazard and Operability (HAZOP) analysis. In addition, bow-tie methodology, is one of the simplest and pragmatic hazard identification approach (Hamzah, 2012). Bow-tie technique is a graphical representation used to show hazardous events in such a way to easily show the connections between hazards/threats and their consequences (Hamzah, 2012). In this technique the hazards and the possible consequences are linked to a top event. The evaluation of the hazards can also help to generate information for other purposes, for example to attract attention to a specific hazard or a cumulative of hazards.

The evaluation of the hazard/risk Influencing Factors (IF's) is another part of the assessment. Hazard/risk influencing factors are factors that affect barriers and barrier performance (Aven, 2008). The evaluation process comprises estimation of the various effect of the operational environment of the cold Arctic region on the occupational performance. Environmental conditions such as icing, wind speed, wind direction, temperature, wind chill effect, and polar low must be described and quantified based on the way that they can affect the occupational performance. Some of these environmental conditions can be combined with each other and make new influencing factor. For example, the air temperature combines with wind speed to describe the wind chill factor, which is the effect of these two parameters on exposed skin. The evaluation also needs to include the assessment of technical IF's (such as design, material characteristic and technical condition), organisational IF's as well as human-related IF's (such as competence, workload, and working environment).

Thereafter, the evaluation of the planned barriers, such as technical, administrative, and organisational barriers need to be carried out. During this process the identification of the available/planned barriers that controls or reduces the occupational hazards needs to be performed. Throughout this identification and evaluation process, the results from the assessment of the potential occupational hazards are compared against to the planned goals or objectives. This identification process will also help the user to differentiate the "steel" barriers (effective and reliable barriers) and "paper" barriers (less effective or reliable barriers) (Neogy et al., 1996). Moreover, the evaluation process can provide feedback which may be expected to modify the occupational hazards management plan and lead to redefinition of the main objectives.

After evaluating the planned barriers as well as the influencing factors, then, the assessment of the occupational hazards within the defined susceptible hazards/risks exposed area need to be performed. The susceptible hazards/risks exposed area can be defined as per expert's judgement (opinions) and past experience. For example, a checklist analysis which is an experience based approach, can be used to identify known types of occupational hazards, potential accident situations, or design deficiencies (Neogy et al., 1996). Thereafter, the hazards needs to be classified as well as prioritise based on the standards, regulations and statutory requirements.

In the case of the identified OH's are above the acceptance criteria, the next step will be reviewing the already defined OH's management plan. Acceptance criteria are criteria used as a basis

for decisions about acceptable risk—a risk that is accepted in a given context based on the current standards, regulations and values of the company (Rausand, 2013). The review will include reinforcing the already identified barriers, exploring and/or evaluating new (realistic) barriers as well as evaluating the hazards/ risk reduction measures.

Finally, after assessing and evaluating the hazards the occupational hazards management plan will be approved, when the results suggests that all required acceptance criteria are met. The decision utilises the evaluation, identification as well as analysis results in order to eliminate and manage the occupational hazards related with handling of drilling wastes in cold Arctic region. Thereafter, the approved OH's management plan will be monitored by establishing the OH's exposure monitoring program. This monitoring program helps to detect any changes in the operating environment and its effect on the workers occupational performance.

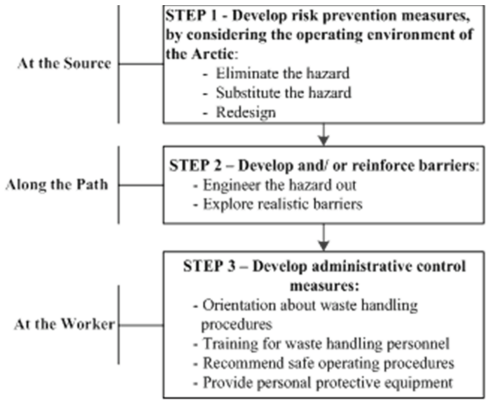


Figure 3. A step-by-step hazards/risks reduction and control measures during the handling of drilling wastes in the cold Arctic region.

4 STEP-BY-STEP OCCUPATIONAL HAZARD/RISK REDUCTION MEASURES

Working in the cold Arctic environments has the potential if not managed properly to cause an increase in incidences and injuries. However, if managed properly through the appropriate controls and at the design stage the hazards/risks can be minimised. Waste handling and disposal workers following safety guidance will reduce their total on-site occupational hazards exposure (US Department of Health and Human Services, 1985). In addition, to guard against the cold and harsh Arctic environment, the worker are recommend (US Department of Health and Human Services, 1985): to wear appropriate clothing; to have warm shelter readily available; to carefully schedule work and rest periods, as well as to monitor workers' physical conditions. In addition, it is important to factor the effect of the cold environment on the workers, in the pre-employment phase to identify any conditions that may be exacerbated by working in a cold environment as well as review the status of the existing staff moving into a cold environment (Cameron, 2013).

To propose measures and address the impacts of cold exposure as well as to mitigate the associated hazards: recognizing, predicting and interpreting information about the potential hazard/risk influencing factors on the performance of the workers, will be very helpful. Figure 3 shows the step-by-step measures that can help to prevent, reduce and/or control the occupational hazards associated with the handling of drilling wastes in the cold Arctic environment. At the first step, risk prevention measures needs to be determined and developed. In this process, the measures or procedures that are essential for eliminating or reducing the identified occupational hazards needs to be established.

According to Public Services Health and Safety Association (2011), hazard/risk prevention or control measures can be implemented at the source level (e.g. elimination of the hazard, substitution, and redesign), along the path (e.g. during processing and transporting of the drilling waste), and at the worker.

For example, careful development of cold weather clothing materials, taking into account the waste handling personnel, the tasks to be performed and the environmental conditions, can guarantee comfortable sensations and good performance during exposure to cold weather (Jussila et al., 2010). Developing a realistic barrier as well as reinforcing the available barriers is the next step. In this step the various types of guard as well as safety devices needs to be provided. Moreover, the engineered control measures need to be evaluated and implemented. For example, engineer the hazard out can be effective means of controlling hazards.

The third step is developing different measures which can help to reduce and control the hazards/ risks, such as: administrative controls, orientation, training and supervision, waste handling work procedures, emergency planning, and cold protective clothing (Public Services Health and Safety Association, 2011).

5 CONCLUSION

Workers involved in drilling waste handling operations may be exposed to various occupational hazards. In addition, it is clear that the performance of the drilling waste handling workers in cold Arctic regions can be greatly influenced by the operational conditions

such as low temperature, snow and ice. Furthermore, the chosen drilling waste handling technology poses its unique occupational hazards. Therefore, in order to minimize and manage the occupational hazards and risk profile during handling of drilling wastes in cold Arctic regions, the principles of risk-based approaches need to be implemented.

The proposed risk-based approach can help the user to examine the occupational hazards, by considering the main influencing factors which are caused by the operating environment of the cold Arctic region. By employing the proposed approach, the effective occupational hazard management plan—with better risk management and reduction measures can be selected and implemented. In addition, the proposed approach can be verified through replication of findings in more case studies.

REFERENCES

Aven, T. 2008. *Risk analysis—Assessing uncertainties beyond expected values and probabilities*, West Sussex, John Wiley & Sons Ltd.

Ayele, Y.Z., Barabadi, A. & Barabady, J. 2013. *Drilling waste handling and management in the High North.* IEEE International Conference on Industrial Engineering and Engineering Management, Bangkok, Thailand.

Barabadi, A. & Markeset, T. 2011. Reliability and maintainability performance under Arctic conditions. *International Journal of System Assurance Engineering and Management*, 2, 205–217.

Broni-Bediako, E. & Amorin, R. 2010. Effects of drilling fluid exposure to oil and gas workers presented with major areas of exposure and exposure indicators. Research Journal of Applied Sciences, *Engineering and Technology*, 2, 710–719.

Cameron, T. 2013. *Working in cold environments: Thermal comfort through design & control* [Online]. Available: http://www.safetyrisk.net/working-in-cold-environments/ [Accessed 12.12.2013].

Det Norske Veritas (DNV). 2009. *Barents 2020: Assessment of international standards for safe exploration, production and transportation of oil and gas in the Barents Sea*.

Geller, E.S. 2005. Behavior-based safety and occupational risk management. *Behavior modification*, 29, 539–561.

Giedraityte, L. 2005. *Identification and validation of risk factors in cold work*, PhD thesis, Luleå University of Technology.

Gudmestad, O., Alhimenko, A., Løset, S., Shkhinek, K., Tørum, A. & Jensen, A. 2007. *Engineering aspects related to Arctic offshore developments*. St. Petersburg, Lan, 255.

Hamzah, S.Z. 2012. *Use bow tie tool for easy hazard identification*. 14th Asia Pacific Confederation of Chemical Engineering Congress, Singapore.

Holmer, I. 1994. Cold stress: Part I—Guidelines for the practitioner. *International Journal of Industrial Ergonomics*, 14, 139–149.

Holmer, I. 1999. Risk assessment in cold environment. *Barents Newsletter.*

IPIECA & OGP. 2009. *Drilling fluids and health risk management—A guide for drilling personnel, managers and health professionals in the oil and gas industry*. In: IPIECA, International Petroleum Industry Environmental Conservation Association and OGP, International Association of Oil & Gas Producers, London. United Kingdom.

ISO15743:2008, *Ergonomics of the thermal environment—Cold workplaces—Risk assessment and management*.

Jussila, K., Valkama, A., Remes, J., Anttonen, H. & Peitso, A. 2010. The effect of cold protective clothing on comfort and perception of performance. *International Journal of Occupational Safety and Ergonomics,* 16, 185–197.

Kumar, R., Barabady, J., Markeset, T. & Kumar, U. 2009 Improvement of performance of oil and gas production facilities in Arctic regions by applying human factors/ergonomic principles at the design phase. *Proceedings of the 20th International Conference on Port and Ocean Engineering under Arctic Conditions*: June 9–12, 2009, Luleå, Sweden.

Lindøe, P., Olsen, O. & Lie, T. 2006. Systematic occupational health and safety management in complex industrial settings. *Proceedings from IEA-Conference*, Maastricht, 10–14.

Markeset, T. 2008. *Design for High Performance Assurance for Offshore Production Facilities in Remote Harsh and Sensitive Environments*. OPSEARCH, 45, 275.

Mearns, K., Whitaker, S.M. & Flin, R. 2003. Safety climate, safety management practice and safety performance in offshore environments. *Safety Science*, 41, 641–680.

Neogy, P., Hanson, A., Davis, P. & Fenstermacher, T. 1996. *Hazard and barrier analysis guidance document. Technical Report EH-33*, Department of Engery, Office of Operating Experience Analysis and Feedback, USA.

Ontario Ministry of Labour. 2013. *Workplace Hazards: FAQs* [Online]. Ontario, Canada. [Accessed 07.10 2013].

Paulsen, J.E., Hoset, H., Rørhuus, T., Larsen, V., Alm, D., Birkeland, O. & Marker, R. 2005. *Exploration drilling in the Barents Sea; prevailing zero discharge regime challenges and learning from two recent exploration wells*. SPE Asia Pacific Health Safety and Environment Conference and Exhibition. Society of Petroleum Engineers.

Public Services Health and Safety Association. 2011. *Fast facts: Risk assessment and job hazard analysis*. Toronto, Canada.

Rausand, M. 2013. *Risk assessment: theory, methods, and applications*, John Wiley & Sons.

Risikko, T., Makinen, T.M., Påsche, A., Toivonen, L. & Hassi, J. 2003. A model for managing cold-related health and safety risks at workplaces. *International journal of circumpolar health*, 62.

Robson, L.S., Clarke, J.A., Cullen, K., Bielecky, A., Severin, C., Bigelow, P.L., Irvin, E., Culyer, A. & Mahood, Q. 2007. The effectiveness of occupational health and safety management system interventions: a systematic review. *Safety Science,* 45, 329–353.

Safe Work Australia. 2011. *How to manage work health and safety risks: Code of practice Australia*.

US Department of Health & Human Services. 1985. *Occupational Safety and Health Guidance Manual for Hazardous Waste Site Activities*. Public Health Service.

Veerasingam, S. 2011. *Hazard/ risk identification* Malaysian Society for Occupational Safety and Health (MSOSH).

Veil, J. 2002. *Drilling waste management: past, present, and future.* SPE Annual Technical Conference and Exhibition.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Estimating individual occupational risk using registration data

P.H.G. Berkhout & M. Damen
RIGO Research Consultants, Amsterdam, The Netherlands

ABSTRACT: In this paper the occupational risk of individual employed workers is assessed using merged registration data. The analysis features a negative binomial count data regression model for statistical inference. In the model the hazard rate is determined by variables characterizing the personal background and working conditions, such as age, sex, tenure, contract type, working hours and sector. The estimation results can be used to assess individual occupational risk and identify high-risk groups and branches of industry. The main contribution of the paper to the literature is the fact that calculations include the entire population at risk and are based solely on registration data on individuals, jobs, firms and accident casualties.

1 INTRODUCTION

Risk assessment is a cornerstone of the European approach to prevent occupational accidents and ill health. European legislation with respect to risk assessment is grounded on the Framework Directive 89/391, which has been transposed into national legislation of member states. The European Agency for Safety and Health at Work (EU-OSHA) suggests a stepwise approach to risk assessment: 1) identifying hazards and those at risk; 2) evaluating and prioritizing risks; 3) deciding on preventive action; 4) taking action and 5) monitoring and reviewing. Clearly, the process of risk assessment builds on identifying hazards and the workers at risk in the initial step. This paper sets out to quantify the occupational risk of all registered employed workers, based on merged registration data and conventional statistical methods.

Usually statistics on occupational accidents are presented on the aggregate level. Risk assessment of individual workers is complicated, since it requires detailed information on outcomes of all workers at risk, not only the accident casualties. Information gathering is usually initiated when occupational accidents occur; the counterfactual—workers who under the same circumstances did not get involved in an accident—is not observed. For instance, Rivas et al. (2011) analyze with the help of data-mining techniques 62 questionnaires to be completed whenever an accident occurred. They conclude that data-mining outperform conventional statistics in terms of the predictive function and the possibility of identifying interactions between variables with a bearing on accidents. However, the question is whether inferences drawn from a sample of accidents only can be extrapolated to the workers who did *not* get involved in an accident. In experimental lingo this is referred to as the external validity, see Shadish, Cook & Campbell (2002). In sample surveys of the population at risk generalization is usually not a problem. But sample surveys are usually too small in relation to the probability of observing enough accident casualties in the survey sample.

In the present paper we will demonstrate that plausible estimations of individual occupational risk can be extracted from detailed registration data representing the entire population at risk. The negative binomial count data model is used to estimate the individual rate of accident occurrence per working day. To this end complete registration data on casualties of serious occupational accidents was merged to individual registration data describing the entire population at risk. In the model occupational risk may vary for individual workers as a result of differences in their human capital (age, gender, flex worker, nativity, tenure, hours worked per week) and the hazardous nature of the work (instrumented by 262 sector fixed-effects covering the entire economy).

Since the available data cover a time span of thirteen years (1999–2011), the analysis is not only focused on cross-sectional explanation of occupational risk. In addition, time trends and business-cycle effects were identified. A declining number of accident casualties in this decade was in fact one of main reasons why this study was initiated. Estimation results show a decline of 27% in the average rate of accident occurrence in time. This raises the question whether occupational safety in The Netherlands has truly improved to such extent. We conjecture that structural changes in labor market supply and demand have contributed significantly to changes in the observed average accident rate. For one, ageing of the worker population

pushes the average rate upward (since occupational risk tends to rise with age for workers older than 30). The size of this ageing effect is considerable, due to an increase in the average age of the worker population from 36.3 in 1999 to 39.5 in 2011. On the other hand, a hazard-biased destruction of jobs over time has changed the composition of the job-pool in favor of the less hazardous jobs. A lower average rate of accident occurrence would be the result. Roughly estimated this composition-effect accounts for one third of the total decline. All in all, a 'true' decline in the accident rate of 19% in 13 years remains, implying a considerable improvement in occupational safety in The Netherlands in the past decade.

The paper is structured as follows. In Section 2 the observed individual occupational risk is considered within the conceptual framework of labor market matching of workers to jobs. Data, definitions and a formal description of the empirical model are presented in sections 3 and 4. In Section 5 estimation results are presented. Section 6 concludes.

2 CONCEPTUAL FRAMEWORK

2.1 *Labor market matching of individual skills to job requirements*

In this paper the rate of occurrence of occupational accidents—the accident frequency—is analyzed within the human capital framework of labor market matching of workers to jobs. On the labor market the skills of individual workers are matched to jobs requiring certain skills. Each worker-job match results in a hazard rate specific to that particular match.

Each existing job represents an objective hazard potential intrinsic to the job. This potential is not affected by the worker selected for the job. The job hazard potential is an unobserved (latent) variable in the framework. One might say that in case an accident occurs, part of the potential's hazardous energy is released and observed. The hazards require skills to handle them. These hazard handling skills are supplied by the workers. Anything contributing to the ability of handling hazards successfully can be considered: vitality, experience, responsiveness, knowledge etc. We refer to the aggregate all of such characteristics as the 'hazard handling skills'. In the framework of matching workers to jobs these skills can be treated as any other requirement for the job.

Workers are heterogeneous in their skills endowment, jobs are heterogeneous in their hazard potential. Since occupational accidents involve costs (and accident prevention reduces these costs), the employer treats the worker's hazard handling skills as any productive skill. Depending on relative prices, there's a trade-off between the cost evading hazard handling skills on the one hand and productive skills incurring revenue on the other hand. Should accidents incur high expected costs employers will emphasize hazard handling skills in the selection of workers. Vice versa, hazard handling skills will have low value to the employer if expected costs of accidents are low. Expected costs are defined by actual costs multiplied by the accident probability. Given a worker-job match, the job's latent hazard potential is transformed into an observed occupational risk. Thus from the worker's perspective his individual occupational risk will vary with the job he is matched to. From the employer's perspective the occupational risk related to his jobs varies with the matched workers.

In the present analysis the individual occupational risk is defined as the rate of accident occurrence per working day. For the sake of brevity we will refer to the rate of accident occurrence as the '*hazard rate*'. This concept is commonly used in survival analysis, defining the rate at which individuals leave a certain state, conditional on having survived up to that point. In the present context we might say workers 'survive' as long as they are not involved in an occupational accident. Note that the term 'hazard' does not refer to the actual occupational hazards (i.e. risks or dangers) the worker is confronted with in his job. Instead, it refers to the risk of 'not surviving', that is of getting involved in an accident. The hazard rate is estimated on the individual level. Hazard handling skills are instrumented by age, sex, nativity, hours worked, tenure and type of contract. On the demand side fixed-effects for 262 sectors of industry are estimated, representing job average hazard potentials.

2.2 *Structural changes in labor supply and demand*

The above matching framework is used to explain changes in the population average over time. That is, developments on the macro level are related to mechanisms operating on the micro level of matching workers to jobs. We will assume matching technology did not change during the thirteen years of observation. With the matching technology given and fixed relative prices of hazard handling skills and productive skills, two different ways to change the average accident frequency on the demand side of the market are identified. First, the safety conditions in existing jobs may be affected by technological progress (e.g. improved gear and materials), investments in the firm's safety culture and regulation by authorities. These factors affect the hazard potential in existing jobs. One might say they are associated with the 'intrinsic' or real occupational safety. Second, on the demand side

there is on-going dynamic process of destruction and creation of jobs. This process in itself may be hazard-biased in a sense that it is selective with respect to hazard potential. When for instance due to technological progress relatively hazardous job are destroyed and relatively safer job are created, the composition of the job-pool changes over time. All else held constant, this will be revealed in a declining average hazard rate. However, such a composition-effect can also contain a spurious improvement of occupational safety. For example, when relatively hazardous jobs are shifted to self-employed individuals the average hazard potential in the entire job population declines, but occupational safety from the national perspective remains unaltered (the hazardous work is still done, but not by employed workers). In this respect one might argue that outsourcing tasks to countries with low labor costs does not change occupational safety in global perspective; it only reallocates hazards geographically. Thus, as long as the destructed jobs are associated with hazardous work that has become redundant, the job-pool composition-effect will represent a real change in occupational safety. If destruction of jobs is associated with a reallocation of hazardous tasks (e.g. from employed workers to self-employed workers), the job-pool composition-effect is in essence no more than a spurious change in occupational safety.

On the supply side of the market the matched worker population is equipped with hazard handling skills determining how much of the hazard potential is transformed into observed accident frequencies. Clearly, the amount of these skills present at any moment in time is subject to changes. One interesting hypothesis in this respect is for instance the effect of an ageing worker population on the accident frequencies. Presumably, as workers get older their hazard handling skills seem to deteriorate. The Dutch data show a steadily with age rising accident frequency for workers older than 30. In theory, this suggests that ageing of the worker population induces a higher accident frequency.

3 DATA

3.1 *Registered population at risk*

The population at risk is defined as all employed workers registered to be living in The Netherlands. Self-employed individuals and foreigners not formally registered are excluded from the analysis. Micro register data on the population at risk was supplied by Statistics Netherlands (CBS). Information of several registrations is combined in the so-called SSB, which is the Dutch abbreviation of 'social statistical micro data'. The SSB is in essence based on the municipal registrations of inhabitants, registrations of social insurances of employed workers and income taxes. The following information was used:

- date of birth; gender; first and second generation foreign descent;
- beginning and end dates of jobs; contract hours; type of contract (flex workers)
- sector of industry (distinguishing 262 sectors).

Individuals are uniquely identified by a personal code derived from the citizen service number (BSN). Sectors of industry are identified using the Dutch Standaard Bedrijfsindeling (SBI 2008) which is based on the activity classification of the European Union (Nomenclature statistique des activités économiques dans la Communauté Européenne, NACE) and on the classification of the United Nations (International Standard Industrial Classification of All Economic Activities, ISIC). In the present paper the first three digits allow differentiating between 262 sectors of industry.

3.2 *Registered accident casualties*

The Dutch labor inspectorate (I-SZW) registers the casualties of serious occupational accidents. These accidents are serious in the sense that they lead to death, permanent injury or hospitalization of the casualty. Traffic accidents on the road, in the air and on sea or waterways are not included in this registration. Furthermore accidents with dangerous substances (e.g. fireworks, asbestos, radioactive materials) and natural resources (gas) are excluded. All these excluded accidents are investigated by other specialized inspectorates. The I-SZW registration however covers the vast majority of serious occupational accidents in The Netherlands. From all registered casualties in 1999–2011 only the employed workers were selected. Self-employed individuals and collateral casualties (e.g. passers-by) were excluded from the analyses.

Although reporting of accidents is mandatory/compulsory, there is suspicion of underreporting. This may occur when a serious accident is erroneously not reported to the inspectorate. The amount of underreporting is estimated to range from 1000 to 1500 accidents per year (Schouten et al. 2008). This amounts to say 30–40% of the yearly average of serious accidents investigated by I-SZW or say 25% of the 'true' number of accidents. However, the estimate by Schouten et al. should be treated with caution, since it is based on a comparison with registered casualties of a small sample of first-aid centers unevenly spread across the country.

Since there is no evidence of a selection bias due to underreporting, we will treat the registered casualties as a representative 75%-sample of the true casualty population.

3.3 *One-to-one merging*

Data was assembled by one-to-one merging of several registers by means of a unique identifier of individuals: the citizen service number (BSN). The BSN-code of the casualties was not registered by I-SZW but derived by CBS on the basis of date of birth, gender and address (zip-code and house number). In 1999–2011 a total of 30,424 casualties were registered in all inspected serious accidents in The Netherlands. The citizen service number of 6,353 (20,9%) of these casualties could not be identified, mostly due to lacking or incorrect personal information. Also casualties who were not formally registered as inhabitants or as tax-paying workers could not be identified. The remaining 24,071 (=30,424 – 6,353) identified casualties compare very well to the total number of casualties counted in the Storybuilder database, in which all serious accidents are bow tie modelled by hand (Bellamy et al. 2006, 2007, 2008). This suggests that the quality of gathering of personal information by I-SZW may fall short when it turns out during the course of the investigation that the incident does not formally qualify as a serious accident. In general, identification failure does not give rise to a selection bias, with the exception of lethal accidents. Since the count of lethal accidents is well-established in Storybuilder we estimate a loss of say 10 out of the expected number of 75 deaths per year. From the 24,071 identified casualties another 2,842 were excluded because they were not identified as members of the population at risk (employed workers). The final sample of occupational accident casualties consists of 21,229 individuals.

4 DEFINITIONS AND EMPIRICAL MODEL

4.1 *Definitions*

The time axis is measured in months, resulting in 156 time periods t in the years 1999–2011. In each t the actual number of workers—on average 7.5 million workers per period—is selected using the dates marking the beginning and ending of a job. The duration of exposure to occupational hazards per month is measured in full time (8 hour) working days according to the contract, denoted as d_{it}. For part time workers the working hours are transformed to full time working day equivalents. For instance, a half-time job of four days per week adds up to two full time working days. Workers with flexible hours are separated from other workers. Exposure is corrected for weekend days, varying length of the calendar months and Christian and national holidays. Sick leave and vacations could not be corrected for. The job hours of workers with two (or more) jobs at the same time are added up. Should these jobs be in separate sectors of industry, the sector of the largest job is assigned to the smaller ones. In each period t an indicator C_t expresses the state of the Dutch business cycle (DNB, 2013). A discrete indicator A_{it} expressing whether member i of the population at risk was registered as an accident casualty in period t was constructed by one-to-one merging the casualties to the population at risk. Indicator A_{it} is defined as:

$$A_{it} = \begin{cases} 1 & \text{member } i \text{ of the population identified} \\ & \text{by data merging as casualty in } t \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

With on average 7.5 million workers per period we observe approximately one billion A_{it} in 1999–2011. In order to bring down this number to manageable size, groups of population members are defined. Each group g contains all population members i in period t who are homogenous with respect to characteristics vector X_i. This vector includes the variables: age, gender, native versus non-native workers, flex versus normal workers, part time workers, new recruits and 262 sectors of industry. This results in on average 90.000 homogeneous groups g in any period t. Note that regression-wise no information is lost since there are no variables left to differentiate within the groups. Within groups g the total number of accidents N_{gt} in period t is defined as:

$$N_{gt} = \Sigma_{i \in g} A_{it} \quad (2)$$

and the group's total amount of exposure to hazards measured in full time working days is calculated as:

$$D_{gt} = \Sigma_{i \in g} d_{it}. \quad (3)$$

Since N_{gt} is a nonnegative integer count it can be regressed on explanatory variables by means of a count data model.

4.2 *Empirical model*

The literature offers a wide variety of count data models to regress a count variable on a set of independent variables (see for example Cameron and Trivedi, 1998). A well-known example is the Poisson model. The applicability of this model however is limited due to the fact that it imposes equi-dispersion, which means that the conditional mean and variance are equal. This is a rather strong assumption. A more flexible count data model is obtained when unobserved heterogeneity is introduced in the Poisson intensity parameter λ. The most commonly used extension to the Poisson model is the negative binomial model (negbin),

which results when λ is mixed with a gamma distribution. The negbin-model imposes over-dispersion, meaning that the conditional variance exceeds the mean. The model contains the Poisson model as a directly testable special case. The negbin-model is written as:

$$\mathrm{P}(N_{gt} = y) = \frac{\Gamma(\rho^{-1} + y)}{\Gamma(\rho^{-1})\Gamma(y!)}\left(\frac{\rho\lambda_{gt}}{1+\rho\lambda_{gt}}\right)^{y}(1+\rho\lambda_{gt})^{-\rho^{-1}} \tag{4}$$

where the non-negative parameter ρ captures the degree of over-dispersion. If ρ converges to zero, the model reduces to the Poisson model. We will use the negbin type I model, which is parameterized such that ρ is scaled by λ_{gt}. This means that λ varies across individuals and that—conditional on covariates—the count variance is a linear function of the count mean. The model is estimated using the nbreg procedure in STATA (version 12).

In the present application of the model the intensity parameter λ is be interpreted as the mean rate of occurrence of serious occupational accidents per 8-hour working day. In short we will refer to λ as the *hazard rate* of getting involved in an occupational accident. Hazard rate λ is modelled to vary with group characteristics X and may vary in time t. Time variation may be due to structural tendencies (as a result from changes in the matching of supply and demand on the labor market), seasonal patterns and the business cycle C_t. In short:

$$\lambda_{gt} = \exp(X_g, f(t), C_t, D_{gt}) \tag{5}$$

with the log of D_{gt} enclosed as an offset to correct for group differences in exposure and $f(t)$ capturing a yearly trend and a seasonal pattern. A seasonal pattern is modelled by dummy variables for the twelve months. However these estimates are likely to be biased by the fact that season-biased sick leave and vacations cannot be corrected for in D_{gt}. For instance, since many workers spend most of their time off during the summer holidays, exposure D_{gt} is probably overestimated in July and August leading to a (spurious) decline in the hazard rate λ in these months. Therefore, any observed seasonal pattern in λ is attributed to unobserved patterns in absence from work due to sickness and vacations.

In the specification of eq. (5) mainly 0/1-indicator variables are included. Initially, indicator variables for all ages ranging from 15 to 64 were estimated, revealing a declining accident frequency only for worker between 20 and 30 years of age. Therefore, in the final model linear effects were estimated for three age intervals: 15–19, 20–29 and 30–64. The effect of job tenure is estimated discretely using an indicator for 'new recruits'. New recruits are defined as workers not registered to have been working in the preceding year. In each age interval a fixed effect for new recruits is estimated. Three job size intervals are specified: part-time workers of 1–49% and 50–89% of a working week and full-timers (90–100%). The model also includes 262 coefficients for sectors of industry, one for male workers, one for flex workers, one for non-native workers and eleven for the months February to December (January was chosen as reference). A linear time trend is included by counting the years as of 1999.

4.3 *Hazard ratio*

We will denote the estimated coefficients by β. Whenever β refers to a 0/1-indicator variable $exp(\beta)$ can be interpreted as a hazard ratio. For instance, let β be estimated coefficient for male workers. Hazard ratio $exp(\beta)$ then expresses the relation between the incidence rate of male and female workers. An estimate of say 0.69 would imply that the incidence rate of occupational accidents among male workers is twice the incidence rate of females since $exp(0.69) = 2$. We will express the hazard ratio with respect to a reference group (within the indicator set) with the mean hazard rate closest to the population average.

5 ESTIMATION RESULTS

In this section the results of the estimated negbin-model are discussed. The estimated model results in 286 coefficients of which 262 are fixed-effects for sectors of industry. We will address these sector effects separately by means of descriptive statistics in subsection 5.3. In subsections 5.1 and 5.2 we will discuss the remaining coefficients reflecting differences in age, gender and nativity and the worker-firm relationship. Subsection 5.4 focusses on the question to what extent the results can be interpreted as an achieved improvement in Dutch occupational safety.

5.1 *Worker heterogeneity*

The average hazard rate of serious occupational accidents in The Netherlands in 1999–2011 per 8-hour working day is estimated at 1.03×10^{-6}. Taking into account a possible underreporting of 30–40 percent the mean hazard rate would be approximately 1.4×10^{-6}. That means 1.4 serious accidents on one million full time working days. The hazard rate varies strongly over the population at risk. The distribution of hazard rates is skewed to the right, showing a relatively large amount of mass beneath the mean. The median is less than half the mean: 0.6×10^{-6}.

The ratio of the hazard rates defining the 1st and 99th percentile of the worker population is approximately 700. This means that the risk determinants incorporated in the model (age, sex, nativity, worker-firm relationship and sector) can account for large risk differentials within the worker population. However, further improvement of the model could be achieved if workers within the sectors are differentiated according to the hazard potential of their jobs, for instance by means of the International Standard Classification of Occupations (ISCO). This information was not available in our data.

The male-female hazard ratio is estimated at 4.2, implying male hazard rates of on average say four times the female hazard rate. It is likely that this large hazard ratio is to some extent due to selection of male workers in jobs with high hazard potential (in for instance construction work and industry). A remarkable hazard-age pattern is observed. An initial specification of the model with separate fixed-effects for all ages revealed that the hazard rate peaks at the age of 19 and subsequently declines with age in the interval 20–29. For workers older than 30 the hazards rate increases steadily as they grow older. On the basis of this observation separate linear effects were estimated for the intervals 15–19, 20–29 and 30–64. Results are displayed in Table 1.

As Table 1 shows, the hazard rate increases at a rate of 9 percent per year for workers younger than 20. The hazard ratio for workers of 15 and 19 years of age equals 1.42, implying a 42 percent higher rate for the 19-year old workers compared to workers 15 years of age. An explanation for this remarkable difference may be found in the fact that young students in low vocation education are formally employed by firms but spend half of their contractual working hours in school. As their education evolves, their actually worked hours converges to full time hours. This suppresses their true exposure to hazards at younger ages, resulting in low estimated hazard rates. Since trainees and their true working hours cannot be identified in our data, this explanation could not be elaborated on in more detail. Presumably, effects of dual vocational education is minimal for young workers older than 20, since most programs end before 20.

Table 1. Estimated age effects.

			Hazard ratio	
	B	Std error	Year-to-year	Interval min to max
Age 15–19	0.088	0.028	1.09	1.42
Age 20–29	–0.023	0.005	0.98	0.81
Age 30–64	0.006	0.001	1.01	1.23

For workers 20–64 year of age the hazard-age pattern is U-shaped. In the first ten years the hazard shows a 19% decline of the hazard from age 20 to 29. Subsequently the hazard gradually rises as workers grow older. From age 30 to 64 an increase of 23 percent is estimated. The estimated effects are significant beyond statistical doubt. The average hazard rate for all age cohorts is depicted in Figure 1.

The hazard ratio of non-native workers in The Netherlands equals 1.3, implying a significantly higher accident rate among workers with at least one parent born in a foreign country. In a preliminary specification of the model (not presented in this paper) an effect was tested for second generation non-natives. For those workers the hazard rate turned out to be approximately equal to the hazard rate of Dutch natives. From this one may conjecture that later generations of non-native workers:

- end up in less hazardous jobs than earlier generations, and/or
- are better equipped with hazard handling skills.

The literature provides little solid empirical evidence supporting relatively high hazard rates of foreign/migrant workers. In Berkhout et al. (2014) an analysis of foreign accident casualties in the Netherlands shows that 15% of all casualties was foreign, whereas their share in the total number of worked days is estimated at 5–10%, depending on how one deals with multiple nationalities. They show that most of the differential can be accounted for by selection of foreigners in high-risk sectors. High accident rates of foreigners prevail in some high-risk sectors, such as the construction industry. In Dressler (2012) it is argued that there is a relation between occupational risk and the extent to which workers are familiar with safety regulations, cultural settings and the dominant language at the workplace. In the present framework migrant workers are in that case

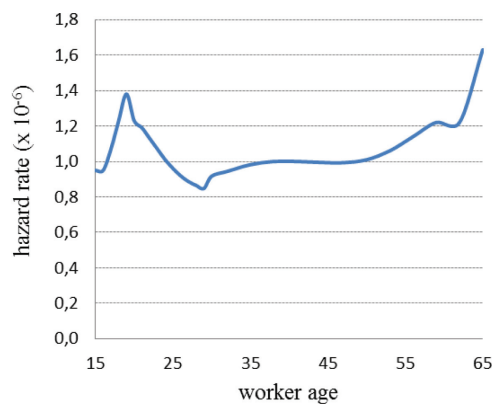


Figure 1. The average hazard rate and worker age.

on average less endowed with hazard handling skills. On the other hand, it is sometimes claimed that cultural differences will force foreign workers to work more safely than their local counterparts, grounded by a sense of responsibility towards the family and their financial needs (Grøn, 2012).

5.2 *Worker-firm relationship*

Whether the worker-firm relationship is associated with hazard rate differentials is tested by three variables: job size (i.e. hours worked per week), flexible hours and tenure. Estimates indicate that ceteris paribus the hazard rate tends to decrease with increasing job size. That is, part time workers have higher hazard rates than full timers. See Figure 2.

The hazard ratio of flex-workers is estimated at 1.3, indicating that workers flexibly affiliated to the firm tend to have higher occupational risk. A job tenure effect was tested by separating new recruits—those entering the labor force for the first time or after an absence of at least one year—from the more experienced workers. Effects in the three age intervals 15–19, 20–29 and 30–64 were estimated, none of which were found significant by conventional standards. This means we find no evidence of higher occupational risk for new recruits in general.

5.3 *Sector hazard ratios*

Sectors of industry were defined using the first three digits of International Standard Industrial Classification of All Economic Activities (ISIC). This results in 262 sectors for all of which a fixed-effect is estimated. For all sectors the hazard ratio with respect to sector Manufacture of Communication Equipment (ISIC-code 26.3) is calculated. This sector is chosen as reference since its average hazard rate is closest to the total weighted population average.

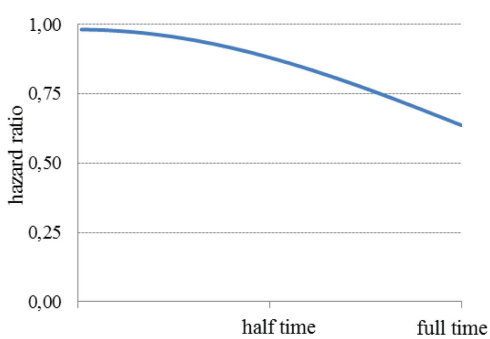


Figure 2. The job size hazard ratio.

By definition the sector hazard ratios express average job hazard potential differentials, controlled for worker selection. However, sector differentials will in fact be larger if male workers are selected into hazardous jobs. That is, if jobs with high hazard potential are mostly done by male workers. If that would be the case, the estimated male-female hazard ratio merely reflects this selection effect rather than a gender difference in hazard handling skills. A high percentage of male workers in a sector then presumably signals the presence of hazardous jobs. Therefore an alternative sector hazard ratio incorporating sector differences in male-female composition is presented. This correction inflates the standard deviation of the sector hazard ratios from 1.4 to 1.7. The maximum hazard ratio increases from 6.5 to 7.9. Descriptive statistics of the 262 gender-corrected sector hazard ratios are displayed in Table 2.

The sectors Manufacture of Weapons & Ammunition (25.4) and Other First Processing of Steel (24.3) show the highest hazard ratio and can be regarded as the most risky sectors to work in. The top 10 high-hazard sectors features three branches of the metals industry, two mining branches and two branches closely related to construction: Demolition & site preparation (43.1) and Manufacture of articles of concrete, cement and plaster (23.6). Various branches in the construction sector show hazard ratios ranging from 4.0 to 5.2.

Table 2. Sector hazard ratios (male-female composition included).

		Percentiles	Hazard ratio
Average	1.5	p(10%)	0.12
Standard deviation	1.7	p(25%)	0.30
Minimum	0.0	p(50%)	0.75
Maximum	7.9	p(75%)	2.20
N (sectors)	262	p(90%)	4.10
10 highest hazard ratios w.r.t. Manufacture of communication equipment (ISIC 26.3)			
Manufacture of weapons and ammunition (25.4)			7.9
Other first processing of steel (24.3)			7.8
Casting of metal (24.5)			6.9
Manufacture of basic precious and other non-ferrous metals (24.4)			6.4
Mining of stone, sand and clay (08.1)			6.2
Demolition and site preparation (43.1)			6.1
Materials recovery (38.3)			6.1
Manufacture of articles of concrete, cement and plaster (23.6)			6.0
Sawmilling and planing of wood (16.1)			6.0
Other mining and quarrying (08.9)			6.0

Occupational accidents are unevenly distributed over the population at risk. This can be shown graphically by means of a Lorentz curve, which is commonly used in economics to analyze inequality in the distribution of wealth and income. Inequality can be measured by the Gini-coefficient, calculated as the ratio of the area enclosed by the curve and diagonal and the total area beneath the diagonal. For the sector distribution of occupational accidents in The Netherlands the Gini-coefficient is estimated at 0.37. In Figure 3 the Lorentz curve of occupational accidents is depicted.

For example, from Figure 3 we have inferred that 36 percent of all serious occupational accidents are registered in just a handful of sectors representing 14 percent of total employment. These sectors (in the upper right corner of Fig. 3) are:

Sector (ISIC-code)	Share in accidents
Temporary employment agencies job pools (78.2)	8.8%
Roofing and other specialized construction (43.9)	4.6%
Construction installation (43.2)	4.0%
Construction of buildings (41.2)	3.6%
Manufacture of structural metal products (25.1)	2.7%
Other specialized wholesale (46.7)	2.6%
Building completion (43.3)	2.5%
Construction of roads, railways, bridges (42.1)	2.4%
Freight transport by road (49.4)	2.4%
Cleaning activities (81.2)	2.2%

Temporary employment agencies are at the top of the list. This implies that temporary workers can be considered a high-risk group of workers that may need special attention in preventive policy measures.

5.4 *Effects of structural changes in labor supply and demand and the business-cycle*

Over the years 1999–2011 a significant decline of the hazard rate of 1.9% per year is estimated. This adds up to a total decline of 27% between 1999 and 2011. The observed population average hazard rate decreased from 1.60×10^{-6} in 1999 to 1.20×10^{-6} in 2011, including structural changes in labor supply and demand. On the supply side ageing of labor supply affects the hazard rate if hazard handling skills of workers gradually deteriorate when they grow older. Between 1999 and 2011 the average age of workers increased from 36.3 to 39.5. The share of workers older than 30 increased from 67.4% to 72.4%. As was mentioned in section 5.1 (see Table 1), the hazard rate of workers older than

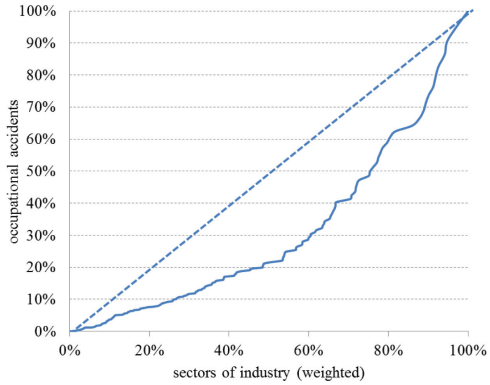


Figure 3. Lorentz curve of occupational accidents in The Netherlands.

30 significantly increases each year by 0.6%. From this we estimate an ageing effect of approximately 2%. Thus, without ageing the average hazard rate in 2011 would have been approximately 1.15×10^{-6} instead of the observed 1.20×10^{-6}. On the other side of the market structural changes in the sector composition of labor demand affect the population average hazard rate. Holding the sector composition of 1999 constant, the hazard rate corrected for ageing is estimated at 1.30×10^{-6} in 2011.

We conclude that in the absence structural changes in labor demand and supply the population average hazard rate would have decreased by 19% in 13 years. This may be interpreted as the achieved improvement of occupational safety in 1999–2011. The observed 27% decline between 1999 and 2011 is obscured by a small ageing bias (+2%) on the one hand and a somewhat larger hazard-biased destruction of jobs on the other hand (–10%). The former pushes total decline downward (towards zero), since older workers are associated with high hazard rates. The latter amplifies the decline, as jobs with high hazard potential are more often subject to job destruction.

A business cycle effect was tested by incorporating a monthly national business cycle indicator in the model. The results show a positive significant effect. That is, in an economic boom the accident frequency is 4–6% higher than in a slump.

6 CONCLUDING REMARKS

This paper sets out to quantify the occupational risk of all registered employed workers, based on merged registration data. By means of a negative binomial count data model cross-sectional differences as well as time trends are analyzed. In cross-sectional perspective the model predicts a hazard

ratio between the 1st and 99th percentile of the worker population of approximately 700 on the basis of age, sex, nativity, worker-firm relationship and sector. A 27% decline in the hazard rate over the years is partly explained by structural changes in labor supply and demand (e.g. ageing and hazard-biased jobs destruction). All in all, a considerable 'unexplained' improvement of occupational safety in The Netherlands remains.

In The Netherlands the use of registration data for statistical purposes has become common practice in the past decade. In this study a registration of casualties of serious occupational accidents was merged to the entire population of employed workers. The analysis combines data from individuals, jobs, firms and casualties. As the paper shows, the registration data can be transformed into accurate policy information when the proper statistical tools are utilized. Accuracy of the results would improve considerably if a job classification could be made available. But all in all, the paper shows that the hazard rate of individual workers can be assessed effectively by combining registration data. We consider this the main contribution of the paper to the literature.

Finally, we have shown that occupational accidents may be analyzed within the standard labor economics framework of matching skills (human capital) to job requirements. The skills needed to handle a job's hazard potential—say the hazard handling skills—may be treated as any productive—revenue generating—skills workers are endowed with. Since it is practically impossible to measure the hazard potential of jobs, we believe the focus of attention should be on the actual hazard rate which results from particular job-worker matches. The paper shows that by using complete registrations we are able to identify the effects of structural changes in labor supply and demand on occupational safety in national perspective.

REFERENCES

Bellamy L.J., Oh J.I.H., Ale B.J.M., Whiston J.Y., Mud M.L., Baksteen H., Hale A.R., Papazoglou I.A., 2006, Storybuilder: The New Interface for Accident Analysis. Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management [PSAM], May 13–19, 2006, New Orleans, ASME, New York, 2006, ISBN 0-7918-0244.

Bellamy, L.J., Ale B.J.M., Geyer T.A.W., Goossens L.H.J., Hale A.R., Oh J., Mud, M., Bloemhof A, Papazoglou I.A., Whiston J.Y., 2007, Storybuilder¬A tool for the analysis of accident reports, *Reliability Engineering and System Safety*, 92(2007): 735–744.

Bellamy L.J., Ale B.J.M., Whiston, J.Y., Mud M.L., Baksteen H., Hale A.R., Papazoglou I.A., Bloemhoff A., Damen M. and Oh J.I.H., 2008. The software tool storybuilder and the analysis of the horrible stories of occupational accidents. *Safety Science*, 46(2008): 186–197.

Berkhout P.H.G., M. Damen, L.J. Bellamy, M. Mud, H.J. Manuel and J. Oh., 2014. Serious occupational accidents of non-Dutch workers in The Netherlands, In: Safety Reliability and Risk Analysis: beyond the horizon, R.D.J.M. Steenbergen, PH.A.J.M. van Gelder, S. Miraglia and A.C.W.M. Vrouwenvelder (eds.).

Cameron, A. Colin, and Pravid K. Trivedi, 1998. Regression Analysis of Count Data, Cambridge University Press, New York.

DNB, (2013). DNB-business cycle indicator, ww.dnb.nl.

Dressler, D., 2012. Increased occupational risks among migrant workers in Austria, ISSA, WOS 2012.

EU-OSHA, 2014 https://osha.europa.eu/en/topics/riskassessment.

Grøn, S., and Cruz G., 2012. National differences in safety practice, Centre for Maritime Health and Safety, University of Southern Denmark, University of the Phillipines. WOS 2012.

Rivas, T., M. Paz, J.E. Martin, J.M. Matias, J.F. Garcia, J. Taboada, 2011. Explaining and predicting workplace accidents using data-mining techniques, Reliability Engineering and System Safety, Vol. 96, pp. 739–747.

Schouten, M.J., A. Faas en J. Hoeben, 2008. Achtergronden dodelijke en ernstige arbeidsongevallen op basis van in 2007 afgesloten ongevalsonderzoeken, Arbeidsinspectie, december 2008 (in Dutch).

Shadish, W.R., Cook T.D. and Campbell D.T., 2002. Experimental and quasi-experimental designs for generalized causal inference, Houghton Mifflin Company Boston New York.

United Nations, 2008. International Standard Industrial Classification of All Economic Activities, Statistical Papers, Series M, revision 4.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantification of risk rates of occupational accidents

I.A. Papazoglou & O. Aneziris
National Centre for Scientific Research "DEMOKRITOS", Aghia Paraskevi, Greece

L.J. Bellamy
White Queen, Hoofddorp, The Netherlands

M. Damen
RIGO, Amsterdam, The Netherlands

B.J.M. Ale
TU Delft, Delft, The Netherlands

H.J. Manuel
National Institute for Public Health and Environment, Bilthoven, The Netherlands

J.I.H. Oh
Ministry Social Affairs and Employment, The Hague, The Netherlands

ABSTRACT: Occupational risk rates per hour of exposure are quantified for 63 occupational hazards for the Dutch working population. Data were obtained from the analysis of more than 9000 accidents that occurred over a period of six years in the Netherlands and resulted in three types of reportable consequences under Dutch law: a) fatal injury, b) permanent injury, c) recoverable injury requiring at least one day hospitalisation. A Bayesian uncertainty assessment on the value of the risk rates has been performed. Annual risks for each of the 63 occupational hazards have been calculated including the variability induced by the variability of the annual exposure of the working population to these hazards. Suitability of three risk measures, individual risk rates, individual annual risk and number of accident occurred is examined and commented upon.

1 INTRODUCTON

Occupational health and safety is a major concern to many countries since occupational accidents represent a major source of risk. In 2010, accidents at work killed 3691 workers in in EU-28, while 2721629 workers were injured, with absence of work more than three days (Health and Safety at Work).

Traditional occupational safety methods are legislation, regulation, standards, safety guidelines, collection of best practices, accident statistics, investigations and inspections, analysis of safety management systems and personal behaviour. The most significant standards used for occupational safety are the British (BSI, 1996, 1999) and the international standard by ILO (ILO, 2001). In addition various analyses of occupational accidents have examined the causes of occupational injuries and fatalities such as those performed for construction, electric power and extractive industry by Carnero & Pedregal (2010) Silva & Jacinto (2012) and Ale et al. (2008).

A number of attempts to a more systematic and consistent approach to quantitative occupational risk assessment have appeared in the literature. A model has been developed to predict the frequency of occupational accidents in offshore oil and gas industry, based on direct, corporate and external factors, as proposed by Attwood et al. (2006). Quantified risk for various occupational groups in Sweden based on the number of accidents and relevant exposure has been calculated by Larsson and Forsblom (2005). A method has been proposed by Ivan et al. (2010) for risk assessment of several trades in the construction industry, based on estimating the overall frequency and severity from historical data of accidents in Hong Kong and their consequences regarding injuries, days lost and compensation cost. Fuzzy methods have been

Table 1. Point risk rate (/hr) and variability characteristics of risk rates (/hr) for fatality accidents for various single hazards.

Hazards	Point risk	5%	90%
1.1.1.1 Fall from height - placement ladder	2.38E-08	1.64E-08	3.52E-08
1.1.1.2 Fall from height - fixed ladder	1.87E-08	9.21E-09	4.28E-08
1.1.1.3 Fall from height - step ladder or steps	4.74E-09	2.16E-09	1.23E-08
1.1.2.1 Fall from height – working on mobile scaffold	5.64E-08	3.31E-08	1.02E-07
1.1.2.2 Fall from height - working on fixed scaffold	1.77E-08	1.01E-08	3.32E-08
1.1.2.3 Fall from height – (de-)Installing scaffold	1.88E-08	9.85E-09	3.96E-08
1.1.3.1 Fall from height – roof	2.26E-07	1.77E-07	2.92E-07
1.1.3.2 Fall from height – floor	6.41E-08	4.48E-08	9.39E-08
1.1.3.3 Fall from height – Fixed platform	4.37E-08	2.80E-08	7.08E-08
1.1.4 Fall from height – hole in the ground	1.68E-09	6.89E-10	5.30E-09
1.1.5.1 Fall from height - moveable platform	8.02E-08	5.69E-08	1.16E-07
1.1.5.2 Fall from height - non-moving vehicle	5.15E-08	2.93E-08	9.68E-08
1.1.5.3 Fall from height – other	1.79E-08	9.79E-09	3.53E-08
1.2 Fall on same level	1.20E-10	5.46E-11	3.09E-10
1.3 Fall down stairs or ramp	3.73E-09	1.53E-09	1.17E-08
2. Struck by moving vehicle	1.15E-08	9.08E-09	1.47E-08
3.1 Contact with falling object – crane or load	3.61E-08	2.27E-08	5.97E-08
3.2 Contact with falling object - mechanical lifting	5.78E-09	2.36E-09	1.82E-08
3.3 Contact with falling object – vehicle or load	2.72E-10	2.78E-10	1.38E-08
3.4 Contact with falling object - manual handling	2.22E-10	2.27E-10	1.12E-08
3.5 Contact with falling object – other	1.64E-07	1.13E-07	2.43E-07
4.1 Contact with flying object – machine or handheld tool	1.34E-09	5.49E-10	4.23E-09
4.2 Contact with flying object – object under pressure or tension	5.88E-09	3.35E-09	1.11E-08
4.3 Contact with flying object – blown by wind	5.69E-11	1.05E-10	5.66E-09
5 Hit by rolling/sliding object	1.79E-09	8.16E-10	4.62E-09
6.1 Contact with object used or carried–hand held tool	5.47E-13	1.36E-11	7.89E-10
6.2 Contact with object used or carried - NOT handheld tool	4.04E-10	1.44E-10	1.91E-09
7 Contact with hand held tools operated by self	1.04E-12	9.45E-12	5.43E-10
8.1.1 Contact with moving parts of a machine – operating	5.17E-10	1.84E-10	2.45E-09
8.1.2 Contact with moving parts of a machine – maintaining	5.26E-09	2.15E-09	1.65E-08
8.1.3 Contact with moving parts of a machine – clearing	5.51E-08	3.02E-08	1.09E-07
8.1.4 Contact with moving parts of a machine – cleaning	6.73E-09	2.39E-09	3.17E-08
8.2 Contact with hanging/ swinging objects	8.85E-09	5.46E-09	1.50E-08
8.3Trapped between	1.20E-08	8.03E-09	1.85E-08
9 Moving into object	1.17E-12	8.02E-12	4.58E-10
10 Buried by bulk mass	2.27E-12	8.60E-11	5.01E-09
11 In or on moving vehicle with loss of control	1.39E-08	1.07E-08	1.83E-08
12.1 Contact with electricity – high voltage cable	1.91E-08	9.40E-09	4.36E-08
12.2 Contact with electricity – tool	6.28E-10	3.28E-10	1.32E-09
12.3 Contact with electricity – electrical work	7.94E-09	4.90E-09	1.35E-08
13 Contact with hot or cold surfaces or open flame	1.15E-12	2.85E-11	1.66E-09
14.1 Release of hazardous substance out of open containment	1.75E-11	4.56E-11	2.51E-09
14.2 Exposure to hazardous substance without Loss of Containment	1.79E-09	7.40E-10	5.50E-09
15.1 Release of a hazardous substance out of a closed containment – adding, removing or opening	3.06E-09	1.25E-09	9.62E-09
15.2 Release of a hazardous substance out of a closed containment – transport	2.57E-11	5.19E-10	3.01E-08
15.3 Release of a hazardous substance out of a closed containment- closing	1.55E-11	1.24E-09	7.24E-08
15.4 Release of a hazardous substance out of a closed containment – working nearby	8.87E-09	3.63E-09	2.79E-08
17.1 Fire - hot work	7.87E-10	2.80E-10	3.74E-09
17.2 Fire - working near flammables	1.83E-09	7.50E-10	5.78E-09
17.3 Fire - fire fighting	4.00E-11	4.82E-10	2.78E-08
20.1 Human aggression	4.57E-10	2.08E-10	1.18E-09
20.2 Animal behavior	3.58E-09	1.46E-09	1.13E-08
22.1 Hazardous atmosphere in confined space	2.30E-08	1.45E-08	3.80E-08
22.2 Hazardous atmosphere through breathing apparatus	2.23E-08	9.11E-09	7.00E-08
23.1 Impact by immersion in liquid – working in or under	2.51E-08	8.92E-09	1.19E-07
23.2 Impact by immersion in liquid – working nearby	6.47E-08	4.55E-08	9.41E-08
25.1 Extreme muscular exertion – handling objects	1.22E-13	9.77E-12	5.70E-10
25.2 Extreme muscular exertion – moving around	1.96E-13	3.15E-11	1.84E-09
27.1 Physical explosion	2.16E-09	9.86E-10	5.59E-09
27.2.1 Chemical explosion – vapour or gas	9.26E-09	6.20E-09	1.43E-08
27.2.2 Chemical explosion – dust	1.06E-09	3.76E-10	5.03E-09
27.2.3 Chemical explos. – explosives	7.52E-13	4.83E-11	2.82E-09
27.2.4 Chemical explosion – exothermic reactions	2.20E-13	3.54E-11	2.06E-09

used for risk assessment of occupational accidents in a steel company by Mure and Demichela (2009), at construction sites by Gurcanli and Mungen (1009), Pinto (2014) and Liu and Tsai (2012), and workplaces by Grassi et al. (2009). Artificial neural networks and a fuzzy inference system have been proposed to assess occupational injury risk indexes and predict number of injuries by Ciarapica & Giacchetta (2009).

The Ministry of Social Affairs and Employment in the Netherlands developed, a large scale project during 2003–2008 to improve the level of safety at workplace, by introducing quantitative occupational risk. This project had four major parts: assembly and analysis of accident and exposure data, generalisation of these data into a logical risk model, deriving improvement measures and their costs and developing an optimizer that supports cost effective risk reduction strategies, as described by Papazoglou et al. (2008), Ale et al. (2008) and Oh & Sol (2008). Results of the Workgroup Occupational Risk Model (WORM) project are presented in RIVM (2008) and its main achievements are: (a) construction of logic models (bowties), which allow for the quantitative assessment of risk of 63 activities of workers, such as fall from ladders, scaffolds, roofs Papazoglou & Ale (2007) and Aneziris et al. (2008a), hit by falling objects Aneziris et al. (2008a), etc., built on the detailed analysis of 12500 accident reports in the Netherlands extracted from the Occupational Accident Database GISAI (Gemeenschappelijk Informatie Systeem Arbeidsinspectie) (GISAI, 2005) and data concerning the exposure of the Dutch population to various hazards, as reported by Kuiper et al. (2008) and (b) the development of the probabilistic occupational risk model (ORCA), which performs risk calculation of workers performing various tasks and exposed to several hazards, as presented in construction and manufacturing case studies Aneziris et al. (2010a, 2010b, 2012).

Occupational accidents can result in health damages of various degrees. Occupational risk from accidents is quantified when the degree of severity of the potential health damage can be measured along with the relative likelihood with which each level of damage is expected to occur. In the WORM model the damage to the worker's health is discretized to three possible values: a) recoverable injury; b) permanent injury; and c) fatality. Every time a worker performs a work-related activity and faces a particular hazard he faces the possibility of an accident that may result in one of the above consequence levels. Such a consequence does not happen with certainty but rather randomly in the work-population and during the lifetime of the workers. The associated risk is quantified when the probability with which each of these possible consequences such as recoverable injury, permanent injury or fatality, can occur during a specific period of time is known. Thus for our purposes the risk is quantified when the three probabilities have been assessed or by the triplet {p1,p2,p3}, where it is understood that p1 is the probability of recoverable injury, p2 is the probability of permanent injury and p3 is the probability of death. These probabilities should always be thought in association with a given period of time during which the accident might happen.

The WORM project identified 36 hazards with the potential of causing an accident during work with detrimental health effects. The 36 hazards were further developed into the sixty three (63) hazards listed in Table 1. Consideration of the particular 63 hazards was mainly dictated by the need to identify hazards simple enough that can be attributed to various jobs and activities without the need to differentiate between industrial sectors or types of jobs.

The purpose of this paper is to present the quantification of the risk rates, that is the probability per unit of time (hour) for each and every of the 63 hazards. The paper is organised as follows: Section 2 outlines the modelling of the arrival of occupational accidents as a Poisson random process and briefly describes the procedure followed for identifying the number of accidents and the exposure of the Dutch working population to the occupational hazards during a given period of time. With these two sets of data point estimates of the risk rates are obtained. Section 3 presents the assessment of the uncertainties associated with this estimation following a Bayesian approach. Finally Section 4 discusses the obtained results.

2 MODEL AND DATA REQUIREMENTS

Occupational accidents occur randomly in time. As "*time-to-accident" (t)* we define the time elapsing between the start of a certain job that involves the exposure to a given hazard and the onset of an accident. This analysis assumes that accidents happen randomly as the worker performs the job and that accidents arrive according to a *Poisson* random process. This means that the times-to-accidents are exponentially distributed with parameter λ or that the probability density function (pdf) of the random variable t is given by

$$f(t) = \lambda e^{-\lambda t} \tag{1}$$

If a worker is exposed to an accident hazard for τ hours during a calendar period (e.g. a year) then the probability that there will be an accident anytime during this period is equal to the probability

that the time of accident arrival will be less than τ or

$$p = F(t \le \tau) = 1 - e^{-\lambda\tau} \tag{2}$$

2.1 *Sampling and likelihood of sample*

The parameter λ is estimated from observations of the random process and recording of the times at which accidents occur.

This is usually done by observing a population of N workers each for a given period of time t_0. During this period some of the workers will actually suffer an accident with given consequences and some will simply work the whole period t_0 without an accident. Let k be the number of workers suffering an accident at times $(t_1, t_2, \ldots, t_k)$. Then N-k is the number of workers without an acciden, that is each of them worked for t_0 without an accident.

Assuming that the occurrence of each accident does not depend statistically to the other occurrences or non-occurrences, and that if a worker has an accident at t_i she is no more exposed to the hazard for up to t_0, it is possible to calculate the probability of such an outcome also called *likelihood.* The likelihood of a sampling outcome like the one described before is given by

$$\begin{aligned} L &= \prod_{i=1}^{k} \lambda e^{-\lambda t_i} \prod_{j=k+1}^{N} e^{-\lambda t_0} \\ &= \lambda^k \exp\left[-\lambda\left(\sum_{i=1}^{k} t_i - \sum_{j=k+1}^{N} t_0\right)\right] = \lambda^k e^{-\lambda T} \end{aligned} \tag{3}$$

where T is the total exposure given by

$$T = \sum_{i=1}^{k} t_i + (N-k)t_0 \tag{4}$$

From equations (3,4) it follows that the likelihood of the sample depends only on the statistics $\{k, T\}$ and not on the individual observed times (t_k). For this reason the statistics $\{k, T\}$ are called *sufficient statistics* of the sampling procedure.

It can be shown that the estimation of the accident rate $\hat{\lambda}$ that maximizes the likelihood L given by Eq. (3) is given by

$$\hat{\lambda} = \frac{k}{T} \tag{5}$$

Equation (5) is widely used to obtain a point estimation of the accident rate λ. It has been used in the calculation of the point estimates of the various hazard rates given in Table 1.

2.2 *Sampling a random process—sufficient statistics*

The general expression for the sufficient statistic T of a sample taken from a Poisson random process is given by Eq. (4). There are, however, some special cases that are amenable to further analysis. The distinction of the various types of sampling schemes has to do with the way the sample is taken and in particular on the way the sampling procedure is terminated.

In the WORM project a fixed period of time (calendar years) has been chosen and the number of accidents that occurred during this period has been determined. This is equivalent to a *Poisson* type of sampling.

In the Poisson type of sampling, the sampling procedure stops when a certain predetermined total exposure has been achieved and the number of accidents that have occurred has been recorded. In this case the number of accidents (k) to be observed is random.

Poisson sampling without replacement

$$T = \sum_{i=1}^{k} t_i + t \tag{6}$$

where $\{t_i,\ i = 1, \ldots, k\}$ are the k times to accident and t the remaining time (can be equal to zero) to complete the fixed time period T.

If there are N workers in the sample to be observed, then the duration of observation of each one is set to t_0. If in addition there is no replacement of a worker having an accident, then

Poisson sampling of size N without replacement

$$T = \sum_{i=1}^{k} t_i + (N-k)t_0 = Nt_0 - \sum_{i=1}^{k} (t_0 - t_i) \tag{7}$$

If there is replacement of a worker in the sample when she have an accident then

Poisson sampling of size N with replacement

$$T = Nt_0 \tag{8}$$

In all these cases the statistic T is predetermined and known and the statistic k is random determined after the sampling ends.

2.3 *Number of accidents*

In the WORM project the constant accident rate for each of the 63 single hazards has been estimated following the analysis of section 2.2 A number of 9387

accidents reported according to the Dutch labour law that occurred in the 1998–2004 period (6.23 years) and contained in the GISAI (Geïntegreerd Informatie Systeem ArbeidsInspectie) data base have been analysed using the STORYBUILDER tool developed by Bellamy et al. (2007). This tool allows the building of scenarios or accident sequences incorporating all the factors that have contributed to the accident and eventually builds a logic model connecting the ultimate consequence (death or injury) to the underlying factors and in general the working environment conditions. The 9387 accidents are distributed across 36 Storybuilds, graphical structures in the software StoryBuilder, each representing a type of occupational accident, characterised and named in each case by the event that characterizes the accident also called "Centre Event". The 36 qualitative models have been subdivided into 63 more specific hazards for which detailed logical models have been developed. A number of reports had unidentified consequences. These accidents have been redistributed to the permanent or recoverable injuries, since it is believed that deaths are reported precisely. The results are given in Table 1.

2.4 *Exposure to hazards*

Exposure is the time that a worker is at risk of having an accident. The exposure for each of 63 hazards has been determined by defining the activities/situations—known as *missions*—that can lead to these accidents and then conducting a nationwide survey in the Netherlands to establish the exposure to each mission (expressed as duration in hours). For example for Hazard #2: Struck by moving vehicle the mission is defined as:

> "Number of hours workers are as a pedestrian at locations with moving vehicles during work. This includes working on industrial premises, in warehouses or at loading/unloading bays, or along the public highway in the role of (for example) road construction worker, garbage collector, roadside vehicle repair mechanic/pick-up service or police officer. Normal traffic activity as a user of the public highway (including commuting and business travel) is not included."

In November 2006 the mission survey was carried out among a random net sample of 30000 from the TNS-NIPO Internet Panel that has approximately 200000 members of which about 50000 constitute a representative sample of the Dutch working population; so in practice the 30000 were drawn from the 50000. For each mission the respondents filled out how many hours they were exposed in the week preceding the survey. To obtain representative exposure data for the Dutch working population, major deviations from the survey sample with known population distributions were corrected for over and under representation by applying a weight factor, as proposed by RIVM (2008) and Hahn & Shapiro (1994). Aspects of the population distribution that were considered in this weighting procedure were: industry sector, job type, type of employment, education level, age and gender. The weighting procedure also took into account the changes in composition of the working population in the period 1998–2004 (the period from which accidents were analysed) and 2006 (the year the exposure was measured). Since the accident population did not include some specified occupational groups, these occupational groups were excluded from the exposure data. The same holds for the self-employed when not working under the authority of others (as they are also excluded from the available accident data).

The weekly exposure was extrapolated to a yearly exposure, effectively based on a 42 working weeks year. The week in November was an average working week; however, the impact of seasonal labour on the total exposure Figures is probably missed. Next the survey sample was extrapolated to the whole of the Dutch working population. Figure 1 demonstrates one example of this exercise.

The average exposure time per year is in this case 506.52 hours. The total number of exposed workers is 1.28×10^6. Hence, total number of exposure hours in this case is 648×10^6 per year. Since the observed number of fatalities in this case corresponded to a period of six years and two months the total exposure used in equation (5) is $\sim 4 \times 10^9$ hours. During the same period the number of reported fatalities from accidents with moving vehicles has been 46. Hence equation (5) calculates the fatality risk for the occupational accident "struck by a moving vehicle" as equal to 1.15×10^{-8}.

It is noteworthy that in this quantification it has been assumed Poisson sampling with replacement (see Eq. 8). This approximation, however, is very

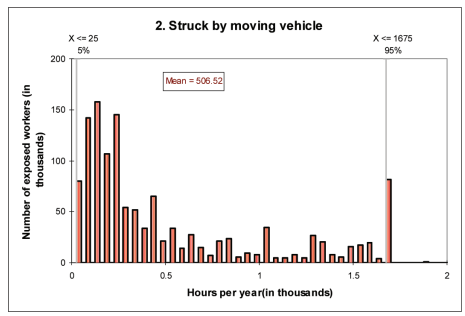


Figure 1. Histogram of frequencies of various yearly exposure times for hazard "struck by moving vehicle". Extrapolated to the total Dutch working population.

good. The term $\sum_{i=1}^{k}(t_0 - t_i)$ in Eq. 7 is less than kt_0 which in this case is $46 \times 506.52 \times 6.12 = 142{,}595$ h ours; a negligible amount when compared to the total of 4×10^9.

3 UNCERTAINTY ASSESSMENT

Uncertainties owning to the limited size of the sample or the equivalent sufficient statistic $\{k, T\}$ can be quantified following the Bayesian approach, proposed by Lindley (1965) and Bedford & Cook (2001).

3.1 *Prior distribution of accident rate* λ

Prior to obtaining the sampling results the state of knowledge is described by assuming that the accident rate (λ) is distributed according to a gamma-1 pdf or

$$f'(\lambda) = f_{\gamma_1}(\lambda|\alpha,\beta) = \frac{e^{-\lambda\beta}(\lambda\beta)^{a-1}}{\Gamma(\alpha)}\beta \quad \alpha > 0, \beta > 0 \tag{9}$$

The gamma-1 distribution has been chosen simply for calculation convenience since the gamma-1 pdf is the natural conjugate distribution to the likelihood of sample from a Poisson random process resulting in a gamma-1 posterior distribution.

Parameters (α, β) are chosen so that the mean and the standard deviation are getting desirable values.

Even though the accident rate λ is the basic parameter of our model the risk measure of interest is the annual probability for an accident. It is more natural then to express the state of knowledge on the probability of an accident during the course of a year. Complete lack of knowledge on the value of this probability would imply a uniform pdf spanning the interval (0,1).

Since the p and λ are connected through equation (2) the parameters (α, β) in the prior of $f'(\lambda)$ can be chosen such that the prior of p is non-informative. This is done as follows.

The pdf of p is uniform over an interval (a,b) hence,

$$f(p) = \frac{1}{b-a} \tag{10}$$

By virtue of equation (2) it follows that

$$\frac{\partial p}{\partial \lambda} = \tau e^{-\lambda\tau}$$

and since the pdf of λ $g(\lambda)$ is given by $g(\lambda) = f[p(\lambda)](\partial p/\partial\lambda)$ it follows that the prior of λ is given by

$$f(\lambda) = \begin{cases} 0 & if \quad \lambda \le \lambda_L = \dfrac{-\ln(1-a)}{\tau} \\ \dfrac{1}{b-a}\tau e^{-\lambda\tau} & if \quad \lambda_L \le \lambda \le \lambda_U \\ 0 & if \quad \lambda \le \lambda_U = \dfrac{-\ln(1-b)}{\tau} \end{cases} \tag{11}$$

If (a,b) is the whole interval (0,1) then the prior of λ is

$$f'(\lambda) = \tau e^{-\lambda\tau} \quad = f_{\gamma_1}(\lambda|1,\tau)$$

That is the prior of λ is a gamma-1 distribution with parameters

$$\alpha = 1 \quad \text{and} \quad \beta = \tau \tag{12}$$

This prior for $\tau = 2000$ hrs is shown in Figure 2. For the variable p and in Figure 3 for the variable λ. It is noteworthy that the 95% percentile is 2.6×10^{-3} while the 5% percentile is 1.5×10^{-5}. This means that the 90% probability interval for the accident rate λ is [2.6×10^{-5}, 1.5×10^{-3}]. Equivalently this means that the 90% probability interval for the yearly risk is [0.05, 0.95].

The value of τ = 2000 hrs has been chosen because it represents an upper limit to the amount of working hours in a calendar year.

The sufficient statistics of a sample generated by a Poisson process is the number of accidents observed (k) and the total exposure of the population (T) as described in 2.1.

3.2 *Posterior distribution of* λ

It can been shown that given the sufficient statistics of the sample (k,T) the posterior distribution

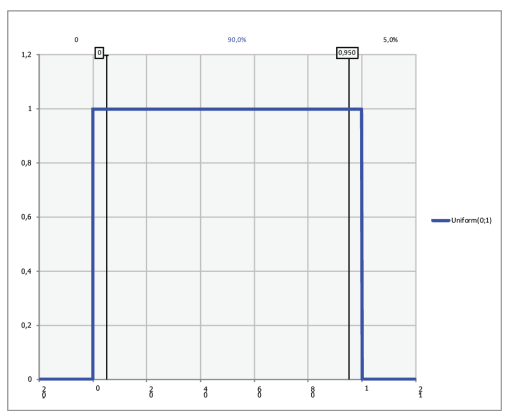


Figure 2. Prior distribution for annual accident probability.

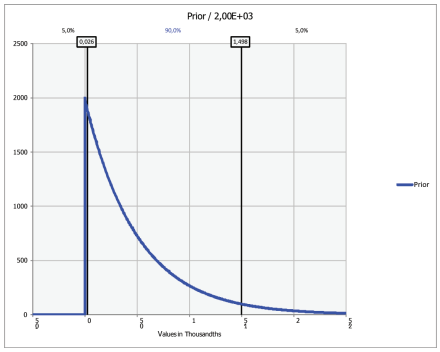


Figure 3. Prior distribution for λ.

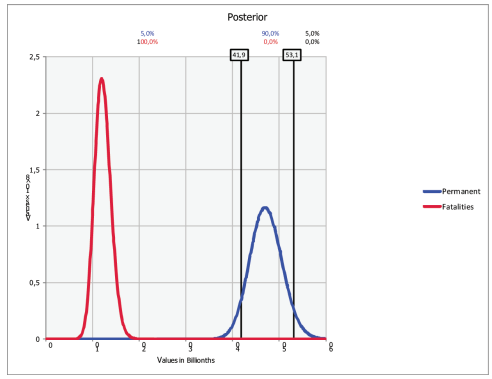


Figure 4. Posterior distributions for risk rates for fatal and permanent injuries for the hazard "Struck by a moving vehicle".

of λ $\{f''(\lambda)\}$ is also gama-1 distribution with parameters

$$\alpha'' = \alpha' + k \quad \text{and} \quad \beta'' = \beta' + T \tag{13}$$

and

$$f''(\lambda) = f_{\gamma_1}(\lambda \mid \alpha' + k, \beta' + T) \tag{14}$$

As a demonstration of this approach the posterior distributions for the accident rates for permanent injuries and fatal injuries for the hazard "Struck by a moving vehicle" are given. As below for the hazard "Struck by moving vehicle" the observed number of incidents and the Total Exposure during the observation period are:

	Number of accidents	Total exposure (hours)
Fatal injuries	46	4.01×10^9
Permanent injuries	189	4.01×10^9

Given these sufficient statistics Equations (13) and (14) provide the posterior distributions given in Figure 4.

It is noteworthy that the uncertainty in the posterior assessment of the risk rates is extremely small given the size of the available evidence (sufficient statistics). Characteristic values of the assessed uncertainty are:

	5% percentile	Mean	95% percentile	Maximum likelihood
Fatal injuries	0.9×10^{-8}	1.17×10^{-8}	1.47×10^{-8}	1.15×10^{-8}
Permanent injuries	4.2×10^{-8}	4.74×10^{-8}	5.3×10^{-8}	4.71×10^{-8}

It follows that the uncertainty owning to the limited amount of experiential evidence is relatively small. Additional evidence would not improve the uncertainty range significantly since the 90% probability interval spans a factor of 1.6 for fatal injuries and only 1.26 for permanent injuries. Similar results are obtained for all 63 single hazards and are given in Table 1 for fatalities.

4 DISCUSSION

Occupational risk rates constitute a quantitative measure for prioritising individual occupational risk. The results given in Table 1 indicate that, even after consideration of the associated uncertainty, the riskier occupations per unit of time is "working on the roof of a building"—a rather intuitively expected result but- also working in a space where loads stuck in piles or shelves are present a rather not expected result. While working on a roof a worker can fall from protected or unprotected edges or through existing holes on the roof. The mean value of the fatality risk rate is 2.32×10^{-7}/hr while the 90% probability interval is extremely narrow [1.77×10^{-7}/hr, 2.92×10^{-7}/hr] with an error factor of 1.65. Working in an area where loads are piled up or set in shelves a worker can be hit by a falling load. The mean value of the fatality risk rate is 1.73×10^{-7}/hr while the 90% probability interval is [1.13×10^{-7}/hr, 2.43×10^{-7}/hr] with an error factor of 2.15.

In general working in heights are among the riskier occupational hazards for causing fatal injuries while handling (lifting) objects, falls on the same level, and moving into sharp objects are the safest.

Probability intervals are narrow for types of accidents that have generated incidents and increase

inversely proportional to number of incidents. The relative position of the interval in the x-axis depends on the size of the exposure. For example, no deaths have been observed for work involving closing vessels containing a hazardous substance (accident #15.3) with a total exposure of 420×10^6 hours. The 90% probability interval is [1.24×10^{-9}/hr, 7.24×10^{-8}/hr] with an error factor of 58. Similarly no deaths have been recorded for hazard "working in an area where one can be buried by a balk mass" with an exposure of 600×10^6 hours. The 90% probability interval is [8.60×10^{-11}/hr, 5.01×10^{-9}/hr] with an error factor of 58. This time the probability interval although having the same size is moved to the left by an order of magnitude.

It should be emphasized that occupational risks rates refer to individual risk per unit of time of exposure. Full comparison among alternative hazards should include the exposure to this hazard. Consequently, working on the roof of a building for one hour (Hazard #7) is less dangerous than working on moveable platform (Hazard #11) for 5 hours. The former has a probability for a fatal injury equal to 2.32×10^{-7} while the latter has a fatality probability equal to 4.2×10^{-7} (~5 hrs $\times$ 8.4×10^{-8}/hr).

Often individual occupational risk is confused with group or collective occupational risk. The latter includes not only the time of exposure to a particular hazard but also the worker population exposed to the hazard. An interesting case is the risk of an accident while working on a mobile ladder versus a mobile scaffold. Over the period examined in the WORM project there were 18 deaths 159 permanent injuries and 628 recoverable injuries from accidents that occurred while working on a mobile ladder. The corresponding numbers for accidents involving work on mobile scaffolds for the same calendar period were (8 deaths, 44 permanent injuries and 193 recoverable injuries). Obviously on a collective basis working on a mobile ladder looks riskier than working on a mobile scaffold. Care must be exercised, however, before rushing to the recommendation that mobile ladders must be replaced my mobile scaffolds. Data analysis (taking into consideration the number of workers and the exposure time involved) indicate that the individual risk rate for working on a mobile ladder is 2.51×10^{-8}/hr for fatal injuries, 2.11×10^{-7}/hr for permanent injuries and 8.30×10^{-7}/hr for recoverable injuries. The corresponding values for working on a mobile scaffold are: 6.34×10^{-8}/hr, 3.20×10^{-7}/hr, 13.6×10^{-7}/hr. Obviously the individual occupational risk per hour while working on a mobile scaffold dominates the risk of working on a mobile ladder. A recommendation to replace a mobile ladder with a mobile scaffold would be meaningful if this replacement reduces the time required to perform a specific task by a factor of 3 or more. In this case the exposure to the hazard of an accident while working on a mobile scaffold will be less than one third of the exposure on a mobile ladder and the probability of an accident will be less for the case of scaffold.

REFERENCES

Ale B.J.M., L.J. Bellamy, H. Baksteen, M. Damen, L.H.J. Goossens, A.R. Hale, M. Mud, J. Oh, I.A. Papazoglou, J.Y. Whiston, 2008. Accidents in the construction industry in the Netherlands: An analysis of accident reports using Storybuilder, Reliability Engineering & System Safety, 93, 10, 1523–1533.

Ale B.J.M., Baksteen H., Bellamy L.J., Bloemhof A., Goossens L., Hale A.R., Mud M.L., Oh J.I.H., Papazoglou I.A., Post J., Whiston J.Y., 2008. Quantifying occupational risk: The development of an occupational risk model. *Safety Science*, 46(2): 176–85.

Aneziris O.N., I.A. Papazoglou, D. Kallianiotis, 2010. Occupational Risk of tunneling construction, Safety Science, Volume 48, Issue 8, 964–972.

Aneziris O.N., E. Topali, I.A. Papazoglou, 2012. Occupational Risk of building construction, *Reliability Engineering and Systems Safety*, Volume 105, 36–46.

Aneziris O.N., I.A. Papazoglou, O. Doudakmani, 2010. Occupational Risk of an aluminium industry, International Journal of Industrial Ergonomics, Volume 40, Issue 3, 321–329.

Aneziris O.N., Papazoglou I.A., Baksteen H., Mud M., Ale B.J., Bellamy L.J., Hale A.R., Bloemhoff A., Post J., Oh J., 2008. Quantified Risk Assessment for Fall from Heights. *Safety Science*, 46(2):198–220.

Aneziris O.N., Papazoglou I.A., Mud M., Baksteen H., Ale B.J., Bellamy L.J., Hale A.R., Bloemhoff A., Post J., Oh J., 2008. Towards Risk Assessment for crane activities. Safety Science, 48(6):872–84.

Attwood D., Khan F., Veitch, 2006. Can we predict occupational accident frequency, *Process Safety and Environment Protection*, 2006, 84, 208–221.

Bedford T., Cooke R., 2001. Probabilistic Risk Analysis: Foundations and Methods, University Press, Cambridge.

Bellamy L., Ale B.J.M., Geyer T.A., Goossens L.H.J., Hale A.R., Oh J., Mud M., Bloemhof A., Papazoglou I.A., & Whiston, J.Y., 2007. Story Builder a Tool for the analysis of Accident Reports. *Reliability Engineering and System Safety 92*, pp 735–744.

BSI, 1996. BS 8800: Guide to Occupational Health and Safety Management Systems. British Standards Institution, London.

BSI, 1999. OHSAS 18001: Occupational Health and Safety Management System—Specification. British Standards Institution, London.

Ciarapica, F.F., Giacchetta G., 2009. Towards an international limit value for occupational trauma risk: industrial exposures associated with occupational trauma, permanent impairment and fatalities in a five-year national claims material. *Safety Science*, 47, 39–46.

GISAI "Geintegreerd Informatie Systeem Arbeids Inspectie", Algemene Interface en Opzet, Arbeidsinspectie (Labor Inspectorate), 1 December 2005, Den Haag, The Netherlands.

Grassi A., Gamberini R., Mora C., Rimini B., 2009. A fuzzy multi-attribute model for risk evaluation in workplaces, *Safety Science*, 47, 707–716.

Gürcanli G.E., Müngen U., 2009. An occupational safety risk analysis method at construction sites using fuzzy sets, International Journal of Industrial Ergonomics, 39, (2), 371–387.

Hahn G.J., & Shapiro S.S., 1994. *Statistical Models in Engineering*, John Wiley & Sons.

Health and safety at work in Europe http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAcion.do;jsessionid=9ea7d07d30e329a862ebf65f4dbab47dccee9bdbf4a1.e34OaN8PchaTby0 Lc3aNchuMchaOe0.

Hao-Tien Liu, Yieh-lin Tsai., 2012. A fuzzy risk assessment approach for occupational hazards in the construction industry, *Safety Science*, 50, 1067–1078.

International Labour Office, 2001. Guidelines on Occupational Safety and Health Management Systems. ILO-OSH 2001. International Labour Office, Geneva.

Ivan W.H. Fung, Vivian W.Y. Tam, Tommy Y. Lo, Lori L.H. Lu, 2010. Developing a Risk Assessment Model for construction safety, International Journal of Project Management, 28, 6, 593–600.

Joaquim F. Silva, Celeste Jacinto, 2012. Finding occupational accident patterns in the extractive industry using a systematic data mining approach, *Reliability Engineering & System Safety,* 108,108–122.

Kuiper J.I., Bloemhoff A., Leidelmeijer K., Damen M., 2008. Exposure of workers to occupational hazards and risk related working conditions, 4th International Conference Working on Safety, WOS 2008, Iraklion, Crete.

Larsson T.J., Forsblom M., 2005. Towards an international limit value for occupational trauma risk: industrial exposures associated with occupational trauma, permanent impairment and fatalities in a five-year national claims material, *Safety Science*, 43, 61–71.

Lindley, D.V., 1965. Introduction to Probability and Statistics from a Bayesian Viewpoint (2 Volumes), University Press, Cambridge.

María Carmen Carnero, Diego José Pedregal, 2010. Modelling and forecasting occupational accidents of different severity levels in Spain, *Reliability Engineering & System Safety*, 95,11, 1134–1141.

Marhavilas P.K., Koulouriotis D.E., 2008. A risk estimation methodological framework using quantitative assessment techniques and real accidents data: Application in an aluminium extrusion industry, *Journal of Loss Prevention in the Process Industry*, 21, 596–603.

Mure S., Demichela M. "Fuzzy Application Procedure (FAP) for risk assessment of occupational accidents", Journal of Loss Prevention in the Process Industry, 2009, 22, 593–599.

Oh J.I.H., Sol V.M., 2008. The policy program improving occupational safety in The Netherlands: An innovative view on occupational safety. *Safety Science*, 46:155–63.

Papazoglou I.A., Ale B.J.M., 2007. A logical model for quantification of occupational risk. Reliability Engineering and System Safety, 92:785–803.

Papazoglou I.A., Bellamy L.J., Leidelmeijer K.C.M., Damen M., Bloemhoff A., Kuiper J., Ale B.J.M., Oh J.I.H., 2008. Quantification of Occupational Risk from Accidents, International Probabilistic Safety Assessment and Management Conference, PSAM 9, 18–23 May 2008, Hong Kong, China.

Pinto A., 2014. QRAM a Qualitative Occupational Safety Risk Assessment Model for the construction industry that incorporate uncertainties by the use of fuzzy sets, *Safety Science*, 63, 57–76.

RIVM Report 620801001/2008, The Quantification of Occupational Risk. The development of a risk assessment model and software, WORM Metamorphosis Consortium.

This page intentionally left blank

Quantitative risk assessment

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability assessment method for Ion thruster based on competing failure analysis and performance degradation data

Zhiteng Zheng, Shu Dong, Liang Zhang & Danjun Xu
China Academy of Aerospace Standardization and Product Assurance, Beijing, China

Huabing Tian & Tianping Zhang
Science and Technology on Vacuum and Cryogenic Technology and Physics Laboratory, Lanzhou Institute of Physics, Lanzhou, China

ABSTRACT: In this paper, the method to evaluate the reliability of ion thruster system was discussed on the basis of components and assembly information. Combined with the survey results of domestic and foreign literatures and validation test for ion thruster assembly, the key assembly influencing reliability of ion thruster are accelerator grid and hollow cathode. The main failure modes for accelerator grid are electron-backstreaming due to accelerator grid erosion and structure failure due to ion sputter erosion. As to the two complicated failure modes, the competing failure model was introduced to evaluate the reliability of the accelerator grid system. The main failure mode for cathode is depletion failure of the emitter, so method to analyze the reliability information of the cathode assembly was based on the performance degradation data. Finally, CMSR method combined with system validation test information is adopted and the point estimation and lower confidence limit of reliability for the ion thruster system was calculated meaningfully.

1 INTRODUCTION

Ion thruster is an advanced stand-alone system for space propulsion. Commercial applications of electric propulsion include north-south and east-west station-keeping, attitude controlling, momentum dumping, de-orbit and orbit raising. The low-thrust nature of electric propulsion results in the requirement for very long thruster operating times for deep-space missions. Required operating times of thousands of tens of thousands of hours are typical. Due to small sample size, long service life and diverse failure modes characteristics, having a scientific evaluation on its working life and reliability by the traditional reliability assessment methods is necessarily inadequate. Therefore, in order to provide guidance and technical support for reliability modeling and assessment of long life, high reliability electric propulsion system, systematic assessment method for ion thruster is discussed in this paper.

2 FAILURE MODES ANALYSIS FOR ION THRUSTER

A typical ion thruster is mainly composed of cathode, accelerator grid, neutralizer, gas insulating device and discharge chamber as shown in the reliability block diagram in Figure 1. According to the block diagram, we can know that the ion thruster system is a series model and the system reliability is

$$R_s(t) = \prod_{i=1}^{5} R_i(t) \tag{1}$$

where R_s is the system reliability and R_i is the assembly reliability.

According to the failure mechanism, the failure modes for ion thruster can be divided into accidental failure modes and wear-out failure modes. The occurrence for accidental failure modes is mainly because the devices are subjected to the exceeded voltage, temperature or pressure environment, which can be avoided by adjusting the operating parameters and environment suitable for working correctly. However, wear-out failure modes

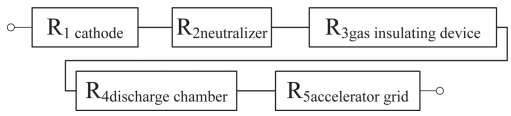


Figure 1. Reliability block diagram for ion thruster.

are associated with the accumulation of continuous operation of the thruster. For example, some key components subjected to ion sputtering environment have performance degradation or failure phenomenon, resulting in end-life of the entire propulsion system. Currently, the main countries for ion thruster research are the USA and Japan. They have conducted substantial ground life tests and durability tests for ion thruster and obtained considerable valuable data. According to the investigation at home and abroad and the life test results of ion thruster system in Lanzhou Institute of physics, the main wear-out failure modes are shown in the following Table 1.

Through the analysis, we select accelerator grid and cathode as the key assembly for ion thruster system assessment and the technological process for systematic assessment is shown in Figure 2. And the details for ion thruster assessment will be discussed in further.

Table 1. Ion thruster wear-out failure modes.

Assembly	Failure modes
Accelerator grid	Accelerator grid groove erosion from neutralizer ion
	Accelerator grid structural failure due to ion sputter erosion
	Accelerator grid electron-backstreaming due to grid erosion
Cathode	Cathode heater failure
	Cathode-to-keeper short
Neutralizer	Performance reduction due to orifice clogging
Gas insulating device	Gas insulator seam failure
	Electrical insulator failure caused by high voltage

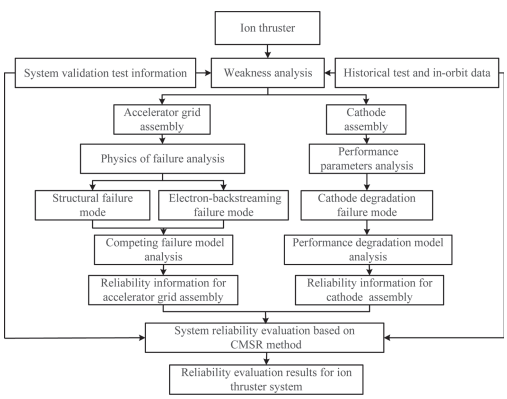


Figure 2. Reliability assessment method for ion thruster.

3 COMPETING FAILURE MODEL ANALYSIS FOR ACCELERATOR GRID ASSEMBLY

3.1 *Failure modes and mechanism for accelerator grid*

The structure of accelerator grid unit is shown in Figure 3(a). Because of the bombardment from Charge Exchange Xenon (CEX), the atoms at accelerator downstream surface are sputtered out. Along with the sputtering process, the eroded orifice brim of accelerator grid gradually becomes thinner. As shown in Figure 3(b), when the hexagon is penetrated completely, the orifice falls off and the grid short happens. What needs to be emphasized is that the structural failure phenomenon usually occurs in the center of the grid due to the maximum central current density.

In operation time, in order to maintain electrically neutral property of the spacecraft, neutralizer will launch electron flow to neutralize the beamlets. And the role of negative voltage on accelerator grid is to prevent the counterflow of the electrons to the discharge chamber. The potential distribution around the accelerator grid is shown in Figure 4. Dotted lines are the potential distributions at different radial positions from beamlet axis and solid line is the potential distribution between beamlets, i.e. the potential distribution on the grid boundary. From Figure 2, we can know that the lowest point (saddle point) of beamlets potential on the axis is higher than the accelerator potential points, which is the potential barrier the electronic refluxes need to overcome when flowing into the discharge chamber. The central orifices of accelerator grid become larger at the effect of ion beamlets, then the potential of grid becomes smaller. As a result, the electrons having enough energy are able to pass the accelerator grid to the discharge chamber and

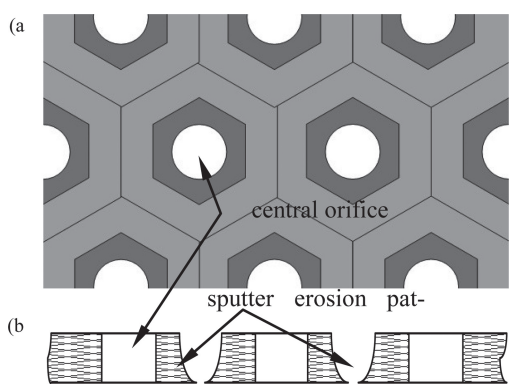


Figure 3. Schematic for accelerator grid (a) accelerator structure unit (b) profile for failure.

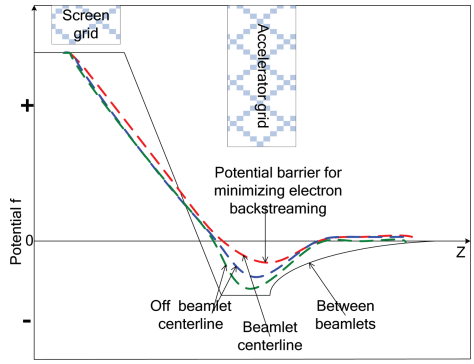


Figure 4. Schematic of potentials distribution at different radial positions around accelerator grid.

electron-backstreaming phenomenon happens. The occurrence of electron-backstreaming will cause unnecessary power consumption, decrease of ion thruster performance and local high temperature, even lead to the end of life.

3.2 *Competing failure model analysis*

As for structural failure mode and electron-backstreaming failure mode, the happening of any one of the two will bring deadly trouble to the propulsion system. However, which failure mode happens firstly is not completely clear yet, so competing failure model is introduced to analyze the life and reliability information of the accelerator grid assembly. According to the failure characteristics and principle of competing failure method, the following assumptions are correct:

1. The distribution of the two failure mode are independent;
2. The kind of earliest occurrence failure mode will lead to accelerator grid failure.

Through abundant investigation home and abroad of failure mechanism, we know that the life for structural and electron-backstreaming failure modes submit Normal and Weibull distribution separately. In order to make the data more abundant, Monte-Carlo simulation method is used to obtain the solution of competing failure model and the procedure is as follows:

1. On the basis of the two kinds of distribution parameters, the created random life sample is

$$\begin{cases} T_{structure} = \{T_{structure1}, T_{structure2}, \ldots, T_{structuren}\} \\ T_{backstreaming} \\ \quad = \{T_{backstreaming1}, T_{backstreaming2}, \ldots, T_{backstreamingn}\} \end{cases} \tag{2}$$

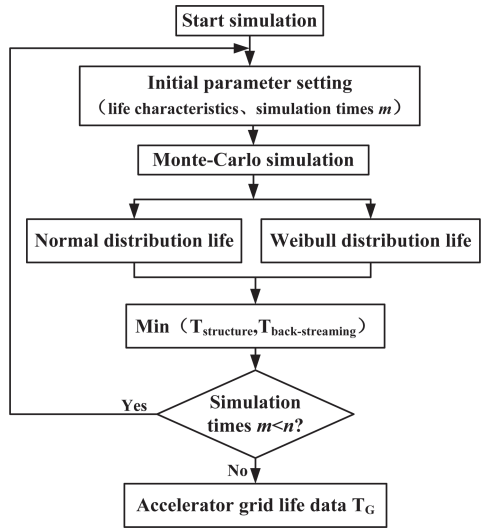


Figure 5. M-C simulating process for competing failure mode.

2. Then the life for accelerator grid assembly system T_G is

$$T_G = \min\{T_{structure}, T_{backstreaming}\} \tag{3}$$

3. Repeat procedure (1) and (2) m times (according to different precision requirements, the simulation times can be increased properly), the M-C simulation process is displayed in Figure 3. Then the simulated life sample for accelerator grid assembly can be obtained

$$\{T_{G1}, T_{G2}, \cdots, T_{Gm}\} \tag{4}$$

And the M-C simulation process is displayed in Figure 5.

Then the lower reliability limit R_{LG} and point estimation R_G of accelerator grid can be obtained by confidence degree γ, simulation times m according to GB/T 4885.

4 PERFORMANCE DEGRADATION DATA ANALYSIS FOR CATHODE ASSEMBLY

4.1 *Failure modes and failure mechanism for cathode*

The key component of cathode assembly is hollow cathode which mainly consists of LaB_6 emitter, heater coils, cathode tube and keeper, which is shown in Figure 6. Among them, the life of emitter is the decisive factor influencing the properties of cathode

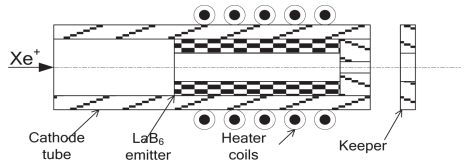


Figure 6. Schematic of the cathode assembly.

assembly. The main failure mode for LaB_6 emitter is depletion failure due to evaporation at high temperature. Because the depletion process is very slow, even subjected to higher accelerated stress, the failure phenomenon can't be observed yet. Therefore, performance degradation data analysis method is adopted to obtain the life and reliability information of cathode assembly, greatly reducing the test time and improving the economic benefits.

4.2 *Performance degradation data analysis*

For ion thruster hollow cathode, degradation model has the following two basic hypotheses:

1. Performance degradation process is irreversible;
2. One degradation model corresponds to only one degradation process or failure mechanism.

Considering the characteristics of cathode, anode voltage or keeper voltage is chosen as the performance degradation parameter generally. According to the variation characteristics of voltage data, the degradation model is as follows:

$$v(t) = b\varphi(t) + a + \varepsilon \tag{5}$$

where $v(t)$ is the variable value of voltage, b is the drift coefficient characterizing the degradation rate, a is unknown parameter and ε is the residual error.

The degradation data analysis processing is as follows:

1. The cathode sample number is n and the number of degradation data for each sample is $m_i (i = 1, 2, \ldots, n)$, according to the detected voltage and the correspondent time, the unknown parameters can be calculated;
2. The data processing procedure adopts least square method, then the estimation value for a and b can be obtained;
3. According to equation (6), the performance data equation for n sample is

$$\begin{cases} v_1(t) = \hat{a}_1 + \hat{b}_1 \cdot \varphi(t) \\ v_2(t) = \hat{a}_2 + \hat{b}_2 \cdot \varphi(t) \\ \vdots \\ v_n(t) = \hat{a}_n + \hat{b}_n \cdot \varphi(t) \end{cases} \tag{6}$$

4. Then the pseudo life T_{ci} *of each cathode* can be calculated by equation (6);

$$\{T_{C1}, T_{C2}, \cdots, T_{Cn}\} \tag{7}$$

5. As for degradation failure mode, the life submits Weibull distribution, and the reliability model is

$$R(t) = \exp\left[-\left(\frac{t}{\eta}\right)^m\right] \quad t > 0 \tag{8}$$

where m is the shape parameter, η is the characteristic life and t is task life.

6. The shape parameter m can be calculated by equation (9);

$$\frac{1}{m} + \frac{\sum_{i=1}^{n} \ln T_{Ci}}{n} - \frac{\sum_{i=1}^{n} {T_{Ci}}^m \ln T_{Ci}}{\sum_{i=1}^{n} {T_{Ci}}^m} = 0 \tag{9}$$

7. Then the point estimation of characteristic life $\hat{\eta}_C$ and the point estimation $\hat{R}_C$ and lower confidence limit R_{LC} of reliability for cathode can be obtained easily by equation (10).

$$\begin{cases} t^* = \sum_{i=1}^{n} {T_{Ci}}^m \\ \hat{\eta}_C = \left(\frac{t^*}{n}\right)^{\frac{1}{m}} \\ \hat{R}_C = \exp\left[-\left(\frac{t}{\hat{\eta}_C}\right)^m\right] \\ R_{LC} = \exp\left[-\frac{t^m}{2t^*}\chi^2_\gamma(2r+2)\right] \end{cases} \tag{10}$$

where t^* is the equivalent total test time and $\hat{\eta}_C$ is the estimation of characteristic life.

5 RELIABILITY ASSESSMENT OF ION THRUSTER SYSTEM BASED ON CMSR METHOD

Because the reliability information of ion thruster consists of assembly information, system validation test data, prior information etc, CMSR (Combined Modified Maximum Likelihood & Sequential Reduction) method combined with system validation test information is used to evaluate the reliability of the ion thruster system.

5.1 *Reliability information conversion for accelerator grid and cathode*

For accelerator grid and cathode assembly, the reliability information is obtained already. Then the equivalent exponential data for each assembly can be calculated separately. By equation (11), the total accumulating test time T_G for accelerator grid and T_C for cathode can be obtained.

$$\begin{cases} R_L = \exp(-\lambda_U t) \\ \lambda_U = \chi^2_\gamma(2r+2)/2T \end{cases} \tag{11}$$

Then the equivalent failure number r_G for accelerator grid and r_C for cathode can be calculated by equation (12):

$$\begin{cases} \hat{R} = \exp(-\hat{\lambda} t) \\ \hat{\lambda} = r/T \end{cases} \tag{12}$$

5.2 *Assembly reliability information calculation*

According to the standard—Assessment methods for spacecraft reliability(Q/W 8B 2007) issued by China Academy of Space Technology, the reliability point estimation $\hat{R}_A$ for accelerator grid and cathode assembly and its variance $D_A(\hat{R})$ are

$$\begin{cases} R_A = R_G \cdot R_C \\ D_A(\hat{R}) = \hat{R}_A^2 \left(\dfrac{r_G t_G^2}{T_G^2} + \dfrac{r_C t_C^2}{T_C^2} \right) \end{cases} \tag{13}$$

where t_G and t_C are the task time for grid and cathode separately.

Then the equivalent task number η_A and the equivalent failure number r_A for accelerator grid and cathode assembly are

$$\begin{cases} \eta_A = -\dfrac{\hat{R}_A^2 \ln \hat{R}_A}{D_A(\hat{R})} \\ r_A = -\eta_A \ln \hat{R}_A \end{cases} \tag{14}$$

5.3 *Ion thruster system reliability calculation*

After the conversion of assembly reliability information, the results for system validation test should also be considered so as to make the system information more abundant and the evaluation result more convincing. And the conversion method for assembly assessment information and system test information is shown in the following equations,

$$\begin{cases} \eta_S = \eta_A + \eta_{SV} \\ r_S = r_A + r_{SV} \end{cases} \tag{15}$$

where η_S and r_S is the the equivalent task number and equivalent failure number for ion thruster system seperately, η_{VS} and r_{SV} is the the equivalent task number and equivalent failure number for system validation test seperately.

After the conversion of equivalent test information, the point estimation $\hat{R}_S$ and lower limit of reliability R_{LS} for ion thruster system are

$$\begin{cases} \hat{R}_S = \exp(-\hat{\lambda} t) = \exp\left(-\dfrac{r_S}{\eta_S} \right) \\ R_{LS} = \exp(-\lambda_U t) = \exp\left(-\dfrac{\chi^2_\gamma(2r_S+2)}{2\eta_S} \right) \end{cases} \tag{16}$$

Above all, the estimation value of system reliability can be calculated meaningfully by sequential information reduction adding the system validation test information.

The reliability assessment method discussed in this paper has got good achievement in a certain type of ion thruster developed by Vacuum & Cryogenic Technology and Physics Laboratory in Lanzhou. For security reasons, public discussion of test data is prohibited here.

6 SUMMARY

The method to evaluate the reliability of ion thruster system was discussed elaborately on the basis of components and assembly information. Accelerator grid and cathode were chosen as the key assembly influencing reliability of ion thruster. And the competing failure model was used to analyze the electron-backstreaming and structure failure mode for accelerator grid and performance degradation data analysis method for depletion failure mode of the cathode emitter. Then CMSR method combining system validation test information was elaborated properly and the point estimation and lower limit of reliability for the system were obtained separately. The method is an investment for the assessment of ion thruster with small sample size, long service life and high reliability properties and also provides guidance and technical support for the reliability research of other complicated aerospace products.

ACKNOWLEDGMENT

The research described in this paper was carried out by the China Academy of Aerospace Standardization and Product Assurance, under a contract with the Science and Technology on Vacuum & Cryogenic Technology and Physics Laboratory.

REFERENCES

Brask A, Kutter J.P., Bruus H. Long-term stable electroosmotic pump with ion exchange membranes, Lab Chip 5, 2005:730–738.

Brophy John R., Polk James E., Randolph Thomas M. Lifetime Qualification of Electric Thruster for Deep-Space Mission, AIAA/ASME/ASEE Joint Propulsion Conference & Exhibit, 2008:5148–5185.

Guo Weichang, Liao Jiongsheng, Xiao Mingxin, Q/W 8B-Assessment methods for spacecraft reliability, 2007: 4–8.

Illiams John D., Geobel Dan M., Wilbur Paul J. Analytical Model of Electron Backstreaming for Ion Thrusters, AIAA, pp. 2003:4549–4560.

Jonathan L, Noord V, Life time Assessment of the NEXT Ion Thruster, AIAA 2007:5274.

Yanhui1 Jia, Zhongming Li, Tianping Zhang, The effect of grids system electronbackstreaming on ion thruster life, Vacuum & Cryogenics, 2012:21–25.

Young, Brian T., Richand Jacques C., Lattice Boltzmann, Models of Xe, Xe^{+}, Xe^{++}, Flow through Ion Thruster Optics, AIAA, 2003:5006.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparison of risk profiles for chemical process plants using PLATYPUS

C. van Gulijk & B.J.M. Ale
Delft University of Technology, Delft, The Netherlands

D. Ababei
Lighttwist Software, Delft, The Netherlands

M. Steenhoek
Shell Global Solutions, Rijswijk, The Netherlands

1 INTRODUCTION

1.1 *General introduction*

Recent disasters in high hazard industries such as Oil and Gas Exploration (The Deepwater Horizon) and Petrochemical production (Texas City) have been found to have causes that range from direct technical failures through organizational shortcomings right up to weak regulation and inappropriate company cultures. Traditionally, risk models for process plants concentrate upon technical failures because there is relatively concrete technical failure data available for risk modeling. Modeling human activities, and their interaction with the process plant is a quite different proposition. Yet it is imperative to incorporate the human. Humans contribute to safety measures in process plants and thereby become integral part of the safety functions in process plants.

The Platypus software integrates both technical and human performance for the prevention of process leaks. That is to say, it models the left-hand-side of the bow-tie. Thus the safety effects of technical failure, human failure, and to some extent organizational failure are directly modeled through the appearance of leaks in process plants.

1.2 *The development of Platypus*

Platypus models the left hand or fault-tree side of a bowtie model for process safety by using a Bayesian Belief Net (BBN). That is to say, it calculates the frequency of occurrence of leaks of arbitrary size in process equipment. A leak or Loss of Containment (LoC) event does not necessarily lead to a catastrophe but in some cases leads a loss of containment can have severe consequences ranging from accidents or catastrophes. Most of the BBN-based method was developed in 2011 and 2012. The background information for the model can be found elsewhere. (Ale et al., 2014; Ale et al., 2011; Hanea et al., 2012; Lin et al., 2012, Sillem et al., 2012; Van Gulijk et al., 2012; Van Gulijk et al., 2013).

The first version of Platypus was made in May 2013. Though the initial program could already be used to calculate an entire site it was not very user friendly. Since then, there was a strong drive to improve the functionality of the program, especially with respect to the improvement of analysis tools. Improvements included: an engine to read equipment lists, an engine to change parameters in subsets of process equipment in a plant and copying subsets of the plants. This combination of features has led to a piece of software that enables left-hand side BBN-based risk analyses of entire chemical—or process plants, something that was never done before.

Note that detailed scientific information is not disseminated in this paper. Rigorous scientific reporting will take place after full testing of the program. Nevertheless, the reader may increase their understanding by reading earlier publications about this project that explain the philosophy and theoretical framework of Platypus.

1.3 *This paper*

This paper is limited to a description of the capabilities of Platypus. It shows the results of case study that was performed with Platypus version 0.7.10. The case study involves test calculations for the reactive section in an ethylene oxidation process that contains 4 reactors.

Since the program is still under development, these results are preliminary. That means that the results in this paper are used to demonstrate how the results that Platypus yields and how they can be used for risk-analyses of process plants. The results should not be interpreted as exact.

A brief description of the structure and some of the software features of Platypus is enclosed in this paper.

2 ABOUT PLATYPUS

2.1 *Structure of Platypus*

Some explanation is necessary to understand how the results presented in this paper came to be. This section explains the relevant elements in the structure of the Platypus software.

2.1.1 *Parameter excursions*

Any part of the chemical process plant is designed to contain hazardous chemicals under operational process conditions with a built-in safety margin. These margins are typically subject to rigid design standards. In this work deviations of the process parameters beyond these margins are called parameter excursions. Parameter excursions are quantifiable entities that have probability of occurrence [year^{-1}].

2.1.2 *Barriers*

Ordinarily, there is at least one safety barrier that controls parameter excursions. Barriers have a probability of failure per activation [activation^{-1}] or [–]. The failure probabilities are the input parameters for a barrier.

2.1.3 *Excursion control path*

For process parameter excursions (like temperature or pressure) there may be up to three or more consecutive, independent barrier systems to prevent loss-of-control. In that respect this work follows the LOPA method (Dowell, 2001). This methodology leads to a chain of barriers that may be activated when a parameter excursion takes place. The parameter excursion, including the initiating parameter excursion and the activation of the chain of barriers is termed an excursion control path. The combination of starting frequencies and the frequency of failure of the barriers leads to an annual frequency of occurrence for LoC's.

2.1.4 *LoC*

A Loss of Containment or LoC of process equipment follows when all barriers fail. The uncontrolled deviations from normal or abnormal process conditions and operations that are so extreme that leaks, cracks, ruptures or failing barriers cause the uncontrolled transport of materials from inside process equipment to the outside. In the current version of Platypus, the LoC's are of arbitrary size. That is to say that Platypus does not predict the size of the leak. The reason for that is the size of the leak is a consequence rather than a cause, which puts it in the right-hand side of the bow-tie.

2.1.5 *Combination of LoC's in equipment*

For a given piece of equipment, a number of excursion controls combine; for instance corrosion, wrong installation, and overpressure combine (amongst others) into a vessel equipment model. It is important to remember that an excursion control path links a single type of a parameter excursion (say, corrosion) to a LoC. The combined LoC's model the LoC frequency of the equipment. Detailed information about the equipment models are proprietary information that cannot be repeated here.

Note that the inputs in Platypus are distributions into the non-parametric BBN's and that the results are distributions from those BBN's. That is why the standard deviation that represents aleatory uncertainty is reported along with the central estimate.

So far, eleven pieces of equipment were modeled. They are:

1.	vessels HC only	V-HC
2.	vessels L-L separator	V-LL
3.	reactors	R-GEN
4.	pipework	PW
5.	centrifugal pump	P-C
6.	reciprocating pump	P-R
7.	furnace	F-GEN
8.	fin-fan coolers	E-FF
9.	tubular heat exchanger	E-TS
10.	centrifugal compressor	C-C
11.	reciprocating compressor	C-R

2.2 *Software features of Platypus*

Platypus can import process equipment lists of a process plant or a site that houses several process plants. The equipment list is translated into a hierarchical model structure to represent the plant and represent individual safety barriers for process control. Currently, the barriers are grouped into 11 individual Equipment LoC template models (EqLoC's) but Platypus can be used to build any barrier-structure in a process plant. The templates provide quick references that contain estimates for global average leak rates for a predetermined set of leak scenario's. These templates function as a first estimate when assessing the leak rate of a site or a plant. Someone that is familiar with the program can make this first estimate within the time span of 15 minutes or less for any given chemical site or process plant.

3 METHOD

3.1 *Process under consideration*

This paper demonstrates seven calculations that were performed by Platypus version 0.7.10. The program runs on a 64 bit Intel i7-2640M CPU at 2.80 GHz with a RAM memory of 4 GB.

The calculation (known as BBN sampling) is a Monte Carlo simulation with 50.000 passes. The calculation takes about 30 seconds.

The process unit that is under consideration is a reaction section in an ethylene oxidation plant. It consists of the following parts:

– 8 HC vessels only
– 4 reactors
– 1 centrifugal pump
– 11 heat exchangers
– 208 pipework sections.

This equipment list draws 5 types of equipment in Platypus out of 11 are standard equipment LoC models.

3.2 *Interventions*

For this paper, a few technical interventions in that reaction section are calculated. The interventions represent alterations in the assembly or operation of the unit. The interventions are presented as changes to the base-case calculation. That is to say the calculation that only incorporates unaltered equipment LoC models. The results for the base-case are presented section 4.1. The interventions are treated in the subsequent sections. Section 4.2 treats changes of the PRVs (Pressure Relief Valves) in the unit. That is to say, SIL 3 PRVs are replaced by SIL 4 PRVs. Section 4.3 treats the complete elimination of hoisting activities in the vicinity of the unit. Section 4.4 treats a redesign of pipework in the sense that less connections with measurement instrumentations are designed. Section 4.5 treats the redesign of pipework in the sense that less pipework is installed. Section 4.6 treats the complete elimination of corrosion as a factor in all equipment. Section 4.7 treats improved maintenance operations for the centrifugal pump.

4 PRELIMINARY RESULTS

4.1 *Baseline calculation*

The baseline calculation for the process unit under consideration yields the results in Table 1. Figure 1 is a graphic representation of the distribution of the leak frequency.

4.2 *SIL4 PRVs*

One possible safety intervention is the replacement of SIL3 PRVs with SIL 4 PRVs. So the existing pressure relief valves, that are usually the last line of defense in overpressure LoC scenario's, are changed to more reliable systems.

Table 1. Platypus results for the case study: Base case.

	LoC frequency/ [year^{-1}]	
Part of unit	Freq.	Stdev.
Base case	6.68	0.674
In which the contribution to the mean equal:		
Reactors (4)	0.056	–
HC vessels (8)	2.35	–
Heat exch. (11)	2.02	–
Centrifugal pump (1)	0.0051	–
Pipework (208 units)	2.25	–

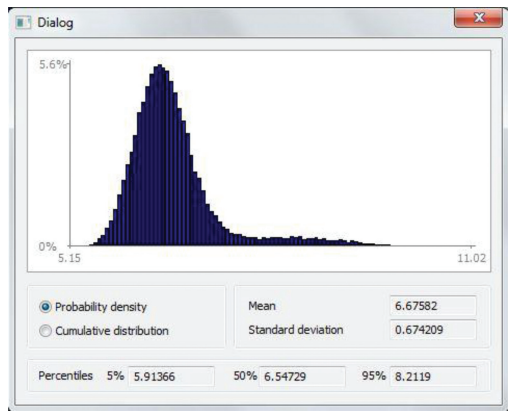


Figure 1. LoC frequency distribution for unit.

Table 2. Platypus results for various cases.

	LoC frequency/ [year^{-1}]	
Analysis case	Freq.	Stdev.
Base case	6.68	0.674
SIL4 PRVs	6.67	0.674
Eliminate hoisting	4.95	0.634
Less connectors in pipes	6.58	0.67
Less number of pipes	5.26	0.642
No corrosion	6.68	0.674
Sup. pump maintenance	6.68	0.677

Table 2 shows the results from Platypus. Note that the change in the overall leak frequency is nearly negligible which demonstrates that the overall contribution of replacing ordinary PRVs by high-quality PRVs does not yield much safety gain in the sense that they do not lower the LoC frequency distribution.

4.3 *Eliminate hoisting activities in the unit*

The second intervention is the complete elimination of hoisting activities of any kind. Table 2 shows the results. The LoC frequency dropped to 11% to 4.95, which is substantial in this case. This large change is mostly due to the fact that all pieces of equipment are prone to this threat. Despite that explanation, current thinking is that this effect may be overestimated in Platypus.

4.4 *Less connectors to a pipe*

Our current information says that a piece of pipework has 26 connectors and flanges associated with it. Each of those is prone to installation errors. If the number of connections is lowered, the probability of having installation errors lowers and the overall LoC frequency should drop. In fact lowering the connectors from 26 to 10 yields 6.58 ± 0.67. This is a relatively small change for the entire unit. That is to say, the influence of installation errors in pipework contribute to the total LoC prediction is relatively small.

4.5 *Less pipework*

Less pipework influences the LoC frequency considerably. When the piping layout is simplified (*viz.* 208 units of pipe are reduced to 80 units of pipe) the frequency lowers to 5.25 ± 0.642; a reduction of over 20% on the overall. This suggests that clever layout of pipework reduces LoC's in a process plant.

4.6 *Corrosion-resistant materials*

In this case the influence of corrosion is completely eliminated from the threat scenario's. The lowering of the frequency for LoC's is negligible. This means that the current corrosion controls are sufficiently effective in preventing LoC's.

4.7 *Improved pump maintenance*

For this case, the maintenance of the centrifugal pump is better in the sense that people make no omissions in the tasks that have to be performed in the maintenance and repair of the pump. In this case, it means that the probability of skipping a safety-sensitive maintenance activity is effectively reduced to zero. The effect on the overall LoC frequency of the centrifugal pump clear; the mean has lowered by 17% from 0.0051 ± 0.00452 to 0.0042 ± 0.00452. However, the contribution on the LoC's of the whole unit is negligible since just one pump is installed in this case.

5 DISCUSSION

It has to be stressed that Platypus is still under development and these results are preliminary. That means that the results in this paper are used to demonstrate how the results that Platypus yields and how they can be used for risk-analyses of process plants. The results should not be interpreted as exact.

5.1 *Distribution of LoC probabilities*

The results from the calculations yield a distribution function for the LoC frequency. Figure 1 shows the results for the base case. The figure should be read as follows. On the x-axis is the frequency of an LoC event of arbitrary size in [year^{-1}]. On the y-axis is the percentage of the frequency distribution histogram where the histogram has 100 equidistant size bins between the minimum LoC frequency (5.15 year^{-1}) and the maximum LoC frequency (11.2 year^{-1}). This means that it is estimated that the LoC frequency is between 5.15 and 11.2. Any leak frequency rate between those limits may be expected in the observation of the unit. There is a 90% probability interval between 5.91 year^{-1} and 8.21 year^{-1}, which narrows the likely occurrence of an observable LoC rate. The mean is 6.68 year^{-1} the standard deviation is 0.674 year^{-1}. The median is 6.55 year^{-1}.

It is tempting to compare the mean or the median to traditionally used point-estimators for failure frequencies but that diminishes the added value of working with a distribution. For instance, with a point estimator, an LoC frequency of 6.68 year^{-1} it would be easy to judge an observed frequency of 11.2 as a serious safety issue but in reality, it is still within possible bounds (even if it is unlikely).

Another reason to consider a distribution is setting safety standards. The distribution shows that it is not very useful to set a safety standard that says that the leak frequency should not be higher than the mean of 6.68 year^{-1} because in nearly 40% of instances this threshold will be exceeded anyway. Alternatively, it would be more useful to set thresholds based on the 95% threshold of 8.2 year^{-1} (for instance exceeding that value in to consecutive years).

5.2 *Comparison of cases*

Several possible safety-interventions were modeled with Platypus. These are examples of interventions that a safety-manager may consider. Three interventions are operational and three from the design of the unit. The replacement with better pressure relief valves, elimination of hoisting, and

improving pump maintenance can be decided by a local safety manager. Changing piping layout and using corrosion resistant materials can be decided in the design phase. Platypus easily shows which of the safety interventions provides the best safety gain in the sense that less leaks are expected. It is this type of sensitivity analysis that will help improve the safety performance of the process plant most.

This case study demonstrates that once a model can be loaded into Platypus, it is relatively easy to test safety interventions in process plants. In that sense, Platypus is a rapid analysis tool that immediately provides insight into the safety gain that a safety intervention might yield in an existing process plant. This rapid analysis also enables relatively straightforward comparison between different options for intervention.

Note that an extensive sensitivity analysis may be developed to optimize a mix of safety interventions to a maximum safety yield. We believe that this will remain a task for safety experts and not for users in the field. In the future, an extensive sensitivity analysis functionality may be added to Platypus but at this time that is not included in the software.

5.3 *Generic and detailed analysis*

The information that was used for this simulation is generic data. That is to say, the information about the process unit is limited to an instrument count and the instruments were modeled with generic equipment models. This is the coarsest application of the Platypus software that we term the 'generic analysis'. A detailed analysis is also possible. In that case, the total length of pipework, the number of connections to a vessel, the SIL level of technical safety barriers may be modeled to represent the unit as closely as possible. Historic failure data of the plant can also be implemented. This is possible because Platypus allows for the adaptation of the generic models on each level of detail of the model. This makes it very flexible but the workload associated with modeling an entire process plant (which may literally consist of thousands of pieces of equipment) may not be very practical. In addition, it may be hard to find relevant data.

5.4 *Data requirements*

Since the calculations are performed with distributions, the data-requirement for input data is more challenging than it already is in QRA calculations for process safety. Now, a central estimate failure rate does not suffice but a whole distribution is required. In this work, we use a triangle to represent distributions that we do not know (*viz.* when only point estimate failure data is available). However, the further implementation of Platypus may require more advanced failure data than are commonly available today.

6 CONCLUSION

Platypus presents unique advantages over any other risk analysis software.

Firstly, the use of a BBN as an advanced method for risk calculations yields new possibilities for risk analysis. Platypus generates risk analyses that yield risk distributions rather than point estimations. These risk distributions automatically address aleatory uncertainties in risk analysis (whose origin lies in randomness) and identifies instances of high risk that are overlooked in setting risk standards. The distribution will also yield new leading risk indicators and new methods and instruments for risk management. When estimates of epistemic uncertainty ranges are available, these can be incorporated in the overall distributions as well.

Secondly, Platypus provides insight into the factors that influence the frequency of LoC events before accidents have taken place, whereas traditionally that information could only be derived from historical data. In Platypus, technical, organizational and human factors elements are integrated which enables an in-depth analysis of causes of LoC and the effectiveness of measures. This paper demonstrates how easy it would be to perform such an analysis.

Thirdly, due to its efficient calculation engine, initial LoC estimates for entire sites can be calculated in a matter of minutes which makes it very easy to minimize the LoC frequencies in process plants in the future.

We believe Platypus is a leap forward in estimating leak frequency rates for process plants. We believe it will change the face of risk analysis in the process industries and beyond that work area.

ACKNOWLEDGEMENT

This work was funded by Royal Dutch Shell plc.

REFERENCES

Ale, B., Van Gulijk, C., Hanea, A., Hanea, D., Hudson, P., Lin, P.H. And Sillem, S. (2014) Towards BBN based risk modelling of process plants. Safety Sci., http://dx.doi.org/ 10.1016/j.ssci.2013.12.007.

Ale, B.J.M., Hanea, D., van Gulijk, C., Lin, P.-H., Sillem, S., Hudson, P. (2011) Towards an integrated risk model for hydrocarbon industry operation, Proceedings of the European Safety and Reliability Conference, ESREL 2011 18–22 September 2011 Troyes France, Advances in Safety, Reliability and Risk Management–Bérenguer, Grall & Guedes Soares (Eds.), Taylor & Francis Group, London.

Dowell, E.M., (2001) Layers of protection analysis, AIChE, New York.

Hanea, D. Hanea, A. Ale, B. Sillem, S., Lin, P., Van Gulijk, C. and Hudson, P. (2012) Using Dynamic Bayesian Networks to Implement.

Lin, P., Hanea, D., Ale, B., Sillem, S., Van Gulijk, C. and Hudson, P. (2012) Integrating Organisational Factors into a BBN Model of Risk. PSAM 11, Esrel 2012, Helsinki 25–29 juni 2012.

Van Gulijk, C. and Ale, B.J.M. (2012) Bankruptcy by catastrophes for major multinationals: stock exchange sensitivity for three catastrophes. PSAM 11, Esrel 2012, Helsinki 25–29 juni 2012.

Van Gulijk, C., Hanea, D., Almeida, K., Steenhoek, M., Ale, B. and Ababei, D. (2013) Left-hand BBN model for process safety. *RESS special publication* Beyond the Horizon, Steenbergen (Eds.) Taylor & Francis, London.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The use of the combination of indexing and semi-quantitative methods in audits for individual risk assessment in the field of fire and explosion protection

A. Leksin & U. Barth
University of Wuppertal, Wuppertal, Germany

D. Adeulov
Agency PB, GCE Group, Limited Liability Company, Saint Petersburg, Russia

R. Mock
Zurich University of Applied Sciences, Winterthur, Switzerland

ABSTRACT: In the field of fire and explosion protection the assessment of individual risks often bases on heuristics or indexing methods because a full-scale probabilistic approach is infeasible in many cases for en-terprises. On the other hand, this established procedure undermines efforts of Quantitative Risk Assessment (QRA) to assess frequencies of undesired events and their consequences as accurately as possible. The paper outlines an approach to objectify the process of a QRA audit. Based on an online search, the available QRA and indexing tools are characterized. The combination of the indexing method and semi-quantitative approaches allows to carry out an audit, which is based on weighting procedures utilizable for risk rating and benchmarking for individual risk quantification. Regarding this, audits are facilitated and the quality of the outcome increases. The approach is exemplified by a prototype tool (MS EXCEL). The paper concludes with outlining the benefits and constraints of QRA audit tools.

1 INTRODUCTION

Risk analyses are performed to provide data for decision making, e.g., about the necessity of fire prevention actions with regard to compliance. In this case a qualitative risk assessment is carried out as only specified attributes of the prevention systems and hazards are necessary.

On the other hand, risk analyses identify specific hazards and asses their impact on humans, environment and business.

Procedures, goals and levels of detail of specific risk assessment approaches have to be tailored by the auditor considering resources, regulatory requirements, etc.

There exists no universal method for the assessment of fire and explosion risks which would be accepted as obligatory in the standard regulation in the field of fire and explosion safety of industrial buildings and associated facilities indoor. At the same time these regulations allow the application of qualitative and quantitative approaches, including index methods and the full probabilistic approach.

However, the limits of resources usually results in simplistic risk assessment approaches based on heuristics and expert judgment (checklists, FMEA, etc.). Thus, the common QRA approaches are unable to cope with individual risks in a level of detail as preferable.

Taking up the authors' preliminary studies (Leksin et al. 2013, Mock et al. 2012) and linking up the indexing method and semi-quantitative risk assessment approaches result in an enhanced QRA audit methodology. Within the scope of this methodological and operational framework, the paper is structured as follows:

Chapters 2 and 3 outline the context of the tool development, i.e., definitions, methods and tools. Results of an Internet survey show software tools supporting indexing and QRA methods. Chapter 4 covers the general audit principle. Chapter 5 extends the indexing and semi-quantitative approaches and their combination. Chapter 6 sketches the audit application by a prototype tool (MS EXCEL). The concluding chapter 7 discusses pros and cons of QRA audit and of the presented risk audit approach.

2 TERMS AND DEFINITIONS

The synopsis of scientific literature and normative documents shows an inconsistent terminology in

QRA. The paper follows to the definition of (DIN EN ISO 13943 2010):

Fire hazard: physical object or condition with a potential for an undesirable consequence from fire, whereas
Fire risk: probability of a fire combined with a quantified measure of its consequence (it is often calculated as the product of probability and consequence).

Other definitions can be found, e.g., in the British (PAS 79 2011) or in the Russian (GOST 12.1.033–81 1982).

The definitions of explosion hazard and explosion risk are limited even more on account of the specitity of this topic. The paper follows (Dic. Academic 2013):

Explosion hazard: set of the factors causing possibility of formation of the explosive atmosphere in volume, exceeding 5% of room volume, and its ignition. Such factors are: combustible substance, oxidizer and an ignition source (translated from Russian).

A definition of *explosion risk* wasn't found in international standards. For this *explosion risk* is defined by analogy with *fire risk*.

3 RISK ANALYSES IN FIRE AND EXPLOSION PROTECTION

The common Fire and Explosion Protection (FEP) approaches can be differentiated into two categories: hazard and risk analyses.

Hazard analysis focuses on the study of characteristics of a fire and its impact on humans and property at the set scenario, which includes a set of basic data on room geometry, parameters for the center of the fire, conditions of ventilating apertures, a starting position of people in the building, etc. Here, deterministic mathematical (integrated, zonal or differential) or physical (full-scale or reduced in sizes) fire models are used. Research focuses on quantitative data, environment characteristics of fire and explosion scenarios, its striking action and potential property damage.

Risk analysis focuses on the assessment of both consequences and probabilities of occurrence of scenarios.

The central place of these methods is taken by the analysis of accidental factors (e.g., arrangement of a place of fire, quantity of the materials involved, FEP measurements).

The analysis of hazards and consequences of scenarios are included in risk analysis because any of the listed factors have a big impact on the scenarios (Hall & Watts 2008, Hurley & Bukowski 2008).

3.1 *Characterization of methodology*

Fire and explosion risks consider both probability of an undesired event, and severity of its consequences. For risk analysis purposes, the analyst defines the level of detail and system boundary. The common qualitative, quantitative, semi-quantitative risk assessment approaches are supposed to be known to the reader (IEC/FDIS 31010 2009).

Semi-quantitative methods use qualitative as well as quantitative evaluation procedures. Methods of indexing and ranging of risks also belong to this method. From the practical point of view, it is difficult to appraise the value of indexing methods for risk analysis purposes. Unlike qualitative methods it gives a quantitative assessment of a risk level, but differs in straightforwardness demanding for computer recourses. It also uses a small number of parameters to assess the efficacy of the FEP measurements.

3.2 *Literature survey*

The up-dated survey of (Leksin et al. 2013, Mock et al. 2012), considers many computer models for fire and explosion risk assessments, e.g., CRISP and CRISP2 (UK), FiRECAM (Canada), FRAME (USA), AgenaRisk (UK), AssessNET (UK), Synergi Life Risk Management (Norway), SITIS, based on (GOST 12.1.004-91 1992, et al.) (Russia), and TOXI+, based on (RD-03-26-2007 2008) (Russia). These tools seemingly show the current practice in the area of *quantitative risk assessment* audits as all of them name the risk term (Leksin et al. 2013). However, these tools often use a risk terminology in a market-oriented manner whereas their descriptions often remain unclear whether the tools are used for risk estimation or hazard identification.

Where the strict quantitative analysis of risk by probabilistic methods is difficult or impossible, analysts appreciate fast heuristics. Such methods are *fire risk indexing, point schemes, scoring methods* (Hall & Watts 2008, Watts 2002). However, it should be noted that these methods are only practical when carrying out a fast analysis at the level of fire protection equipment, as well as to determine the necessity of additional fire prevention measures.

The literature survey also shows the current practice in the area of indexing point schemes audits:

– *Dow Chemical Method*—developed by The Dow Chemical Company (USA) "… provides a simple method of rating the relative acute health hazard potential to people in neighboring plants or communities from possible chemical release incidents. Absolute measures of risk are very difficult to determine, but the CEI system will

provide a method of ranking one hazard relative to another. It is not intended to define a particular design as safe or unsafe.

The CEI is used:

– For conducting an initial Process Hazard Analysis (PHA).
– As a screening tool for further study
– In Emergency Response Planning

It is a simple method for predicting dispersion of vapors/gases from process leaks, and the Index is used as part of Dow Risk Assessment" (Dow Chemical Method 2013).

– *FRIM (Fire Risk Indexing Method)* for Multistory Apartment Buildings. This method adjusts fire-prevention systems of wooden houses by comparison of an index of fire risk with a similar index for buildings with nonflammable bearing designs. This method is in fact a method of hazard assessment as no likelihoods are considered (Karlsson 2002).
– *FSES (Fire Safety Evaluation System)* evaluates the overall level of a fire safety of buildings. It provides means of comparing the effectiveness of proposed improvements by producing a comparative baseline and shows the relative gain in fire safety for proposed improvements (NFPA 101A).
– *SIA 81 or Gretener method and its modifications* "… is used to evaluate and compare the level of fire risk of alternative concepts by grading the elements of a building and their performance. The grading factors are claimed to be based on expert knowledge, a large statistical survey and tested by a wide practical application. The calculated risk is compared to the accepted risk, where the latter is a function of the number and the mobility of the persons involved and of the location of the relevant fire compartments within the building" (Larsson 2000). Methods like, ERIC—Evaluation du Incendie par le Calcul (Cluzel & Sarrat1979), Fire Risk Assessment Method for Engineering (FRAME) etc. are modifications of SIA 81.

The literature survey testifies that probabilistic and index methods are beneficial tools, which take their own place in the range of approaches to a problem with regard to QRA. However, the application needs a profound expert knowledge about their area of application. Furthermore, these methods are only applicable for fire risks and do not consider explosions risk.

4 RISK AUDIT PRINCIPLE

The paper suggests a technique to assess individual risks for industrial objects in the field of fire and explosion safety. This method rests upon on

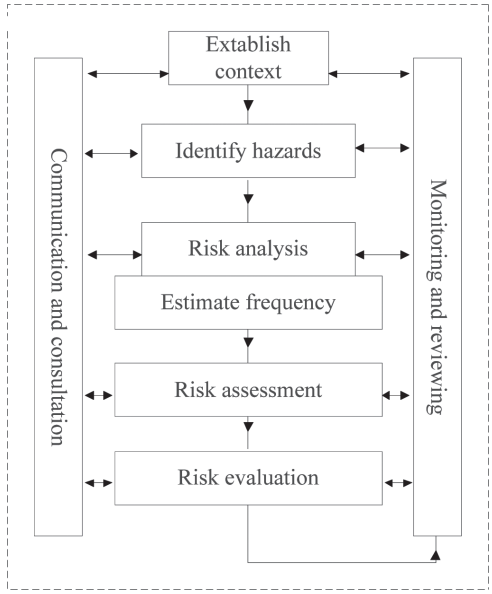


Figure 1. Risk management process.

specified FEP zones at the audited enterprise and then supports threat analysis as well as the overall audit approach.

In order to advance the methodology introduced in (Mock et al. 2012), two major problem areas needs to be addressed:

– an audit approach has to exclude time consuming procedures as well as excessive workload. This problem is addressed by the introduction of the revised indexing method to calculate the individual risk.
– individual risk figures only rely on semi-quantitative or qualitative approaches. The method suggested in this paper introduces reasoned weighting factors (from 0 to 100%).

The following chapters process these steps of the audit development.

This approach follows the risk management process of (Fig. 1) based on e.g., standards as (ISO-GUIDE-73 2009, ISO-31000 2009) and (ISO/TS 16732 2005).

5 EXTENDED AUDIT APPROACH

5.1 *Indexing approach*

The set of hazards and protection measures are considered as factorial indicators which define an indexing equation.

To each factorial indicator of the system, a specified number of points is attributed by rules,

i.e., the assessment of a condition of the system is made from various points of view.

The common indexing methods are developed to assess fire hazards supported by factorial indicators which consider aspects causing fires (fire loading, ignition sources etc.) as well as measures to mitigate fire hazards (availability of fire extinguishing systems, fire resistance of design, existence of an alarm system and evacuation ways, etc.). The calculated index of fire risk expresses a level of fire hazards. The formal goal of the suggested method is to comprise index calculations into QRA.

By combining the risk equation $R = F \cdot C$ (i.e., risk R is a function of frequency F and consequence C of an undesired event; (ISO-Guide-73 2009)) with the indexing model, the resulting equation of individual risk becomes:

$$R_{Ind} = F_F \cdot P_\tau \cdot C_S, \tag{1}$$

where R_{Ind} = individual risk [1/a]; F_F = frequency of a fire at the enterprise [m^2/a]; P_τ = probability of presence of the personnel; C_S = coefficient of safety.

5.1.1 *Influence of the fire frequency*

As mentioned in (Leksin et al. 2013), risk values are industry specific. The probability F_F of a fire at the enterprise is derived from statistical data for the analyzed enterprise. Average values can be obtained from international statistical data and standards like (Purple Book 2005, FZ 1994). Table 1 exemplifies branches and frequencies in use.

Because these values can be different from country to country, an additional factorial indicator, which corrects the suggested frequency of a fire, is considered. The impact of offence in the audited enterprises is determined by this factorial indicator.

5.1.2 *Influence of the personnel presence*

The calculation of individual risk needs to consider the probability of personnel presence at an endangered zone:

$$P_\tau = \tau/24, \tag{2}$$

where τ = working time of a person [h].

Table 1. Fire frequencies of branches (Mock et al. 2013).

Industry	Frequency 10^{-5} [m^2/a]
Power generation	1.20
Storage (chemical production)	1.38
Manufacturing	0.73
…	…
Metal industry	1.78

5.1.3 *Influence of the safety coefficient*

Risk to a single person depends on a number of hazards and safety measures. The set of hazards and protection measures is considered as a variety of factorial indicators which define a function based on the indexing method. These factorial indicators are considered by the calculation of the coefficient of safety:

$$C_S = F_S \cdot F_{Hrisk}, \tag{3}$$

where F_S = factorial indicator of safety, which dependends on the safety measures; F_{Hrisk} = factorial indicator of hazard, which is dependent on the Worst Case path of an Event Tree (relative to indexing factor, which is dependent on the hazard measures).

Because risk considers the frequency F of an event and its consequence C, we have a scale from the Best Case to the Worst Case Scenario which is also considered in ETA (Event Tree Analysis).

In order to consider all scenarios of the event tree and to achieve a more exact calculation of the individual risk, factorial indicators of hazard measures for the worst case and best case scenarios are developed. Figure 2 will show this approach in an extended context in section 5.2. There, the substantiation of factorial indicators of hazard measures is also discussed.

5.1.4 *Influence of the safety factorial indicator*

The influence of the safety factorial indicator F_S is

$$F_S = \overline{M}_{\text{arch}} \cdot \overline{M}_{\text{tech}} \cdot \overline{M}_{\text{org}} = \frac{1}{n}\sum_{i=1}^{n} M_{i,\text{arch}} \cdot \frac{1}{m}\sum_{i=1}^{m} M_{i,\text{tech}} \cdot \frac{1}{k}\sum_{i=1}^{k} M_{i,\text{org}}, \tag{4}$$

where $\overline{M}_{\text{arch}}$ = arithmetic mean of safety architectural measures; $\overline{M}_{\text{tech}}$ = arithmetic mean of safety

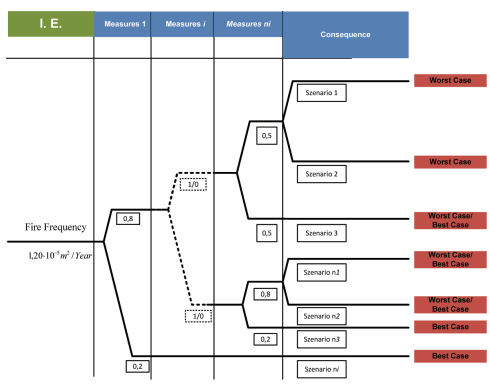


Figure 2. ETA in the audit process (I.E.: initiating event).

technical measures; $\overline{M}_{org}$ = arithmetic mean of safety organizational measures.

5.1.5 *Influence of the hazard factorial indicator*

The influence of the hazard factorial indicator F_{HRisk} is

$$F_{HRisk} = \overline{H}_{fut} \cdot \overline{H}_{f} \cdot \overline{H}_{ex} = \frac{1}{x}\sum_{i=1}^{x} H_{i,fut} \cdot \frac{1}{y}\sum_{i=1}^{y} H_{i,f} \cdot \frac{1}{z}\sum_{i=1}^{z} H_{i,ex}, \quad (5)$$

where $\overline{H}_{fut}$ = arithmetic mean of further hazards (e.g. amount of dangerous substance, room category, technological process etc.); $\overline{H}_{f}$ = arithmetic mean of fire hazards; $\overline{H}_{ex}$ = arithmetic mean of explosion hazards.

As the proposed method bases on the classical risk equation, the risk decreases automatically by simple multiplication of the measure factors. Therefore it is important to use the arithmetic mean of all micro parameters, which form the macro parameter.

5.1.6 *Influence of the safety index*

Parallel to the individual risk estimation the safety index I_S is calculated. Its function is to additionally assess and evaluate the calculated risk adequately:

$$I_S = \frac{F_S}{F_{HInd.}}, \quad (6)$$

where $F_{HInd.}$ = factorial indicator of hazard, which is dependent on the Best Case path of ETA (relative to indexing factor, which is dependent on the hazard measures).

The safety index is based on the classical indexing method—weighting the safety and hazard measure (which is dependent on the Best Case path of Event Tree). As we consider the spent time of the personal in the endangered area, the calculated risk can be acceptable if the probability of the presence of personnel is very small. In the other hand, the frequency of a fire at the enterprise is also small but safety measures can be unacceptable. This gives a signal to the auditor that safety measures have to be raised.

5.2 *Semi-quantitative approach*

In practice, the common QRA approaches are unable to cope with individual risks in a level of detail as needful, e.g., for business and insurance purposes. Taking up authors' preliminary studies (Leksin et al. 2013, Mock et al. 2012), a semi-quantitative approach is used and integrated within a common checklist approach and FMEA-like procedure. As mentioned in the indexing mathematical function of e.q. (1) hazard and safety measures are considered and developed in form of an alternative checklist. This checklist contains indicators of hazard measures, e.g., general hazards, fire hazards, explosion hazards, designated as macro parameters. Every macro parameter has a number of micro parameters, which are evaluated by an auditor. The same applies for the safety measures. This context is outlined in Table 2.

This kind of check list characterizes all scenarios of an Event Tree, which enriches the audit process and takes into account the Worst and Best Case paths of this ETA, as shown in Figure 2. Risk is computed as the sum of all worst case scenarios.

The next step in the semi-quantitative approach is the evaluation of the macro and micro parameters (hazard and safety measures). For this, weighting factors are used.

The weighting factors of Table 3 are used for safety parameters.

For hazard parameters (e.g., common, the amount of dangerous substances), there are weighting factors for both, worst case and best case.

Table 2. Check list of parameters.

1. General hazards
1.1 Amount of dangerous substance
1.2 Room category
1.3 Technological process
1.x …
Value of General hazards
2. Fire hazards
2.1 Dangerous goods
2.y …
Value of Fire hazards
3. Explosion hazards
3.1 Instability/Reactivity
3.2 Classification of combustible substances
3.z …
Value of Explosion hazards
I. Architects measures
I.I
I.II
II. Technical measures
III. Organization measures

Table 3. Weighting factors for safety parameters.

Compliance	Weighting factors
Irrelevant	0.95
Unacceptable	0.50
Acceptable	0.20
Accepted	0.05

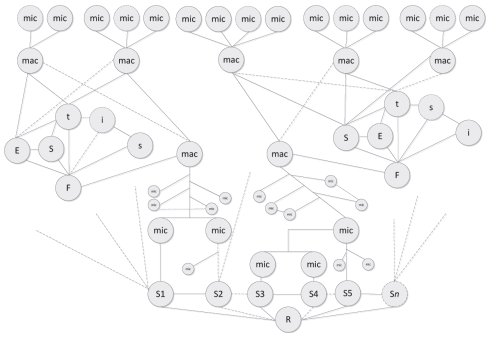


Figure 3. Schematic diagram of a risk analysis (explanation see text).

Table 4. Weighting factors for best and worst case scenarios.

Compliance	Best case	Worst case
Hazard free	0.95	0.05
Low	0.75	0.25
Average	0.50	0.50
High	0.25	0.75
Maximum	0.05	0.95

The weighting factors represent an important step for an objective evaluation of the calculated risk as the auditors cannot manipulate the factors.

FMEA like procedures, which give information about the risk spectrum of estimates as well as the standard deviation, are taken into account. Due to the complexity of formulas and the dependency among the factorial indicators, the mathematical context is not presented in this chapter. A more visual explication can be found in chapter 6.

In addition to the weighting factors, which are used by the auditor, there are suggested correction factors (e.g., emergency exit—escape route—0.8 and 0.2) to get a more exact statements about the risk.

The dependency of hazard factors and measures is taken into consideration in the same way. By these mathematical combinations between factorial indicators and weighting factors of the evaluated scenario, more exact statement about the calculated risk values are possible.

In this case, the developed checklist actually takes a position about the scenario and thereby about the complete event tree, which can only be visualized in form of a complex graph. Figure 3 shows, how such a graph might look like.

Figure 3 use the following notation: mic/mac = micro and macro parameters of hazard and safety measures; F = fire, e.g., for an I.E.; E = existing violations; t = presence of personnel; i = fire frequency of industry branch; s = substance/material (dust, liquefied gas, etc.); S = area of testing zone; S1-Sn = scenarios; R = risk.

To simplify the application, the approach is rendered in to an MS EXCEL prototype tool, which is present in the following chapter.

6 AUDIT APPLICATION

The combination of methods results in a probabilistic approach, which leads to an audit approach, which bases on weighting procedures. This approach allows to compare input data and

Table 5. Data input mask.

1. Industry	Chemical industry	Correction factor
2. Area of testing zone	1'000 [m²]	–
3. Presence of personnel	8 [h]	–
4. Existing violations	Be absent = 0.5	–
a. Dust	A lot	–
b. Combustible liquids	Middle	–
c. Liquefied natural gas	Absent	–
d. …	…	–

Table 6. Data input mask of hazard measures.

1. Further hazards		Correction factor
1. x …	Hazard free	0.2
2. x …	Low	0.1
1.A. Maximum value	Standard deviation of the mean	–
1.B. Normal value	$\bar{H}_{fut}$	–
1.C. Minimum value	Standard deviation of the mean	–
2. Fire hazards	…	–
3. Explosion hazards	…	–

Table 7. Data input mask of safety measures.

I. Architects measures		Correction factor
I.n …	Unacceptable	1
I.n …	Acceptable	1
I.A. Maximum value	…	–
I.B. Normal value	…	–
I.C. Minimum value	…	–
II. Technical measures	…	
III. Organization measures	…	

factorial indicators with the auditor's experience. The application has to be easy to handle because of limited resources. Therefore the auditor uses an input mask. First, a parameters check has to be carried out and some audit specific data are entered. The final risk assessment compares the identified frequencies of individual risk with a given tolerance value. The threshold value of the acceptable risk is set for example to 10^{-6} [1/a], which corresponds to European standards (Dijm 2009).

The auditor has also to do the compliance check of hazard parameters, as shown in Table 2.

The compliance check of safety parameters must also be entered.

The resulting risk prioritization and safety index values I_S and their evaluation are given in Table 8 and 9.

If R_{Ind} > value of the acceptable risk, e.g., 10^{-6} [1/a], then the compliance factor for risk is 1.

If $R_{Ind} \leq$ value of the acceptable risk, then the compliance factor for risk is 0.

If $I_S > 1$, then the compliance indicator for index is 1.

If $I_S = 1$, then the compliance indicator for index is 0.5.

If $I_S < 1$, then the compliance indicator for index is 0.

The general class of hazard is the sum of existing violations and the compliance indicators for risk and index.

Table 8. Data output mask of individual risk.

Individual risk (R_{Ind})		Compliance indicator for risk
Maximal individual risk	$8.43 \cdot 10^{-4}$ [1/a]	1
Normal individual risk	$9.90 \cdot 10^{-5}$ [1/a]	1
Minimal individual risk	$2.49 \cdot 10^{-6}$ [1/a]	1

Table 9. Data output mask of safety index.

Safety index (I_S)		Compliance indicator for index
Maximal safety index	13.7765	1
Normal safety index	1	0.5
Minimal safety index	0.04070	0

Table 10. Data output mask of general class of hazard.

Common class of hazard	Increased	5

Table 11. General classes of hazard.

Common classes of hazard	Sum of existing violations and the compliance indicators
Minimal	1
Low	2
Moderate	3
Middle	4
Increased	5
High	6
Maximum	7
Maximum	8
Maximum	9

For the definition of the common class of hazard exists a rating scale is used.

The auditor can draw conclusions about the fire and explosion risk (e.g., that explosion constitutes a bigger danger than a fire) with the help of additional diagrams (not presented in this paper).

7 CONCLUSIONS

This paper is roughly structured into two parts:

First, it summarises a survey about operative indexing and QRA audit software tools in the field of FEP. Second, the authors continued to formalize their audit approach by the combination of the indexing method and semi-quantitative approaches. By combining the two methods the resulting probabilistic method allows to carry out an audit, which bases on weighting procedures utilizable for risk rating and benchmarking.

The number of commercial indexing and QRA assisting software tools is surprisingly small. Furthermore these tools are only applicable for fire risks and do not consider explosion risks and hazards. Currently, there is no clarity which of the specified tools is more preferable to the quantitative analysis. Often these tools do not asses risk but hazards (i.e. ignoring the frequentistic risk element) or only weight and evaluate the overall levels of fire safety of buildings, which is characteristic for indexing methods.

The probabilistic model of the individual fire and explosion risk discussed in this paper considers the most important aspects in the field of fire and explosion risk protection such as:

- quantitative risk assessment, based on an extended risk equation and
- controls probability of hazard and safety measures, based on a FMEA-like procedure that gives information about the risk spectrum of estimates.

Therefore, the uniqueness of the presented method lies in the robust, easy to understand

approach that combines various systems into a more stringent decision making process. This combining allows to consider a big number of scenarios, which are dependent from aspects causing fires, as well as aspects reducing fire hazard, by the initiating event "fire".

This approach is still depended on expert judgment. However, the auditor is supported with statistical data and reasonable weightings factors.

The audit approach presented as a MS EXCEL prototype tool shows a practice oriented possibility to check quantitative individual risk in the field of fire and explosion protection at enterprises.

The authors feel encouraged to continue their R&D efforts in this area as no tool or method could be found combining QRA methods in the proposed manner.

REFERENCES

Cluzel, D. & P. Sarrat, 1979. Methode ERIC. Evaluation du Risque Incendie par le Calcul. In: *Proc. CIB Symposium on Systems Approach to Fire Safety in Buildings, Vol. I*, p. II/37—II/58.

Dic. Academic 2013. Academic Dictionaries and Encyclopedias (http://dic.academic.ru/dic.nsf/enc_chemistry/769/%D0%92%D0%97%D0%A0%D0%AB%D0%92%D0%9E%D0%9E%D0%9F%D0%90%D0%A1%D0%9D%D0%9E%D0%A1%D0%A2%D0%AC#sel=20:4,20:5)

DIN EN ISO 13943 2010. *Fire safety—Vocabulary. German and English version.* (ISO 13943:2010). Berlin: DIN Deutsches Institut für Normung e.V.

DowChemicalMethod2013.S2S.TheEuropeanWebPortal for Process Safety. (http://www.safetys2s.eu/modules.php?name=s2s_wp4&idpart=2&op=v&idm=34).

Duijm, N. 2009. Acceptance criteria in Denmark and the EU. *Environmental Project No. 1269 2009 (Miljøprojekt),* Danish Ministery of the Environment—Environmental Protection Agency.

FRAME. Fire Risk Assessment Method (for) Engineering (www.framemethod.net; www.framemethod.net/indexen_2.html; v.: June 11, 2013).

FZ 1994. *About fire safety (No. 69-FZ)*. Federal Law of the Russian Federation. Moscow, Russia: Dec. 21, 1994.

GOST 12.1.033-81 1982. Occupational safety standards system. Fire safety. Terms and definitions. *Safety standarts*. Moscow: State committee of standards USSR.

GOST 12.1.004-91 1992. Occupational safety standards system. Fire safety. General requirements. *Safety standarts*. Moscow: IPK State committee of standards.

Hall, J. R. & J. M. Watts, 2008. Fire Risk Analysis. In*: Fire Protection Handbook*, Cote, A.E. (ed.), NFPA, Ch. 8, pp. 3-135-3-143.

Hurley, M. J. & R.W. Bukowski (008. Fire Hazard Analysis Techniques. In: *Fire Protection Handbook*. Cote, A.E. (ed.), NFPA, Ch. 7, pp. 3-121–3-134.

IEC/FDIS 31010 (2009). *Risk management—Risk assessment techniques* (IEC/FDIS 31010:2009). Geneva: International Electrotechnical Commission.

ISO-31000 2009. *Risk management—Principles and guide lines* (ISO 31000:2009). Geneva: International Standards Organisation.

ISO-GUIDE-73 2009. ISO/IEC. *Risk Management—Vocabulary—Guidelines for Use in Standards* (ISO GUIDE 73:2009(E/F). Geneva: International Standards Organisation.

ISO/TS 16732 2005. *Fire safety engineering—Guidance on fire risk assessment*. (ISO/TS 16732:2005). Geneva: International Standards Organisation.

Karlsson, B. 2002. Fire Risk Index Method—Multi Storey Apartment Buildings. *FRIM-MAB. Version 2.0*. Trätek, Rapport 0212053.

Larsson D. 2000. Developing the Structure of a Fire Risk Index Method for Timber-frame Multistorey Apartment Buildings. In: *Report 5026.* Lund University: Department of Fire Safety Engineering.

Leksin, A., R. Mock & U. Barth 2014. The Potential of QRA Audit Tools in Industrial Fire and Explosion Protection. In *Proc. of European Safety and Reliability Conference (ESREL 2013)*. In: *Safety, Reliability and Risk Analysis: Beyond the Horizon,* Amsterdam, the Netherlands: 1895–1901.

Mock, R., U. Barth, A. Franz, S. Brunner & A. Leksin 2012. Computer-assisted risk assessment audit on operational level. In *Proc. PSAM 11 & ESREL 12 Vol. 5,* Helsinki, Finland: 4093–4102.

NFPA 101 A 2001. *Alternative Approaches to Life Safety* (2001). Quincy, MA: National Fire Protection Association.

PAS 79 2011. *Fire risk assessment—Guidance and a recommended methodology*. (PAS 79:2011). British Standards Institution.

Purple Book 2005. Guidelines for quantitative risk assessment. CPR 18E. *Publication Series on Dangerous Substances (PGS 3)*. Committee for the prevention of disasters. The Hague.

RD-03-26-2007 2008. Методические указания по оценкепоследствий аварийных выбросов опасных веществ. *Regulatory document*. Moscow: Federal environmental, industrial and nuclear supervision service of Russia.

Watts, J. M. 2002. Fire Risk Indexing. In: *SFPE Handbook of Fire Protection Engineering,* Ch. 10. Section 5, Fire Risk *Analysi*s, pp. 5-125–5-142. Quincy, MA: National Fire Protection Association.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Estimation of the impact probability of fragments produced by explosions of vessels: A case study

M.F. Milazzo, R. Lisi & G. Consolo
University of Messina, Messina, Italy

G. Maschio
University of Padova, Padua, Italy

ABSTRACT: In order to incorporate domino effect scenarios, deriving from the projection of fragment (so-called missile), within the standard QRA (Quantitative Risk Analysis), a probabilistic model for the estimation of the impact probability of such fragment was developed by applying a Monte-Carlo method to the analytical solution of the set of equations describing the motion of the missile. The objective of this work is to further extend this probabilistic approach, which was previously developed for cylindrical vessels, to make it applicable also to spherical tanks. A case study is presented, it is the accident occurred in the refinery of Feyzin (France); the influence of the size and shape of the fragments on the impact probability is assessed.

1 INTRODUCTION

The term *domino effect* denotes a chain of accidents generated by an initiating accident, which occurs in an industrial unit and causes more severe events in other units (*accident escalation*), either in the same establishment or in neighbouring industries (Delvosalle, 1996). The literature provides some relevant examples, i.e. see the survey performed by Fabiano & Currò (2012), however a complete inventory of domino effects was given by Abdolhamidzadeh et al. (2011). According to Khan & Abbasi (2001), a domino effect may be initiated by several events: (i) fires (pool fire, flash fire, fireball, and jet fire); (ii) explosions (vapour cloud explosions VCE, boiling liquid expanding vapour explosion BLEVE, vented explosion, confined vapour cloud explosion, dust explosion); (iii) toxic release (instantaneous or continuous release of toxic lighter and heavier than air gases, release of toxic liquids and dust), in this latter case aspects of the emergency management are involved.

According to the Council Directive 96/82/EC and subsequent laws, the analysis of domino effects due to explosions and fires is carried out using simplified methods based on damage thresholds. This estimation is based upon technical assessments, which are not probabilistic methods and do not take into account uncertainties (Milazzo & Aven, 2012). Concerning domino effects triggered by fires, the evaluation of the influence of the flame extent and temperature has been amply explored by Palazzi & Fabiano (2012). In this framework the problem of the projection of fragments is not completely faced.

A multi-step approach for the deterministic estimation of the domino effects due to the projection of fragments was proposed by the Centre for Chemical Process Safety (CCPS, 2000). Such method consists in computing: (i) the explosion energy; (ii) the number and size of missiles produced by the vessel fragmentation; (iii) the initial velocity and angle of departure for each fragment; and (iv) the distance of fallout. Afterwards, by analyzing the plant layout, facilities located in the range of potential fallout of missiles are identified; these could be the potential sources of the accident escalation. To include the quantification of such domino effects into the QRA, the consequence and the frequency of the scenario must be estimated, their probabilistic implementation is necessary to extend studies such as those of Baesi et al. (2013) and Milazzo et al. (2010). The frequency of the domino scenario is the product of the frequency of the primary event and the probability of the following sequence of events (given the occurrence of the primary event). This probability is obtained by multiplying the probabilities of the fragmentation, of impact on a target and of damage given the occurrence of the impact (Nguyen et al., 2006). In this frame Holden and Reeves (see Lees 1996) developed models for the estimation of the fragmentation probability. Approaches to the modelling of the impact probability based on the

analysis of the fragment flight are due to Hauptmanns (2001) and Gubinelli et al. (2004). Finally, correlations for the calculation of the probability of damage are reported in Lees (1996).

Lisi et al. (2014a) recently reviewed the analytical solution of the set of ordinary differential equations describing the flight of a fragment proposed by Hauptmanns (2001). Then they validated the reviewed solution by using the accident occurred in the Italian refinery of Milazzo in 1993. The same authors extended the approach, which was previously developed for cylindrical vessels, also to spherical tanks (Lisi et al., 2014b).

This paper aims to investigate the influence of the size and shape of the fragments on the impact probability; to achieve this aim the data of the incident occurred in the refinery of Feyzin (France) in 1966 have been used. The paper presents the methodology in the section 2; in section 3 the incident of Feyzin and the setting up of the parameters for the analysis are described; in section 4 the results of the application of the methodology are shown; finally some conclusions are given.

2 METHODOLOGY

The methodology, presented in this section, has been developed for the estimation of domino effects due to fragments originating from a BLEVE (Boiling Liquid Expanding Vapour Explosion). Thus the proposed procedure accounts for the Baum's model (Baum, 1995) to compute the initial velocity of fragments. The methodology is composed of two steps:

1. Deterministic modelling of the flight of the fragment (i.e. derivation of the trajectory equation for the fragment);
2. Probabilistic modelling of the impact probability of the fragment.

2.1 *Deterministic modelling of the flight of the fragment*

In order to derive the trajectory equation of a fragment, its shape and angle of departure must be known.

Some studies on cylindrical vessels are due to Baum (1998, 1999, 2001); these report about two main types of fragmentation mode:

1. a fragmentation, along the welding, leads to an end-cap fragment, then the crack propagates axially along the shell. In some cases, the end-cap remains linked to a portion of the shell (oblong end-cap). The cylinder usually generates five fragments.
2. a fracture at the middle part of the cylinder is usually due to manufacture defects. The fragmentation unfolds the cylinder, then it propagates towards the edges of the vessel and generates one or two end-caps. Also in this case the end-cap sometimes remains linked to the complete cylinder or part of it.

In case of spherical tanks, the fracture can start anywhere in the vessel. As shown by Baum (1998), it can propagate either in a circular mode, generating a half sphere fragment, or along several directions, generating flat fragments.

If a large number of fragments are produced (in case of the explosion of cylindrical or spherical vessels) the departure angle cannot exactly be defined a priori; anyway each generated fragment has its own vertical and horizontal departure angles, respectively, indicated as θ and φ in Figure 1 (see Mebarki et al., 2009). Obviously, the departure angle is well known in case of a fitting projection (Lees, 1996).

The trajectory of the fragment is described by solving the motion equations in two spatial dimensions (see the axes rotation in Fig. 1), taking into account the air resistance. The lift (F_L) and the drag (F_D) are the components of this force, respectively, perpendicular and parallel to the direction of motion.

The equations of motion in the form of a system of second-order ordinary differential equations are:

$$\begin{cases} \ddot{x} + k\dot{x}^2 = 0 \\ \ddot{y}_A + k_A \dot{y}_A{}^2 + g = 0 \\ \ddot{y}_D - k_D \dot{y}_D{}^2 + g \end{cases} \quad (1)$$

In the system (1), the dot notation stands for the time derivative of the indicated variable; x and y_i ($i = A,D$) are, respectively, the horizontal and vertical components of the trajectory and g is the gravitational constant. The first equation describes the time evolution of the horizontal component of the trajectory, the last ones account, respectively, for the ascending and descending vertical branches.

In (1) the following coefficients are defined as:

$$k = \frac{\rho C_D A_D}{2m_i} \quad (2)$$

$$k_A = \frac{\rho(C_D A_D - C_L A_L)}{2m_i} \quad (3)$$

$$k_D = \frac{\rho(C_D A_D + C_L A_L)}{2m_i} \quad (4)$$

where ρ = air density; m_i = mass of the i-th fragment; C_D = drag coefficient; C_L = lift coefficient; A_D = drag area; A_L = lift area.

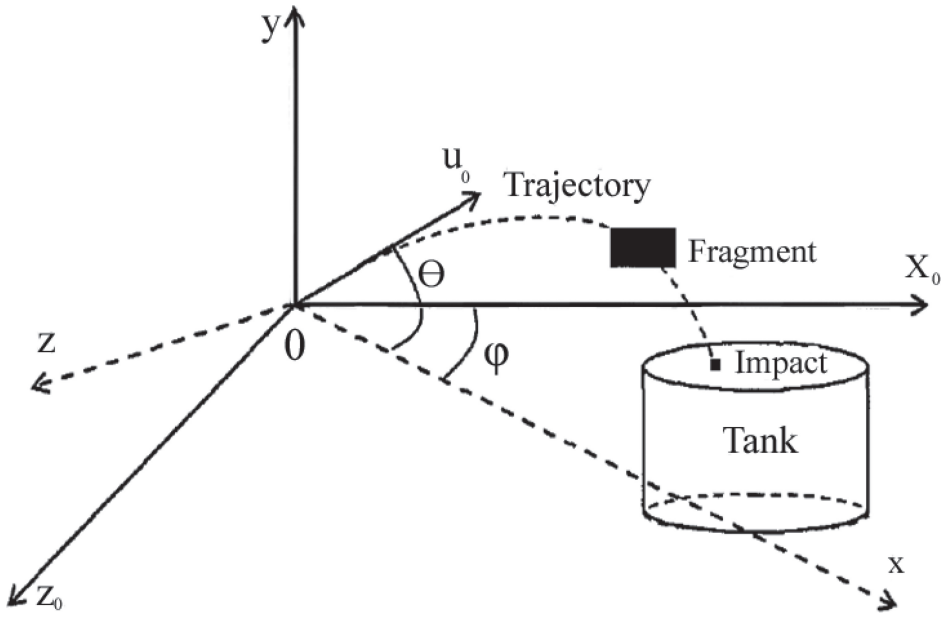


Figure 1. Fragment trajectory and impact on the target (tank).

Lisi et al. (2014a) solved the system (1) by using the initial conditions (5):

$$\begin{cases} x(0) = 0 \\ x(0) = u_o \cos\theta \\ y_A(0) = 0 \\ y_A(0) = u_o \sin\theta \\ y_D(t^*) = \max(y_A(t)) \\ y_D(t^*) = 0 \end{cases} \quad (5)$$

where u_o = initial velocity of the fragment; t^* = time at which the ascending of the trajectory reaches the maximum height.

The lift coefficient rises for asymmetric surface of the fragment (Daugherty et al., 1989), thus in case of cylindrical vessel, it should be considered for the end-cap and the shell. C_L is expressed as:

$$C_L = 0.351 + 0.6723 \cdot \alpha \quad (6)$$

where α = angle of attack.

It is worth noting that C_L is supposed to be equal to zero when the angle of attack ranging outside the interval [0°, 10°].

The drag depends on the several factors, i.e. the geometry, the surface roughness and the fragment orientation with respect to the direction of the initial velocity. An acceptable range values for C_D is [0.8–1.1] for tank end-caps and a range values [1.1–1.8] for the rings (see Baker et al. 1983).

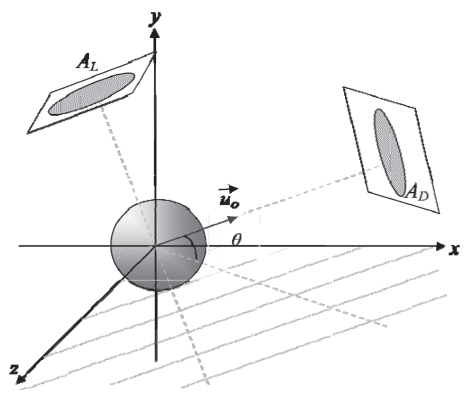


Figure 2. A_D and A_L for a sphere.

To understand the meaning of both the fragment projection on a plane perpendicular to the motion direction (A_D) and on a plane parallel to the motion direction (A_L), Figure 2 shows representation of these areas for a sphere (u_o is the initial velocity and θ is the initial angle with respect to the plane of xz).

2.2 *Probabilistic modelling of the impact probability of the fragment*

To model the impact probability of fragments originated by a BLEVE, a Monte Carlo method has

been applied to the solution of the system (1). The initial velocity and the departure angle are assumed to be stochastic variables. It has been assumed that both the variables obey: (1) a uniform and (2) a Gaussian (normal) probability density functions.

To compare the results obtained by using these probability density functions, the half-amplitude of the interval occurring in the uniform distribution is taken equal to twice the standard deviation of the normal distribution; while the expectation value of the Gaussian distribution is set at the centre of the interval of the uniform distribution.

3 CASE-STUDY

As previously mentioned, the case-study in this work is the incident of Feyzin (France). The effects, due to the fireball and the blast wave of the whole scenario, were investigated by Török et al. (2011). Lisi et al. (2014b) used this case-study to estimate the impact probability of fragments, produced by spherical vessels, by the application of the procedure described in Section 2; their work allowed a further validation of the method.

In this section, an investigation of the influence of the size and shape of the fragments on the impact probability is given. The data of the incident has been extracted from the report produced by the Ministère Chargé de l'Environnement (2006).

3.1 *The incident of Feyzin (France)*

The incident occurred in the refinery of Feyzin in 1966 and caused 18 dead and 81 injured. The refinery, located near to Lyon, was built in the 1964 for the treatment of 1.7 million barrels per year of petroleum. It had a storage area of Liquefied Petroleum Gas (LPG) under pressure of about 13,100 m^3. The LPG storage area, which was located in the Southern of the production units, comprised 10 tanks, 8 spheres and two cigars (Fig. 3), it also includes storage tanks for the heating oil, the gasoline and the premium gasoline.

The incident was caused by the uncontrolled release of propane from a storage sphere (T61 443), due to the misbehaviour of the operators involved in the purge operation. These did not execute the correct instructions for the blockage of the two safety valves (located at the base of the sphere) and caused a leakage of propane.

As reported by Kletz (1985), an operator was draining the water from the sphere T61 443 (the volume of the vessel was ~1,200 m^3) nearly full of propane. To execute the operation, the drain valves A and B of the vessel (see Fig. 4) were opened. When the drainage was completed (this was underlined by traces of oil), the operator shut the valve A. The team of workers intended to close the valves, but the upstream valve did not perfectly close. It seems that the leakage was caused by the freezing of the valve due to the drain work.

It must be pointed that, if the pressure is lowered to atmospheric pressure, the temperature of the propane drops to –40°C. At this temperature, a leak of propane leads to a moisture with frozen air and also forms a solid hydrate. If this occurs either the valve handle can be stuck by the frozen moisture or the valve could not be closed tightly as a result of the hydrate formation. Considering the possibility of ice formation, two drain valves are mounted in series at the bottom of the tanks (Fig. 4). The drainage operation requires (IChemE, 1987): (i) the upstream valve (A) must be fully opened and the inlet side of the downstream valve (B) has to be pressurized, (ii) the downstream valve is gradually

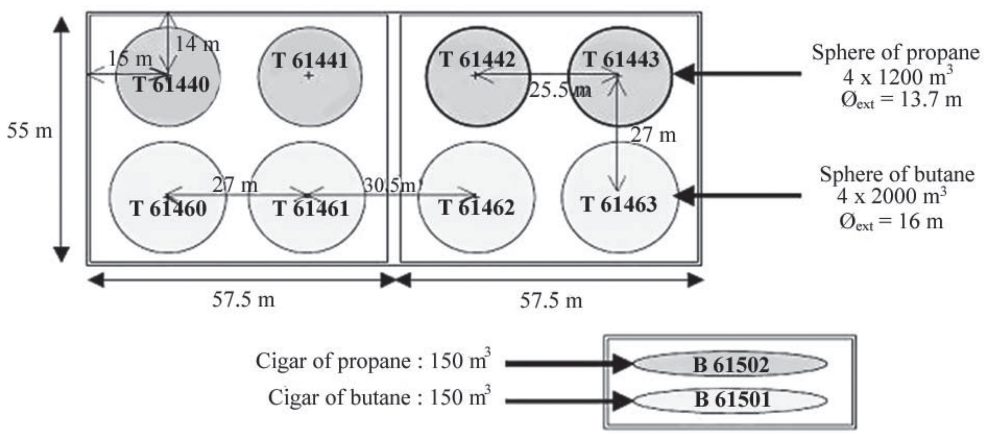


Figure 3. LPG storage area in the Feyzin refinery (source: Ministère Chargé de l'Environnement, 2006).

opened, starting from a slight open and then adjusting it to create the necessary flow rate. If the inlet of the valve B is pressurized, the temperature at the valve A does not drop. The outlet side of the downstream valve is cooled under the operation, and it is also important to ensure a sufficient distance between A and B, so that the upstream valve does not drop to a low temperature.

This accident was believed to be caused by the following causes: the valve A was not opened fully and the pressure at the outlet of this valve was near the atmospheric pressure, thus it was cooled by the pressure difference. It was absolutely forbidden to operate in this condition. Therefore, the cause of the accident was either the operator's human error or a mistake of the plant management in not to explain the proper execution of the operation (website HSE). Moreover another cause was that the operator did not close the downstream valve, this was probably due either to the ice formation or a rapid propane leak so that the operators could not close the valve.

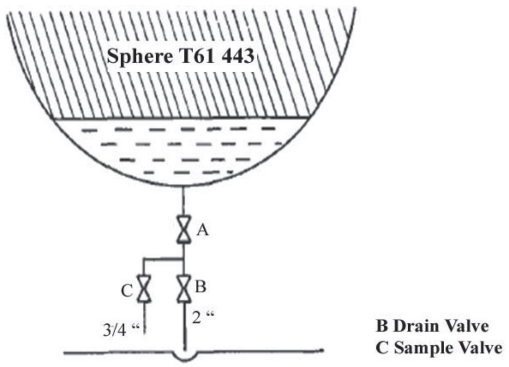


Figure 4. Drain valves' structure of the sphere T61 443.

The cloud of propane vapour spread, until it was ignited by a car that was driving along the local road. The pool of propane caused the storage tank to be engulfed in flames, which produced a BLEVE and, thus, the tank rupture. The released substance resulted in a fireball which killed and injured firemen and spectators. Flying missiles broke the legs of an adjacent sphere (T61 442) causing another BLEVE.

Three further spheres toppled due to the collapse of support legs which were not adequately fire protected. Three other spheres were broken during the accident, without generation of fragments. After the explosions of the spheres T61 442 and T61 443, many fragments were projected within an area having a radius of 800 m (Fig. 5), some of which weighed more than 80 tons. The characteristics of the exploded spheres are given in Table 1, whereas Table 2 shows the sizes, masses and distances of fallout of the main fragments.

3.2 *Deterministic analysis*

The deterministic analysis has been started with the calculation of the initial velocities by using the model proposed by Baum (Van den Bosch and

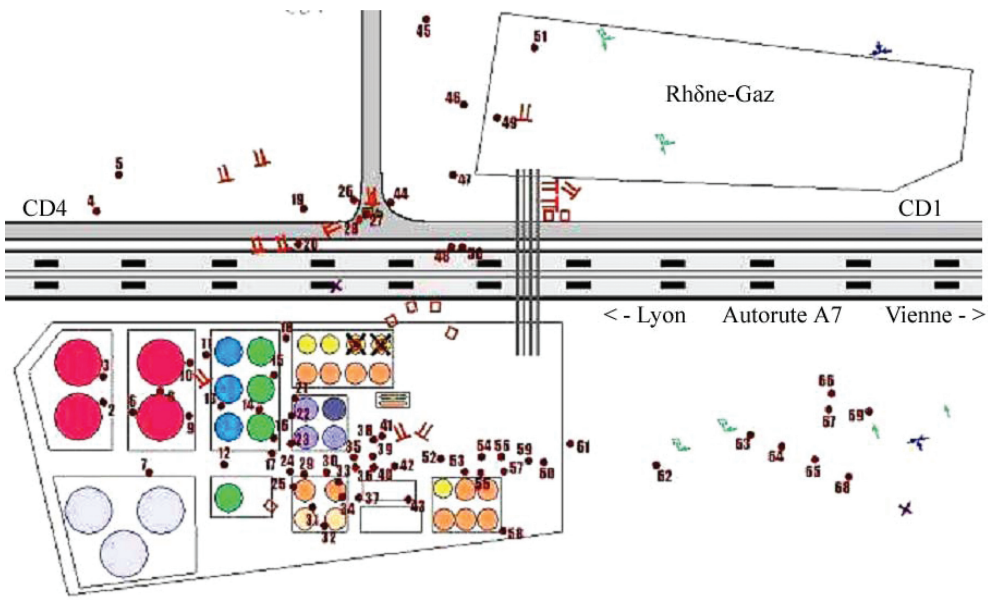


Figure 5. Localization of the fragments (source: Ministère Chargé de l'Environnement, 2006).

Table 1. Characteristics of the tanks (source: Ministère Chargé de l'Environnement, 2006).

Tank	Volume [m³]	Dimension [m]	Pressure [bar]	Empty weight [t]
Sphere of propane	1218	13.27 (d*)	18.7÷28.05	220
Sphere of butane	2038	15.74 (d*)	7.97÷11.95	186
Cylinders of propane/ butane	161	3.04 (d*) 20.80 (l**)	28.05	Unknown

*d = diameter; **l = length.

Table 2. Main fragments (source: Ministère Chargé de l'Environnement, 2006).

Item	Description	Weight [t]	Distance [m]	Dimension [m × m]
A1	T61 442	88.2	138	19 × 21.5
A2	T61 442	47.7	325	10.5 × 18.3
A3	T61 442	53.1	222	12.6 × 14.5
B1	T61 443	48	85	10.5 × 15
B2	T61 443	2.8	82	4 × 3
B3	T61 443	18	228	4.2 × 11.5
B4	T61 443	79	248	16.8 × 18.2
B5	T61 443	37	270	10.5 × 17.5

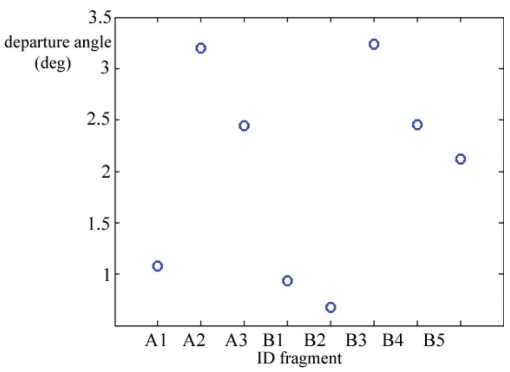


Figure 6. Deterministic estimation of the departure angles (θ).

Weterings, 2005) because it seems the most suitable for BLEVE.

The numerical integration of the equations of motion provided the values of the departure angles (θ) for the fragments, given the knowledge of the fallout distance reported in Table 2. This analysis allowing setting-up the numerical values of the parameters involved in the phenomenon (extracted from the survey after the accident) with the aim to verify whether, once inserted them into the equation of motion, they realistically reproduce the experimental data (the fallout distance have been calculated and compared with real data).

Figure 6 shows the results of the deterministic estimation of the departure angle θ of each fragment. The range of variability is $0° < \theta < 5°$.

4 RESULTS

The impact probability (P) has been evaluated as a function of the spatial position of the target. Results are shown in Figure 7 and lead to the following considerations. All the fragments depart almost parallel to the floor (as underlined in Fig. 6); the impact probability for the fragment produced by the fragmentation of both the spheres, T61 442 (A1, A2 and A3) and T61 443 (B1, B4 and B5), exhibits a monotonically decreasing dependence on the target disstance.

Figures 7(a) and 7(b) show the results obtained by using a uniform probability distribution function for the stochastic variables (P_U vs. target distance), whereas in Figures 7(c) and 7(d) these variables have been assumed to obey to a Gaussian one (P_G vs. target distance).

Appreciable differences cannot be observed by comparing the results obtained from all fragment types. In particular, in all cases, the probability is about 0.4 at 120 m, using a uniform probability distribution function (Figs. 7(a) and 7(b)), and 150 m, in case of a Gaussian one (Figs. 6(c) and 6(d)); then in all cases it smoothly decreases down to 10^{-3} at 450 m. Figure 7(e) and 7(f) show the deviation (given by the difference $P_U - P_G$) vs. target distance, and provide the following information: at distances lower than ~80 m, no appreciable difference can be observed by comparing all fragment types (A and B); the use of the Gaussian probability distribution function makes the estimation more conservative.

Concerning the size and shape of the fragments, it can be stated that according to the data of Table 2, the mass (m_i) of the fragments has the following order: $m_{A1} > m_{A3} > m_{A2}$ and $m_{B4} > m_{B1} > m_{B5}$. This order does not coincide with the trend of the impact probabilities given by the curves of Figure 7.

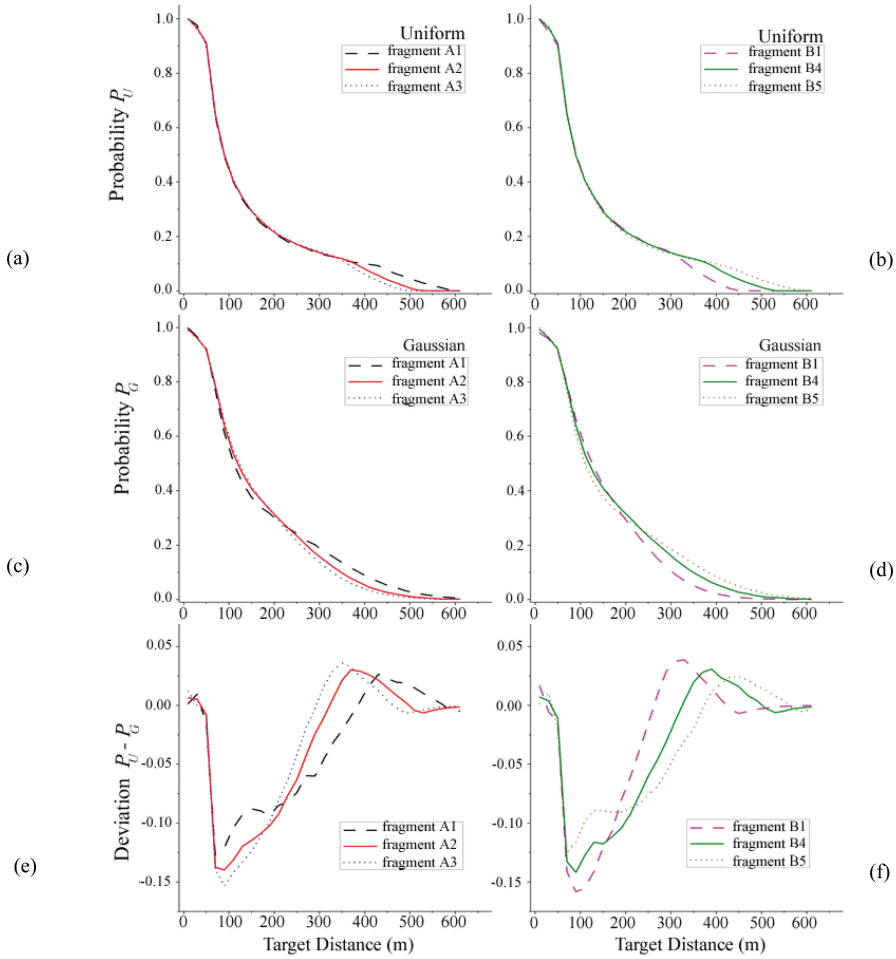


Figure 7. LPG storage area in the Feyzin refinery (source: Ministère Chargé de l'Environnement, 2006).

Table 3. Inputs to the probabilistic model.

Item	Vessel	A_D [m^2]	C_D [--]	A_L [m^2]	C_L [--]
A1	T61 442	408.5	0.351	0.76	1.2
A2	T61 442	192.1	0.351	0.42	1.2
A3	T61 442	182.7	0.351	0.504	1.2
B1	T61 443	157.5	0.351	0.42	1.2
B2	T61 443	12	0.351	0.16	1.2
B3	T61 443	48.3	0.351	0.168	1.2
B4	T61 443	305.8	0.351	0.672	1.2
B5	T61 443	183.7	0.351	0.42	1.2

As all the fragments depart almost parallel to the ground, the most significant contribution to the fallout distances and, thus, to these probabilities is given by the values of A_L. The extent of these areas has the following order: $A_{L,A1} > A_{L,A3} \sim A_{L,A2}$ and $A_{L,B4} > A_{L,B1} = A_{L,B5}$ (Table 3). This last parameter is the one influencing the final probability.

5 CONCLUSIONS

In this paper the methodology, proposed by Lisi et al. (2014), for the estimation of the impact probability of fragments originated by tank explosions (BLEVE), has been validated through its application to spherical tanks. The set-up of the model has been made by using the data of the incident occurred in the refinery of Feyzin. The probabilistic model for the estimation of the impact probability of the fragments has been developed by applying a Monte-Carlo simulation to the analytical solution of the trajectory of fragments, where the departure angle and the velocity are assumed to

be stochastic variables obeying either a uniform or a Gaussian distribution. The trend of the impact probability with respect to the target distance has shown a monotonically decrease.

The proposed approach allows the integration of the domino projection of fragments in the QRA. In fact, once potential domino scenarios have been identified, the proposed framework allows estimating the impact probability of a given fragment on each selected target.

REFERENCES

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D. & Abbasi, S.A. 2011. Domino effect in process-industry accidents An inventory of past events and identification of some patterns. *Journal of Loss Prevention in the Process Industries* 24: 575–593.

Baesi,S, Abdolhamidzadeh, B., Hassan, C.R.C., Hamid, M.D. & Reniers, G. 2013. Application of a multi-plant QRA: A case study investigating the risk impact of the construction of a new plant on an existing chemical plant's risk levels. *Journal of Loss Prevention in the Process Industries* 25(5): 895–903.

Baker, W.E., Cox, P.A., Westine, P.S., Kulesz, J.J. & Strehlow, R.A. 1983. *Explosion Hazards and Evaluation*, Elsevier, Amsterdam.

Baum, M.R. 1995. Rupture of a gas-pressurised cylindrical vessel: the velocity of a detached end-cap. *Journal of Loss Prevention in the Process Industries* 8, 149–161.

Baum, M.R. 1998. Rocket missiles generated by failure of a high pressure liquid storage vessel. *Journal of Loss Prevention in the Process Industries* 11(1): 11–24.

Baum, M.R 1999. Failure of a horizontal pressure vessel containing a high temperature liquid: the velocity of end-cap and rocket missiles. *Journal of Loss Prevention in the* Process Industries 12(2): 137–145.

Baum, M.R. 2001. The velocity of large missiles resulting from axial rupture of gas pressurised cylindrical vessels. *Journal of Loss Prevention in the Process Industries* 14(3): 199–203.

Centre for Chemical Process Safety (CCPS) 2000. *Guidelines for chemical process quantitative risk analysis*. AIChe, New York.

Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. Official Journal L 010, 14/01/1997: 0013–0033.

Daugherty, R.L., Franzini, J.B. & Finnermore, E.J. 1989. *Fluid Mechanics with Engineering Applications*, Mc Graw Hill Book.

Delvosalle, C. 1996. Domino effects phenomena: definition overview and classification. *Proc. European Seminar on Domino Effects*, Leuven (Belgium).

Fabiano, B. & Currò, F. 2012. From a survey on accidents in the downstream oil industry to the development of a detailed near-miss reporting system, *Process Safety & Environmental Protection* 90: 357–367.

Gubinelli, G., Zanelli, S. & Cozzani, V. 2004. A simplified model for the assessment of the impact probability of fragments. *Journal of Hazardous Materials* A116: 175–187.

Hauptmanns, U. 2001. A Monte-Carlo based procedure for treating the flight of missiles from tank explosion. *Probabilistic Engineering Mechanics* 16: 307–312.

Health and Safety Executive: http://www.hse.gov.uk/Comah/sragtech/casefeyzin66.htm (accessed on 30th April 2014).

Institution of Chemical Engineers (IChemE) 1987. The Feyzin Disaster. *Loss Prevention Bulletin* 077: 1–9 (October).

Khan, F.I. & Abbasi, S.A. 2001. An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. *Journal of Loss Prevention in the Process Industries* 14(4): 283–306.

Kletz, T.A. 1985. *What Went Wrong, Gulf Publication Company*. United Kingdom.

Lees, F.P. 1996. *Loss prevention in the process industries*. Butterwoth Heineman, United Kingdom.

Lisi, R., Consolo, G., Maschio, G. & Milazzo, M.F. 2014a. Estimation of the impact probability in domino effects due to the projection of fragments. *Process Safety & Environmental Protection,* in press doi: 10.1016/j.psep.2014.05.003.

Lisi, R., Consolo, G., Maschio, G. & Milazzo, M.F. 2014b. Domino Effects Due to the Projection of Fragments: Estimation of the Impact Probability Using a Monte Carlo Simulation. *Chemical Engineering Transactions* 36: 361–366.

Mebarki, A., Mercier, F., Nguyen, Q.B. & Ami Saada, R. 2009. Structural fragments and explosions in industrial facilities. Part I: Probabilistic description of the source terms. *Journal of Loss Prevention in the Process Industries* 22: 408–416.

Milazzo, M.F., Lisi, R., Maschio, G., Antonioni, G. & Spadoni, G. 2010. A study of land transport of dangerous substances in Eastern Sicily. *Journal of Loss Prevention in the Process Industries* 23(3): 393–403.

Milazzo, M.F. & Aven, T. 2012. An extended risk assessment approach for chemical plants applied to a study related to pipe rupture. *Reliability Engineering & System Safety* 99: 183–192.

Ministère Chargé de l'Environnement 2006. *BLEVE in LPG storage area of a refinery. On January 4th, 1966 Feyzin (69)—France.* Report (in French).

Nguyen, Q.B., Mébarki, A., Mercier, F., Ami Saada, R. & M. Reimeringer M. 2006. The Domino Effect and Integrated Probabilistic Approaches for Risk Analysis. *Proc. Eight International Conference on Computational Structures.*

Palazzi, E. & Fabiano, B. 2012. Analytical modelling of hydrocarbon pool fires: Conservative evaluation of flame temperature and thermal power. *Process Safety & Environmental Protection*. 90: 121–128.

Török, Z., Ajtai, N., Turcu, A.T., Ozunu, A., 2011. Comparative consequence analysis of the BLEVE phenomena in the context of Land Use Planning; Case study: The Feyzin accident. *Process Safety & Environmental Protection* 89(1): 1–7.

Van den Bosch, C.J.H. & Weterings, R.A.P.M. 2005. *Methods for the calculation of physical effects (Yellow Book),* The Hague, The Nederland.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dynamic risk assessment: Development of a basic structure

N. Paltrinieri & P. Hokstad
Safety Research, SINTEF Technology and Society, Trondheim, Norway

ABSTRACT: The availability of real-time data provided by solutions for Integrated Operations (IO) in the petroleum industry may allow the development of advanced risk assessment techniques previously considered time-consuming and ineffective. For this reason, an approach for monitoring performance of barriers and assessing their influence on the overall risk picture is being developed. This approach aims to support the process of decision making both in the engineering and operational phases. The contribution shows the basic structure of this dynamic risk assessment approach. A case-study on sand erosion issues is taken as representative example. The application of this approach leads, on one hand, to the detailed modelling of safety barriers and their mechanisms and, on the other hand, to the definition of the barriers relative importance at affecting the overall risk picture.

1 INTRODUCTION

The Center for Integrated Operations (IO) in the Petroleum Industry is a research-based innovation centre that aims to develop new methods and tools for the integration of people, organizations, work processes and disciplines through new information and communication technology. For instance, IOs are being developed to improve capture of real-time safety barrier data and to process, visualize and share this information for closer onshore-offshore collaboration and more effective expert support.

One important question that can emerge from the assessment of safety barriers in a plant is how their performance can affect the overall risk picture. A technique capable to assess this and effectively visualize the result would provide an important decision support not only during daily operations but also on the medium term. For example, it would allow defining a maintenance plan by assessing the effect on the overall risk of temporary impairment of specific safety functions.

These are critical questions that industry is trying to answer with various solutions. One example is the Technical Integrity Management Programme (TIMP) by Statoil (Statoil 2013), which focuses on measuring the integrity of the technical barriers, but does not explicitly relate it to the overall risk. Within the IO Center, a tool aiming to continuously monitor risk picture changes and support decision making, named "Risk barometer", has been built (Paltrinieri et al. 2013). This tool is influenced by previous analogous methods, such as the ORIM (Organizational Risk Influence Model) (Øien 2001) and Risk OMT (risk modelling—integration of organisational, human and technical factors) (Vinnem et al. 2012).

As a prerequisite, the Risk Barometer should be based on an existing Quantitative Risk Analysis (QRA), in order to identify the most risk-affecting QRA parameters (e.g. probabilities of failure on demand of safety barriers). Factors describing the condition of barriers, named Risk Influencing Factors (RIF), are then defined for each QRA parameter. A set of risk indicators are finally introduced to measure the status of the various RIFs.

The study this contribution describes initially considers the Risk Barometer approach and adapts it to a specific case-study where no QRA is performed in advance. An alternative and case-specific basic structure is developed by means of expert input and judgment.

The case-study is based on an actual sand erosion issue present in an offshore oil production system. Material degradation due to processes of erosion/corrosion is the main focus. The production system is located subsea and connected to a spread-moored FPSO (Floating Production Storage and Offloading) unit, which is used as a hub, processing the fluids produced from the subsea wells.

In the following sections the case-study and the related scenario are described in detail by means of a bow-tie diagram. A methodology is then proposed for dynamically assessing the risk connected. To conclude, a set of simulation results are shown in order to illustrate the application of the methodology.

2 CASE-STUDY

A bow-tie diagram was used to visualize the case-study (Fig. 1—the terminology follows the one

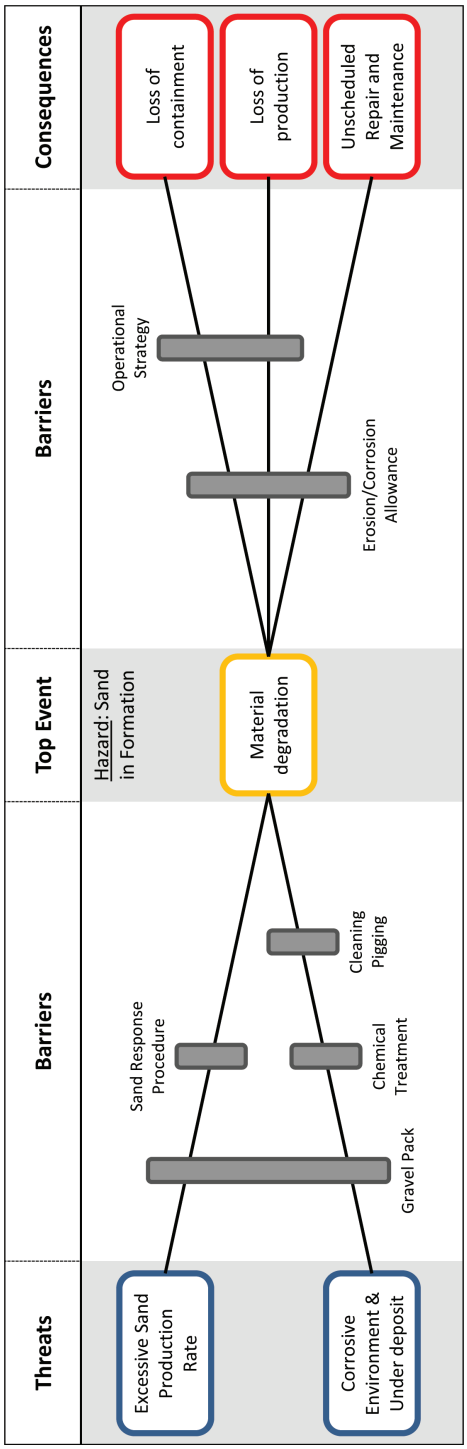


Figure 1. Bow-tie diagram illustrating the case-study (adapted from the result obtained with BowTieXP®).

used by the software BowTieXP®). In fact, the bow-tie technique in its visual form makes an accident scenario easy to understand, and can show what safeguards protect against particular initiating causes (or threats) and loss event consequences (CCPS, 2008).

In this case, the threats are:

- excessive sand production rate;
- corrosive environment & under deposit of sand.

The top event is material degradation due to sand erosion/corrosion. The identified consequences that can derive from sand erosion/corrosion are:

- loss of containment;
- loss of production;
- unscheduled repair and maintenance.

Between threats, top event and consequences, safety barriers are implemented in order to stop the development of the scenario by either preventing or mitigating the events considered. The barriers are described in the following section.

The elements displayed in the diagram do not specifically refer to discrete events, but continuous processes. For instance, the occurrence of material degradation can be better described by a degradation rate than a probability. The definition of a correlation between causes, top-event and consequences is addressed in the following sections.

2.1 *Hazard of sand in formation*

During oil production from a subsea well sand may be produced. In order to control sand formation and retain potential erosion and corrosion of oil production pipelines, several safety barriers are in place.

Material degradation may be caused by sand erosion or corrosion. As shown in Figure 1, two potential threats leading to sand erosion or corrosion are identified. The first threat focuses on excessive sand production rate. This does not only mean that there is an increase in sand production, but also that the velocity of the flow in which sand is carried exceeds a critical threshold. In order to prevent this threat to develop into pipeline material degradation, two safety barriers are in place:

- Gravel pack
- Sand response procedure

A gravel pack is a downhole filter, which is held in place with a properly-sized screen. In case the gravel pack is not enough, and excessive sand production is detected, a specific sand response procedure should be put into action.

Thus sand detectors are considered as a technical measure of the sand response procedure barrier. In this case-study two means for detecting sand production were considered:

1. An Acoustic Sand Detector (ASD) that performs on line monitoring and gives immediate information. It records the noise produced by sand carried in the process flow. The detectors are placed on the outside of the flow line bends and detect the noise made when sand collides with the pipeline wall.
2. An erosion probe, i.e. an metallic surface inserted in the well stream which is physically eroded by sand particles passing. This detector only reports accumulated effects over a longer time period.

The sand response procedure implies that if sand is detected and its rate exceeds a specific threshold, the flow line should be choked back until the sand production rate is acceptable. Generally the acoustic sand detector is used for dynamic monitoring and the erosion probe represents a later confirmation of the result obtained.

As shown by Figure 1, also corrosive environment and sand under deposit can lead to degradation (in this case corrosion) of the pipeline wall. The gravel pack is again indicated as safety barrier because it can prevent sand production and, thus, sand deposit where the flow is slowed down by line bends.

Injection of appropriate chemicals into the fluids in order to inhibit corrosion (chemical treatment) is a safety barrier defined to prevent corrosive environment, which is itself composed by technical and operational measures, such as the equipment used and its management.

"Pigs" are devices that are placed inside the pipe and traverse the pipeline. Thus, pigging is considered as safety barrier because allows cleaning the pipeline from sand deposit.

From a safety point of view, sand production is critical because it is threatening the integrity of the pipeline and to some extent also safety valves. If these threats are not stopped by the safety barriers mentioned, they can lead to material degradation, (shown in the middle of the bow-tie diagram as top event—Fig. 1).

An erosion corrosion allowance is present in the pipeline wall. The thickness is defined also by taking into account these factors. This represents a further safety barrier mitigating material degradation and preventing worse consequences, such as unscheduled repair and maintenance, loss of production or loss of containment.

Operational strategy is also a safety barrier. In fact, change of strategy when a critical situation is acknowledged can be the last option in order to prevent loss of production or loss of containment. For instance, in a condition of highly degraded material, production strategy can be modified and the production rate decreased, in order to reduce the pipeline stress load and avoid the formation of a leak of hydrocarbon into the sea.

3 METHODOLOGY

3.1 *Description of the proposed model*

The bow-tie diagram in Figure 1 was further re-elaborated (Fig. 2) in order to:

- Show the interaction of the threats; excessive sand production rate (T1) is a stand-alone threat, while corrosive environment (T2) and

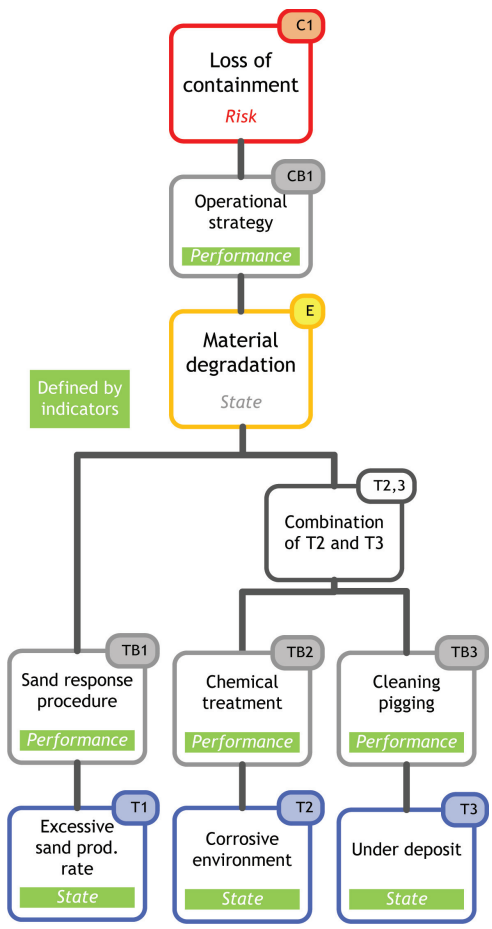


Figure 2. Model structure. The labels indicate both the model elements and their state/performance (Table 1).

sand under deposit (T3) must occur jointly in order to get material degradation.
- Omit the barriers whose performance cannot be controlled (e.g. inherent design issues); gravel pack and erosion/corrosion allowance are passive barriers and for this reason were omitted.

Focus on the worst-case consequence; risk was defined as the risk of loss of containment.

This Figure 2 allowed defining a semi-quantitative model for risk assessment, combining both the assessment of the related threats and the performance of barriers employed. The risk of loss containment is dependent on both the state of the threats and the performance of the barriers (which in turn should stop the threats).

For the development of this model, the Risk Influencing Factor (RIF) approach (Øien 2001a, b) was taken as a reference. For this reason, the main model elements (state of threats and the performance of barriers) are defined by means of indicators, as explained in Table 1 and the following sections.

Once assessed, the state of the threats is expressed on a scale from 1 to 6, where 1 is unlikely and 6 is very likely. This value is then multiplied by a probability of failure of the safety barrier, which is the result of the performance assessment by means of the indicators (Table 1). Thus, if the barrier can completely stop the threat (or the top event if CB1 is considered) the conditional probability will be equal to 0. If the barrier is negligible or impaired, the associated conditional probability will be equal to 1.

While T1 is an independent threat that can lead to material degradation without any other "co-factor", T2 and T3 should occur together in order to result into the top event. Between the two threats there is an "and-gate" and the combination of T2 and T3 is expressed by a weighted sum (Table 1). A weight is assigned to T2 and T3 on the basis of their effect on material degradation. Expert judgment is used for this task.

The state of material degradation is obtained by summing up the two contributions from the two branches (Table 1). This value is then multiplied by the probability of failure of CB1 in order to obtain the risk of loss of containment (Table 1).

Table 1. Definition of model elements.

Model elements	Definition
Threats	The threat state is defined by a set of indicators. The indicators (x_{Ti}) are measured on an arbitrary scale and translated into marks from 1 to 6. $m_{Ti} = \mathrm{M}(x_{Ti})$ A weight (w_{Ti}) is assigned to each indicator and the threat state (T) is obtained by a weighted sum on a scale from 1 to 6. $T = \sum w_{T,i} m_{T,i}$
Barriers	The barrier performance is defined by the performance of the barrier measures, which in turn are defined by indicators. The indicators of each measure ($x_{B,MPi}$) are measured on an arbitrary scale and translated into marks from 1 to 6. $m_{B,MP,i} = \mathrm{M}(x_{B,MP,i})$ A weight ($w_{B,MPi}$) is assigned to each indicator i, and then performance of measure j (MP_j) is obtained by a weighted sum on a scale from 1 to 6. $MP_j = \sum w_{B,MP,i} m_{B,MP,i}$ A weight (w_{Bj}) is assigned to each barrier measure j and the overall barrier performance (B) is obtained by a weighted sum on a scale from 1 to 6. $B = \sum w_{B,j} MP_j$ The barrier performance is translated into a probability of failure (p). $p = \mathrm{P}(B)$
Combination of T2 and T3	A weight (w_T) is assigned to T2 on the basis of its effect on E (material degradation) and the combination of T2 and T3 (state $T_{2,3}$) is obtained by a weighted sum on a scale from 1 to 6. $T_{2,3} = T_2 p_{TB2} W_T + T_3 p_{TB3} (1 - W_T)$
Top event	The state of the top event (E) is obtained by summing up the two contributions from the two branches. $E = T_1 p_{TB1} + T_{2,3}$
Consequence	The consequence risk (C) is obtained by the multiplication of E and p_{CB1}. $C = E p_{CB1}$

3.2 *Assessment of threat state*

Threat state is defined by a set of indicators. These indicators can be chosen among production data, detection results, related barrier demand rate, etc. This type of indicators should be measurable, have some degree of relevance with the threat and indicate the presence of the threat.

However, not all the indicators have the same degree of relevance and reliability. Thus, there may be indicators that are more important than others. For this reason, weights should be assigned to them in order to define the threat state by means of a weighted sum. In this way, the threat state is expressed by a number from 1 to 6 (Table 1).

3.3 *Assessment of barrier performance*

The assessment of barrier performance is based on two activities:

- Definition of the barrier structure (technical and operational barrier measures)
- Identification of suitable indicators

Each barrier is the result of a synergy of various measures. These measures (such as detection or procedure measures) play a part in realizing the task or role of the barrier and their performance is essential for the overall performance of the barrier. The measures of a barrier can be technical or operational and may have a different relative importance in the barrier structure. For this reason, each barrier considered in this contribution was broken down into measures and for each measure a specific weight was assigned.

Indicators should then be defined. This type of indicators focuses on the performance of the barrier measure, i.e. they should be able to show if the measure can deliver the desired outcome or if the measure has failed in delivering it. They should be measurable values and weights should be defined for them, in order to consider also their relative importance at describing the measure performance. In fact, also in this case indicators may have different grades of relevance and reliability.

The indicators are used to assess the barrier measure performance by means of a weighted sum. The performance values of the single measures are finally composed in a new weighted sum in order to define the overall performance of the barrier (Table 1).

3.4 *Weighting*

The assessment of the relative importance of indicators and barrier measures is based on expert judgment. Despite the fact that these elements are organized according to a hierarchical structure (as the Figs. 2–4 show) and their relative importance is defined on the basis of their effect on the governing (upper) element, the experts involved in this phase of the analysis may find it rather challenging and time-consuming. In order to facilitate this process, the technique of

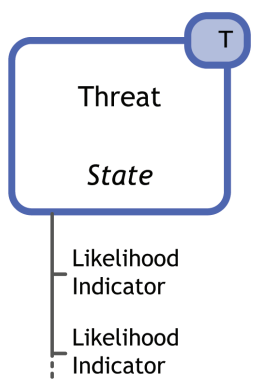


Figure 3. Threat structure.

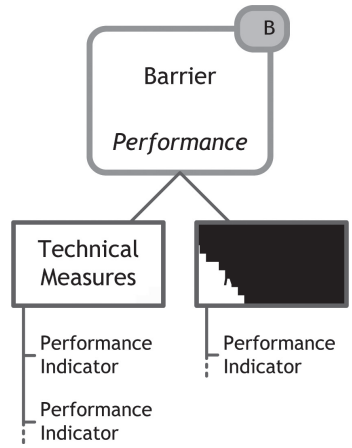


Figure 4. Barrier structure.

Table 2. Scale of relative importance (adapted from Saaty 1983).

Intensity of relative importance	Definition	Explanation
1	Equal importance	Two activities equally affect the governing level above.
3	Moderate importance of one over another	Experience and judgment slightly favor one activity over another.
5	Essential or strong	Experience and judgment strongly favor one activity over another.
7	Very strong importance	An activity is strongly favored and its dominance is demonstrated in practice.
9	Absolute importance	The evidence favoring one activity over another is of the highest possible order of affirmation.
2, 4, 6, 8	Intermediate values between the two adjacent judgments.	When compromise is needed.

If element A dominates over element B, then the whole number integer is entered in row A, column B and the reciprocal (fraction) is entered in row B, column A. If element B dominates element A then the reverse occurs.

Analytical Hierarchy Process (AHP) (Saaty 1983) can be applied.

AHP can help in defining the relative weights of hierarchically organized elements by means of pairwise comparisons among the elements. This produces a square matrix of judgments. The pairwise comparisons are done in terms of which element dominates another. These judgments are then expressed following the judgment values shown in Table 2 (these judgment values can be used also in the combination of T2 and T3). This produces a square matrix of judgments.

Finally, the calculation of the square matrix eigenvector is composed by the relative weights of the elements considered. However, before using the weights, a consistency test should be performed, as indicated by Saaty (1983) and Alonso (2006).

4 RESULTS

A workshop session with personnel from a major oil company allowed the completion of the model structure. A set of indicators was defined for each threat and a structure with specific technical and operational measures were outlined for each barrier of the case-study described. Moreover, weights were assessed on the basis of expert judgment. Table 3 lists all these elements. For the sake of brevity, only some examples of the indicators used are reported in Table 3.

The model was applied in two different conditions (represented by the times t_1 and t_2) with different indicator values. In the first case (t_1), the values of the indicators are completely random and can possibly simulate an average condition of the system. In the second case (t_2), the representative indicators shown in Table 3 describing the threat T1 (excessive sand production rate) and the related barrier TB1 (sand response procedure) were given values between 5 and 6 on purpose, in order to simulate a critical condition of sand production. Moreover, the barrier CB1 was defined as poorly performing. All the other input data, such as weight were assessed on the basis of expert judgment and kept constant.

The state of threats and top event, the performance of the barriers and the risk of loss of containment are visualized by means of a color scale, as it is planned to be performed by the risk barometer graphical interface:

- 1–2 White (W)
- 2–3 Green (G)
- 3–4 Yellow (Y)
- 4–5 Red (R)
- 5–6 Dark Red (DR)

Table 3. Model simulation at the times t_1 and t_2.

Model elements	Indicators	t_1	t_2
T1, Excessive sand production rate		Y	R
	Acoustic sand detection	5.51	5.70
	Erosion probe detection	2.38	5.50
	Daily output of production data	2.34	4.95
T2, Corrosive environment		Y	G
	Corrosion model results	3.03	2.84
T3, Under deposit		Y	Y
	Daily output of production data	4.26	2.49
	Inspection results	3.54	4.32
TB1, Sand response procedure		G	R
Acoustic sand detector	Age of the system	2.07	5.22
Erosion probes	Loss of signal	3.53	4.89
Manual well-flow sampling	Availability of laboratory system	5.43	5.97
Response to sand detection	Formalization and availability of procedure	2.18	5.00
TB2, Chemical treatment		Y	R
Active corrosion inhibition system	Capacity of injection	3.28	1.96
Managing chemical treatment	Competence and training	1.46	6.00
TB3, Cleaning pigging		Y	R
Maintenance	Compliance to schedule	2.69	4.39
Managing pigging/equipment selection	Experience	2.69	3.52
$T_{2,3}$, Combination of T2 and T3		W	G
E, Material degradation		G	DR
CB1, Operational strategy		Y	R
Regular inspection	Overdue inspection	2.60	5.76
Unscheduled inspection	Formalization and availability of procedure	3.17	5.30
Production strategy	Competence and training	5.05	4.77
C1, Loss of containment		W	R

5 DISCUSSION

The results illustrated by Table 3 give two representative examples of how the proposed model can be applied to assess the risk of loss of containment on the basis of the state of the threats and the performance of the barriers.

In the first case (t_1), a random value from 1 to 6 was defined for each indicator. This simulation does not only represent a possible average condition of the system, but shows also how threats with a relatively critical state (all the threats have a yellow state—Table 3) can be mitigated by the safety barriers in place.

In fact, the performance of the barrier TB1 is satisfactory (green performance) and can effectively mitigate the threat of exceeding sand production rate. The performance of the barriers TB2 and TB3 may be improved (yellow performance), but it is enough to mitigate the two threats, which in turn have only a partial weight on $T_{2,3}$. For this reason, this last element has an optimal state (white state).

In t_1 the state of material degradation is acceptable (green state) and this leads to an optimal value of loss of containment risk, described by the white color.

In the second case (t_2), a value between 5 and 6 was given to the representative indicators shown in Table 3 describing the exceeding sand production rate and the related barrier. Thus, T1 and TB1 have respectively a very critical state and performance (red state and performance—the state is not dark red because other indicators with random values were also considered for T1 and TB1). This very critical condition is reflected by the state of material degradation (dark red state because it consider also the contribution of T2 and T3) and the overall risk of loss of containment (red risk because the performance of the barrier CB1 is very critical itself and is not enough to mitigate E).

These two examples demonstrate the importance of threats and barriers. The firsts are a serious issue that should be adequately treated. The seconds are part of the treatment strategy and their performance is essential for the prevention of the overall risk.

5.1 *Future developments*

This study is still ongoing and there are several aspects that need further development and may become interesting topics for future research.

First of all, aggregation of data may lead to several issues. In fact, the indicators defined are collected on different levels of the system and in some cases represent only a part of it. For instance, the acoustic sand detection is performed on the well level, the erosion probes are applied on the flow-line level and the daily output of production data addresses the whole system. It should be investigated what is the best option for the aggregation of indicators. For example, should these indicators on the well/flow-line level aggregated into one indicator or considered singularly?

Moreover, the combination of T_2 and T_3 ($T_{2,3}$) is carried out by means of a weighted sum. This approach is justified by the fact that the model should be kept relatively simple and directly understandable by the operative personnel. In fact, operators would possibly trust more the risk prediction of a model they can understand than a black-box model based on complex data elaboration. However, this choice should be demonstrated by appropriate on-field tests.

Finally, the gravel pack and the erosion/corrosion allowance are not considered in the analysis because there cannot be a direct control on them and their performance cannot be actively improved if needed. Thus, this model makes the assumption that these two barriers performance is constant and does not affect the dynamic assessment of loss of containment risk. However, the ageing of the two systems is an important aspect to be considered. In particular, if the erosion/corrosion allowance is in a critical state, decision-makers will have to take different decisions and properly respond to this serious issue.

For this reason, these two barriers should be re-considered in future research activities, together with an appropriate modelling of their degradation with time. This would produce a more reliable prediction of the risk of loss of containment and improve the dynamic modelling of the system.

6 CONCLUSIONS

A dynamic method is described to follow up on the current risk level of an activity, by utilizing indicators to assess both the current state of the threats and performance of relevant safety barriers to prevent/mitigate the effect of unwanted events/scenarios. This method aims to give the personnel of oil companies a support in critical decisions concerning safety barrier management.

An example is given, considering the threats of erosion/corrosion in the petroleum production. This example shows how the proposed model deals with different operative conditions and how the risk of loss of containment is affected by them. In this way, the importance of both the state of the threats and the performance of the barriers is demonstrated. An effective action of risk prevention should be then focused on both of them by giving priority to the improvement of poor barriers connected to critical threats.

Finally, some related topics for future research activity were identified. In fact, this is an ongoing study and there is still room for improvement. For this reason, future developments of this model are being planned, in order to refine what was outlined in this first phases and further investigate a topical

and challenging field such as real-time assessment of risk.

ACKNOWLEDGMENTS

The authors acknowledge the colleagues of the Center for Integrated Operations in the Petroleum Industry who are contributing in the realization of this project.

REFERENCES

Alonso J.A., 2006. Consistency in the Analytic Hierarchy Process: a New Approach, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 14: 445–459.

CCPS e Center for Chemical Process Safety. 2008. *Guidelines for hazard evaluation procedures*. New York, USA: America Institute of Chemical Engineers (AIChE).

Øien K., 2001a. A framework for the establishment of organizational risk indicators, *Reliability Engineering & System Safety*, 74(2), 147–167.

Øien K., 2001b. Risk indicators as a tool for risk control, *Reliability Engineering and System Safety.* 74(2): 129–145.

Paltrinieri N., Hauge S., Dionisio M., Nelson W.R., 2013, Towards a dynamic risk and barrier assessment in an IO context. In Steenbergen R.D.J.M., van Gelder P.H.A.J.M., Miraglia S., Vrouwenvelder A.C.W.M (eds.), *Safety, Reliability and Risk Analysis: Beyond the Horizon*, CRC Press, Boca Raton, FL.

Saaty T. L., 1983, Priority Setting in Complex Problems, *IEEE Transactions on Engineering Management*, 30: 140–155.

Statoil 2013. Annual Reporting Compendium, Annual Report/2012, Statoil.

Vinnem J.E., Bye R., Gran B.A., Kongsvik T., Nyheim O.M., Okstad E.H., Seljelid J., Vatn J., 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations, *Journal of Loss Prevention in the Process Industries*, 25(2), 274–292.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Joint applicability test of software for laboratory assessment and risk analysis

D.N. Pluess & Th. Meyer
Group of Chemical and Physical Safety, Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

J. Mašin, P. Mikulášek & M. Ferjenčik
Institute of Energetic Materials, University of Pardubice, Pardubice, Czech Republic

ABSTRACT: Most of the available risk management methods are not directly applicable to academic research laboratories. One solution to systematically perform risk analyses in this environment is the Laboratory Assessment and Risk Analysis (LARA) method. This method was developed to allow untrained personnel to identify of possible risks and rank them according to their importance. The purpose of this study was to find out, if this method can be used as a holistic risk management technique in different environments, and which are the differences when comparing the results to other, well-established risk analysis techniques. The risk analyses were performed at two European universities and for various procedures. The results show, that the LARA procedure ismore easily performable and giving more adequate results than the other methods. Being applicable by non-experts, this holistic risk analysis method for research laboratories can help to reduce the accident rate in the academic environment.

1 INTRODUCTION

In most sectors of industry, the rate of occupational accidents decreased during the past decades. This fact is due to intensified efforts in occupational safety as well as more strict regulations and laws. Risk management techniques helped to guide those efforts in the desired direction, since they help to allocate the measures according to the relative importance of risks. Most of those methods originate from a specific field of application and are suited for the demands of this field (e.g. Hazard and Operability studies (HAZOP) for the chemical industry (Bluvband et al. 2004)). For academic research laboratories, such a specific technique was never developed; existing methods are often only working for a definite application and cannot be used to perform a risk analysis in different fields (Pluess et al. 2013). Since improving occupational safety gained more importance at universities after various accidents (Marendaz et al. 2013), there is a need for specific risk management technique for research laboratories (American Chemical Society, 2013).

Various solutions were presented in the literature (Kremer et al. 2009, Langerman 2009). However, those methods are still too specialized to serve as a universal risk analysis method for academic research and teaching laboratories (Pluess et al. 2013). A new approach to fulfill the demands of academic research is the Laboratory Assessment and Risk Analysis (LARA) method (Ouedraogo et al. 2011). This method was developed at the Ecole Polytechnique Fédérale de Lausanne (EPFL) to analyze and manage risks even for non-experts and facilitate the risk management process at universities. One of the main features of LARA is taking into account the special setting of this environment (e.g. high personnel turnover, emerging technologies, etc.) and including synergies between different risks (Pluess et al. 2013).

Since the method was developed based on safety regulations of EPFL and originates from its safety culture, the feasibility of LARA to other environments was not demonstrated yet. For the further development and the improvement, the adaption to other universities is a crucial element. The use of LARA at other universities can help to find improvement potential and is able to show if untrained personnel with different occupational safety background can fully benefit of this risk management method. For this reason, joint tests were performed at the Institute of Energetic Materials at the University of Pardubice (Czech Republic) and the Institute of Chemical Sciences and Engineering (ISIC) of EPFL (Switzerland).

The purpose of this study is to answer following question: "can the LARA method be used as a holistic risk management technique in different academic environments and what are the main differences when comparing to the results obtained by industrial risk analysis techniques?" In order to answer these questions, risk analyses of different procedures were performed using LARA, Failure Mode, Effects, and Criticality Analysis (FMECA), and HAZOP. The experiments analyzed are standard operations performed at University of Pardubice and at EPFL. The main differences of the results using the different methods will be pointed out and compared.

2 METHODS

In order to compare the results of LARA with well-established risk management methods, two examples were selected: one from the University of Pardubice and one from EPFL. To have a variety of laboratory tasks, both chemical experiments and routine tasks were considered in the comparison. The first example was analyzed using the LARA method and a HAZOP procedure, whereas the second example was analyzed using the LARA method and the FMECA procedure. Both of these risk analysis procedures are widely acceptedtools to identify and manage risks (Bluvband et al. 2004).

The joint tests described in this article are performed under conditions that simulate the environment for which the method is intended. The risk evaluations were performed and guided by a group of scientists, being familiar with the methods and having experience in performing FMECA and HAZOP procedures. For the LARA method, those scientists had a short introduction, but no information about the principles of the method. This was intended, since non-experts are the designated users of the LARA method. The scientists involved in the experiments provided the analysts with all information necessary, including details about the laboratory environment.

The test results highlight the different aspects of this new method to assess laboratory risks. The results do not only focus on the successfully evaluated risks, but also on the other factors of the evaluation, such as prerequisites and effort to perform the analysis. The tests provides us with answers for questions whether if the LARA method is easily performed, how quick it can be completed and if it is capable to uncover all risks connected with an experiment. In this article we focus on identification and evaluation of the risks; we omit the aspect of applying corrective measures, which is important part of risk analyses, but is not as relevant for this comparison.

2.1 *HAZOP*

The HAZOP technique is as systematic approach to investigate the processes by determining possible deviations from the process intentions and consecutive effects on whole facility. Its strength is in dividing assessed process in the small sections called nodes and thus ensuring examination of each part of the system. The nodes are analyzed by a small multi-disciplinary team, whose members should be able to answer the most questions about given issue on spot. The members have the authority to recommend anyneeded changes in design (Dunjoa et al. 2010).

This scenario-based method relies on using guidewords (e.g. as, no, more, less) in combination of process parameters (such as temperature, pressure, flow). The aim of this combination is to reveal deviations from the process intention (e.g. no flow, more temperature, less pressure). There is a defined list of guidewords, which are applied on each examined node. Once deviations are determined, their possible causes and consequences are discussed by the team of experts. For both cause and consequence safeguards must be identified. The safeguards are corrective measures that could prevent, detect or mitigate the hazardous situation. If there are not feasible safeguards, a change in intended design must be considered (Guidelines for Hazard Evaluation Procedures, 2011).

2.2 *FMECA*

The FMEA systematically analyze a system for potential failures and their consequences on the system. The procedure divides a process or a system into specific components according to their function. Then, the possible failure modes are determined on every component. Failure mode describes how equipment could fail, what will happen if operated improperly and how the failure could cause an accident or contribute to accidents occurrence. Once the failure modes are determined, the systems response to the failure leads to a certain effect. The effects provide a feedback for determining where system changes or improvements should be made (Guidelines for Hazard Evaluation Procedures, 2011). Each individual failure is considered independently without a relation to other failures in the system, except for the subsequent effects it can produce. Results of this procedure are qualitative unless FMEA is extended to FMECA by including the criticality of the failure mode; the priority ranking is based on the failures severity and their probability (R.I. Wagoner 1988). FMECA uses quantitative or semi-quantitative scales to describe the likelihood and impact of a potential incident. After assigning likelihood of occurrence and impact values to each incident, a

matrix is used to prioritize incidents importance (W.E. Jordan 1982).

2.3 *LARA*

During the past several years, various severe accidents (injury and death of scientists, financial losses, and interruptions of the scientific research as consequences) happened at different universities worldwide (Marendaz et al. 2013), emphasizing the need to improve the occupational safety and health in this environment. Differences between research and industrial environment (e.g. equipment and processes at development stage, high turnover of collaborators, scarce statistical data on reliability and accidents) made attempts difficult to implement existing risk analysis methods and are not leading to useful results (Ouedraogo et al. 2011). Solutions for this problem were already presented in the literature, e.g. for biology (Kremer et al. 2009) and chemistry (Langerman 2009). However, most of them focus on a narrow field of scientific research, such as biology. In order to tackle this problem, EPFL's Group for Chemical and Physical Safety (GSCP) is currently developing a holistic risk analysis technique for the academic research setting, called LARA. The goal of this development is to design a risk management method with following properties (Pluess et al. 2013):

- Easily performable by non-experts.
- Less resource-demanding compared to other available methods.
- Semi-quantitative and improved risk estimation.
- Consider the special conditions encountered in academic research laboratories.

First results of risk analyses for different sectors of the academic research environment were already presented by (Ouedraogo et al. 2011). Based on the development, a web application software was developed. The workflow of the LARA method is presented as following:

1. Risk identification: every element (equipment, chemicals and activities) involved in a process is determined. Based on these elements, each hazard present in this process is selected out of a database. This database contains a large number of different hazard categories, based on regulations, past accident data, measurements and expertise. Additionally, the users of the software are able to suggest hazards and expand the database.
2. Risk description: the semi-quantitative risk estimation is a crucial element to reach the goals of the method. In such an estimation method, verbal statements are used to describe the risk factors. According to these verbal statements, a value on a numerical scale is assigned for each hazard. For all the variables a scale of integer numbers between one and five was used. LARA uses four different main factors to describe and estimate the risk related to a hazard: severity, probability, detectability and worsening factors.

   To improve the risk estimation and to take into account the special conditions in academic research laboratories, GSCP introduced the concept of worsening factors (Ouedraogo et al. 2011, Pluess et al. 2013) in addition to the commonly used elements in different risk analysis techniques (severity, probability and detectability). This new concept integrates specificities of research laboratories, which can aggravate the outcome or the probability of an accident. GSCP classified this worsening factors into three groups: general worsening factors are those types of influences which are not directly related to a certain kind of hazard, but which can influence the probability, the severity or the detectability. Hazard-specific worsening factors are directly influencing a certain risk. Synergetic worsening factors are describing synergies between two risks, in particular situations where a risk can be worsened or enabled by the presence of another risk (Pluess et al. 2013).
3. Risk calculation: GSCP developed a new method using Bayesian networks to calculate a risk index called Laboratory Criticality Index (LCI) for each hazard. This improved method is based on Bayesian networks, being used in various applications of risk management (Marhavilas et al. 2011). Bayesian networks are using probability tables (Fenton and Neil 2012) with different states for each node of the network. For LARA, these states represent the different verbal statements for a risk factor. The probability tables used for the factors were created using a ranked node concept described by Fenton et al. (2007). This concept helps to generate the probability tables using truncated Gaussian probability distributions. For better comparison of the differentrisks, the LCI is finally calculated as single crisp number (this calculation is based on a method presented by Yang et al. (2008)). This calculation approach based on Bayesian network is capable of overcoming various disadvantages of other risk estimation methods used in semi-quantitative risk analysis by giving reliable results with a constant variance through the whole spectrum of the results (Pluess et al. 2013).
4. Risk mitigation: Once the LCI value for each hazard is determined, the risk mitigation takes place. The board of the institution sets the limits, which LCI values are not acceptable and which are acceptable. For risks with an acceptable LCI value, no measure is necessary to pro-

ceed with the experiment. The unacceptable risks are treated regardless of the costs and the effort necessary and are re-evaluated. The risks, which are neither acceptable nor unacceptable, should be reduced As Low As Reasonably Practicable (ALARP). Since the academic environment has different demands than the industrial sector, the choice of corrective measures is realized using an allocation matrix. With this matrix, other aspects, such as acceptance and feasibility of the corrective measures are taken into account as well.

3 RESULTS

3.1 *Example 1: Synthesis of methyl nitrate*

Description of process: There is an intention to produce methyl nitrate for testing reasons at the Institute of Energetic Materials of the University of Pardubice. This uncommon, sensitive liquid explosive should be produced regularly in amounts of several kilograms. The synthesis and the product properties are well described in literature (Black 1943). Although the process itself does exhibit difficulties, it requires a certain level of experience. The laboratory intended for the preparation of this explosive does not differ much from standard laboratories equipped for organic synthesis. A couple of tests have been already performed in smaller amounts.

The synthesis is carried out in a beaker. A mixture of nitric and sulfuric acid is poured into a beaker. Methanol is then added dropwise while the reaction mixture is stirred well and cooled in an ice bath. The temperature of the reaction mixture must be kept between 15–20°C. When the whole amount of methanol is added, the reaction mixture is left for five minutes at room temperature. Methyl nitrate is separated from the acid residue, washed with cold water and sodium carbonate solution.

An accident occurred during one of the test synthesis; a sudden decomposition of the product occurred. Later it was discovered that this was caused by the presence of ricin oil in methanol, which was used as a key precursor for methyl nitrate. It is highly probable that if the decomposition would have occurred in larger amounts, it would have caused an explosion.

Safety aspects of the synthesis were discussed with the leader of the project. According to his statement the most important risk is connected with sensitivity of methyl nitrate even a small friction in a part of the equipment used for the synthesis could lead to an explosion. The accident mentioned above emphasizes that only pure chemicals (p.a.) should be used for this synthesis. The acids and toxic materials present during this synthesis may lead to increased risks as well, but can be reduced to minimum by appropriate safety measures.

HAZOP results: The HAZOP analysis was performed according to BS IEC 61882:2001 by the team consisting of organic chemists, explosives and safety engineering experts. The synthesis was divided into six nodes: methanol nitration, stirring, cooling, pouring into separation funnel, separation and washing. Overall eighty-eight deviations were considered. Table 1 shows the six most serious hazards of the methyl nitrate synthesis. However HAZOP does not provide the quantitative risks evaluation and prioritization, therefore the relative importance of risks were chosen according to the experts opinions. The analysis is well performable on a laboratory scale, although is designed mainly for industrial environment. HAZOP gives appropriate results and reflects the experience and predictions of experts. Despite the applicability and realistic results, the procedure is relatively complicated, time and resources consuming and not suited to be performed by non-expert.

LARA results: LARA analysis performed by the same scientists revealed that all 15 identified risks arise from hazardous properties of the involved substances. The relevance of the analysis results is given by risk prioritization, which corresponds to the particular laboratory practice. The procedure determined that methyl nitrate explosives properties have the highest risk priority. Among

Table 1. Most important risks according to HAZOP.

No.	Guideword	Element	Deviation	Possible causes	Consequences
1	More	Methanol	Faster dropping	Funnel valve leaky	Exothermic reaction, explosion
2	As well as	Methanol	Impure methanol	Error at supplier	Exothermic reaction, explosion
3	As well as	Separation funnel	Valve grease washout	Inappropriate grease	Exothermic reaction, explosion
4	No	Stirring	No stirring	Stirrer failure	Local overheating, explosion
5	Other than	Pouring	Reaction mixture poured out	Personnel failure	Irritation and intoxication
6	No	Separation funnel	Valve grease not applied	Personnel failure	Explosion caused by friction

the risks with highest importance belongs methyl nitrate toxicity, corrosive effects of nitric acid and methanol flammability. All these risks are mentioned in laboratory rules and personnel is periodically familiarized with them during safety training. The most important risks according to this analysis are presented in Table 2.

Comparison: Table 1 and Table 2 reveals the most important hazards of this activity based on the results of both analyses. Almost all deviations identified by HAZOP lead to exothermic reaction and/or explosion of methyl nitrate. According to LARA, explosive properties of methyl nitrate have the highest priority. However these results do not reflect the experiences of the experts who performed HAZOP analysis, thus it is not so clear in which particular situation methyl nitrate explosive properties could exert. Remaining risks determined by LARA procedure are connected with the effect of involved substances on the personnel. This is in agreement with the deviation pointing out leakage of the reaction mixture identified by HAZOP.

3.2 *Example 2: Medium scale purification of solvents*

Description of process: the second example, which was chosen to test the LARA method, is the purification of larger quantities of solvents. This process is realized at the laboratory of asymmetric catalysis and synthesis (LCSA) at EPFL. Large amounts of solvents, mainly ethyl acetate and pentane, are used in this laboratory for chromatographic purposes. Since the commonly available solvents are not sufficiently pure enough, a further purification is performed directly in the lab. The task is realized according to a planning, which obligates each member of the group to perform this process periodically. Even thought the task is planned and recurring, there is no Standard Operation Procedure (SOP) available.

Table 2. Most important risks according to LARA.

No.	Risk
1	Explosion caused by methyl nitrate
2	Intoxication (inhalation) caused by methyl nitrate
3	Intoxication (skin) caused by methyl nitrate
4	Irritation (skin) caused by methyl nitrate
5	Intoxication (oral) caused by methyl nitrate

For the purification, a Heidolph LABOROTA 20 medium scale rotary evaporator was used. The purification is realized several times per week with a quantity between 5 L and 10 L of solvent each time. For the ethyl acetate, the device is heated to 50°C and the pressure was set to 25 kPa. For the purification of pentane, the device was heated to 50°C and the pressure was set to 95 kPa. Until now, no accidents have occurred. According to the responsible scientist, the main risk in this process is related to the flammability of the solvents. Other hazards related to the chemical properties of the solvents, such as the hazards for the environment or toxicity, are estimated to be negligible.

FMECA results: a team of scientists performed a systematical risk analysis of the most important components using the FMECA method. In total, 29 potential failures were identified and their relative priorities for applying measures were determined. Seven of these failure modes are only influencing the operability itself and are not relevant form a safety point of view. From the remaining 22 failure modes, 6 are related to mechanical operations and the remaining 16 are indirectly related to the hazardous properties of the solvents. Since those properties are not directly evaluated by the procedure, the relative importance and magnitude of the effects remain unclear after the FMECA analysis.

LARA results: the same team of scientists used the LARA method to perform a risk analysis on this activity. This analysis revealed nine different hazards originating from different sources (chemicals and devices). All of those hazards are relevant from an occupational safety point of view. Four of the hazards are directly related to the hazardous properties of the solvents. The other five hazards present according to the LARA analysis are related to mechanical or physical risk.

Comparison: Table 3 shows the most important hazards of this activity based on the results

Table 3. Comparison of the risk priorities in example 2 using LARA and FMECA method.

Hazard	Risk	Priority in LARA	Priority in FMECA
Blast shield	Injuries due to unintended closing	2	1
Lowering mechanism	Injuries due to pinching	2	5
Toxic substance (solvent)	Intoxication by inhalation	1	2/3/4
Irritating substance (solvent)	Eye irritation	3	2/3/4
Flammable substance (solvent)	Fire	5	2/3/4

of both analyses. The most important hazard determined by the LARA method is the toxic properties (aspiration toxicity) of both solvents. In the FMECA analysis, the toxicity is indirectly related to the failure modes with the relative priority 2, 3 and 4 (all those failure modes are leading to leakage of solvent). Based on the FMECA method, the blast shield of the apparatus is the most hazardous element of this process, which is ranked second in the LARA method. The mechanical hazards do have the same importance according to the LARA method, since both do have similar occurrences and exposures. The FMECA analysis however ranked the similar hazards in a different order, even though the hazards are comparable. The FMECA analysis fails to differentiate between the different hazards originating from the chemical properties of the solvent.

4 DISCUSSION

The results of this study suggest, that the LARA can be used as a holistic risk analysis method in the academic laboratory environment. Even though only two examples were examined, the joint test at two universities showed the advantages compared to established risk analysis techniques.

One of the most important features of a risk management method is the capability to identify risks. Since no method is able to identify all the possible risks, an appropriate method should be capable of discovering the most important risks of a process. On the contrary, the more risks a method can identify, the higher is the probability to identify scenarios, which are either highly improbable or of no importance for occupational safety. In the first example, the HAZOP procedure identifies several scenarios, which are influencing the performance of the process, but are not important to the safety of the involved scientists. Such irrelevant scenarios (in terms of safety) can detract from the safety-related relevant scenarios; additionally, they are extending the analysis itself in terms of complexity. The LARA method is capable of identifying the same relevant scenarios as the HAZOP method. Additionally, the method is able of identifying relations, which the HAZOP procedure is not capable of. The same results were shown in the second example, comparing the results from LARA with the ones of the FMECA procedure.

The effort needed to perform a risk analysis is another important aspect, which influences the feasibility of a method. An ideal risk analysis method for academic research laboratories should not require too demanding resources, since both qualified personnel in safety and time is a rare commodity in this environment. The systematic approach of the HAZOP procedure is not complex itself; however, in order to perform the analysis, an experienced user (the HAZOP moderator) needs to participate to find most of the scenarios. In contrast, the examined example showed that the LARA method is more intuitive when performing the risk analysis. Both methods anyhow need expertise about the process, but LARA needs less experience about the risk management method itself.

However, the comparison has shown some limitations of the LARA method as well. The method relies on a database, and is therefore as accurate as the database is. This drawback can be overcome by systematic use of the software at universities in order to fill the databases with possible hazards and risks.

5 CONCLUSIONS

Since there is no dedicated technique, performing risk analysis in academic research and teaching environment is a challenging task. Nevertheless, being aware of the possible risk is crucial in an environment dealing with emerging technologies and equipment in experimental states. Even though the impact might be less significant compared to accidents in the industry, the accident rate is still unacceptably high. To lower this rate, a specific and holistic risk management method serves as an important tool. The LARA method is such an approach; it was developed specifically for the use at universities and research laboratories. Different experiments and procedures, performed at two European universities were analyzed using the LARA method and compared to well-established risk management techniques. This comparison shows the capability of LARA to be used as a holistic approach, used in various fields of research and for various kinds of tasks. The findings in this article emphasizes that an academic environment could benefit from the introduction of this technique. In order to integrate this method to an environment, it should be embedded into an existing safety framework. Further studies will be comparing more examples and the ease of implementing this technique into such an existing safety framework.

REFERENCES

American Chemical Society (2013). *Identifying and Evaluating Hazards Hazards in Research Laboratories*. ACS.

Black, A.P; Barbers, F.H. (1943). *Methyl nitrate, in E.H. Blatt (ed.)*, Volume 2 of *Organic Synthesis*. Wiley and Sons.

Bluvband, Z., P. Grabov, & O. Nakar (2004). Expanded FMEA (EFMEA). In *Reliability and Maintainability, 2004 Annual Symposium—RAMS*, pp. 31–36.

Center for Chemical Process Safety (2011). *Guidelines for Hazard Evaluation Procedures* (3rd ed.). Wiley.

Dunjoa, J., V. Fthenakis, J.A. Vilchez, & J. Arnaldos (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials 173*(13), 19–32.

Fenton, N. & M. Neil (2012). *Risk Assessment and Decision Analysis With Bayesian Networks*. CRC PressINC.

Fenton, N.E., M. Neil, & J.G. Caballero (2007). Using ranked nodes to model qualitative judgments in bayesian networks. *IEEE Transactions on Knowledge and Data Engineering 19*(10), 1420–1432.

Jordan W.E. (1982). Failure modes, effects and criticality analysis. *Proceedings of the Annual Reliability and Maintainability Symposium, San Francisco*.

Kremer, G.G., S. Switzer, & T.J. Ryan (2009). *A Risk Assessment Method and Safety Plan for a University Research Lab*, pp. 263–268. New York: Amer Soc Mechanical Engineers.

Langerman, N. (2009). Lab-scale process safety management. *Journal of Chemical Health and Safety 16*(4), 22–28.

Marendaz, J.-L., J.-C. Suard, & T. Meyer (2013). A systematic tool for Assessment and Classification of Hazards in Laboratories (ACHiL). *Safety Science 53*(0), 168–176.

Marhavilas, P.K., D. Koulouriotis, & V. Gemeni (2011). Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009. *Journal of Loss Prevention in the Process Industries 24*(5), 477–523.

Ouedraogo, A., A. Groso, & T. Meyer (2011). Risk analysis in research environment part i: Modeling lab criticity index using improved risk priority number. *Safety Science 49*(6), 778–784.

Pluess, D.N., A. Groso, & T. Meyer (2013). Expert judgements in risk analysis: A strategy to overcome uncertainties. *Chemical Engineering Transactions 31*, 307–312.

Wagoner R.I. (1988). *Hazards Analysis of Petroleum Systems (HAPS): An Adaptation of the Failure Modes and Effect Analysis (FMEA) Technique*. AREYE Corporation, Friendswood, TX.

Yang, Z., A.K.Y. Ng, & J. Wang (2008). A new risk quantification approach in port facility security assessment. *Transportation Research Part A: Policy and Practice 59*(0), 72–90.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Is a QRA-based method suitable to guide Land Use Planning decisions in India?

A. Sengupta
Faculty of Geo-Information Science and Earth Observation (ITC), University of Twente, Enschede, The Netherlands
European Commission, Joint Research Centre (JRC), Institute for the Protection and Security of the Citizen (IPSC), Ispra, Italy

D. Bandyopadhyay, C.J. van Westen & A. van der Veen
Faculty of Geo-Information Science and Earth Observation (ITC), University of Twente, Enschede, The Netherlands

ABSTRACT: In this paper, we have applied a quantitative risk assessment method to map cumulative risk levels arising from a number of hazardous installations located in Haldia, one of the industrial towns of India. The methodology consists of the following steps: frequency and consequences assessment of the select reference accident scearos; estimation of grid-level population distribution using a dasymetric interpolation approach; and finally risk estimation using both individual and societal risk metric. The risk maps were prepared in using common GIS tools and functions, and their sensitivity to various factors ascertained using uncertainty analysis techniques.

Keywords: industrial accidents; population estimation; societal risk estimation; landuse planning; India

1 INTRODUCTION

Over the last few decades, a number of large-scale industrial accidents have occurred world-wide, resulting in damage and loss of life in the surroundings. Among these events, the Bhopal accident in India (1984) is ranked as the world's worst ever industrial catastrophe. In the neighbourhood of the Union Carbide plant, more than 150 people died within a few minutes because of acute exposure to the highly toxic methyl iso-cyanate gas which had leaked and dispersed into the air; within a few days of the accident more than a thousand people died (Lees, 1996). Amongst many other reasons, lack of restrictions in uses of land in the surrounding of highly hazardous industrial site and presence of densely populated residential areas in close proximity, were reported as the key reasons for resulting into high number of fatalities in Bhopal.

However, even several decades after the Bhopal accident, there has been no significant improvement with regard to management of risk originating from hazardous industries in India (NDMA, 2007). At present, the country is densely populated and is home to about 17% of the world's population in roughly 2% of total available land area. With steady economic development, there has been considerable growth in the manufacturing sector during the last two decades, including a large number of hazardous industries. According to the inventory available with central agencies, as of 2008, there were 1949 Major Accident Hazard (MAH) establishments located in 260 districts (MoEF and CPCB, 2008) and since then the numbers have grown further. Many of these establishments co-locate in industrial towns to take advantage of common infrastructural facilities. 170 such towns were identified to have a cluster of more than 5 MAH units, when the inventory was being undertaken. Acting as engines of industrial and economic growth, these towns often witness steady influx of population thus resulting in increasing levels of risk.

Nonetheless such a situation is not typical of India alone—many industrialized western European countries have encountered similar challenges in the past and evolved systematic methods for assessing risk from hazardous industries which then led to the adoption of suitable risk reduction strategies (Pasman and Reniers, 2013). In order to assess cumulative risk arising from a cluster of hazardous industrial establishments and to evaluate options for area level risk mitigation measures, few studies were carried out in countries like Netherlands, UK and Italy during the 1970's. Some examples of these studies include those undertaken in Rijnmond, the Netherlands, Canvey Island in the UK and the Ravenna area in Italy etc. But then, it is only after the accidents in Bhopal

and Mexico (both happened in 1984), importance of restricting the uses of land around hazardous installations became widely accepted throughout the EU Member States as a measure for limiting the adverse effects of such accidents.

Accordingly, the first EU Directive 82/501/EEC—so called Seveso Directive of 1982, focused on the prevention of major accidents, was amended to the Seveso Directive II (96/82/EC). Following the Directive II, EU Member States have laid down different approaches for risk assessment and acceptability or tolerability thresholds in accordance to their political, cultural, technical, legal and societal backgrounds (Christou, Struckel, et al., 2006). These methods range from a consequence-based approach to a risk-based approach based on results of Quantitative Risk Assessment (QRA) as practiced in the Netherlands and the UK (Hauptmanns, 2005). Countries like France and Italy have formulated a hybrid approach as a combination of both approaches (Cozzani, Bandini, et al., 2006; Taveau, 2010).

In India, though certain regulations deal with the safe siting of hazardous industries, but the legal provisions often do not provide any specific criteria which can guide landuse planning decisions. Section 41 A of the Factories Act (MoL, GOI, 1987) requires that the location of hazardous industries has to be evaluated from the safety point of view by a site appraisal committee; however fails to provide a mechanism through which such siting decisions can be linked to landuse planning considerations for an industrial area. Although the EIA Notification (MoEF, GOI, 2006) does provide the scope for assessment of risk originating from new hazardous industries, but in practice these EIA studies seldom evaluate the alternative sites based on risk contribution to the neighbourhood communities or provide recommendations for mitigating offsite consequences from potential accidents. Besides, the Central Pollution Control Board (CPCB) of India prepared the 'Zoning Atlas for Siting of Industries' taking environmental considerations into account, but risk is yet to be factored into criteria for zoning of an industrial area (Punihani, Ravi, et al., 2002). The Zoning Atlas even fails to provide a linkage to the existing landuse planning framework as proposed by the Urban Development Plans Formulation & Implementation (UDPFI) guideline (MoUA&E, GOI, 1996). Later, at the Second India Disaster Management Congress (2009), a consensus was reached on the need for adoption of landuse planning principles as a strategy for risk reduction and mitigation (NIDM, 2009).

However, for the adoption of a systematic approach for risk informed landuse planning in any industrial town, the availability of information on the hazards present in industries and the vulnerability in the surrounding residential areas are vital. In India, an effort to consolidate such information was made through the Risk Management Information System (RMIS) which is capable of storing spatial and related attribute data of industries, including nature of the chemicals that they stored or handled, storage conditions, also information about vulnerabilities in terms of exposed buildings and population at different time periods (Bandyopadhyay, Sengupta, et al., 2011).

The key objective of this research is to apply a methodology based on Quantitative Risk Assessment (QRA), with necessary adaptation, for estimating and spatially representing cumulative risk originating from a cluster of hazardous industries, based on spatial and related attribute information available in the RMIS database. In doing so, we evaluated whether techniques that have been developed and applied in the Netherlands or the UK, could suitably be adapted to an Indian context, using simple GIS tools and techniques. In this study, we have calculated cumulative risk levels, taking into consideration reference accident scenarios from several hazardous units, and spatially overlaying them to arrive at a measure of risk in terms of probable fatalities to resident population. This method can result in the formulation of deterministic risk metrics based on scientific rationale, which can then be used to guide risk informed landuse planning decisions for the area in question.

2 STUDY AREA

The study was carried out in Haldia, near the metropolitan city of Kolkata in West Bengal. The Haldia industrial area, one of the largest industrial areas in the eastern part of India, is supported by a large port complex and other infrastructural facilities (Fig. 1). Presently there are 42 industrial units, of which 17 are identified as MAH industries according to the Manufacture Storage and Import

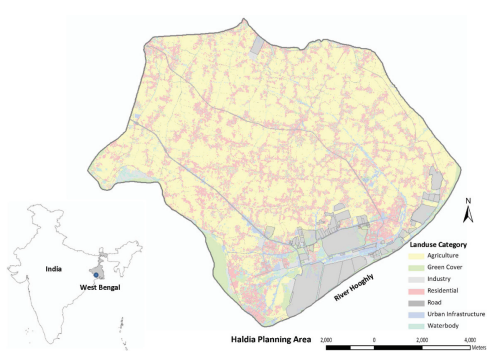


Figure 1. Location of Haldia in India.

of Hazardous Chemicals (MSIHC) Rules 1989 and subsequently amended in 2000 (MoEF, GOI, 2000). Several new industries are also planned in this area. These industrial units are juxtaposed with residential areas with a total population of about 170,000 persons (as per Census 2001), including a large area with informal settlements in close vicinity of these hazardous industries.

3 METHODOLOGY

In this research, we applied a QRA-based approach to estimate the risk originating from hazardous industries for surrounding communities and also to assess the degree of effectiveness of such a risk measure for guiding the landuse planning decisions in the area. In the following sections, the steps are described.

3.1 *Scenario selection*

An accident scenario is one of many specific situations that might evolve at the end of an accident sequence. Here, we have considered eight accident scenarios of Vapour Cloud Explosion (VCE), Boiling Liquid Expanding Vapour Explosion (BLEVE) and toxic release events originating from different hazardous industries located in the study area (Fig. 2). The as 'reference scenarios' were selected with an inherent assumption of having the potential of causing Maximum Credible Loss (MCL) (Khan and Abbasi, 2002) as identified on the basis of facility level risk assessment (Table 1).

For each scenario, possible release types for example pipe rupture, formation of holes in pressurized vessels, major or catastrophic failure etc. were identified which can cause in high loss of life in the surroundings. To ensure that the method remains workable, we propose that a select number of credible accident scenarios per industry, which may lead to potential offsite consequences, be considered.



Figure 2. Location of storages for reference scenarios.

Table 1. Scenario description.

ID	Installation	Containment	Frequency*	Capacity
A	Tank	Motor spirit	$5 \cdot 10^{-6}$ (1)	4200 MT
B	Tank	Ammonia	$4 \cdot 10^{-4}$ (2)	10000 MT
C	Tank	Motor spirit	$2.5 \cdot 10^{-3}$ (1)	24150 MT
D	Tonner	Chlorine	$4 \cdot 10^{-6}$ (3)	1MT
E	Tank	Motor spirit	$1 \cdot 10^{-4}$ (1)	xx
F	Bullet	Propane	$5 \cdot 10^{-6}$ (4)	160 MT
G	Sphere	Butane	$9 \cdot 10^{-7}$ (5)	915 MT
H	Bullet	Butane	$1 \cdot 10^{-5}$ (4)	30 MT

*Numbers in the brackets are corresponding references listed at the footnote.

3.2 *Assigning frequency and probability*

Once the possible scenarios are selected, the next step in QRA requires the estimation of their frequencies. However a review of several industry-specific risk assessment reports of MAH establishments in Haldia point to an absence of any definitive estimate of failures that could result in a major accident with potential offsite consequences. Even at a broader level, no such failure frequency statistics is also known to exist in India. As an alternative, we have used generic failure-frequency databases, such as the TNO's Purple Book, the HSE's Failure Rate and Event Database (FRED) etc. The assigned frequency for the above mentioned scenarios from the available HSE's Failure Rate and Event Database is presented in Table1.

Additionally, in contemporary QRA methodology, the potential incidents for which data is available from failure-frequency databases are further analyzed to obtain the conditional probabilities of a range of possible accident sequences. However, in the present research, the probability of an accident sequence was considered to be equal to the probability of the initiating event (i.e., no mitigation measures were considered) due to the lack of information.

3.3 *Consequence assessment*

The consequence assessment involves determining the impact of an event in terms of its physical extent

[1]Derived from historical data by Glossop (HSE internal report: RAS/01/06); pp. 9.
[2]Documented in a HSE internal report (RAS/00/10) by J. Gould; pp.14.
[3]Reported in the Major Hazard Assessment Unit Handbook; pp. 23.
[4]Documented in a HSE internal report (RAS/06/04) by Keeley and Prinja; pp. 33.
[5]Proposed by M. Selway, 1988; pp. 26.

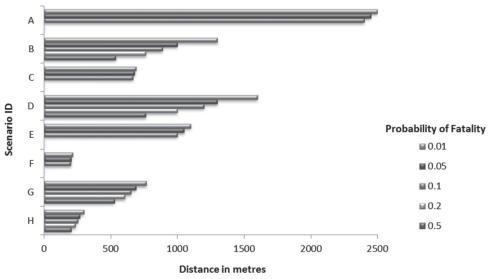


Figure 3. Effect-distances of the reference scenarios.

and severity (Lees, 1996). The physical extent of an accident scenario usually involves the calculation of the effect-distance (i.e. maximum distance with certain intensity) from the source within which people might get affected. The severity of an event is expressed as the level of harm to people such as injury or fatality. Existing QRA approaches generally apply two sets of models for estimating the consequences of an accident scenario: a mathematical model to predict the physical effect (i.e. thermal radiation, overpressure and toxic dose) of an accident and vulnerability model to estimate the impact of an accident on humans (Fabbri and Contini, 2009).

In this research, physical effects of the reference scenarios were calculated using ALOHA[6], one of the widely accepted atmospheric dispersion model used for evaluating releases of hazardous chemical vapors, including toxic gas clouds, fires, and explosions. For calculation purpose, we used data about the hazardous facilities, as obtained from the RMIS database and the most frequently occurring atmospheric condition with an average wind speed of 3.0 m/s, 35°C temperature and stability class of D as input parameters.

The severity of the accident scenarios was estimated in terms of fatalities that may because due to effects of thermal radiation, overpressure wave or concentration of toxic substances. The damage potential in terms of death of a non-protected person from such phenomena was estimated based on threshold values used have been derived from Probit functions as represented in the following equations:

Thermal Radiation:

$$Pr = -14.9 + 2.56 \ln (Q4/3 \cdot t_1) \quad (1)$$

Overpressure:

$$Pr = 1.47 + 1.37 \ln (p) \quad (2)$$

[6]Areal Location of Hazardous Atmospheres

Table 2. Threshold values used.

	Radiation[8]	Overpressure[9]	Toxic release[10]	
PF[7]	Butane	Propane, MS	Chlorine	Ammonia
1	65.00	120.00	8000	18000
0.5	26.50	13.10	870	4000
0.2	20.78	7.15	470	2525
0.1	18.25	5.20	340	2030
0.05	16.42	3.95	260	1680
0.01	13.42	2.40	160	1200

Toxic release:

$$Pr = a + b \cdot \ln (Cn \cdot t_2) \quad (3)$$

where,
Pr = Probit corresponding to the probability of death;
Q = Heat radiation (kW/m^2);
t_1 = Exposure time (sec);
p = Peak overpressure (psig);
Cn = Concentration (mg/m^3);
t_2 = Exposure time (minutes); and
a, b, n = Constants describing the toxicity of a substance.

The calculated threshold values for each reference scenario for different levels of fatality mentioned above are shown in Table 2. Accordingly, the effect-distances calculated for 1, 5, 10, 20 and 50 percent fatality were then overlaid on the map of the area concerned using GIS technique, to visualize the spatial spread of the scenario impact in terms of fatality. The effect-distances were mapped with respect to the storage associated with the identified accident scenario as the point of origin.

3.4 *Risk estimation*

Finally, risk was estimated by combining frequency (section 3.2) with their consequences (section 3.3). As risk to the people concerned, two indices were used: individual risk and societal risk.

3.4.1 *Individual risk*

Individual Risk (IR) is the probability at which an individual may be expected to sustain a given level of harm from the realization of specified hazards (ICheM, 1985). In simple terms it measures the distribution of risk over an area in order to adopt

[7]Measured in mg/m^3.
[8]Probability of Fatality (%).
[9]Measured in kW/m^2.
[10]Measured in psi.

measures that reduce risk to an acceptable level. Generally, the IR estimation takes into account an annual frequency of occurrence of a reference damage (e.g. fatalities) in any area for a person present 24 hours/day and 365 days/year without protection and possibility of being sheltered or evacuated.

Graphically IR can be represented as a set of risk contours around a hazardous installation. In order to generate individual-risk contours, it first requires to estimating the effect of all individual scenarios at each location. Accordingly, risk resulting from each reference scenario was estimated combining frequency of the initiating event (i.e. incident), conditional probability of the scenario (i.e. sequence) and the corresponding probability of fatality (i.e. Probit). In particular, the following expression was used to estimate IR at a given location for a particular accident scenario.

$$IR_{(x,y,i)} = [f_i \cdot PF_i] = [(f_{\text{incident i}} \cdot P_{sequence\ i}) \cdot PF_i] \quad (4)$$

where: $IR_{(x,y,i)}$ is the individual risk at the geographical location (x, y) for a particular reference scenario I, f_i is the frequency of occurrence of the accident scenario i (y^{-1}), PF_i is the probability of fatality that the accident scenario i will result at location (x, y).

The resulting overall IR at that particular location (x, y) was then calculated as the sum of the individual IR's corresponding to each reference scenario.

$$IR_{(x,\ y)} = \sum \text{IR}_{(x,\ y,\ i)} \quad (5)$$

where: $IR_{(x,y)}$ is the overall IR at the geographical location (x, y) for all reference scenarios.

Important to mention that all events were considered to have radial effects, except for the scenarios involving toxic release which were considered as a directional footprint with its spread distributed in a sector of 22.5 degrees.

3.4.2 *Societal risk*

Societal Risk (SR) another risk measure of QRA is the relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazards (ICheM, 1985). Therefore, if no people are present around the hazardous activity, SR is zero whereas IR may be quite high (Bottelberghs, 2000).

A number of measures can be found in the literature to estimate or express the societal risk (Laheji, Post, et al., 2000). Among them, we have chosen the PLL measure as it allows spatial display of the risk to society by combining the damage potential with population density estimates. It is expected that the result would be helpful for the planners and other decision makers to understand the severity of existing risk level and accordingly identify the areas where risk stabilization measures should be adopted, or where to focus for adopting risk reduction strategies either in the form of rehabilitation or restrictions for no further residential area development. It is important to mention here that the societal risk estimation is conservative since it considers all people to be unsheltered and always present at their residences. Here, we have estimated SR in terms of Potential Loss of Life (PLL) using the following expression as adapted from the literature (Jonkman, v. Gelder, et al., 2003).

$$PLL_{(x,\ y)} = [IR_{(x,\ y)} \cdot NP_{(x,\ y)}] \quad (6)$$

where: $PLL_{(x,\ y)}$ is the Potential Loss of Life at a geographical location (x, y); $IR_{(x,\ y)}$ is the individual risk at location (x, y); and $NP_{(x,\ y)}$ is the number of people at a geographical location (x, y).

To be able to estimate PLL across a spatial grid, it is necessary to have a high-resolution spatial population database for the area. This is not readily available for the Haldia area. In order to do so, the area was divided into a series of grid cells measuring 100 m × 100 m's. The number of people per grid cell was estimated by interpolating the census population data (available per administrative unit) to the spatial spread of residential areas using a dasymetric approach (Bhaduri, Bright, et al., 2007).

4 RESULTS

4.1 *Cumulative risk maps of Haldia*

The methodology presented in section 3, was applied in a subset area of about 100 sq. km of the larger Haldia Planning Area to estimate the cumulative risk to the people in the vicinity of the hazardous industries. Figure 4 shows iso-risk contours depicting the probability of an unprotected individual being killed in the vicinity of such industries per year. Finally, the societal risk in terms of the number of probable fatalities that may be caused in an area has been estimated using a PLL function by combining the IR with the number of persons residing in each cell of the grid. The societal risk (unit being no. of people in each grid who can suffer fatalities/year) is presented in Figure 5.

4.1.1 *Uncertainty analysis*

The methodology was designed based on a traditional QRA approach. However, for applying this method in an Indian situation, several assumptions had to be made. These included the frequency of initiation events, the probability of sequence

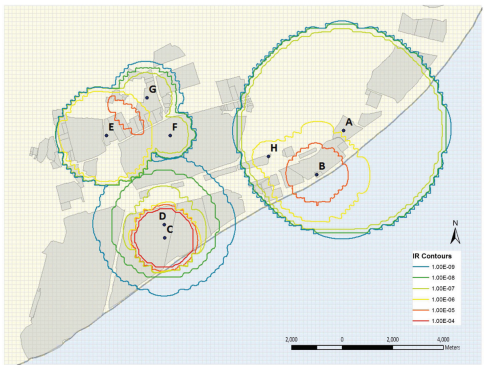


Figure 4. Individual risk. Iso-risk contours of all reference scenarios.

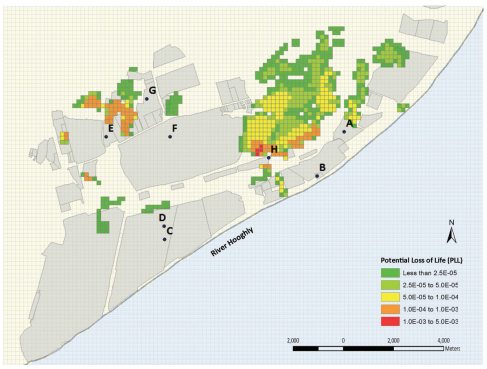


Figure 5. Societal risk. Expected PLL of each grid from all reference scenarios.

leading to the accident scenario, the selection of a limited number of scenarios based on a pre-set criteria and Probit coefficient. Therefore, the reliability of the results presented in the above section, are dependent on these assumptions. To evaluate the validity of these assumptions, an uncertainty analysis was carried out for the key variables on which the sensitivity of the results may vary (Amendola, Contini, et al., 1992). Hence, a discussion can stimulate between risk assessment professionals and planners may intend to apply this methodology.

4.1.1.1 Scenario frequency

To perform a consistent QRA, it is essential to determine frequency of an event as realistic as possible. Alternatively, over or under-estimation of the value can lead to an error of more than one order of magnitude in risk calculation. In general, the estimation of failure frequency for QRA is done based on data obtained either from different research projects, historical analysis of accidents or by the expert's judgment, which are documented in the generic failure-frequency databases. Accordingly, frequency of each scenario was estimated based on an international generic failure database. However, whether these levels of failure frequency are viable for Indian MAH installations has to be discussed and agreed upon, since frequency might vary due to many factors like enforcement of the regulations on maintenance, replacement, safety management etc. Hence, the alteration of risk contribution from different scenarios was studied, based on the variation of scenario frequencies. A comparison between estimated frequencies based on HSE's database and as a common frequency, an indicative of tolerable risk and assumed to be 1×10^{-4} for all scenarios, is presented in Table 3. From Table 3, it is evident that further research needs to be carried out to establish frequency of the initiating event and probabilities of the possible sequences which may result.

4.1.1.2 Weather condition

The results of consequence predictions can vary to a significant extent based on input weather factors like wind speed, direction, stability class etc. (Marx and Cornwell, 2009). The variability in individual risk levels, when using actual wind direction data recorded at a weather station compared to an assumed equal probability wind direction averaged across eight wind directions, is shown in Figure 6.

Table 3. Scenario contribution to PLL estimation (%).

Scenario ID	Estimated Fre^n (as per HSE)	Assumed common Fre^n (1×10^{-4})
A	39.72	75.08
B	9.17	0.22
C	0.00	0.00
D	0.25	0.59
E	28.52	2.70
F	0.00	0.00
G	0.43	4.58
H	21.90	16.83

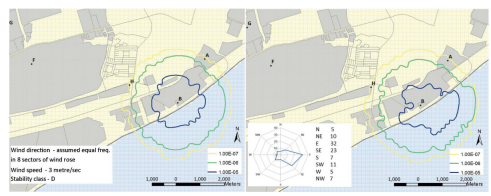


Figure 6. Variation in IR levels accounting for wind direction probability—based on assumed weather data (left); and from wind rose (right).

Table 4. Comparison of area affected in both approaches.

Iso-risk contour value	Risk-based		Consequence-based	
	Area (km^2)	(%)	Area (km^2)	(%)
Within 10^{-4}	1.67	5.92	0.00	0.00
10^{-4} to 10^{-5}	1.84	6.53	0.00	0.00
10^{-5} to 10^{-6}	5.48	19.44	20.60	72.51
10^{-6} to 10^{-7}	12.70	45.05	5.66	19.92
10^{-7} to 10^{-8}	3.58	12.70	1.83	6.44
10^{-8} to 10^{-9}	2.92	10.36	0.32	1.13

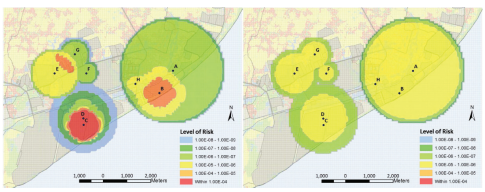


Figure 7. Application of risk-based approach (left); consequence-based approach (right) to study area.

5 DISCUSSION AND CONCLUSION

The research presented here shows that a simplified methodology based on the contemporary QRA approach can be applied for estimating the spatial extent of risk originating from a number of hazardous facilities using select reference scenarios. On one side, the outcomes of this research can lead to backward linkage with harmonization of industrial risk assessment method based on standards and criteria as acceptable to the risk management actors. At the other, there is a scope for using the outcomes in the exploration of forward linkage with the adoption of risk-informed landuse planning strategies based on agreed levels of acceptable risk at the societal level. However, testing the proposed methodology in an Indian context revealed several important concerns requiring further research and discussion.

The implication of the accident scenario in risk-informed landuse planning decisions is two-fold. First is the selection of the scenario with an off-site-impact. The experts of the European Working Group on Land-use Planning (EWGLUP) indicated that for the purpose of risk-based landuse planning, accident scenarios have to be selected based on their frequency of occurrence and the severity of their consequences. On contrary, in India risk analysis presently undertaken by the MAH industries are based on the MCL scenarios representing the probable scenario that can cause maximum offsite consequences only. However, no clear criteria or limit is yet formulated for identifying such scenarios at the national level (NDMA, 2007). The choice of MCL scenario is dependent on the methodology adopted for facility level risk assessment, based on a number of assumptions made during the exercise and then presented through a safety report, which will bring in inherent uncertainties in QRA studies involving multiple facilities. Hence, there is a need for arriving at a commonly acceptable method for risk assessment which would enable a cumulative risk assessment study otherwise the results may be faulty and thus convey a wrong picture.

Second is the accuracy or trustworthiness of the scenario and the resulting risk estimation. It has been noted that alteration of any modeling assumptions or variables may exhibit substantial variations in the size of the impact area and thereby the consequences from similar scenarios (see section 4.1.2). Therefore to arrive at a harmonized result, recommended parameters and other input variable (like threshold values for effect-distance calculation, Probit equations etc.) to estimate the consequence of an accident scenario, need to be done in order to generate consistent risk scenarios prevailing in an industrial area.

The next important issue is the number of scenarios that have to be accounted for in order to arrive at a decision. In this research we have only used eight 'reference scenarios'. However, in reality there could be an N-number of such scenarios in an industrial area like Haldia which could have major consequences for the residential areas located in between. In such cases, criteria need to be formulated for selection of the reference scenarios to assess the existing level of risk. The selection of the number of scenarios is also critical as the total individual risk is calculated by adding up the values of the individual scenarios. Ideally all possible scenarios should be taken to arrive at a correct IR value; but that may mean considering thousands of scenarios. So for practical purposes, the scenarios to be considered have to be restricted using certain limiting criteria. In this study, we have estimated individual risk taking eight scenarios, which may lead to an underestimation of the existing risk levels. Nevertheless, the results can be used to analyze areas where the risk level, considering the eight scenarios only, already surpasses international risk acceptability levels.

In India, a specific risk acceptability criterion is not yet defined; hence we made an attempt to compare the results with the Dutch and UK criteria used for landuse planning decision. It has been observed that the application of these criteria might be difficult in India as it would result in too much unacceptable area for landuse planning decisions. Thus further research is required for

establishing risk acceptability criteria for India in accordance with its societal background and existing regulatory framework.

Regarding risk-informed landuse planning decisions, as mentioned earlier, many European countries have formulated different risk assessment approaches. From a methodological point of view two main approaches can be distinguished viz. consequence-based and risk-based approach. The first one is based on consequences of the reference scenarios only considering the probability of the accident intrinsically, while the second one considers both probabilities and consequences. Therefore, for a given hazardous installation, consequence-based approach shows the consequence area for lethal effects and serious injuries resulting from the reference scenarios assessed, whereas risk-based approach shows an area within which there is a given probability of a specified level of harm resulting from the large number of possible accident scenarios. Resultantly in proposing a risk-based approach, in comparison to a consequence-based approach, the proposed methodology assigns due weight to the issue of optimal use of scarce land resources for planning purposes in India. For this purpose, both approaches were tested in the study area (Fig. 7) and percentages of total area affected as well percentage of affected area under different landuse category were compared in the Table 4 respectively. It is evident that a risk-based approach results in stricter landuse planning.

A host of analytical approaches have been formulated and used by risk analysts to predict potential damage, in terms of injury or fatality, from an accident involving a toxic release, fire or explosion in a hazardous installation. Regulatory authorities have varying opinions on the outcome of consequence modeling. Some agencies like Environment Protection Agency in the US, stress the use of simple consequence modeling equations for prediction of worst case damage distances to specific end-points whereas other agencies, like RIVM in the Netherlands or the HSE in the UK, prescribe the use of specific tools like SAFETI and RISKAT respectively, to be applied based on certain requirements and boundary conditions (Ale, 2005; Pasman, 2011). Several independent evaluations undertaken in this regard, however, point to the need for adhering to agree upon benchmarks and prescribed calculation methods for undertaking such risk analysis. Therefore adapting such methods would lead to a reliable and standardized estimate of risk or for judging the severity of consequences which could subsequently be summed up to arriving at a measure of cumulative risk.

Another key aspect of the methodology presented for estimation of risk measures in a spatial context is that no complex or proprietary software tool has been used in realizing the method. The proposed approach takes advantage of using simple GIS functions and the ALOHA model, one of the known and accepted effect models by the regulatory and industrial communities. Therefore, the methodology aligns with the accepted framework set by many countries, should not be a preserve of risk analysts, but a decision maker or planner should be able to apply the same after receiving a basic training. For fast growing industrial areas, landuse planners can thus easily consider various risk scenarios and spatially overlay them on the present landuse in order to allocate future land for future industrial and residential development.

In addition, the present approach also applies a novel method to estimate PLL based on a grid-basis population data derived from the Census data using dasymetric interpolation technique. Generally, for risk estimation purpose, ward-level population as extracted from the Census database is used without considering the exact location of population. However, often this leads to the wrong picture; hence we have interpolated the Census population into a 100 m $\times$ 100 m grid using the cadastral-level landuse map in order to get a fair estimation of number of people who might be affected. Nevertheless, it is important to mention here that grid-wise population data used is just cumulative of all people including the sensitive people as well reside in that grid.

REFERENCES

Ale, B.J.M. 2005. Tolerable or Acceptable: Comparison of Risk Regulation in UK and NL. *Risk Analysis* 25(2): 231–241.

ALOHA *User's Manual, U.S. Environmental Protection Agency*. 2007. National Safety Council, Washington.

Amendola, A., Contini, S., Ziomas, I. 1992. Uncertainties in chemical risk assessment: Results of a European benchmark exercise. *Journal of Hazardous Materials* 29(3): 347–363.

Bandyopadhyay, D., Sengupta, A., van Westen, C.J., van der Veen, A. 2011. *Bridging risk management deficits in India using a geo-ICT based tool*. Enschede, The Netherlands, ITC Working Paper Series.

Bhaduri, B., Bright, E., Coleman, P., Urban, M.L. 2007. Landscan USA: A high-resolution geospatial and temporal modeling approach for population distribution. *Geo Journal* (69): 103–117.

Bottelberghs, P.H. 2000. Risk analysis and safety policy developments in the Netherlands. *Journal of Hazardous Materials* 71(1–3): 59–84.

Christou, M.D., Struckel M., Bieerman, T. 2006. *Land Use Planning Guidelines in context of Article 12 of the SEVESO II Directive 96/82/EC as amended by Directive 105/2003/EC*. European Commission, Joint Research Centre, Major Accident Hazards Bureau, Ispra, Italy.

Cozzani, V., Bandini, R., Basta, C. Christou, M.D. 2006. Application of land-use planning criteria for the control of major accident hazards: A case-study. *Journal of Hazardous Material* 136(2): 170–180.

Environmental Impact Assessment (EIA) Notification (2006). Ministry of Environment & Forest (MoEF), Govt. of India. http://www.envfor.nic.in/legis/envclr.htm.

Fabbri, L., Contini, S. 2009. Benchmarking on the evaluation of major accident-related risk assessment. *Journal of Hazardous Materials* 162(2–3): 1465–1476.

Factories Act 1948 (Act No. 63 of 1948) as amended by the Factories (Amendment) Act 1987 (Act 20 of 1987); Ministry of Labour, Govt. of India (1987). http://labour.gov.in/upload/uploadfiles/files/ActsdRules/Service_and_Employment/The%20Factories%20 Act%2C%201948.pdf.

Hauptmanns, U. 2005. A risk-based approach to landuse planning. *Journal of Hazardous Materials* 125(1–3): 1–9.

Health and Safety Executive (HSE); Failure Frequency and Event Database for Land use Planning. http://www.hse.gov.uk/landuseplanning/failure-rates.pdf.

ICheM, 1985. *Nomenclature for Hazard and Risk Assessment in the Process Industry*.

Jonkman, S.N., van Gelder, P., and Vrijling, J.K. 2003. An overview of quantitative risk measures for loss of life and economic damage. *Journal of Hazardous Materials* 99(1): 1–30.

Khan, F.I., Abbasi, S.A. 2002. A criterion for developing credible accident scenarios for risk assessment. *Journal of Loss Prevention in the Process Industries* 15(6): 467–475.

Laheji, G.M.H., Post, J.G., Ale, B.J.M. 2000. Standard methods for land-use planning to determine the effects on societal risk. *Journal of Hazardous Materials* 71(1–3): 269–282.

Lees, F.P. 1996. *Loss Prevention in the Process Industries.* Butterworth—Heinemann, London.

Manufacture, Storage, and Import of Hazardous Chemicals (MSIHC) Rules, 1989. Ministry of Environment & Forest (MoEF), Govt. of India.

Marx, J.D., Cornwell, J.B. 2009. The importance of weather variations in a quantitative risk analysis. *Journal of Loss Prevention in the Process Industries* 22(6): 803–808.

National Chemical Management Profile for India. 2008. Ministry of Environment & Forest (MoEF) and Central Pollution Control Board (CPCB), Govt. of India. http://cpcb.nic.in/upload/NewItems/NewItem_112_nationalchemicalmgmtprofileforindia.pdf.

National Disaster Management Guidelines on Chemical (Industrial) Disaster. 2007. National Disaster Management Authority (NDMA), Govt. of India; New Delhi, India. http://ndma.gov.in/ndma/guidelines/Chemical-Disaster.pdf.

Outcome of Second India Disaster Management Congress. 2009. National Institute of Disaster Management (NIDM), Govt. of India, New Delhi, India. http://nidm.gov.in/idmc2/PDF/Outcome/Manmade.pdf.

Pasman, H.J. 2011. History of Dutch process equipment failure frequencies and the Purple Book. *Journal of Loss Prevention in the Process Industries* 24(3): 208–213.

Pasman, H.J., Reniers, G. 2013. Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP). *Journal of Loss Prevention in the Process Industries*, Article in Press.

Punihani, H., Ravi, K., Dikshit, O., Tiwari, R.S. 2002. Preparation of Zoning Atlas for Siting of Industries Using GIS. *Indian Cartographer*, MUIP-07: 282–288.

Taveau, J. 2010. Risk assessment and land-use planning regulations in France following the AZF disaster. *Journal of Loss Prevention in the Process Industries* 23(6): 813–823.

Urban Development Plans Formulation & Implementation (UDPFI) Guidelines. 1996. Ministry of Urban Affairs and Environment (MoUA&E), Govt. of India, New Delhi. http://mhupa.gov.in/w_new/SummaryUDPFI.pdf.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The effect of maintenance on inflation correction in Dutch PPP projects

D.S. Vervoort
Oxand Netherlands, Iter Fidelis B.V., Utrecht, The Netherlands
Delft University of Technology, Delft, The Netherlands

ABSTRACT: In Dutch large scale and long-term infrastructure projects, the risk of uncertain prices caused by inflation is transferred from the contractor to the public authority. In these projects, an index formula is used to correct for the escalating effect of inflation on a contractor's maintenance expenses. This formula is a rough approximation of the actual price level development and it does not perfectly match actual inflation cost. The difference between the approximation calculated with the formula and the actual cost of inflation is called the "indexation mismatch". The mismatch is influenced by the shape and uncertainty of a project's cash flow, which is in turn influenced by choices made in maintenance regime. This research studies the effect of a chosen maintenance strategy on the performance of the index formula. The study concludes that the performance on indexation of different maintenance strategies is indeed relevant and that, in the case of asphalt resurfacing, the use of rejuvenating measures in the maintenance regime performs best with regard to inflation correction.

Keywords: Public Private Partnership; inflation; indexation; DBFM; ARIMA; Monte Carlo; maintenance

1 DUTCH PPP

1.1 *Introduction*

This paper is the result of a Master's thesis at Delft University of Technology. It was performed at Iter Fidelis, a consulting company in the Netherlands. Iter Fidelis noticed that the interface of technology and finance in Dutch Public Private Partnership (PPP) projects is underdeveloped, especially when it comes to inflation correction. This has been the starting point of this research.

1.2 *Inflation*

Inflation is a worldwide phenomenon that influences cash flows over time. Inflation is the rising of price levels (Mishkin, 2001), or in other words, the devaluation of money (Schöndorff, 2000). Nobody knows how inflation will develop, and thus price levels in the future a uncertain.

In long-term projects with incomes or expenses in the future, it is important to take price level development into account. At the beginning of the project an investor wants to know the size of his expenses and revenues in the future to be able to estimate the profitability of an investment. Inflation rates over the short term, one to two years, can be estimated with low uncertainty, but over the long term, estimates introduce a big risk. Too low estimates of price rise result in higher expenses than expected, causing financially unsuccessful projects. Too high estimates result in an estimate that is not competitive. Therefore, it is important to be able to grasp and mitigate the effects of inflation on cash flows in long term projects such as construction projects. The outline of long term construction projects in the Netherlands will be explained hereafter.

1.3 *DBFM*

Traditionally, the government is responsible for the provision of a country's infrastructure. One of the reasons is that infrastructure construction requires high initial investments and only have a return on the long-term (Yescombe, 2007). This traditional government role changed, in accordance with the zeitgeist of the 1980's called 'New Public Management'. This line of thought prescribes a roll-back of state, and the outsourcing of public services.

The tendency towards a small government has resulted in the involvement of private parties in public responsibilities and with that, the rise of Public Private Partnership throughout the world.

Most governments use a public road authority to manage the country's infrastructure, in The Netherlands this role is fulfilled by Rijkswaterstaat. She is responsible for the main road- and waterway network in The Netherlands. Rijkswaterstaat is increasingly realizing the country's infrastructure demands through integrated Public Private Partnership (PPP) contract types, especially "Design, Build, Finance & Maintain"-contracts (DBFM).

In DBFM contracts with Rijkswaterstaat as principal, the private party is responsible for the design, construction, financing and twenty to thirty years of maintenance of an infrastructure asset. The private party, often three or four contractors organised in a consortium, is subsequently paid with instalments for the infrastructure's availability during its exploitation period. For private parties in these contracts, it is key to be able to estimate both the expenses of construction and maintenance. This estimation is then used to forge an offer including all Design, Build, Finance and Maintenance components. Rijkswaterstaat makes a call for tenders and compares the offers of private parties.

1.4 *Indexation*

Construction projects often take several years, which means they are, to some extent, influenced by inflation. Especially projects that include a maintenance period are subject to inflation. For example, a contractor has to estimate the cost of the construction and outfitting of an office building for its client. This estimation should then include the price rise of the carpet installed three years after the client and the contractor have agreed on a price. The contractor has to estimate the nominal price at the time the carpet is bought. Typically, cost estimates are formed in nominal prices at the start of a project, and escalated with an inflation estimation.

Indexation is a method of escalating cash flows based on independent measurements of price level development over time. Costs or income estimates for a future period are corrected for inflation over that specific period.

An eight-year contract between a client and a contractor for instance, can use indexation. The contractor has to pay the energy bill every year which has an uncertain price level. In such a case the contractor estimates the annual cost in euros at year 0 (in this example €100). Subsequently in the following years, the price of the energy bill rises due to inflation, the difference between the estimate in year 0 and the price rise due to inflation is paid by the client. This is called indexation. This correction is either an addition or reduction of the estimated amount see Figure 1 (Vervoort, 2014).

Indexation is the most commonly used term to describe this inflation correction or cost escalation. The word 'indexation' comes from the method used to define the height of the escalation. The amount of escalation is calculated by the change in price level between two points in time. This is laid down in the price level index which is published periodically by independent organisations like the Central Bureau of Statistics (CBS).

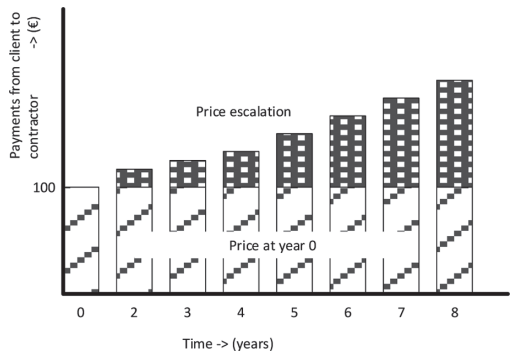


Figure 1. Principle of indexation: escalation of cash flows over time.

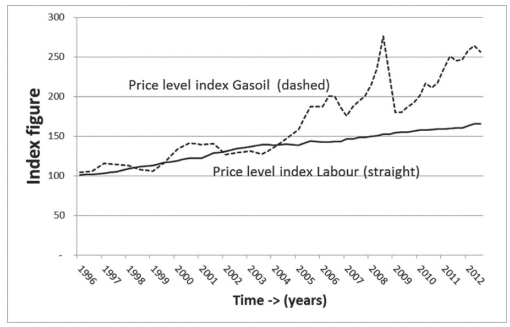


Figure 2. Difference in development of two price level indices; gasoil and labour (CROW, 2012).

The price level index is a series of numbers describing the difference in price at two different moments. Different commodities have different price level developments and have their own price level index. Labour for instance, has a very stable development with an almost constant annual growth of 2–3%. The price of gasoil, on the other hand, is very volatile as it follows geopolitical changes, supply and demand and estimations of reserves. These two different indexes are given in Figure 2. When an index is volatile it is hard to predict future price level thus indexation is more important.

1.5 *Indexation in DBFM contracts*

The contract period of DBFM projects generally ranges between 20 to 30 years, and therefore, introduces inflation risk. Inflation risk is the risk of higher price rise than expected, resulting in higher cost with a negative effect on a project's budget (the risk can also work the other way, causing a positive effect on a project's budget). In accordance with

the PPP-principle, where the party best able to carry a risk, is taking it, the Dutch DBFM agreement includes an indexation clause to transfer the consequences of inflation risk from the contractor to the government.

The goal of this (indexation) mechanism is to escalate the income of the private party in accordance with the increase in expenses resulting from inflation. The starting point of the indexation mechanism is therefore the income of the private party; the periodical instalments called Availability Payments (AP). The AP is paid each quarter in the maintenance phase by Rijkswaterstaat and is the leading parameter on which projects are awarded. The sum of these payments should cover all cost of the private party incurred in the Designing, Building, Financing and Maintaining the infrastructure. Formula 1 shows the index formula used in the standard DBFM agreement (Rijkswaterstaat, 2010).

$$BBV_{t,p} = BBV * Indexnumber_{t,p}$$
$$Indexnumber_{t,p} = 1 + \sum_{n=1}^{6} (a_{n,p} * m_{n.t}) \quad (1)$$

$Indexnumber_{t,p}$ = *Indexnumber for year t in period p;*
index n = available index (*e.g. labour*)
period p = 5-year period
$a_{n,p}$ = *weight factor for index n in period p, laid down at contract close;*
$m_{n.t}$ = *mutation of index n with;*

$$m_{n.t} = \frac{i_{n,t}}{i_{n.ref}} - 1$$

$i_{n.t}$ = *indexfigure of index n in year t;*
$i_{n.ref}$ = *indexfigure of index n in reference year*

The AP is escalated by a multiplication with the indexnumber. The indexnumber is a weighted average of the change of 6 indexes. The weight factor $a_{n,p}$ is fixed by the contractor for each 5-year period. The weight factor resembles the share of expenses of an index as part of the AP. Labour often has a bigger share than gasoil as the largest part of maintenance cost is spent on manpower.

This first section has described the phenomenon, contract and mechanisms at work in this research' field. The following paragraph will elaborate on the problem at hand.

2 PROBLEM STATEMENT

2.1 *Imperfection of indexation method*

The Dutch indexation method uses a formula that tries to model reality (formula 1). Inherent to being a model, it is a simplified version of reality. In order to make the model workable it includes assumptions. This results in residual risk that is not transferred to the public authority. A 'gap' exists between the formula and reality. Two properties of the formula causing this gap are that the price level development is levelled-out over a five-year period and that the moment at which costly replacement maintenance is executed is fixed twenty years in advance. The consequence of this gap is that the actual cost change caused by volatile inflation is not perfectly followed by the inflation correction calculated with the index formula. This mismatch leaves residual risk at the private party and may lead to a negative financial outcome of a project.

2.2 *Influential parameters on inflation correction mismatch*

There are three main parameters that influence the inflation correction mismatch. Firstly, the uncertainty in the maintenance planning. For example, the resurfacing of pavement, it covers the largest part of the maintenance budget in motorway projects. It is planned in a specific year in the exploitation period but there is no accurate information on deterioration over time and therefore it has a wide bandwidth in the maintenance planning. The index formula lacks the ability to cope with this uncertainty, which is one of the reasons for the index-gap.

Secondly, the shape of the cash flow influences the inflation correction mismatch. At what moment and at what cost the maintenance is executed is input for the calculation of the Availability Payment and other parameters in de index formula. The index formula assumes a homogenous spread of cash flow over each 5-year period. However, the spread of cash flow can take many shapes and forms. For the maintenance of pavement, there are different options for the maintenance plan which all have a different cash flow. Normally, there is at least one peak in maintenance cost due to resurfacing of the pavement in a maintenance period of 20 years. But different strategies are possible. For example; rejuvenating measures can be chosen to extend the lifetime of the pavement, in this way the resurfacing peak is delayed a few years. This could result in a maintenance planning with only one resurfacing activity necessary in the exploitation phase, which results in lower maintenance cost and higher availability. This is an area of choice which is currently heavily debated in DBFM projects (Moenielal, 2013) (Spaargaren, 2013).

The third factor that influences the inflation mismatch is the volatility of the price level index within the index formula's resolution of five years. This third factor is also relevant in large asphalt maintenance; resurfacing of asphalt pavements uses products with highly unpredictable price

levels; bituminous products, mostly due to the link with the global oil price.

The three influential parameters on the indexation mismatch described above are all relevant in large asphalt maintenance. The large impact on the cost, uncertainty in planning and volatile price levels make large asphalt maintenance very influential to the inflation correction mismatch. This portion of the cash flow of a DBFM project is therefore chosen as the subject of this research.

2.3 *Problem statement*

There is a lack of knowledge on the mismatch between a DBFM project's inflation cost and its inflation correction payments. Furthermore, the effect of different maintenance plans on this mismatch is unknown as well. The most influential issue on a maintenance budget is the large asphalt maintenance because of its financial weight, numerous maintenance strategies, planning uncertainty and unstable product prices. It would be valuable to know how different resurfacing strategies perform on inflation correction in different scenario's. This is important because correction for inflation influences the tender bid as well as the profitability for the private party. When the parties in DBFM projects are more aware of the inflation correction mismatch and how it can be influenced, the projects will result in a higher value for money for the government and a lower risk profile for the private party. To conclude, the problem is therefore the lack of knowledge of the size and dynamics behind the residual risk of price level development. A better understanding of the impact from different maintenance strategies allows for private parties to improve their tender bid.

2.4 *Research question*

Having defined the problem, the research question is composed to find the knowledge necessary to solve the problem. The research question is formulated as follows:

> *Which resurfacing strategy minimizes the net present value mismatch between inflation correction and actual inflation cost in DBFM road projects in The Netherlands?*

3 RESEARCH METHOD

3.1 *Strategy comparison model*

The three variables that influence the mismatch have been identified as the price level development and the cash flow of the maintenance activities with its uncertainty in planning. To be able to answer the research question without a range of projects to compare, the variables are simulated for four different resurfacing strategies. With such a Monte Carlo simulation, a large number of different future paths is created for one single project. For each future path, a different price level development and timing of maintenance is simulated, resulting in a unique set of performance indicators as output. Doing this for all four resurfacing strategies makes it possible to compare the performance and answer the research question on how to deal with the index gap. An advantage of this artificial method over a real-life case comparison is that the scope, duration and payment mechanism of the project remain the same, resulting in more clear results than a comparison of actual projects with differences in lay-out. An important drawback is that the simulation is based on historical inflation data, which are not necessarily indicators for future inflation development.

3.2 *Model inputs: Case study: A15 motorway*

To make the comparison as close to reality as possible, the simulations are based on an actual case in the Netherlands; the capacity enlargement of the A15 motorway. The road connects the port of Rotterdam, Europe's largest port, with the hinterland while simultaneously facilitating the commuters to and from the area's industry. The road is also the main access to important residential and recreational areas in the Southwest of The Netherlands. With the completion of the recent port expansion and the growth in traffic expected to follow from that, Rijkswaterstaat initiated the project as a DBFM contract.

Key input parameters like pavement area as well as important milestones and payment mechanisms are retrieved from the scope document and DBFM agreement as a basis for this research.

Through interviews with asphalt experts from both the public and private party together with literature on asphalt maintenance, four resurfacing strategies have been identified

Strategy A: Traditional resurfacing
Strategy B: Lifetime extension through Rejuvenation
Strategy C: Replace with innovative asphalt
Strategy D: Start and replace with innovative Asphalt

These strategies all have different cash flows and uncertainties. Heavily loaded lanes are distinguished from lightly loaded lanes, because the deterioration of pavement is highly influenced by the amount of trucks using it. The strategies will be described in more detail in the following sections.

3.2.1 *Strategy A: Traditional resurfacing*

In a traditional resurfacing regime of Double Layer Porous Asphalt (DLPA), the top layer of the pavement is resurfaced when the quality of the road nears its failure condition. In strategy A, the resurfacing of the top layer of the heavily loaded lane is executed at 8 years after construction. 4 years later, the total DLPA package is replaced, both the top and secondary layer on both the heavily and lightly loaded lanes. This is conform the current standard in asphalt maintenance.

3.2.2 *Strategy B: Lifetime extension through rejuvenation*

This second strategy improves the first maintenance regime by extending the lifetime with rejuvenating measures. The embrittlement of the bitumen in the asphalt can be countered by spraying a new bitumious mixture in the porous asphalt. This technique is called 'sealing'. Sealing the pavement twice during its lifetime will extend its total lifetime by two years on average. Besides the lifetime extension, it also reduces the spread of the planning uncertainty.

3.2.3 *Strategy C: Replacement with innovative asphalt*

A more opportunistic strategy is to aim for technological advances in asphalt technology. In this strategy the budget is built on the assumption that at the time of the first traditional resurfacing in year 8, a more durable asphalt type has been developed. The durability of this new asphalt is such that it at least outlasts the contract period. With this strategy only one resurfacing activity is necessary resulting in a much lower tender bid. This risky opportunistic behavior is reality in the current Dutch market in which work is scarce.

3.2.4 *Strategy D: Start and replace with innovative asphalt*

The last strategy that is used in DBFM contracts also aims for only one resurfacing activity during the contract period. But instead of choosing a new asphalt type after using traditional pavement in the first phase of the contract period, this strategy starts with innovative asphalt right away. The exact details are commercially sensitive and therefore confidential but it is a different pavement type than traditional double layer porous asphalt. This strategy is currently being used at the A15 project by *A-lanes A15*, the concession contractor. A major disadvantage is that, when introducing a new asphalt type in the Rijkswaterstaat network, the introducer is obliged to prove the quality of the pavement. Meeting this obligation takes time and money.

Based on experience abroad, the expected lifetime of this innovate asphalt is 12 years for both the heavily and lightly loaded lanes (Moenielal, 2013). Furthermore, there is no need to distinguish between heavily- and lightly loaded lanes; the entire pavement is resurfaced in one go.

These four strategies are compared by running them in the strategy comparison model. The innovative aspect of this model is the way inflation is modelled.

3.3 *Inflation modelling: Autoregressive Integrated Moving Average*

Inflation modelling for probabilistic analysis has to deal with the properties of inflation datasets. These datasets follow an exponential trendline, with a heteroskedastic deviation. Furthermore, the dataset has positive serial autocorrelation and some indexes, like gasoil and bitumen, are strongly positively correlated. These properties are included with a modelling technique used in the field of econometrics, named: ARIMA-modelling.

ARIMA is a sophisticated univariate modeling technique. ARIMA is the abbreviation of *Autoregressive integrated moving average* (also known as the Box-Jenkins model). It was developed in 1970 for forecasting purposes and relies solely on the past behavior of the variable being forecasted. The model creates the value of Y_t with input from previous values of the same dataset. This input includes a factor of previous values Y_{t-p} as well as the elasticity of the previous values ε_{t-q}. In a formula it looks like:

$$Y_t = \Phi_1 Y_{t-1} + \Phi_2 Y_{t-2} + \cdots + \Phi_p Y_{t-p} + \varepsilon_t + \theta_1 \varepsilon_{t-1} + \theta_2 \varepsilon_{t-2} + \cdots + \theta_q \varepsilon_{t-q} \quad (2)$$

With Φ and θ as unknown parameters to be found in a variant study. The ε's are independent and identically distributed normal errors with zero mean. This stochastic error term is called the *innovation* or *white noise*. The number of historical values used to generate value t is p, and is called the number of lags. The number of innovations incorporated in value t is expressed by q.

The ARIMA method uses historical values to set the parameters described above. These datasets can only be used when they have specific properties like homoscedasticity and uniformity. The datasets of inflation do not have these properties, therefore some deformations on the dataset need to be performed. The number of deformations needed is described by the letter d. The theory speaks of ARIMA (p,d,q) models to describe the lag structure. In this research, different ARIMA lag structures are used to model the different indexes. The choices of the p d and q are based on the Akaike Information Criterion (AIC). The modelling is executed with Palisade's @RISK software as plug-in in Microsoft Excel.

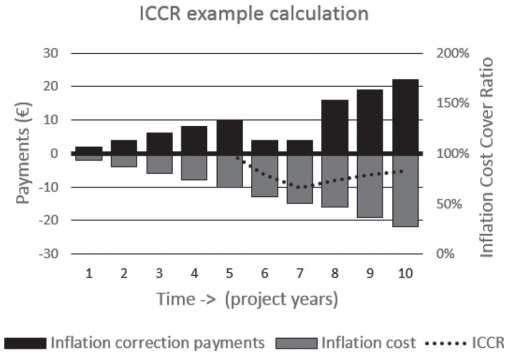


Figure 3. Mechanism of Inflation Cost Cover Ratio performance indicator.

3.3.1 *Inflation Cost Cover Ratio*

In order to answer the research question on the mismatch between inflation cost and inflation correction, a special performance indicator is designed to compare strategies and reveal the mismatch. The indicator is called the *Inflation Cost Cover Ratio* (ICCR) and describes the percentage of extra cost due to inflation, that is compensated by the inflation correction. Because the time value of money is relevant in the comparison of the four strategies, the percentage is calculated with the present values of the inflation cost and inflation correction. The discount rate is 6,25% as used by Rijkswaterstaat to compare tender bids. Figure 3 shows an example of an ICCR calculation of a cash flow. The formula below shows how the ICCR is calculated.

$$ICCR = \frac{PV\ Inflation\ correction}{PV\ Inflation\ cost} * 100\% \qquad (3)$$

In an ideal situation, where all cost for inflation are perfectly compensated by payments from the public authority, the ICCR would be 100% in every quarter. With an ICCR of 100%, there is no mismatch between inflation cost and compensation.

The ICCR is compared to the base case. In this base case, neither volatile price levels nor uncertainty in planning are taken into account. This comparison gives insight in the behaviour of the index formula under uncertainty. The closer the ICCR is to the base case, the better the predictability.

4 RESULTS

Figure 4 shows the probability density function of the ICCR for the four strategies. Here, strategy A has the most positive output; the mean ICCR calculated by the model is 3,1% higher than expected in the base case (the peak is 0,03 right of the y-axis). The high value is in this case caused by conservative budgeting, which anticipates higher costs than probable. Without these extra cost items in the last two years however, the deviation from the ICCR in the base case becomes much lower, as displayed by the line of strategy C.

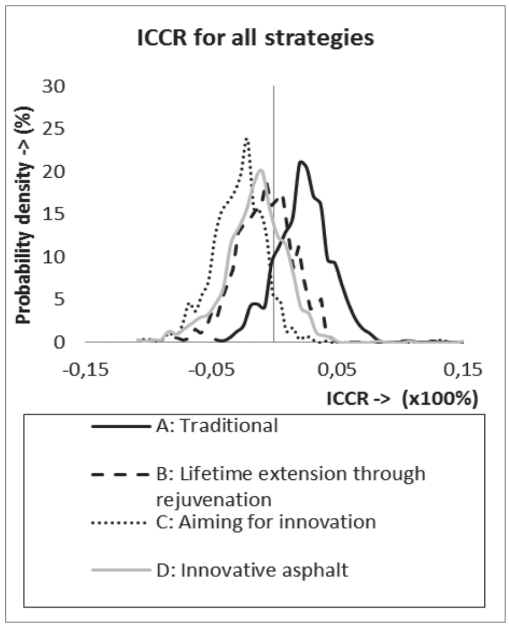


Figure 4. Output ICCR of 4 maintenance strategies. (Vervoort, 2014).

The other two ICCR outputs deviate less from their expected value, with a mean of –0,5 and –1,2% for strategy B and D respectively.

5 CONCLUSION

The answer to the research question is the following: Because strategy B deviates least from the expected outcome of the ICCR, the strategy of *Lifetime extension through rejuvenation* is considered to be the best resurfacing strategy when it comes to the net present value of the mismatch between the inflation correction and inflation cost in Dutch DBFM projects.

As seen in the output figure, the traditional resurfacing regime, Strategy A, performs best for the budget of the private party. With a positive mean ICCR, the inflation correction paid by Rijkswaterstaat, minus the inflation cost, is more than expected in the base case. This is good for the project balance but this strategy outper-

forms the expectations which makes the tender bid commercially not very competitive. This is due to the safe budgeting in this strategy which assumes an unlikely peak in maintenance cost in the final two years of the project. The strategy's cash flow is constructed based on maintenance theory, degradation data and engineering practice. However, in a competitive market, the bid resulting from this strategy is very safe. It is so safe, that the actual cash flow never occurs exactly as budgeted in the simulation. This causes the inflation cost to be much lower than expected, which benefits the ICCR. The safe maintenance strategy is reflected in the high reference bid, making this strategy the losing one in the tender.

Strategy B: *Lifetime extension through rejuvenation* performs almost exactly as expected. The mean of the ICCR outputs is very close to zero and besides that, the spread of the 95th percentile is much smaller than the other two strategies C and D.

Conversely, strategy C: *Replace with innovative asphalt* and strategy D: *Start and replace with innovative Asphalt* on average perform worse than expected (ICCR < 100%). In most simulations, the inflation correction is insufficient to cover the cost of inflation, which causes negative financial outcomes for the private party at the end of the project.

Because strategy B deviates the least from the expected outcome of the ICCR, the strategy of Lifetime extension through rejuvenation is the best resurfacing strategy when it comes to the net present value of the mismatch between the inflation correction and inflation cost in Dutch DBFM projects. This is the answer to the research question.

6 RELEVANCE

To prove the relevance of the inflation correction a hypothetical statement is formulated as follows:

> *It is expected that a choice between two maintenance strategies has a relevant effect on a project's budget, the choice results in a difference in the inflation correction mismatch of over €530.000 in Present Value.*

The value is based on current profits of Dutch construction companies (2–3%). If the difference is larger than a typical profit, it is worth taking into account. Figure 4 shows the different outcomes of ICCR for the four different maintenance regimes. The difference of the outcomes confirms the first part of the hypothesis; the maintenance strategies perform differently on inflation correction. The largest difference in inflation correction is between the *traditional* strategy A and the *Aiming for innovation* strategy B. The difference between their mean ICCR is 5,3%, which comes down to € 2,6 million in terms of present value.

In other words, the choice in maintenance strategy changes the expenses on resurfacing maintenance more than 2% in present value cost. Therefore, the hypothesis is accepted.

This research shows that inflation correction should be taken into account in a variant study of maintenance strategy, because it has a relevant impact on the budget. This means that if contractors take the mismatch of the indexation formula into account, they can present offers that entail better mitigation of risk resulting in better value for money for Rijkswaterstaat in DBFM projects.

In several meetings after publication of this thesis, clients of Iter Fidelis, the host company, affirmed their interest for using this method in upcoming tenders.

7 OTHER FINDINGS AND RECOMMENDATIONS

Besides the answer to the research question and the relevance test, several other findings can be noted. This paragraph describes these other findings.

7.1 *Two kinds of mismatches*

The research shows that there are two kind of mismatches in inflation correction. The first mismatch is caused by imperfections of the index formula even when the cash flow behaves exactly as expected in a deterministic budget. At the moment, this mismatch is taken into account in DBFM projects. The second mismatch occurs when the cash flow deviates from its expected path. This deviation may occur in the price development or the timing or amount of expenditures. This second mismatch is not taken into account in the current DBFM projects. The research suggests the private party should take this into account in the tender bid, because it causes variations in the cash flow of a maintenance plan.

7.2 *Evaluation of index formula*

First of all, the private party should be thankful for the existence of the index formula. The formula is a helping hand for the private party that takes away a lot of uncertainty. A strong property of the formula is that there is little room for strategic behaviour, this benefits equal assessment of the competing parties in a tender. The index formula is constructed in such a way that when commercial parties try to use it for strategic behaviour, it either leads to more risk or a higher offer.

This research shows the index formula is somewhat unrefined in its calculations, resulting in a mismatch. The rough level of detail is chosen for the ease of calculation, changes can be made to the formula in order to reduce the mismatch, but this would introduce discussion as explained hereafter.

7.2.1 *Mismatch 1*

'Inequality between inflation correction spread over 5 years and maintenance expenses peaks' can be removed as follows. The spread-out of the inflation correction over a five year period could be refined to a correction calculated annually or even quarterly in order to reduce the mismatch. In this way, the inflation correction and inflation cost profiles are mirrored better which strongly reduces the mismatch. However, due to the uncertainty of the timing at which the peak expenses are made, fixed weight factors for each year could result in even larger mismatches than with a spread-out over 5 years. If a peak expenditure is made earlier than budgeted, the fixed inflation correction does not match the expenses because the weight factors are based on the budgeted timing of expenses. Thus, the current method in which the weight factors are spread over a 5-year period is a protection against the mismatch cause by flexibility.

To make use of this build-in protection, the peaks must be budgeted in middle year of the five-year period in order to have the biggest chance that the peak expenses remain inside the period.

7.2.2 *Mismatch 2*

'Inflexibility of index formula regarding uncertainty of maintenance activities' timing can also be reduced. An improvement of the formula could be done by introducing flexibility; giving private parties the possibility to change the weight factors as their maintenance activities change from what was budgeted. The drawbacks of this is that it will give room for discussion and strategic behaviour. In the current index formula everything is fixed and undebatable. If weight factors can be changed after the tender offer is made, the client and private party will be debating constantly whether or not the change is reasonable. And with the current state of heavy debates in DBFM projects, an additional point of debate is not welcome.

7.2.3 *Mismatch 3*

'Use of outdated index figure*s in inflation correction*' can be reduced by using quarterly indices in the calculation of the index figure. In the current state of affairs, the formula uses the indices from January, also to calculate the inflation correction for the third, second and fourth quarter. It is possible to use the indices publicized in each respective quarter, but because there is a big delay between the moment of measurement and the moment of publicizing, calculations delay inflation correction payments. Figures of January are publicized two to three months later, making it only possible to calculate the inflation correction in a later stage. With the time value of money in mind, a delay in inflation correction payments is unwanted.

Concluding, the index formula can be improved to reduce the mismatch. However, this introduces debates and slows down the process of inflation correction payments. The current index formula has a good balance between workability and precision, therefore the research recommends Rijkswaterstaat to keep the current indexation method untouched.

7.3 *Use more likely budget for weight factor calculation*

One reason for the mismatch between inflation correction and inflation cost is the fact that the weight factors in the calculations are based on a budget designed with a 85% certainty interval. A recommendation is to use two budgets, a safe one, and a more probable one to be used to define the weight factors.

The second one will have the maintenance peaks planned at a 50% certainty interval, making the match between the out- and inflowing cash flow more probable. This improvement has been tested on Strategy C; aiming for innovation with an improvement of the ICCR from 95,1% to 95,7% (€ 304.000 present value benefit).

In this method, a large part of the weight factor set of are shifted to a more probable period. Because it is also more likely that the expenses will occur in this period, the set of weight factors is more likely to be more accurate. The result is an improvement of the Inflation Cost Cover Ratio.

This improvement has been tested for strategy C, where it results in a better performance from a private party point of view. It is recommended that the private party runs simulations like these to test whether the weight factor calculation can be improved.

7.4 *Limits to conclusions*

It is important and necessary to note that the conclusions are based on assumptions. Especially the assumption on the future development of inflation is debatable. The price level development is based on an extrapolation of historical behaviour of data, but there is no certainty at all that the future will resemble history. Major shifts in geopolitical relations or technological advances may change price level drastically. Also, events like hyperinflation, which occurred not that long ago in Latin

America in the 90's, are not taken into account. Therefore, the conclusions remain confined to a specific assumption on the future.

Furthermore, the assumptions on the lifetime of the pavement is based on historical behaviour of double layer porous asphalt. But a series of very cold and wet winters or a new law allowing heavier trucks would change the degradation of the pavement insofar, that it would fall outside the probability density function expected of the maintenance interval. Therefore, the conclusion must be used with care by taking the assumptions into account.

The incorporation of these two uncertainties oblige the reader to be careful with the interpretation of the results. Especially the quantitative values must not be seen as exact truth, because they are all forecast of the future based on assumptions.

REFERENCES

CROW, 2012. *Indexen ten behoeve van Risicoregeling GWW 1995.* CROW.

Mishkin, F.S, 2001. *The economics of Money, Banking and Financial Markets*. New York: Columbia University.

Moenilal, M. 19-4-2013. *Senior Material Expert*, DIBEC B.V. Interview. (D. Vervoort, interviewer).

Schöndorff, P.D. 2000. *Economie—1500 termen van A tot Z.* Utrecht: Spectrum.

Spaargaren, T. 11-4-2013. *Asphalt Expert*, Iter Fidelis B.V. (D. Vervoort, interviewer).

Rijkswaterstaat, 2010. *DBFM Agreement.* Rijkswaterstaat.

Vervoort, D.S. 2013. The effect of asphalt maintenance regimes on inflation correction in Dutch DBFM contracts. Delft: Delft University of Technology.

Yescombe, E. 2007. *Public Private Partnerships—Principles of Policy and Finance*. Oxford: Elsevier.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Handling dependencies in Probabilistic Risk Assessments using Evidential Networks

D. Wang, Z.J. Cheng, P. Jiang & B. Guo
College of Information System and Management, National University of Defense Technology, Changsha, Hunan, P.R. China

ABSTRACT: Dependencies or failure dependencies in probabilistic risk assessments may lead to significant errors if not properly analyzed. In order to overcome the limitations of traditional methods, a modified Bayesian Network (BN), which is called Evidential Network (EN), was proposed with evidence theory to handle dependencies in Probabilistic Risk Assessment (PRA). Fault Trees (FTs) and Event Trees (ETs) were transformed into an EN which constructs a uniform framework to represent accident scenarios. Dependencies can be processed through the corresponding evidential networks where uncertainties are characterized by basic belief mass. A case study was discussed to demonstrate the proposed approach. Frequencies of end states were obtained and expressed by belief and plausibility measures. The proposed approach can be easily applied to probabilistic risk assessments that involve dependencies while addresses the uncertainties in experts' knowledge.

1 INTRODUCTION

Probabilistic risk assessment is an effective analysis approach that systematically estimates the occurrence frequency of an accident sequence. It has been used in nuclear industry since 1970's (Keller & Modarres 2005) and also widely adopted in space industry (Stamatelatos 2002) and civil engineering (Nývlt et al. 2011).

ETA and FTA are two distinct methods used in PRA. ETA is a technique used to display sequences of system (or human) failures or successes that can lead to specific end states and estimate the likelihoods (frequency) of each end state. FTA is often used to analyze the probability of failure or success of pivotal events in an event tree. A pivotal event is treated as top event and proceeded down to basic events using logic gates in each fault tree. Despite the fact that the two methods are widely adopted, some limitations as the lack of ability of modeling dependencies are suffered (Khakzad et al. 2011).

Failures arising from dependencies are often difficult to identify and, if neglected in modeling and quantifications, may result in an underestimation of risk (Stamatelatos 2002). However, till now, researchers from different industries haven't reached an agreement on the definition of dependency or failure dependency. In a broad sense, dependency implies relationship between failures. Since reliability and safety analysis focus on failures, dependency and failure dependency have the same meaning in this article.

For a proper treatment, dependencies are categorized into intrinsic dependencies and extrinsic dependencies in the report of United States Nuclear Regulatory Commission (USNRC 1998b). In (IAEA 2000) dependencies are divided into 4 types (functional dependencies, physical dependencies, human interaction dependencies and component failure dependencies). Despite the differences in categorization, every kind of dependency should be proper treated in a PRA. For example, the graphic structure of a fault tree is used to handle some of the dependencies among failures (e.g. dependencies of system failures on support electric power failures are included in FTs by including failure of power system components as basic events). For those with logical relationships that cannot be expressed explicitly in FTs or ETs, Common Cause Failure (CCF) analyses are then conducted.

While efforts are made to treat different kind of dependencies properly, dependency across event trees is not often discussed and not much explored. These dependencies may be caused by shared utilities, shared components, or general CCFs underline an event tree. A common method is utilizing a uniform framework to combine FTs and ETs together so that components or events that depend on each other can be connected and processed in a single structure. FTs/ETs can be transformed into an integrated FT which acts as a uniform framework. However, the calculations for a giant FT are cumbersome. Existing scientific

papers related to this issue also tried binary decision diagrams (Andrews & Dunnett 2000) and Petri nets (Nývlt & Rausand 2012) to form the uniform framework. Recently, Bayesian networks are increasingly used for the constructions of system reliability models, risk management, and safety analysis based on probabilistic and uncertain knowledge (Weber et al. 2012). The advantage of using BNs in safety analysis is that a BN combines all factors related to system safety together. These factors range from human errors, environment influences to organization methods. Naturally, BN becomes an alternative for uniform frameworks that combine FTs and ETs (Hosseini & Takahashi 2007). Meanwhile, CCF factors such as β factors are widely used in CCF analyses to measure degree of dependencies. They can bring additional sources of uncertainties to analyses. Together with other uncertain inputs, they bring another challenge to the existing methods.

In this work, a modified Bayesian Network (BN), which is called Evidence Network (EN), is proposed to handle dependencies in PRA. The equivalent EN structures of ETs and FTs are discussed. Specifically, this paper is believed to be the first study dedicated to the transformation of ETs into ENs. Dependencies can then be tackled through the corresponding evidential network where uncertainties are characterized by basic belief mass.

The remainder of the article is organized as follows: In Section 2, the β factor model, which is a typical CCF factor model, is briefly introduced. Uncertainties brought by β factors are discussed and serve as an inspiration of using modified models to deal with dependencies in PRA. The D-S evidence theory and evidential networks are briefly introduced in Section 3. The EN based approach is then discussed in detail in Section 4. In Section 5, a part of a practical probabilistic risk assessment is analyzed using the proposed approach. The conclusion is expressed in the end.

2 FAILURE DEPENDENCY UNCERTAINTY

The dependencies one needs to take into further consideration are those that haven't been explicitly represented in the original FTs. Dependent failures that are not explicitly modeled in FTs are known as Common Cause Failure (CCF). A formal definition follows:

A common cause failure is defined as the failure (or unavailable state) of more than one component due to a shared cause during the system mission (Stamatelatos 2002).

Usually, the dependencies caused by CCFs are depicted using factor modeling such as the α factor model, the Multiple Greek letters (MGL) model and the β factor model. Details about these models can be found in many publications (Barros et al. 2009, Humphreys 1987, USNRC 1998a). Basically, all the mentioned models use a CCF factor to represent the proportions of different type of failures. In this paper, the β factor model is preferred due to its reasonable complexity. Take the β factor model for example, it can be noticed that the factor modeling can bring additional dependency uncertainties.

2.1 *β factor model*

The β factor model initially proposed by Fleming (Fleming 1974) uses a β factor to represent the failure probability due to a common cause given the occurrence of a failure. The expression of β is given by

$$\beta = \frac{P_{(\mathrm{CCF})}}{P_{(\mathrm{T})}} = \frac{P_{(\mathrm{CCF})}}{P_{(\mathrm{I})} + P_{(\mathrm{CCF})}} \tag{1}$$

where $P_{(\mathrm{CCF})}$ is the failure probability due to common cause failures, $P_{(\mathrm{I})}$ is the failure probability due to independent failure and $P_{(\mathrm{T})}$ is the total failure probability.

2.2 *Uncertainties in β factor*

Usually β factors are regarded as crisp values which are evaluated in two approaches. The first approach uses statistic data gathered from systems in operation to obtain β factors. This method is frequently used in nuclear industry (USNRC 1998a, USNRC 1998b). In recent years, researchers in space industry also started to collect data to evaluate β factors. For example, Rutledge evaluated the β factor of redundant electric hardware to be 0.11 after analyzing 473 abnormal flight data provided by NASA (Rutledge & Mosleh 1994). Nevertheless, such data analyses may have not been conducted in other industries yet. Moreover, even the β factors in nuclear industry, which obtained from statistic data of a specific type of reactor, are not applicable for all the plants (Song 2007).

The second approach uses judgment standards to evaluate β factors. For example, the β factor is increased if two generators are placed in the same room or maintained by the same worker. A relatively complete set of standards was proposed by Humphreys (Humphreys 1987) and adopted by Atomic Energy Authority (AEA) (Brand 1996). Generally this approach provides ranges of β values, but the final choice is subjectively done by analyzers.

Summarizing above, both approaches can just get a possible realistic value of β in the context of

a particular analysis. Normally, the actual β factor value agreed by experts is between 0.005 to 0.11 for hardware failure and 0.05 to 0.6 for software failure. However, the exact value is hard to get due to limited data, incomplete or imprecise information. It's reasonable to doubt that a point-valued β factor ignoring uncertainties can lead to a false decision-making. Thus, this paper proposes the using of intervals to represent the value of β factors, allowing experts to express the uncertainty about the grade of dependency.

3 A BRIEF INTRODUCTION TO D-S EVIDENCE THEORY AND EVIDENTIAL NETWORKS

Uncertainties brought by β factors are labeled as epistemic uncertainty (Hoffman & Hammonds 1994). While BN is an effective uniform framework to represent dependencies, it lacks of the ability to handle epistemic uncertainties brought by them.

While few researches on the use of BNs in system reliability and safety analysis take epistemic uncertainty or uncertainty propagation into account, one exception is an interesting work by Simon et al. (Simon et al. 2008) which concerns how a BN can be modified to a so called evidential network to handle epistemic uncertainties. Evidential network is a combination of evidence theory and BN. In this section the basic concepts of D-S evidence theory and evidential network are introduced.

3.1 *Basics of D-S evidence theory*

The D-S evidence theory, is developed by Dempster (Dempster 1967) in the 1960'. Shafer developed the original theory by introducing the concept of belief function. Some basics of D-S evidence theory are given as follows.

3.1.1 *Frame of Discernment (FD)*

The frame of discernment is a finite nonempty exhaustive set of mutually exclusive possibilities denoted by $\boldsymbol{\Theta}$ which includes all the possible propositions. The propositions are called "focal elements". If $\boldsymbol{\Theta} = \{H_1, H_2, \ldots, H_i, \ldots, H_n\}$ then there are n hypotheses in the frame. H_i represents "hypothesis H_i appears".

3.1.2 *Basic Belief Assignment (BBA)*

The sources of information can distribute masses on every subset A_i of the frame of discernment. A_i is expressed by:

$$A_i \in 2^{\boldsymbol{\Theta}},\ 2^{\boldsymbol{\Theta}} = \{\emptyset, \{H_1\}, \ldots, \{H_n\}, \{H_1, H_2\}, \{H_1, H_3\}, \ldots, \{H_{n-1}, H_n\}, \{H_1, H_2, H_3\}, \ldots, \{H_1, H_2, \ldots, H_n\}\}.$$

This process is called basic mass assignment which is represented by a function m defined by:

$$m: 2^{\boldsymbol{\Theta}} \to [0,1] \text{ with } m(\emptyset) = 0,\ \sum_{X \subseteq 2^{\Theta}} m(X) = 1.$$

3.1.3 *Belief function and plausibility function*

The analysis results are demonstrated by an interval which describes the degree of support for a hypothesis. The lower bound is called belief function, denoted by

$$Ble(A) = \sum_{B|B \subseteq A} m(B) \tag{2}$$

The upper bound is called plausibility function, denoted by

$$Pl(A) = \sum_{B|B \cap A \neq \emptyset} m(B) \tag{3}$$

3.1.4 *Combination rules*

Combination rules are used to combine evidence from different sources. The D-S combination rule can be expressed by the following relation:

$$m(C) = m_i(X) \oplus m_j(Y) = \begin{cases} 0 & C = \emptyset \\ \dfrac{\sum_{X \cap Y = C, \forall X, Y \subseteq \boldsymbol{\Theta}} m_i(X) \times m_j(Y)}{1 - \sum_{X \cap Y = \emptyset, \forall X, Y \subseteq \boldsymbol{\Theta}} m_i(X) \times m_j(Y)} & C \neq \emptyset \end{cases} \tag{4}$$

Many other combination rules have also been presented (Smets 1990). The original DS combination rule is used in this study.

3.2 *Evidential network*

An Evidential network can be represented as $G^* = ((N^*, A^*), D^*)$, where (N^*, A^*) represents the graph in which "N^*" is a set of nodes, "A^*" is a set of arcs and "D^*" represents the set of belief distributions that are associated with each node in the graph (Simon et al. 2008). The basic belief assignments are set for some of the nodes (basically leaf nodes) as priori probabilities. A belief propagation is then performed through the so called "Conditional Belief Mass Table (CBMT)" which is equivalent to Conditional Probability Table (CPT) in BN. The belief propagation or evidence propagation in ENs can be done by traditional algorithms developed for inference in BN.

Details about EN can be found in a series articles of Simon et al. (Simon & Weber 2006, Simon & Weber 2009, Simon et al. 2008) So far, applications of EN can be found on the reliability evaluation of power distribution and aircraft servo-actuation

systems (Zhao 2010, Yang et al. 2011). It has also been used to help the safety analysis of aerospace systems (Jiang et al. 2011).

4 EVIDENTIAL NETWORK MODELING

4.1 *FT and equivalent EN structure*

Simon (Simon & Weber 2009) suggested converting a fault tree into an equivalent EN and presented the CBMT of "AND" and "OR" gate in a table form. EN models for other logic gates (e.g. "NOR" gate) that often used in FTA can also be expressed by EN models easily. The transformation of logic gates to EN structures are shown in Figure 1.

Though the equivalent EN structures look the same for the two logic gates in Figure 1, the Conditional Belief Mass Tables (CBMTs) are different. The CBMTs for AND and OR logic gates are defined and shown respectively in Tables 1 and 2 in which "N" means normal, "F" means failure and "$\{N, F\}$" means that the system is exclusively in one of the two conditions without distinguishing exactly which. This allows us to express uncertainties on the states of events in FTs.

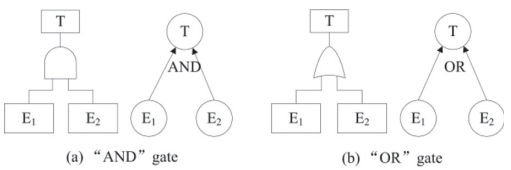


Figure 1. Logic gates and equivalent EN structures.

Table 1. CBMT for AND gate.

	E_1	N			F			$\{N, F\}$		
	E_2	N	F	$\{N, F\}$	N	F	$\{N, F\}$	N	F	$\{N, F\}$
T	N	1	1	1	1	0	0	1	0	0
	F	0	0	0	0	1	0	0	0	0
	$\{N, F\}$	0	0	0	0	0	1	0	1	1

Table 2. CBMT for OR gate.

	E_1	N			F			$\{N, F\}$		
	E_2	N	F	$\{N, F\}$	N	F	$\{N, F\}$	N	F	$\{N, F\}$
T	N	1	0	0	0	0	0	0	0	0
	F	0	1	0	1	1	1	0	1	0
	$\{N, F\}$	0	0	1	0	0	0	1	0	1

Unfortunately, the size of a CBMT increases exponentially with the number of input events. For a logic gate with three inputs, the size of the corresponding CBMT will be 81. This problem can be relieved by converting the logic gate to an equivalent form and add a "dummy" node in the corresponding EN. The process is shown in Figure 2. The sizes of the related two CBMTs in the modified equivalent EN are both 27 which make the total size 54 instead of 81. This greatly alleviates the computational labor when dealing with complex FTs.

4.2 *ET and equivalent EN structure*

Event trees are used to display sequences of events that can lead to specific end states. The headings of an ET are the Initiating Events (IE), the Pivotal Events (PEs), and the End States (ESs). An illustration of an ET is shown in Figure 3(a).

If end states are treated as a single node in ENs, the corresponding frame of discernment would include all the possible outcomes. The corresponding FD for the end states in Figure 3 can be defined by $\Theta = \{\{ES_1\}, \{ES_2\}, \{ES_3\}\}$. Then the power set of the ES node is then defined by $2^\Theta = \{\emptyset, \{ES_1\}, \{ES_2\}, \{ES_3\}, \{ES_1, ES_2\}, \{ES_1, ES_3\}, \{ES_2, ES_3\}, \{ES_1, ES_2, ES_3\}\}$.

We call the elements in the power set of an ES node General End States (GESs) and use them as the states of ES nodes in ENs. For end states of an ET are influenced by all the pivotal events, the graphic representation of ETs in a network form is clear. The graphic representation of the ET in Figure 3(a) is shown in Figure 3(b).

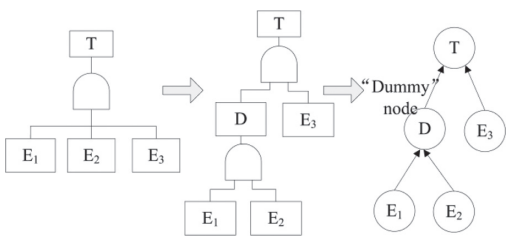


Figure 2. Transformation of logic gates with three inputs.

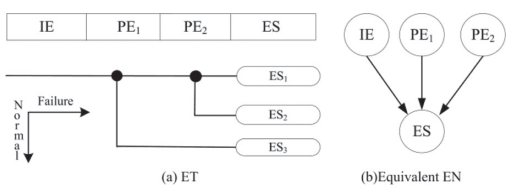


Figure 3. ET and equivalent EN.

In a PRA process, the PEs in an ET are analyzed as top events using FTA techniques. As stated in Section 5.1, the state of each PE is presented by $\{N, F, \{N, F\}\}$. For each combination of states of PEs, the outcome can be found in the state power set of the ES node. The combination of every PE states in Figure 3 and its corresponding (generalized) end states are shown in Table 3.

As shown in Figure 3, when PE_1 is in normal state "N", the end state would be "ES_3" regardless of PE_2. When PE_1 fails, end state would be ES_1 or ES_2 depending on the state of PE_2. We cannot be sure which one will the end state be if the state of PE_2 is characterized by $\{N, F\}$. Then the generalized end state $\{ES_1, ES_2\}$ is adopted. If the states of all the PEs in ET are characterized by $\{N, F\}$ which means the ignorance of which branch will the event sequence take after each PE, the end state is then characterized by $\{ES_1, ES_2, ES_3\}$.

Table 4 shows the CBMT for the EN in Figure 3, which is equivalent to Table 3. The information contained in an ET can be completely transferred into an EN structure with the corresponding CBMT.

Noticing from the CBMT in Table 4, the size of a CBMT also faces the problem of state explosion. With n end states and m pivotal events the size of the ET's CBMT is $3^m \times (2^n - 1)$.

Table 3. PE states and corresponding GESs.

PE_1	PE_2	GES
N	N	ES_3
	F	ES_3
	$\{N, F\}$	ES_3
F	N	ES_2
	F	ES_1
	$\{N, F\}$	$\{ES_1, ES_2\}$
$\{N, F\}$	N	$\{ES_2, ES_3\}$
	F	$\{ES_1, ES_3\}$
	$\{N, F\}$	$\{ES_1, ES_2, ES_3\}$

Fortunately, we don't have to add ES nodes to ENs clumsily. The end states we are interested in must be included in the GESs. By computing the joint probabilities of the combinations of PEs' states corresponding to those GESs, the information of the interested end states can be obtained. Take Table 3 for example, if we want to get the information about ES_1, only general end states $\{ES_1\}$, $\{ES_1, ES_2\}$, $\{ES_1, ES_3\}$, $\{ES_1, ES_2, ES_3\}$ should be considered. Thus, the joint probabilities of corresponding combinations of PEs' states $\{F, N\}$, $\{F, \{N, F\}\}$, $\{\{N, F\}, N\}$, $\{\{N, F\}, \{N, F\}\}$ carries the information of ES_1.

4.3 *Basic belief assignment for basic events*

Leaf nodes in ENs represent basic events. The belief masses must be assigned in order to make the EN inference process work. Expert knowledge is used to define the probability of occurrence. Generally, there are two ways of expressing uncertainties to get the belief masses.

1. Experts give values of $m(N)$, $m(F)$ and $m(N, F)$ of a leaf node directly.
2. Experts give values of the lower and upper bound of $m(F)$ (i.e. $Ble(F)$ and $Pl(F)$) or $m(N)$. From plausibility and belief measures, the basic mass assignment is computed by the Möbius transform. Here we have

$$\begin{cases} m(F) = Bel(F) \\ m(N) = 1 - Pl(F) \\ m(N,F) = Pl(F) - Bel(F) \end{cases} \tag{5}$$

For CCFs, the value of a β factor is given by the interval $[\beta_1, \beta_2]$ $(0 < \beta_1 < \beta_2 < 1)$.

1. If the total failure probability is given as a crisp value $P_{(T)}$, then the failure probability due to CCFs can be obtained as $[\beta_1 P_{(T)}, \beta_2 P_{(T)}]$, the failure probability due to independent failure $P_{(I)}$ can be obtained as $[(1 - \beta_2)P_{(T)}, (1 - \beta_1)P_{(T)}]$.

Table 4. CBMT for EN in Figure 3.

	PE_1	N			F			$\{N, F\}$		
	PE_2	N	F	$\{N, F\}$	N	F	$\{N, F\}$	N	F	$\{N, F\}$
GES	ES_1	0	0	0	1	0	0	0	0	0
	ES_2	0	0	0	0	1	0	0	0	0
	ES_3	1	1	1	0	0	0	0	0	0
	$\{ES_1, ES_2\}$	0	0	0	0	0	1	0	0	0
	$\{ES_1, ES_3\}$	0	0	0	0	0	0	1	0	0
	$\{ES_2, ES_3\}$	0	0	0	0	0	0	0	1	0
	$\{ES_1, ES_2, ES_3\}$	0	0	0	0	0	0	0	0	1

Basic belief assignment of the CCF events can then be calculated using Equation (5).

2. If the total failure probability is given as values of the lower and upper bound of $m(F)$ (i.e. $Ble(F)$ and $Pl(F)$), the failure probability due to CCFs can be obtained as $[\beta_1 Ble(F), \beta_2 Pl(F)]$, the failure probability due to independent failure can be obtained as $[(1-\beta_2)Ble(F), (1-\beta_1)Pl(F)]$. Basic belief assignment of the CCF event can then be calculated using Equation (5).

The belief masses assigned to leaf nodes from different experts are then combined together by the DS combination rule (e.g. Eq. (4)). Combined belief masses are then used in ENs.

5 CASE STUDY

The approach described above has been applied to an ET/FT analysis that described in (Nývlt & Rausand 2012). It's a part of a probabilistic risk assessment of the Strahov highway tunnel in Prague, Czech Republic.

5.1 *Event tree and associated fault trees for the case study*

The event tree is shown in Figure 4. It consists of one initiating event, three pivotal events and five end states. The initiating event is fire in one of the two tunnel tubes.

The pivotal events are listed as follows:

1. Fire and Smoke Detection (FSD). The related FT is shown in Figure 5.
2. Fire and smoke control in the tube where the fire occurred (FSCA). The related FT is shown in Figure 6.
3. Smoke Control in the Escape Tube (SCET). The related FT is shown in Figure 7.

End state "$ICFE_1$" to "$ICFE_4$" means different degrees of insufficient conditions for evacuation. End state "OK" means the system works as planed and safety is secured when fire in one of the two tunnel tubes occurs.

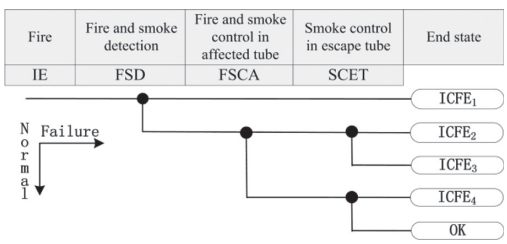


Figure 4. Event tree with initiating event "fire".

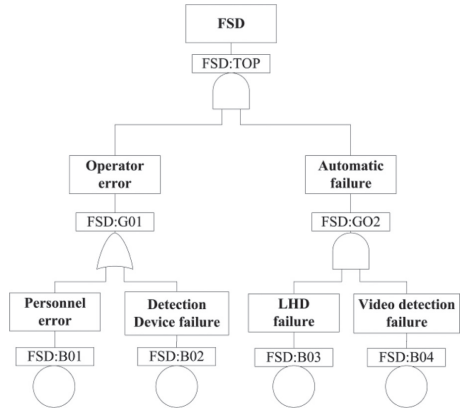


Figure 5. Fault tree for top event FSD.

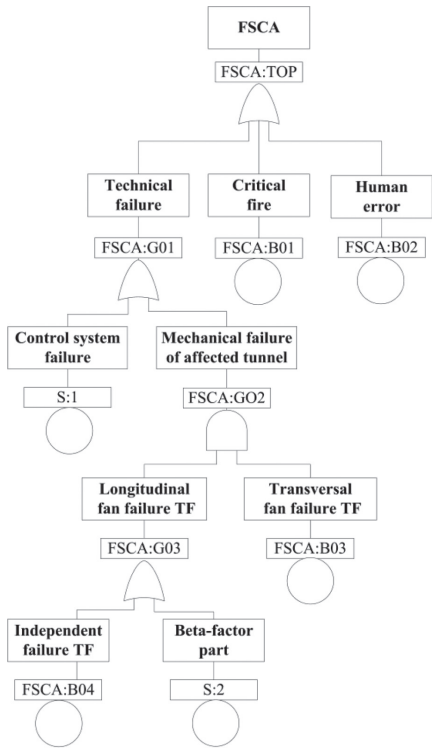


Figure 6. Fault tree for the top event FSCA.

The exact definitions of various events in the fault trees can be found in (Nývlt & Rausand 2012). Codes in the FTs starting with a letter "B" implies basic events, "S" implies shared events. It is evident that the FSCA and SCET fault trees are dependent. Traditional methods reach

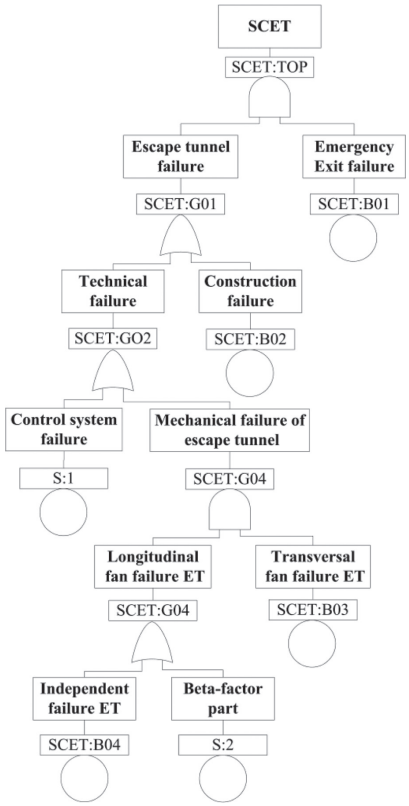


Figure 7. Fault tree for the top event SCET.

their limits, when uncertainties brought by CCF factor models are considered.

5.2 *FT/ET transformed to an EN*

The event tree and associated fault trees for the case study were converted to an EN according the approach described in section 4. The network obtained with the software MSBNX is presented in Figure 8.

5.3 *Basic belief assignment for basic events*

Basic belief masses were given by two unbiased and independent experts. The β factor were given

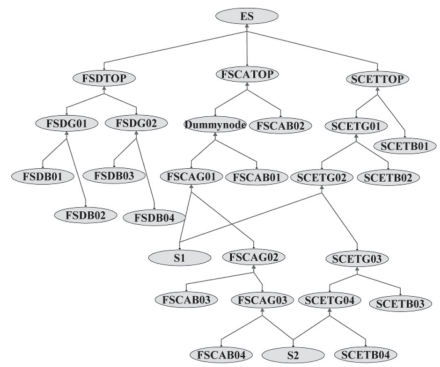


Figure 8. EN corresponding to ET/FTs in Figures 4–7.

Table 5. BBAs for basic events in Figure 7.

Basic events	Expert 1			Expert 2			Combined		
	N	F	$\{N, F\}$	N	F	$\{N, F\}$	N	F	$\{N, F\}$
FSD:B01	0.800	0.100	0.100	0.850	0.050	0.100	0.9657	0.0229	0.0114
FSD:B02	0.850	0.050	0.100	0.850	0.025	0.125	0.9760	0.0107	0.0134
FSD:B03	0.750	0.100	0.150	0.800	0.100	0.100	0.9408	0.0414	0.0178
FSD:B04	0.700	0.200	0.100	0.650	0.250	0.100	0.8489	0.1367	0.0144
FSCA:B01	0.950	0.005	0.045	0.700	0.150	0.150	0.9824	0.0097	0.0079
FSCA:B02	0.600	0.200	0.200	0.800	0.050	0.150	0.9013	0.0617	0.0370
FSCA:B03	0.700	0.200	0.100	0.800	0.150	0.050	0.9184	0.0748	0.0068
FSCA:B04*	0.810	0.090	0.100	0.862	0.088	0.050	0.9692	0.0249	0.0059
SCET:B01	0.800	0.150	0.050	0.700	0.200	0.100	0.9184	0.0748	0.0068
SCET:B02	0.750	0.120	0.130	0.800	0.090	0.110	0.9402	0.0427	0.0171
SCET:B03	0.750	0.150	0.100	0.700	0.200	0.100	0.8993	0.0872	0.0134
SCET:B04*	0.810	0.090	0.100	0.862	0.088	0.050	0.9692	0.0249	0.0059
S:1	0.900	0.020	0.080	0.850	0.020	0.130	0.9845	0.0048	0.0108
S:2*	0.980	0.005	0.015	0.982	0.008	0.010	0.9996	0.0002	0.0002
TPL**	0.800	0.100	0.100	0.8500	0.100	0.050	–	–	–

*BBAs for events related to CCFs were calculated in advance using method introduced in section 4.3.
**TPL is used to demonstrate the total failure probability of longitudinal fans.

Table 6. Probability of GES.

FSD	FSCA	SCET	GES	Probability
N	*N*	*N*	OK	0.86450
		F	ICFE4	0.00291
		{*N*, *F*}	{ICFE4, OK}	0.00154
	F	*N*	ICFE3	0.07614
		F	ICFE2	0.00060
		{*N*, *F*}	{ICFE2, ICFE3}	0.00022
	{*N*, *F*}	*N*	{ICFE3, OK}	0.05253
		F	{ICFE2, ICFE4}	0.00018
		{*N*, *F*}	{ICFE2, ICFE3, ICFE4, OK}	0.00086
F	…	…	ICFE1	0.00019
{*N*, *F*}	*N*	*N*	{ICFE1, OK}	0.00028
		F	{ICFE1, ICFE4}	–
		{*N*, *F*}	{ICFE1, ICFE4, OK}	–
	F	*N*	{ICFE1, ICFE3}	0.00002
		F	{ICFE1, ICFE2}	–
		{*N*, *F*}	{ICFE1, ICFE2 ICFE3}	–
	{*N*, *F*}	*N*	{ICFE1, ICFE3, OK}	0.00002
		F	{ICFE1, ICFE2, ICFE4}	–
		{*N*, *F*}	{ICFE1, ICFE2, ICFE3, ICFE4, OK}	–

Table 7. Frequency of the end states.

ES	Bel	Pl
$ICFE_1$	2.280E-8	6.120E-8
$ICFE_2$	7.200E-8	2.232E-7
$ICFE_3$	9.137E-6	1.555E-5
$ICFE_4$	3.492E-7	6.588E-7
OK	1.037E-4	1.104E-4

as [0.05, 0.1] by the first expert and [0.08, 0.12] by the second expert. Basic belief assignment for basic events in Figure 8 is shown in Table 5. The aggregation is performed using Equation (4). The presented expert estimates are idealized to illustrate the application of the proposed approach. We emphasize that they do not reflect the real failure behavior.

5.4 *Frequencies of end states*

Using the EN structure in Figure 8 and the combined basic belief masses listed in Table 5, the result was derived by BN inference using MSBNX and shown in Table 6.

"–" means the probability of the corresponding general end state is too small ($<10^{-5}$) that we simply ignore it. The initiating event frequency is given by $\lambda = 1.2 \times 10^{-4}$/yr. The frequencies of the end states were obtained using the belief function (e.g. Eq. (2)) and plausibility function (e.g. Eq. (3)). The final results are presented in Table 7.

6 CONCLUSION

The issue of failure dependency is crucial in PRA. Different tools have been used as uniform frameworks, which represent accident scenarios, to solve this problem. Traditional approaches for dependencies handling in PRA can be cumbersome and ignore the uncertainties brought by dependency modeling, which may lead to a false decision-making.

A different method is proposed in this paper. ETs and FTs are transformed into a single evidential network. Expert knowledge containing uncertainty information is combined using evidence theory. Uncertainties in basic events, including dependent events, are propagated through the new uniform structure. The frequency of each end state of interest is obtained. The proposed approach is applicable to handle dependencies in PRA in the following ways:

1. The proposed approach can be applied to dependencies across events in an ET.
2. Uncertainties in dependency measurements and basic events can easily be propagated through ENs with mature BN software.
3. The proposed approach addresses the uncertainties in experts' knowledge and uses knowledge from different sources to reach the final conclusion.

The failure dependency together with other uncertainty source will not be satisfying handled by only a probabilistic way due to limited data,

incomplete or imprecise information. Alternative epistemic uncertainty representation structures are more reasonable. However, many analyzers are still more comfortable with traditional probability distributions. Few would doubt that a probability distribution is an excellent way to depict uncertainties when enough data has been acquired. Thus, the inputs would often in the form of probability distribution, basic belief assignment. The framework for propagating uncertainties in different forms is needed. The construction of a hybrid framework that combines uncertainties in different forms may offer additional future improvement to the approach developed here.

REFERENCES

Andrews, J.D. & Dunnett, S.J. 2000. Event-tree analysis using binary decision diagrams. *IEEE Transactions on Reliability* 49(2): 230–238.

Barros, A., Grall, A. & Vasseur, D. 2009. Estimation of common cause failure parameters with periodic tests. *Nuclear Engineering Design* 239(4): 761–768.

Brand, V. 1996. UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems. AEA Technology.

Dempster, A.P. 1967. Upper and lower probabilities induced by a multivalued mapping. *Annals of Mathematical Statistics* 2: 325–339.

Fleming, K. 1974. A reliability model for common mode failures in redundant systems, In: Report GA-A13284. San Diego, CA, General Atomic Company.

Hoffman, F.O. & Hammonds, J.S. 1994. Propagation of uncertainty in risk analysis assessments: the need to distinguish between uncertainty due to lack of knowledge and uncertainty due to variability. *Risk Analysis* 14(5): 707–712.

Hosseini, S.M.H. & Takahashi, M. 2007. Combining static/dynamic fault trees and event trees using Bayesian networks. In proceeding of Computer Safety, Reliability, and Security: 26th International Conference, Nuremberg, Germany, 18–21 September, 2007.

Humphreys, R. 1987. Assigning a numerical value to the beta factor common cause evaluation. *In Proceeding of National Reliability Conference, Birmingham, England, 14–16 April, 1987.*

IAEA. 2000. IAEA-TECDOC-1135: Regulatory review of Probabilistic Safety Assessment Level 1.

Jiang, J., Li, X., Chen, Y. &s Yang, K. 2011. Evidential network and its application in safety analysis of aerospace systems. *Systems Engineer ing and Electronics* 33(6): 1270–1275.

Keller, W. & Modarres, M. 2005. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering and System Safety* 89: 271–285.

Khakzad, N., Khan, F. & Amyotte, P. 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety* 96: 925–932.

Nývlt, O., Prívara, S. & Ferkl, L. 2011. Probabilistic risk assessment of highway tunnels. *Tunnelling and Underground Space Technology* 26: 71–82.

Nývlt, O. & Rausand, M. 2012. Dependencies in event trees analyzed by Petri nets. *Reliability Engineering and System Safety* 104: 45–57.

Rutledge, P.J. & Mosleh, A. 1994. An analysis of spacecraft dependent failures. Proceedings of the Second International Conference on Probabilistic Safety Assessment and Management (PSAM-II); San Diego California, 20–25 March, 1994.

Simon, C. & Weber, P. 2006. Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. *IEEE Transactions on Reliability* 58(1): 68–86.

Simon, C. & Weber, P. 2009. Imprecise reliability by evidential networks. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability* 223(2): 119–140.

Simon, C., Weber, P. & Evsukoff, A. 2008. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. *Reliability Engineering and System Safety* 93: 950–963.

Smets, P. 1990. The Combination of evidence in the transferable belief model. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 12(5): 447–458.

Song, H. 2007. The Studies of methodology and applications for common cause failure analysis of probabilistic safety assessment for third Qinshan nuclear power plant. Shanghai Jiao-tong University.

Stamatelatos, M. 2002. Probabilistic risk assessment procedures guide for NASA managers and practitioners Version 1.1. Washington D.C, office of safety and mission assurance, NASA headquarters.

USNRC. 1998a. NUREG/CR-5497: Common-cause failure parameter estimations.

USNRC. 1998b. NUREG/CR-6268: Common-cause failure database and analysis system.

Weber, P. Medina-Oliva, G. Simon, C. & Iung, B. 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence* 25: 671–682.

Yang, J., Wen, D., Huang, H. & Sun, R. 2011. Reliability analysis of aircraft servo-actuation systems using evidential networks. *International Journal of Turbo and Jet Engines* 29(2): 59–68.

Zhao, S. 2010. Power distribution system reliability evaluation by D-S evidence inference and Bayesian network method. IEEE 11th International Conference on Probability Methods Applied to Power System (PMAPS), Singapore, 14–17 June, 2010.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The use of geoevents in the risk management of Wastewater Treatments

G. Ancione & M.F. Milazzo
University of Messina, Messina, Italy

G. Maschio
University of Padova, Padua, Italy

ABSTRACT: Volcanic eruptions can endanger human health and threat structures, critical infrastructures and lifelines (such as wastewater treatments, electricity networks, etc.), even relatively moderate events often can cause severe damages and economic losses. Among different volcanic phenomena, this paper focuses on the study of the damage triggered by explosive volcanic eruptions (i.e. those causing volcanic ash emissions), due to the large impact area of the particles dispersion. In particular the focus is on the implementation of a procedure for the management of wastewater treatment equipment by using a GIS (Geographic Information System). To achieve this aim, the volcanic ash dispersion in the atmosphere has been considered a *geoevent* because of the possible description of its evolution by means of its geographical coordinates. The evolution representation for the cloud allows the management of the potential impacts on wastewater treatments.

1 INTRODUCTION

In the last decades, worldwide attention has been focused on the definition of procedures for the risk analysis to support the management of various types of emergency. It must be underlined that several European countries have to face various natural hazards, but appropriate management plans based on the definition of the hazards associated with technological accidents triggered by a natural event (so-called Na-Tech) are not designed (Cruz et al. 2004). In this context, Fabiano & Currò (2012) showed nearly 6.4% of the accidents, occurred in the oil industry, are due to natural phenomena. Furthermore after some important international meetings, various relevant research topics related to the process safety have been emerged, amongst these the Na-Tech category is significant (De Rademaeker et al., 2014). Amongst many natural phenomena (such as earthquake, flooding, tsunami, hurricanes, etc.) a growing attention recently has been paid to Na-Techs caused by volcanic eruptions.

The study of volcanic Na-Techs is relatively recent, some examples relate to the investigation of the effects of volcanic ash fallout on structures: Baxter et al. (1982) analysed the reduction of functionality of water treatment systems and the hazards related to the transportation of hazardous materials due to slippery road conditions; Spence et al. (2004) evaluated the vulnerability of buildings; Rasà et al. (2007) qualitatively described the effects of the ash fallout on building, electric motors and other systems; Milazzo and co-authors analysed the fragilities of atmospheric storage tanks (Milazzo et al. 2013a) and filtering systems (Milazzo et al. 2013b). Some of these studies have been used to manage the risk associated to volcanic Na-Techs trigged by the emission of volcanic ash; an example is given in the work of Milazzo et al. (2013c), which describes a GIS-based tool for the vulnerability mapping of industrial facilities under the impact of volcanic Na-Techs. A recent survey of Ancione et al. (2014) has provided a preliminary study of Na-Techs in a generic wastewater treatment plant. Ancione and co-workers highlighted the most relevant investigations given by the literature; moreover, the causes of failure, associated with the fallout of volcanic ash, have been identified for the main equipment included in such system.

The support of a GIS could be useful for the management of technological hazard triggered by the ash fallout; in this context, the volcanic ash emission in the atmosphere could be considered as a *geoevent*, this term identifies a graphical representation of the evolution of the scenario (in this case the plume and the associated fallout) by means of its geographical coordinates. A *geoevent* can be considered as a dynamic event, in some cases, its graphical representation can provide a valid support to risk managers. It is worth noting that the risk management activities could be difficult if the territory is characterized by the presence of a great urbanization, of numerous chemical industries and of a complex network of lifelines.

In the literature there are few methods and tools, developed for the risk management by using dynamic events; the available methods are applied to the management of the transport of hazardous materials (Giglio et al. 2004) and the terrorist actions accomplished by the use of dangerous substances (Milazzo et al. 2009). Other papers relate the management of industrial scenarios triggered by natural events such as the previous mentioned work of Milazzo et al. (2013c), in which a GIS tool is used to obtain vulnerability equipment to a natural phenomenon. Girgin & Krausmann (2013) provides an on-line, integrated Na-Tech risk assessment and mapping framework; whereas Demichela et al. (2013) use a GIS-based application to make an assessment of the vulnerability for human targets due to volcanic ash fallout.

This paper focuses on the management of Na-Tech hazards in wastewater treatments, triggered by the occurrence of explosive volcanic eruptions with strong ash emission. The use of a GIS provides an integrated management tool, due to the support of advanced systems for the data management, analysis and visualization.

The first part of the paper briefly describes the characteristics of a generic wastewater treatment plant; in the second part, the procedure and the implementation of the GIS-based tool is presented. Finally, in the third part, some results related to a case-study are also given, with a brief discussion.

2 WASTEWATER TREATMENT PLANTS

Water is a very valuable commodity, for this reason water supplies must be preserved and protected, but after its use, it must be purified and reused. The water purification is made through a wastewater treatment plant, which is composed by the combination of some processes' units. These units are briefly described in the following.

The primary mission of the wastewater treatment plant is to treat the wastewater stream, coming from the sewage, to an acceptable level of purity, by reducing or removing organic matter, solids, nutrients, disease-causing organisms and other pollutants; then the stream return to the environment by discharging into a water body or by an immediate reuse (i.e. irrigation, etc.).

A wastewater treatment is divided into three phases, these are as shown in Figure 1: (1) physical or primary treatments, (2) biological or secondary treatments and (3) chemical or tertiary treatments.

In the first stage, primary large solids and grit are removed by means of screenings; then the sewage stands in a tank in order to cause the sinking of suspended solids to the bottom and the rise of oil and grease to the surface. The solids are scraped off

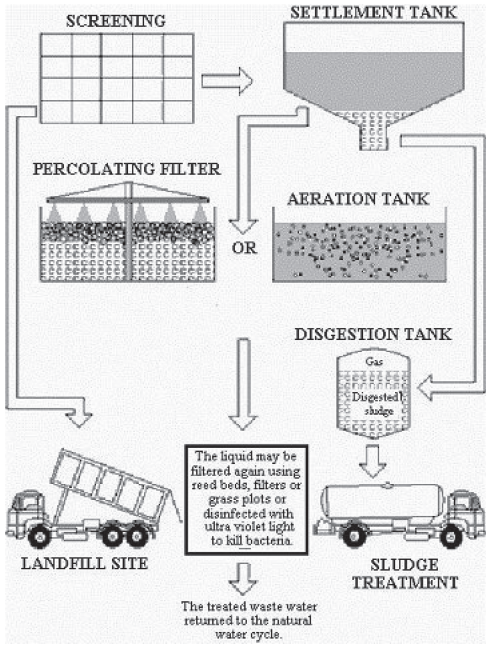


Figure 1. Wastewater treatment (website of The University of Waterloo).

from the bottom and the scum is washed off with water jets. The removed materials form sludge.

In the second stage, the liquid undergoes to a biological treatment; bacteria breakdown the solubilised organic matter. Then the stream is sent to oxidation ponds where heterotrophic bacteria continue the breakdown of the organic matter. Sludge is formed into the whole process; it is treated in large heated tanks, where its decomposition is catalyzed by anaerobic microorganisms (Website of the New Zealand Institute of Chemistry).

In the third phase, the processes aim at the removal of the additional suspended and dissolved solids, the refractory organics, the heavy metals, nitrogen and phosphorus. The equipment used depends on the specific contaminants which have to be removed. Sometimes this phase is not necessary.

3 METHODOLOGY

As mentioned above, the approach described in this paper needs to be supported by a Geographical Information System, or simply GIS. Figure 2 shows a simply scheme of the proposed methodology for the management of Na-Techs.

Firstly two databases must be constructed: the first database collects the volcanic eruptive scenarios and second one stores data about the

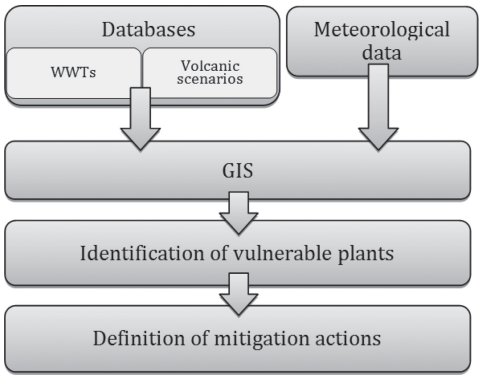


Figure 2. Methodology.

wastewater treatments located on the territory. Furthermore the GIS could be used to include other information related to the distribution of urban centres, the use of the territory, the electric network, the water supply network, etc.

In order to identify the impact areas for each eruptive scenario, a threshold value of thickness for the ash deposit must be defined. To achieve this scope, the data of different works have been examined: Day & Fisher (1980) discussed that serious problems occur with deposit >10 mm (although these are rare events); Blong (2003) reported about the eruption of Mt. Spurr in Alaska, where 3 mm of volcanic ash (~5000 g/m^2) fell on Anchorage in 1992 and caused many pipe blockages; in 2002, during the eruption of Mt. Etna (Italy), small amounts of ash caused the blockages of the rainwater drainage systems in the city of Catania (Barnard 2004), due mainly to the formation of not easily pumped material. To make this analysis conservative, a threshold limit of deposit of 1000 g/m^2 has been considered.

The use of real-time meteorological information (i.e. wind direction and velocity) and the characteristics of the eruption (emission rate) allows the selection of the scenario and its incorporation into the GIS. The impact of the *geoevent* on the territory is then easily evidenced because a map quickly identifies the impact area and the potential WWTs, which are involved at different time from the starting of the eruption. Their identification allows focusing on the mitigation actions for the plants.

The last step of the approach regards the definition of the measures that could be implemented to protect some parts of the wastewater treatment. These can be:

- the timely cleaning of roads;
- putting in place all protective measures for each equipment (i.e. the coverage of settling tanks);
- the extraordinary maintenance of the WWT.

The use of the available resources must be rational, especially when this requires the use of public funding.

4 A CASE STUDY

To show how the approach, implemented within the GIS, works, an application to the surrounding of Mt. Etna (Italy) has been carried out.

4.1 *Databases*

A census of wastewater treatments has been made; Figure 3 shows the graphical inventory, where also a legend of colour highlights the inhabitants for each area identified in the region. The collected data has been extracted by ARPA-Sicilia (2012); it can be observed that the WWTs are distributed in the whole region (Sicily) and several of them serve small urban areas. The number of wastewater treatments per provinces in Sicily is given in Table 1; the total operating plants are 225.http://www.arpa.sicilia.it/UploadDocs/6286_acque_reflue_report_2012.PDF.

Mt. Etna is a volcano located in the Southern Italy; Figure 4 shows the location (Sicily). Its surrounding is characterised by the presence of the city of Catania, many small urban centres and agricultural and industrial areas. The volcano has recently changed its eruptive style, giving more frequent explosive eruptions with strong emission of ash in the atmosphere (Branca & Del Carlo 2013). A number of eruptive scenarios have been collected from the literature and the related iso-deposit maps at different time have been stored in the GIS-database. The effects of the territorial morphology are taken into account during the execution the simulation of the scenarios. The simulations would be executed by considering a number of classes of potential wind direction and velocity and of volcanic ash emission rate.

4.2 *Meteorological data*

The use of the developed GIS-tool allows the representation of the evolution of the deposit by means of the meteorological data. The wind direction is needed to conservatively drawn the deposit formation, which will be selected according to the classes mentioned above for the wind and the emission rate.

4.3 *Identification of vulnerable plants*

The GIS allows discerning those facilities which will be potentially exposed to the ash fallout and

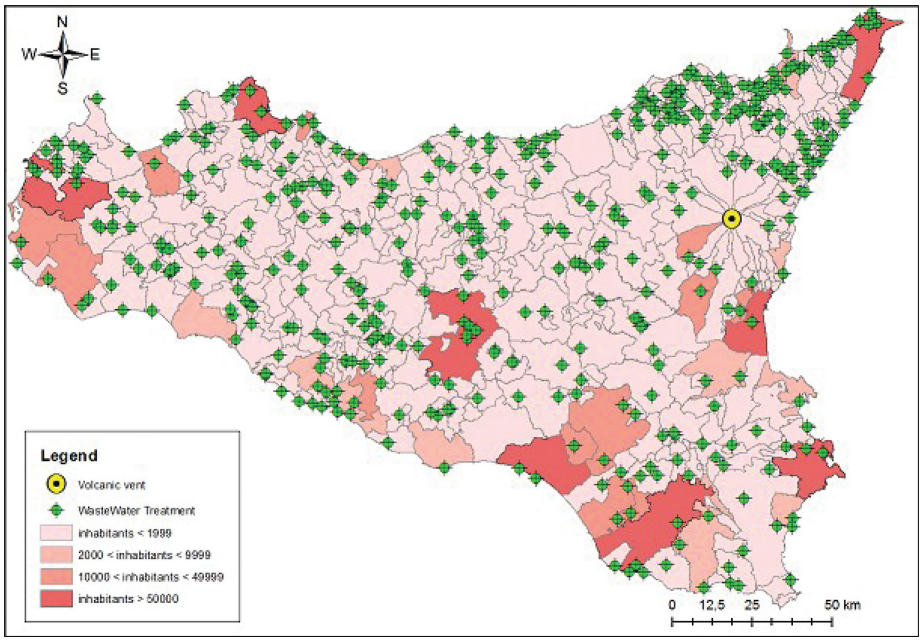


Figure 3. Census of wastewater treatments in Sicily (Italy).

Table 1. Reference samples for the study (ARPA-Sicilia 2012).

City	Plants	Operating plants
Agrigento	50	28
Caltanissetta	28	24
Catania	37	29
Enna	25	13
Messina	114	100
Palermo	70	68
Ragusa	22	21
Siracusa	12	12
Trapani	29	26

the time when the impact will occur. This means that the *geoevent* permits to gain time in activating the rights mitigation actions on WWTs and, thus, minimizing economic losses and human resources.

4.3.1 *Effect of the rainwater on ash deposit (experimental test)*

According to Milazzo et al. (2014), the effect of the water on ash deposit is significant due to the formation of aggregates of particles.

An experimental test has been executed in the laboratory to achieve a qualitative estimate of the amount of ash which will be dragged away by the rainwater. Figure 5 schematizes the simple apparatus used for the experimental test. A valve regulates the water flow rate into a drainage channel where, to simulate the eruptive scenario, a certain thickness of ash was uniformly



Figure 4. Location of Mt. Etna.

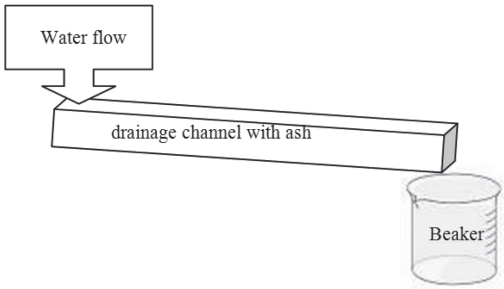


Figure 5. Schematization of the apparatus for the experimental test.

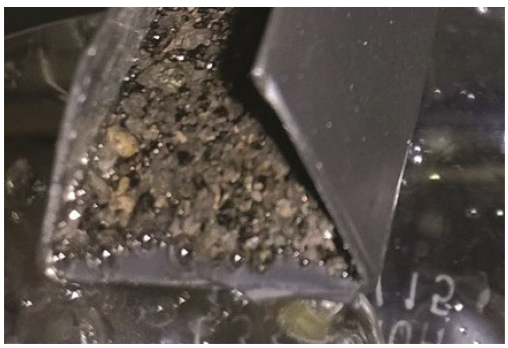


Figure 6. Ash deposit in the drainage channel (non-compacted layer).



Figure 7. Ash aggregates in the drainage channel (compacted layer).

distributed; finally a tank (beaker) collects the water flowing through the channel. It must be underlined that during the experimental test, the water flowed very slowly, simulating a light rain (for 90 min).

To execute the experimental test, 20 g of ash (with particles having an average diameter of 0.5 mm) have been deposited in a drainage channel (length = 20 cm, width = 1 cm). A constant flow-rate of water (~0.0023 L/s) has been set (Fig. 6). To verify the reproducibility of the experiment, it has been performed several times. Each test has shown that about 50% of ash is dragged away, the remaining part forms a compacted layer and the water flows on it (Fig. 7).

5 RESULTS

Ash deposits, related to the case-study, are represented using iso-deposit curves on cartography. Figure 8 refers to the explosive eruption of Mt. Etna occurred on the 11th November 2013. A legend of colours has been defined, where each colour is associated with a class of thickness of ash on the ground. The same figure shows the wastewater treatments which could be impacted if a similar scenario occurs. The GIS quickly provides the information that the risk managers needs to put in effect mitigation measures.

To demonstrate the GIS-tool support in planning the actions to protect WWTs, an example of its use is shown relatively to the case of the occurrence of an event similar to the worst-case scenario of Mt. Etna. The worst case scenario refers to the event occurred in the period 27th October–30th December 2002; its mass flow rates was about 10^5 kg/s. Assuming that the weather condition guide the ash plume as shown in Figures 9 and 10, where the iso-deposit curve related to the previous fixed threshold limit (1000 g/m^2) is shown, it is possible to identify the wastewater treatments involved at different time from the beginning of the explosive eruption.

Figure 9 shows the scenario after 12 hours, the GIS-tool evidences 4 plants are involved. Figure 10 is related to the same scenario after 24 hours, at that time 7 plants are impacted.

The procedure permits to choose the actions to be taken to protect the facilities. The risk manager is able to define their priority and the available resources in real-time. Obviously, actions to mitigate the impact of ash fallout on facilities should be previously stored into the GIS. Thus when the event occurs, the software gives back the adapted information; as an example it is possible: to underline the presence/absence of covers for sedimentation tanks; to highlight which roads need to be swept and their priority, in order to avoid the clogging of drainage systems; to quickly identify the location of the closest disposal sites.

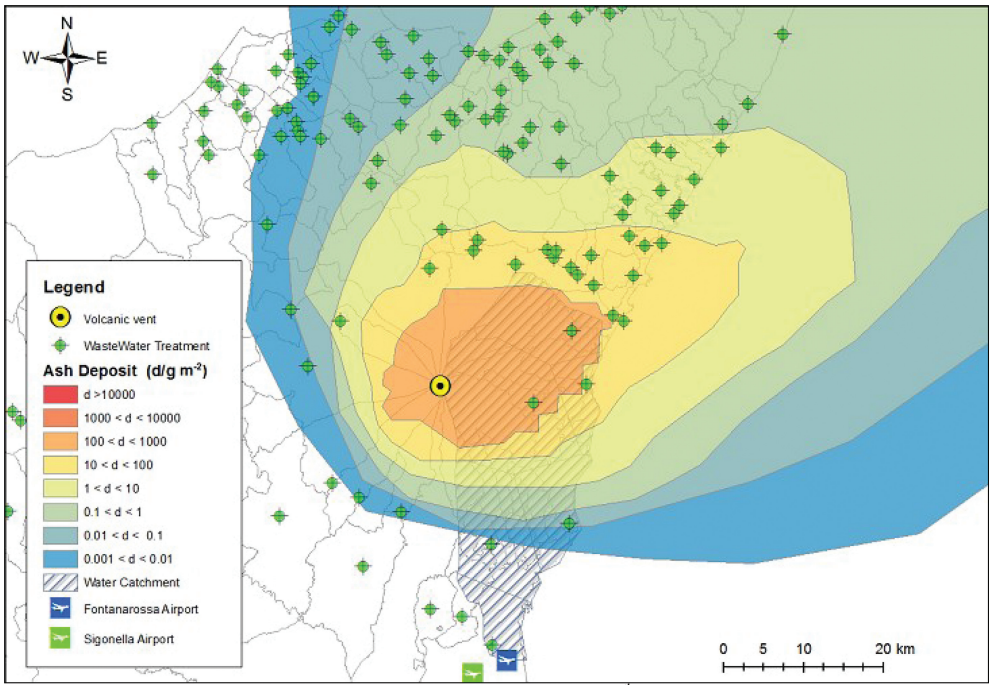


Figure 8. Iso-deposit curves for the explosive eruption of Mt. Etna of the 11th November 2013.

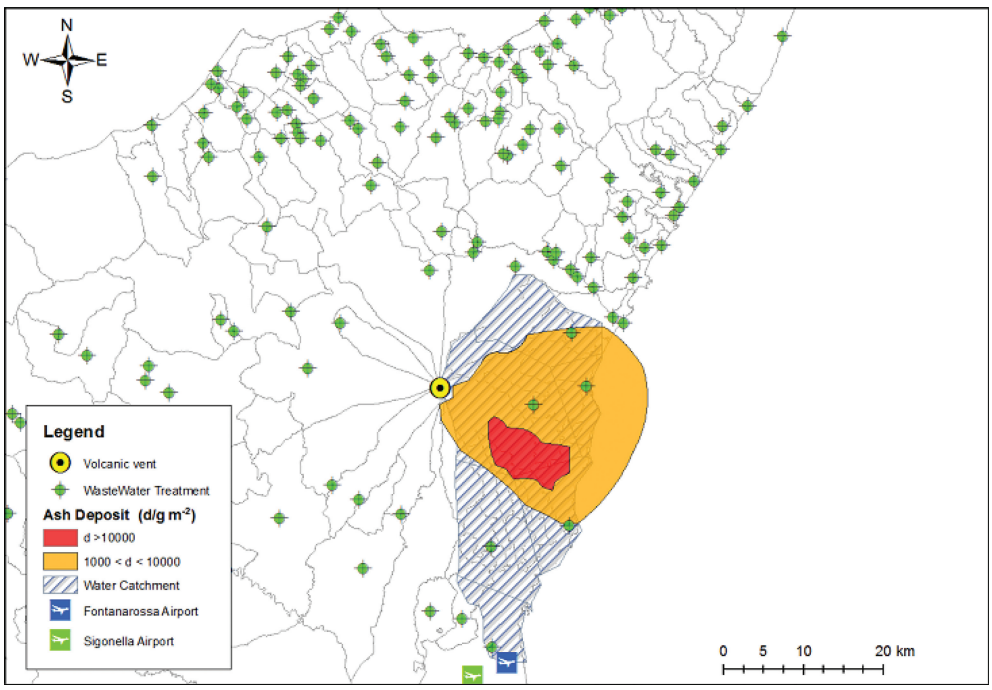


Figure 9. Map of ash deposits of the worst-case scenario after 12 hours.

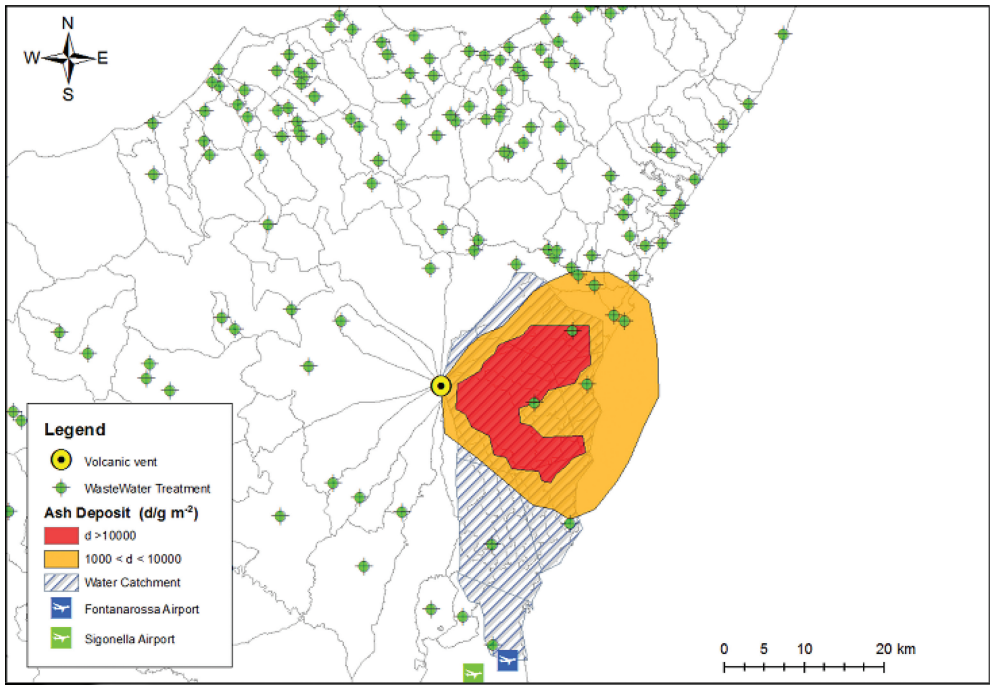


Figure 10. Map of ash deposit of the worst-case scenario after 24 hours.

6 CONCLUSIONS

In this work a procedure for the risk management in wastewater treatments has been defined by means of the representation of *geoevent*.

The objective has been to provide to risk managers and planners useful tools for the emergency planning associated with volcanic Na-Tech scenarios.

The proposed approach is applicable to different case-studies. It requires the knowledge of volcanic scenarios, territorial and meteorological data. It allows the optimum use of resources to manage several wastewater treatment plants. Its use can also be applied to other kind of facility vulnerable to this natural phenomenon.

REFERENCES

Ancione, G., Salzano, E., Maschio, G. Milazzo, M.F. 2014. Vulnerability of wastewater treatment plants to volcanic Na-Tech events. *Chemical Engineering Transactions,* 36, 433–438. doi: 10.3303/CET1436073.

Arpa-Sicilia 2012. Attività di controllo presso gli impianti di depurazione delle acque reflue urbane. Anno 2012. Agenzia Regionale per la Protezione dell'Ambiente.

Barnard, S.T. 2004. Results of a reconnaissance trip to Mt. Etna, Italy: The effects of the 2002 eruption of Etna on the province of Catania. *Bulletin of the New Zealand Society for Earthquake Engineering,* 37, 47–61.

Baxter, P.J., Bernstein, R.S., Falk, H., French, J. Ing, R. 1982. Medical aspects of volcanic disasters: An outline of the hazards and emergency response measures. *Disasters,* 6, 268–276. doi: 10.1111/j.1467-7717.1982.tb00549.x.

Blong, R. 2003. Building damage in Rabaul, Papua New Guinea, 1994. *Bulletin of Volcanology,* 65, 43–54. doi: 10.1007/s00445-002-0238-x.

Branca, S. Del Carlo, P. 2013. Eruptions of Mt. Etna During the Past 3,200 Years: a Revised Compilation Integrating the Historical and Stratigraphic Records. *Mt. Etna: Volcano Laboratory.* American Geophysical Union.

Cruz, A.M., Steinberg, L.J., Arellano, A.L.V., Nordvik, J.-P. Pisano, F. 2004. State of the art in Natech risk management. *European Commission Directorate General Joint Research Centre, EUR,* 21292.

Day, T.G. Fisher, J.E. 1980. Mt. St. Helens: How a Wastewater Plant Coped with Its Aftermath. *Journal (Water Pollution Control Federation),* 52, 2082–2089. doi: 10.2307/25040848.

Demichela, M., Maschio, G., Milazzo, M.F. Salzano, E. 2013. Vulnerability assessment for human targets due to ash fallout from Mt. Etna. *Chemical Engineering Transactions,* 32, 445–450. doi: 10.3303/CET1332075.

De Rademaeker, E., Suter, G., Pasman, H., Fabiano, B. 2014. A review of the past, present and future of the European loss prevention and safety promotion in the process industries. *Process Safety and Environmental Protection*, http://dx.doi.org/10.1016/j.psep.2014.03.007.

Fabiano, B., Currò, F. 2012. From a survey on accidents in the downstream oil industry to the development of a detailed near-miss reporting system. *Process Safety Environmental Protection* 90: 357–367.

Girgin, S. Krausmann, E. 2013. RAPID-N: Rapid natech risk assessment and mapping framework. *Journal of Loss Prevention in the Process Industries,* 26, 949–960. doi: http://dx.doi.org/10.1016/j.jlp.2013.10.004.

Milazzo, M.F., Ancione, G., Lisi, R., Vianello, C. Maschio, G. 2009. Risk management of terrorist attacks in the transport of hazardous materials using dynamic geoevents. *Journal of Loss Prevention in the Process Industries,* 22, 625–633. doi: 10.1016/j.jlp.2009.02.014.

Milazzo, M.F., Ancione, G., Basco, A., Lister, D.G., Salzano, E. Maschio, G. 2013a. Potential loading damage to industrial storage tanks due to volcanic ash fallout. *Natural Hazards,* 66, 939–953. doi: 10.1007/s11069-012-0518-5.

Milazzo, M.F., Ancione, G., Salzano, E. Maschio, G. 2013b. Risks associated with volcanic ash fallout from Mt. Etna with reference to industrial filtration systems. *Reliability Engineering and System Safety*. doi: 10.1016/j.ress.2013.05.008.

Milazzo, M.F., Ancione, G., Salzano, E. Maschio, G. 2013c. Vulnerability of industrial facilities to potential volcanic ash fallouts. *Chemical Engineering Transactions,* 31, 901–906. doi: 10.3303/CET1331151.

Milazzo, M.F., Primerano, P., Ancione, G., Salzano, E. Maschio, G. 2014. Potential damages of atmospheric storage tanks due to volcanic ash aggregations in presence of water. *Chemical Engineering Transactions,* 36, 487–492. doi: 10.3303/CET1436082.

New Zealand Institute of Chemistry. *Sewage Treatment* [Online]. Available: http://nzic.org.nz/ChemProcesses/water/ [Accessed 30-03-2014].

Rasà, R., Tripodo, A., Casella, S. Szilagyi, M.L. 2007. Contributi alla valutazione della pericolosità e rischio vulcanico nell'area etnea ed alla mitigazione dei danni attesi. "Carta Tematica di Rischio Vulcanico della Regione Sicilia" Regione Sicilia Palermo: Ed. C.R.P.R.

Spence, R.J.S., Baxter, P.J. Zuccaro, G. 2004. Building vulnerability and human casualty estimation for a pyroclastic flow: a model and its application to Vesuvius. *Journal of Volcanology and Geothermal Research,* 133, 321–343. doi: http://dx.doi.org/10.1016/S0377-0273(03)00405-0.

University of Waterloo. *Water Treatment* [Online]. Available: http://www.science.uwaterloo.ca [Accessed 02-03-2014].

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Utilizing knowledge-to-number-processes in smaller and less resource intensive risk assessments

T. Askeland & R. Flage
University of Stavanger, Norway

ABSTRACT: Turning knowledge and lack of knowledge into numbers (probabilities) is common practice in risk assessments, and several formal procedures exist today for expert elicitation of probabilities. However, these processes are often quite rigorous and extensive, while many smaller risk assessments have constraints in both cost and time, resulting in limited resources available for such processes, even though the need for numbers based on expert knowledge is essential. Thus, there is a need for less resource intensive knowledge-to-number processes, for use in the increasing number of smaller risk assessments being performed in today's society.

The aim of this paper is to review current literature within formal expert eliciting to identify if there are vital activities that can be applied also in smaller risk assessments with limited time and budgets, and to suggest a simplified process for turning knowledge into number in these assessments.

We start by discussing the fundamental issue of turning knowledge into numbers, before summarizing activities that are commonly recommended in formal expert eliciting processes. We then discuss how these activities can be utilized in smaller risk assessments, pointing out minimum activities relevant to ensure confidence in the result. Including a qualitative strength-of-knowledge assessment step to the suggested process is a main contribution of the present paper.

1 INTRODUCTION

Risk characterization is commonly based on using probability as a tool for describing epistemic uncertainty. Often there is little or no relevant data to base these probabilities on, resulting in significant reliance on expert statements. Expert eliciting processes as described by e.g. Meyer & Booker (1991), Cooke (1991) and O'Hagan et al. (2006) are processes for transforming knowledge and lack of knowledge into numbers (probabilities) through rather extensive processes. Moreover, the increasing use of risk assessments across most sectors in today's society has also led to an increased use of less extensive and less resource intensive risk assessments. Quantifying annual losses due to operational risk events in the bank sector, planning new road or rail tunnels, and documenting acceptable risk when using other than pre-accepted solutions in building design, are all examples of application areas where less extensive risk assessments are ubiquitous. These risk assessments are carried out within a relatively short time-frame and usually do not involve modelling and uncertainty aggregation resulting in overall risk indices, but are rather based on assignment of a single probability and expected consequence for hazards/threats individually. Formal expert elicitation processes involve activities that can then be too time consuming and resource intensive in this context.

Lack of data is a common challenge also for smaller risk assessments, meaning that expert knowledge remains an essential input, but inevitably, without use of the same rigorous framework for identification and training of experts, elicitation of numbers and post-processing that is common in comprehensive Quantitative/Probabilistic Risk Assessments (QRAs/PRAs).

There is hence a need for less resource intensive process for transforming knowledge to numbers for use in smaller risk assessments.

The aim of the present paper is to suggest a common platform and process for the utilization of a knowledge-to-number process in smaller risk assessments. This is done as follows: In Section 2 we first discuss the fundamental issue of turning knowledge into numbers, before reviewing activities that are commonly recommended in knowledge-to-number-processes. In Section 3 we discuss how these processes can be adapted and utilized in smaller risk assessments, resulting in a set of minimum activities necessary to ensure confidence in the result. A qualitative strength-of-knowledge assessment step in the suggested process is a main contribution of the present paper. Section 4 concludes.

2 DEFINITIONS AND FUNDAMENTAL ISSUES IN TURNING KNOWLEDGE TO NUMBERS IN RISK ASSESSMENTS

2.1 *The need for expert knowledge*

Risk assessments commonly use frequencies of observed events (i.e. historical data) as a major part of the basis for the risk assessment. To decide whether some available historical data is relevant for the future situation may be challenging. When in lack of data, or when we believe the past is not relevant for assessing the future, we turn to experts who possess knowledge that we consider relevant and want to apply in the assessments. We ask the experts to provide their opinion, and quantify degrees of belief using subjective probabilities.

2.2 *What is an expert?*

Meyer & Booker (1991 p. 85) define an expert as "… anyone especially knowledgeable in the field of detail being elicited—the individual should not be considered an expert unless he or she is knowledgeable at the level of detail being elicited." O'Hagan et al. (2006 p. 26) use a somewhat broader definition: "An expert may, in principle, just mean a person whose judgments are to be elicited."

Cooke & Goossens (2004) describe that the selection of experts may take place through a formal procedure, where the selection criteria are:

- Reputation in the field of interest
- Experimental experience in the field of interest
- Number and quality of publications in the field of interest
- Familiarity with uncertainty concepts
- Diversity in background
- Awards
- Balance of views
- Interest in the project
- Availability for the project

While Cooke & Goossens (2004) emphasize formal background to be defined as an expert, neither Meyer & Booker (1991) nor O'Hagan et al. necessarily define the expert as an academic person. In a risk assessment, also operational experience for example related to a particular piece of process equipment, or to local conditions in a land area, may be useful information. The knowledge of such details may make a person an expert, even without publications or awards, but through operational experience. A pump mechanic may be the best available expert on the pumps in the plant where he or she works. Requiring an expert to be used to work with probabilities in order to participate in a knowledge-to-number process reduces the availability of experts for smaller risk assessments. In this case, more guidance from the risk analyst may be appropriate, underlining the importance of the analyst's facilitation skills and competence.

2.3 *What is knowledge?*

Knowledge is defined in a wide variety of ways. One definition is that knowledge is "*information, gathered from experience and reasoning, that has been interpreted and can be used*" (Oxford dictionary of Environment and Conservation, 2013). By using this definition, we allow the pump mechanic to be an expert, because he or she through experience with daily use and maintenance of the pumps should be expected to have gathered knowledge about level of functionality, possible failures, etc.

2.4 *Activities in knowledge to number processes*

Several different approaches or processes for expert elicitation can be found in the literature. These are often tailored specifically to certain types of risks and sources of risk (Melnick et al. 2008). Some commonly referred processes are those described by Merkhofer (1987), Meyer & Booker (1991), Cooke & Goossens (2004) and O'Hagan et al. (2006).

Despite some variation in where the processes start and finish, and in the number and order of the steps, some common core elements can be distilled:

- Identification of need for expert knowledge
- Design of elicitation process
- Identification, selection, motivation and training of experts
- Elicitation
- Post elicitation work (aggregation and documentation)

A review of each of these steps is given in the following.

2.4.1 *Identification of need for expert knowledge*

The identification of need is as a trigger of the entire process. It is necessary to clarify why expert knowledge is required in the risk analysis process in the end, to ensure that the result from the process matches the need in the risk analysis. Expert judgment is especially suitable in the following settings (Meyer & Booker, 1991):

- To provide estimates on new, rare, complex, or otherwise poorly understood phenomena
- To forecast future events
- To integrate or interpret existing data
- To determine what is currently known, and what is not known.

2.4.2 *Designing elicitation process*

The references in Section 2.4 all include a design activity related to structuring the questions we want to ask the experts, even though they use some different expressions. Cooke (1991) defines some recognized principles to follow when designing an expert elicitation process:

- Reproducibility—it must be possible for scientific peers to review and to reproduce all calculations.
- Accountability—the source of expert subjective probabilities must be identified.
- Empirical control—expert probability assessments must in principle be susceptible to empirical control.
- Neutrality—the method for combining/evaluating expert opinion should encourage experts to state their true opinions.
- Fairness—all experts are treated equally, prior to processing the results of observations.

Cooke & Goossens (2004) focus on the identification of variables (target variables, query variables and performance variables), so do Merkhofer (1987), while Meyer & Booker (2009) focus on questions (question areas and particular questions). Of course, the identification of variables in the next step has to materialize into some questions before the experts enter the process, and many of the points made in these references are the same.

First, the variables to be considered need to be identified, and a procedure for doing so has to be designed; which may be more or less demanding. Furthermore, the variables may have to be decomposed. There are several reasons for this: First, decomposition gives a better understanding of causes and underlying factors. Secondly, even experts may not have a well-developed comprehension of very small probabilities (Aven, 2012). Decomposition is recommended by Merkhofer (1987), Meyer & Booker (1991) and O'Hagan (2006) as one of the major preparation step to an elicitation or as a part of the work for the experts, e.g. when doing a cause analysis. The use of decomposing improves the quality of the elicitation of subjective probability assessments (Kleinmuntz, 1996). The decomposing also reduces the difficulties experts may have in assessing very small probabilities.

Cooke (1991) argues that the design step should include a testing activity, where experts are tested before the elicitation by giving them questions from within their field of knowledge where the answer is known, although not to the experts. Such testing should be followed by a calibrating session, helping the expert to assess the "right" probability. Aven (2012, p 73) argues that calibration in general is not very useful to evaluate the goodness of the probability assignments in risk analysis, as the probabilities then needs to be evaluated before the observations. He rather sees calibration as a tool for training experts to provide input to the risk analysis, giving increased credibility to the expert.

Practical issues such as budget, time schedule, means of communication, remuneration etc. is a part of this design activity.

2.4.3 *Identify, select, motivate and train experts*

The identification, selection, motivation and training of experts is perhaps the step with the greatest variation between the procedures described in the literature. While Merkhofer (1987) starts the process by motivating the experts (thus presupposing that the expert is already identified and selected), Cooke & Goossens (2004) emphasize that all experts within the given area should be carefully identified according to a set of selection criteria. As many experts as possible should be selected, they argue, and as a minimum four experts.

Meyer & Booker (1991) warn of using too many experts together in an elicitation process, due to potential conflicts that may arise from group dynamics, such as "follow the leader" effect.

O'Hagan et al. (2006) present a similar but shorter list of selection criteria compared to Cooke & Goossens (2004), pointing out that the selection of experts has to be an open process when there is public interest or controversies attached to the process.

Cooke & Goossens (2004) suggest an expert training session, since most experts are not necessarily familiar with stating their degree of belief related to uncertain quantities. In the training session, the expert should be informed about the purpose of the upcoming elicitation process, as well as given practical information related to the process. The importance of giving the experts a good understanding of subjective probability is emphasized.

O'Hagan et al. (2006) propose a three-step training process, and point out that the training must be adapted to the assigned expert, i.e. there needs to be differentiated training depending on the expert's understanding of probabilities. The training should include:

- Probability and probability distributions.
- Information about the most common heuristics and biases, including advice about how to overcome them.
- Practice elicitation, particularly using examples where the true answer is known, but unlikely to be known by any of the experts.

Meyer & Booker (1991) emphasize training not only for the experts, but also for the team managing the process. Organizing a large elicitation process

with many experts and a tight schedule, the team management must be well prepared to avoid mistakes or misunderstandings, both methodically and logistically. However, this is not always relevant for smaller risk assessments, due to a small staff, even though it is a point always being well prepared, also when just eliciting one or a few expert.

Turning knowledge to numbers, through eliciting probabilities from experts, is a heavy mental process. According to Meyer & Booker (1991), the expert will perform four cognitive tasks during elicitation:

- Understanding the question
- Remembering the relevant information
- Making judgments
- Formulating and reporting an answer.

This process is often exposed to heuristics. Many sources concerning heuristics and biases within expert elicitation points at the work of Kahneman, et al. (1982), and in some degree Hogarth (1975). Kahneman et al. (1982) describe how we perform judgments, but are inclined to do so using heuristics—mental shortcuts used when processing information and analysis in human mind, leading to biases in the answers. Both Meyer & Booker (1991) and O'Hagan et al. (2006) emphasizes that giving the expert sufficient knowledge of these biases, as a part of their training is crucial.

2.4.4 *Elicitation*

The elicitation activity in a formal elicitation process is where knowledge actual becomes numbers. The activity may include one or more experts, face-to-face interviews, group sessions, or other types of communication. Garthwaite et al (2005) present an iterative process for this activity:

- Elicit specific summaries of the expert's distribution
- Fit a probability distribution to those summaries
- Assess adequacy: If adequate, then stop; otherwise repeat the process, asking the expert to make adjustments.

Meyer & Booker (1991) describe how different methodologies than face-to-face interviews can be used in a group elicitation, such as the Delphi technique, not to be further commented in this paper.

Even though focus is on turning knowledge to numbers, it must be emphasized that the expert knowledge can be utilized also to increase the understanding of phenomena when necessary. This can be done through a stand-alone activity, often followed by the elicitation of numbers. For example, when building an event tree it is necessary to understand the phenomena in order to establishing the tree, followed by the elicitation of numbers to fill into the tree.

2.4.5 *Post elicitation work*

When eliciting probabilities or distributions from several experts, the experience may be that the experts disagree to some extent. This disagreement can be followed up further, exploring the underlying assumptions, but at some point, we may have to use one number or distribution to represent the experts' input. O'Hagan et al. (2006) describe two ways of aggregating or combining the experts' responses:

- Mathematical aggregation (also called mechanical aggregation)
- Behavioral aggregation

Clemen & Winkler (1999 p. 188) define mathematical aggregation as "processes or analytical models that operate on the individual probability distributions to produce single combined probability distributions", and behavioral aggregation as an "attempt to generate agreement among the experts by having them interact in some way". Mathematical aggregation methods range from more sophisticated methods using axiomatic approaches or modeling of the aggregation process, taking care of dependence between the experts' opinions, to more simple measures, such as the arithmetic mean (Equation 1) or geometric mean (Equation 2).

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

$$\left(\prod_{i=1}^{n} x_i\right)^{1/n} = \sqrt[n]{(x_1 x_2 \ldots x_n)} \tag{2}$$

where n is number of probabilities/observations, and x_i the i'th probability/observation value.

Behaviour aggregation is the process where a group reaches consensus, by "*bring[ing] experts together in a group and eliciting their beliefs as if they were a single expert"* (O'Hagan et al., 2006 p. 186). Challenges with behavioural aggregation is more psychological than mathematical of nature (O'Hagan et al., 2006 p. 187), as the process is subject to several group dynamic biases. Behavioural aggregation may be very time consuming (Meyer & Booker, 1991 p. 118), but it can also increase the understanding of differences between the experts, clarifying the background knowledge available for each expert's view, being a valuable contribution to further analysis.

An interesting point made by Clemen & Winkler (1999) is that both more advanced mathematical approaches and behavioral aggregation often is outperformed by simple mathematical approaches. Furthermore, Meyer & Booker (1991 p. 317) show how little weighting of experts (proposed as a method when having more trust in one expert than

Table 1. Roles in a formal expert eliciting process.

Roles	C&G	Merk.	O'Hagan	M&B
Expert(s)	x	x	x	x
Analyst(s)	x	x	x	x
Statistician (s)	(x)	–	(x)	(x)
Adm. pers.	–	–	(x)	x
Decis. maker	x	–	x	x

in another) affect the mean. Extreme values affect much more, which can be handled by relying on the geometric mean rather than the arithmetic mean.

Kahneman, et al. (1982) argues for using the median rather than the mean in knowledge-to-number processes. They found that when experts were forecasting the mean value in a distribution, in reality they used a value that was more like the median. Kahneman, et al. (1982) found that the shape always had a skew-ness, resulting in an arithmetic mean different from the median. From this, Meyer & Booker (1991 p. 316) argue to use an expert judgment of the arithmetic mean value as median value, or to use the geometric mean.

2.5 *Roles and resources*

The scope and extent of the process will affect the resources needed. Cooke & Goossens (2004) point out that past studies have used between 4 and 20 experts, which probably would require several analysts and administrative personnel to run the process.

O'Hagan et al. (2006) point out that the process can be performed by only two persons if necessary, one expert and one analyst. Often there is also a decision maker included; however, as O'Hagan (2006) says, the expert and decision maker may be one and the same, and if the analyst also is capable within statistics, the process can be performed by only two persons. However, both O'Hagan et al. (2006) and Meyer & Bookers (1991) include more roles to the process. These are often necessary in larger formal expert eliciting processes. Table 1 gives a summary of actual roles described in the processes of the referred literature.

3 UTILIZATION OF KNOWLEDGE TO NUMBER PROCESS IN SMALLER RISK ASSESSMENTS

3.1 *Challenges in smaller risk assessments*

The wide range of situations were risk assessments are required has led to an increased number of risk assessment being performed. Many of these risk assessments are characterized by fewer resources available than what is the case in extensive Quantitative/Probabilistic Risk Assessments (QRAs/PRAs) in for example the oil & gas sector or the nuclear sector. Another typical aspect with these risk assessments is that the need for expert knowledge is huge, as they often are related to new events and/or new surroundings, resulting in lack of data, and perhaps poorly understood causes. The budget of a typical small risk assessment may be between 40 and 200 hours, inevitably giving a weaker foundation for decision than a QRA/PRA (unless given a narrowed scope).

A small amount of available hours gives limitations on how the process can be carried out, and how many experts that can be involved. Cooke & Goossens (2004) say that the amount of expert time required for making the assessments depends on the subject and may vary between a few hours and a week, per expert.

A challenge for most risk assessments, not only the small ones, is that the numbers used do not properly reflect the strength of the knowledge it is based upon. To be aware of the actual knowledge level, we need to identify what we know, but also what we do not know. The strength of knowledge is not visible in a single probability; thus, we may have to assess the knowledge, in some way demonstrate the strength of the available knowledge. This weakness of should also be addressed in the knowledge to number process, identifying the degree of expert knowledge utilized.

3.2 *Recommended activities within knowledge to number in smaller risk assessments*

3.2.1 *Identification of need for expert knowledge*

The need for expert knowledge in smaller and less resource intensive risk assessment may be huge, and the use of expert knowledge is probably the only way to ensure a useful and trustworthy result. However, there will not be much resources available for identifying and evaluating experts, reducing the identification and selection of experts to a limited activity.

The identification of a need for expert knowledge is rather an input to, more than an activity in the process. A need is not an activity by itself, but comes as a result from another activity. This leaves the design activity, including selection of experts, as the first step in the process, with the identification of need for expert elicitation as the trigger.

3.2.2 *Designing elicitation process*

The design of the elicitation process in less resource intensive risk assessments should, as any other elicitation processes, ensure compliance with the main principles mentioned in section 2.4.2 (reproducibility, accountability, empirical control, neutrality, fairness). However, in smaller and less resource

intensive risk assessments the design phase does not have to be very complicated and resource demanding. We believe a restructured process, shortened and simplified, and supported by an assessment to identify the strength of knowledge, will increase the quality of the process. Instead of five major activities (see section 2.4), we propose three as follows:

- Design phase (preparations, designing elicitation process, identification and selection of experts)
- Data collection (elicitation)
- Data analysis (verification, aggregation and documentation)

The word data is here used in the sense of both hard data and expert judgments; Aven (2012).

The design phase starts when the need for expert judgment is identified. The expert(s) are going to use their knowledge of some specific phenomena, e.g. to quantify lack of knowledge about the variables of interest using probabilities. These variables should be identified, and if possible, the need for decomposing should be identified and carried out by analysts if possible. Alternatively, if the analyst has a poor understanding of the knowledge area, the use of expert should include time also to perform the decomposition as one of the activities for the experts. The data may have different formats dependent on the risk assessments methodology used. They can be single numbers (probabilities) or distributions as input to a quantitative model, or they can be probability classes (intervals) or consequence classes if using risk matrixes. Eventually, the data can be knowledge helping the analyst to establish either an event tree or a fault tree, helping the analyst to understand the phenomena, and how it can affect other parts in a given system.

The design should also give input to how many experts are needed. Lack of resources gives limitations; however, within these limitations, referenced literature advice to have as many as possible. Clemen & Winkler (1999) shows that a group of experts tends to outperform the average expert, but that the best expert outperforms the group as a whole. The benefit of using several experts are then obvious, but if in lack of resources or experts, one is better than none, otherwise forcing the analyst to do his/ her own assessments, which often is the alternative. This means that number of experts must adapted to available resources. However, O'Hagan et al. (2006) point out that one man can do the job, if we are confident that we are able to have one excellent expert. We believe always struggling for four or more, as Cooke & Goossens says, are unrealistic within these limitations of resources. As a follow up of this, and to ensure that the decision-maker is made aware of what knowledge is being used, we propose a "*strength-of-knowledge assessment*" to evaluate the expert knowledge available (see 3.3).

The data analysis procedure must be planned. If we use several experts, and if there is a need for aggregated data, referenced literature shows that simple calculations, using the geometric mean, is often to prefer. Then there is no need to spend more time or effort than necessary, but plan to report the data and the geometric mean. However, depending on the scope, further analysis may be appropriate, and this has to be considered in the design phase, but also during the elicitation. Some resources to continuously follow up the data, safeguarding quality, must be secured.

As a part of the design, when we know the expert's knowledge better, elicitation training should be planned. Even though we plan to do the whole process as fast as possible, referenced literature shows that giving experts information and training in front of the elicitation makes sense, especially regarding heuristics and bias. We see no reason to change the 3-step training procedure proposed by O'Hagan et al. (2006). Small assessments usually have at least one one-day workshop. It is possible to plan for both the training and the elicitation during this day, if the amount of elicitation rounds are limited, as expected in smaller and less resource intensive risk assessments.

Information to the expert should include all practical information, and all background information relevant for the scope of the assessment. The information should be sent in advance to the experts, encouraging them to prepare for the day.

3.2.3 *Identify, select, motivate and train experts*

The identification of a need for expert knowledge is a result of a lack of knowledge in a risk assessment. The analyst, or other in charge of the risk assessment, has to identify the field of knowledge needed, and find persons with the demanded knowledge. Is it good enough to have general phenomenological knowledge? Are there any people at all with activity-/system-specific expert knowledge? If in need of e.g. an expert to evaluate landslide risks, the probability that any geologist has knowledge to the current area up front is low, but being a geologist is by definition being an expert in geology, being able to understand and analyze a current situation related to land slide risks. Likewise, if searching for experts regarding a company's internal culture, relevant experts are probably working within the company, probably having sufficient expert knowledge, reducing the search activities to be acceptable also in a less resource intensive risk assessment.

The decision maker must have confidence in the results, leaving him the choice of increasing the resources, if that is the issue, or having less confidence in a result made of the analyst, without expert knowledge.

The activity called "identify, select, motivate and train experts" could be seen as both a part of the preparations in design phase, and the training and motivation is really a activity taking place together with the elicitation, and should be placed there.

3.2.4 *Elicitation*

The elicitation activity, the data collection, is not different in smaller and less resource intensive risk analysis than in other elicitation processes, maybe except for a less comprehensive scope, with fewer runs.

The goal of the elicitation activity is to elicit numbers from the expert, handling heuristics in a way reducing bias. If only one expert is used, group heuristics are reduced, such as anchoring, follow the leader, etc. unless the analyst make some pitfalls.

When the elicitation starts, the expert has participated in the training, giving him/her a basic understanding of probabilities and relevant probability distributions. Further, the expert has knowledge about heuristics, and how to overcome them.

To ease the elicitation activity, the analyst may use software for expert elicitation to run the elicitation smooth and fast.

3.2.5 *Post elicitation work (aggregation and documentation)*

In this step the data analysis activities, data are checked, verified, and if necessary aggregated, prepared to use in a risk model or other tool. Cooke & Goossens (2004) propose weighting of the experts judgments if there is reasons to differentiate the influence each expert should have. However, Meyer & Booker (1991) shows that the weighting must be disproportionately uneven to really affect the result, compared to how variations in the judgment affects the arithmetic mean. With reference to section 2.4.5, the geometric mean could be used instead of arithmetic mean, reducing the need for weighting. Compliance with Cooke's recognized principles (see section 2.4.2) should be documented.

3.3 *Strength-of-knowledge assessment*

As mentioned in section 3.1, a weakness of many risk assessment is the lack of documentation of strength of knowledge. It is common to see the risk assessment as a process where the analyst identifies and documents some defined expert's knowledge in the field studied. Aven & Guikema (2011) say; "*The produced probability assessments are founded on the knowledge of subject matter experts but are heavily filtered through and, in some cases heavily influenced by the expert knowledge of the risk analysts*". The risk assessment should systemize knowledge, but also lack of knowledge, using the probabilities as measures of the related uncertainty. From this follows two points. Firstly, the analyst does apply knowledge to the risk assessment, and the analyst's knowledge should then be seen as a part of the total knowledge available. Secondly, it is crucial, given a phenomenon, to identify what is known, and what is unknown. Doing a risk assessment of a poorly understood phenomenon is often necessary, even though we know there is a lack of knowledge, because societies need decisions. Identifying both knowledge, and lack of knowledge, is crucial when making decision support.

We suggest a "strength-of-knowledge assessment", which is expected to increase the awareness related to both expert's and the analyst's knowledge level, and may support a decision maker, making her/him aware of the level of knowledge used. The following criteria may serve as a guideline.

3.3.1 *Strong knowledge*

All of the following conditions fulfilled:

- Several experts are used, with insignificantly diverging statements.
- All experts are experts both in terms of general phenomenological knowledge as well as in terms of specific system/activity knowledge.
- All experts have both formal competence in probability/statistics as well as practical experience with probability elicitation.
- All the principles of rational consensus (Cooke, 1991) are followed.

3.3.2 *Weak knowledge*

At least one of the following conditions fulfilled:

- Several experts with significantly diverging statements.
- Expert(s) without specific knowledge about the system/activity considered.
- Several of the rational consensus principles are not followed.

3.3.3 *Moderate knowledge*

Conditions between strong and weak, e.g.:

- Several experts with some diverging statements.
- Some experts are only experts in terms of either general phenomenological knowledge or in terms of specific system/activity knowledge.
- Only one expert, but expert both in terms of general phenomenological knowledge as well as in terms of specific system/activity knowledge.
- A few of the rational consensus principles are not followed.

3.4 *Summary of suggested procedure*

Table 2 summarizes the suggested activities for a knowledge-to-number process, in smaller risk assessments, highlighting differences compared to formal expert eliciting processes. It shows the

Table 2. Proposed changes in elicitation process.

Activity	Differences
Identification of need:	Identification of need:
Design:	Simplified elicitation process. – Design – Data collection – Data analysis Simplified plan for data analysis.
Identify/select/ train expert:	Activities allocated in design and elicitation (data collection) Only1–3 experts, better with one real expert than several fair. Focus is to find real expert. Expert does not have to be an academic record, but his/hers knowledge useful in the risk assessment
Elicitation: (Data collection)	Not different, just less Comprehensive, reflecting the nature of smaller risk assessments. Training and elicitation in one day.
After elicitation work: (Data analysis)	Mainly mathematical aggregation, with use of geometric mean. No weighting of expert judgment. Strength-of-knowledge assessment

activities from a formal elicitation process (left), describing the differences in an alternative, scaled-down proposed process (right). The change from the more formal process to this shorter process makes it easier to follow a structured approach for expert eliciting, and transforming knowledge to numbers, as it can be carried out with fewer resources than a formal eliciting process as described by e.g. Cooke & Goossens (2004) and Meyer & Booker (1991).

4 CONCLUSION

The purpose of this paper has been to point out how we can improve smaller risk assessments by improving the use of expert knowledge. Today's utilization of expert knowledge in smaller risk assessments often do not follow proposed formal expert eliciting process activities. Despite limited resources in smaller risk assessments, we believe a simple, yet more structured process will increase the quality and contribute to more valuable decision support, increasing the decision maker's confidence in the result.

This structured process should include a design phase, a data collection phase and a data analysis phase. Just to be aware and plan (design) how to use expert knowledge, is an advance compared to how small risk assessment often are done today. A simple mechanical aggregation, if relevant, without behavioral aggregation or weighting, will simplify the analysis phase.

The strength-of knowledge assessment is a new activity in risk assessments. We believe that a strength-of-knowledge assessment as suggested will increase the analyst's awareness when using experts, forcing analysts to identify and document the level of own and expert knowledge, adding value to the risk assessment as decision support by giving the decision-maker insight into the knowledge base of the analysis.

REFERENCES

Ackoff, R.L. (1989) From data to wisdom. Journal of Applied Systems Analysis, 16, 3–9.

Aven, T. 2012. Foundations of Risk Analysis. Wiley.

Aven, T & Guikema, S. (2011). Whose uncertainty assessments (probability distributions) does a risk assessment report: the analysts' or the experts? Reliability Engineering and System Safety 96(2011)1257–1262.

Clemen, R.T. & Winkler, R.L. 1999. Combining distributions from experts in risk analysis. Risk analysis, Vol. 19, No 2, 1999.

Clemen, R.T & Reilly, T. Making hard decisions. Duxbury Thomson learning, 2001.

Cooke, R.M. 1991. Experts in Uncertainty. Oxford University press. Cambridge.

Cooke, R.M. & Goossens, L.H.J. 2004. Expert judgement elicitations for risk assessments of critical infrastructures. Journal of Risk Research 7 (6), p 643–656.

Garthwaite, P.H., Kadane, J.B., O'Hagan, A. 2005. Statistical methods for eliciting probability distributions. Journal of the American Statistical Association, 100, 680–701.

Hogarth, R.M. 1975. Cognitive processes and the assessment of subjective probability distributions. Journal of the American Statistical Association, 1975, 70, p 271–289.

Kahneman, D., Slovic, P., Tversky, A. 1982. Judgment under uncertainty: Heuristic and biases.

Kleinmuntz D.N., Fennema M.G., Peecher M.E. (1996). Conditioned Assessment of Subjective Probabilities: Identifying the Benefits of Decomposition, Organizational Behaviour and Human Decision Process, 66 (1), 1–15.

Melnick, Edward L, og Brian S. Ever. Encyclopedia of quantitative risk analysis and assessment. Wiley, 2008.

Merkhofer, Miley W. Quantifying Judgemental Uncertainty: Methodology. IEEE transactions on systems, man and cybernetics, 1987: 741–752.

Meyer M.A. & Booker, J.M. 1991. Eliciting and analyzing expert judgment—a practical guide. ASA-SIAM.

Morris, D.E, Oakley, J.E, Crowe, J.A. 2013. A web-based tool for eliciting probability distributions from experts. Environmental Modelling & Software 52 (2014), p 1–4.

Morris, D.E, Oakley, J.E, Crowe, J.A. 2014. A web-based tool for eliciting probability distributions from experts, Environmental Modelling & Software, Volume 52, February 2014, Pages 1–4, ISSN 1364-8152, http://dx.doi.org/10.1016/j.envsoft.2013.10.010.

O'Hagan A. et al. 2006. Uncertain Judgments. Wiley.

Oxford dictionary of Environment and Conservation, 2.ed. 2013. Oxford University press.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk assessment of ground water sources for emergency supply

F. Bozek & L. Jesonkova
Population Protection Department, University of Defence, Brno, Czech Republic

A. Pawelczyk
Faculty of Chemistry, Wroclaw University of Technology, Wroclaw, Poland

Z. Malek
College of Business and Hotel Management, Brno, Czech Republic

J. Dvorak
Language Training Centre, University of Defence, Brno, Czech Republic

ABSTRACT: The paper deals with the procedure of semi-quantitative risk analysis of ground water source earmarked for emergency supply of population with regard to a selected set of natural and anthropogenic hazards. The risk analysis proved that the source is sufficiently resistant to identified hazards and may be included into the regional crisis plan. The proposed method may become a guideline for the risk assessment of ground water sources as one of the significant classification criteria of these important alternative sources of emergency supply with drinking water within the crisis planning system.

1 INTRODUCTION

It is highly topical and important to pay attention to the security aspects of infrastructure supplying population and industry with drinking water. It reflects the development and understanding of global security threats from the EU standpoint (European Council 2003), as well as from the standpoint of the Czech Republic (The Government of the Czech Republic 2011), and close dependence and interrelation of individual branches, elements and services of critical infrastructure. At first, emphasis was not put on water supply in the process of assessment and protection of critical infrastructure. However, in the last decade this branch of critical infrastructure has gained an adequate significance in relation to the assessment of economic, social, health and ecological risks. Generally speaking, there is an increasing risk that either natural impact or anthropogenic intervention on a sensitive spot of water supply system within public network will cause a large-scale and avalanche-like spread of damage (Hubackova et al. 2014).

During crisis and emergency events the supply of drinking water is often interrupted, which results in the paralysis of life of population, the production processes demanding drinking water, the operation of medical facilities, the fire protection of built-up areas and industrial areas (Hubackova et al. 2014). The exploitation of ground water sources may significantly contribute to a state when a situation is managed and a crisis overcome (Bozek et al. 2013). The condition of an effective exploitation of such sources and an easier decision-making process in a crisis is to include the sources into crisis plans on the basis of selection carried out with the help of risk analysis and the assessment of other indicators (Bozek at al. 2012).

2 THE ANALYSIS OF CURRENT STATE

The emergency water supply of population by drinking water during crisis situations or emergency events is not addressed by Community Law in the EU as a whole. The solution of this matter is solely the responsibility of the EU member states.

Most countries transfer responsibility for managing emergency situations from a public sphere to citizens. Fast and effective decision-making is thus individual and has to reflect the awareness of a particular situation and local conditions (National Institute of Public Health 2007). It is usually assumed that the households will supply themselves with water in the amount depending on the number of persons and domestic animals. Some authors even recommend the people afflicted by the interruption of drinking water supply to treat raw water on their own (Lantagne & Classen 2012) and provide them with guidelines how to

do it (Lantagne 2008). The US EPA also presents detailed guidelines on its websites informing the population about what to do in a crisis in case there is not enough bottled water and it cannot be disinfected by boiling (US EPA 2014).

The public sphere solves primarily the situations when water has to be supplied to hospitals, medical facilities (American Water Works Association and Centers for Disease Control and Prevention 2014) and other public institutions, reception camps and centres in which it is necessary to accommodate more people during the crisis (Amar 2010). The US EPA report is not focused only on the practical aspects of local planning in relation to the emergency supply of drinking water, but also on the roles and responsibilities of various levels of state administration. It also includes technical planning elements and presents recommendations how to respond better to post-crisis situations (US EPA 2011). Daniel and Morley also deal with the issue of water supply immediately after the crisis situation is over (Daniel & Morley 2011).

The emergency water supply in the Czech Republic is provided by crisis management authorities through the Emergency Water Supply Service. Depending on the level of disturbance of drinking water public supply systems the population may be supplied in the following ways (Ministry of Agriculture of the Czech Republic 2011):

a. Undisturbed water supply systems or their parts;
b. Undisturbed independent intake structures, mainly wells;
c. Drinking water supplied in tanks;
d. Mobile water treatment plants and other technological facilities;
e. Supply of bottled drinking water as an additional way of supply.

During emergency supply the priority is given to the water supply system capability of supplying drinking water even at lower quality. It is also preferred to exploit primarily the alternative sources of ground waters, especially vertical intake structures, built and equipped for collecting the ground waters of deeper circulation, and possibly also horizontal and combined intake structures (Ministry of the Agriculture of the Czech Republic 2011). The accumulation of surface waters in water reservoirs and watercourses cannot be recommended for the emergency supply due to its high level of vulnerability and often lower water quality. The above mentioned sources should be used only exceptionally and in well justified cases. Even not all hydrogeological structures are suitable, because they are exposed to different hazards and have different levels of vulnerability (Bozek et al. 2011).

At present the alternative sources of ground water for emergency supply of population are classified in the following three categories in the Czech Republic (Bozek et al. 2013–2013):

a. The sources of extra significance, such as ground water intake structures of increased resistance capable of supplying the required amount of drinking water;
b. The sources capable of resisting a small scale damage to the drinking water supply system;
c. The other intake structures not included into the sources of the above mentioned categories, which are used for mass supply of population with drinking water from public water supply systems.

The current classification of water sources is imperfect as it does not stem from the analysis of risks, which may damage or destroy the alternative sources. Therefore the University of Defence participates, together with the GEOtest plc., in the project of security research No. VG20102013066 into "Methodology of Assessing the Emergency Water Supply on the Basis of Risk Analysis" (Bozek et al. 2013–2013), which is financed by the Ministry of Interior of the Czech Republic. The aim of the project is to develop the classification of ground water sources based on the analysis of risks resulting from natural and anthropogenic hazards, health hazards related to water quality, the assessment of traffic accessibility, availability, and richness of the source and the costs of putting the water source into operation. Such an analysis will improve the selection of water sources to be incorporated into crisis plans and will help to manage crises more effectively with accent on the emergency survival of population, important production processes and the functions of public administration.

The implementation of our methodology of assessing the selected natural and anthropogenic risks to ground water sources (Bozek et al. 2012) is presented in the paper on a particular source Drnovice, drill-1, which has been earmarked for the emergency supply of drinking water. The considered hazards include primarily natural hazards, breakdowns, ordinary activities and environmental burdens.

3 APPLIED METHODS

The assessment of risk that a selected ground water source is threatened by natural and anthropogenic hazards stemmed from the index point values of identified hazard/sensitivity pairs assigned to individual elements of hydrogeological structure and technological equipment of water source. Brainstorming was used for indexing the levels of hazards and vulnerabilities (Osborn 1963). The indexation was made at three meetings of seven experts and one laic.

The same brainstorming became the basis also for setting the hazard/sensitivity pairs of individual water source elements. The indexation of the level of j-hazard $f_j(\tau) \in (0; 5\rangle$ was in a set of positive real numbers Re^+ depending on the hazard source activation frequency and considering the historical data. Similarly, the sensitivity index point values $S_{j,i}(\tau) \in (0; 4\rangle$ were determined in the set of Re^+ as the function of damage to i-element of water source caused by the activation of j-hazard source.

The quantification of risk index $R_{j,i}(\tau)$ representing the level of contamination, damage, or destruction of i-element of the assessed ground water source caused by j-hazard in given time τ has been calculated according to relation (1):

$$R_{j,i}(\tau) = const'_i(\tau) \times f_j(\tau) \times S_{j,i}(\tau) \quad (1)$$

Thus risk index $R_{j,i}(\tau)$ represents the product of invariable $const'_i(\tau)$, frequency value $f_j(\tau)$, and sensitivity value $S_{j,i}(\tau)$ expressed in point indexes. The invariable $const'_i(\tau) \in \langle 1; 3\rangle \wedge const'_i(\tau) \in Re^+$ is the reflection of criticality $C_i(\tau)$ of the assessed i-element of water source in given time τ.

Brainstorming has also been applied for determining the values of $const'_i(\tau)$ for i-element of ground water source. During this process it was respected the importance of each element for fulfilling its function as a water source for emergency water supply, as well as the possibility of its substitution or repair, as in case of water intake structures and water treatment plant being substituted by a mobile water treatment facility. The values of invariable $const'_i(\tau)$ are reported in Table 1. They have been acquired as a median from the values suggested by the members of brainstorming team.

Furthermore, the risk acceptability of each i-element of ground water source has been determined in relation to j-hazard by comparing the calculated value of risk $R_{j,i}(\tau)$ with the characteristic of particular interval of risk point values. The characteristic of risk point intervals has been acquired through a complete Delphi method with one iteration (Dalkey & Helmer 1963).

Table 1. The invariable of criticality $const'_i(\tau)$ for the i-elements of monitored water source.

Element of water source	HGC	HR	WQ	WIS	WTP
The values of invariable $const'_i(\tau)$	2.85	2.77	2.55	1.80	1.43

HGC—hydrogeological conditions; HR—hydrological regime, WQ—ground water quality; WIS—water intake structures; WTP—water treatment plant.

4 FINDINGS AND DISCUSSION

The values of activation frequency point indexes $f_j(\tau)$ for the identified j-hazard sources are presented in Table 2 together with the values of sensitivity point indexes $S_{j,i}(\tau)$ for i-elements threatened by j-hazard of the assessed water source.

Based on the known values of invariable $const'_i(\tau)$, values of frequency point indexes $f_j(\tau)$ and sensitivity point indexes $S_{j,i}(\tau)$ the calculation of risk point indexes $R_{j,i}(\tau)$ has been made for each i-element of the assessed ground water source in relation to each j-hazard source. The acquired outcomes are clearly shown in Table 3.

Furthermore, individual intervals of risk point indexes have been defined for assessing the acceptability of risk in relation to each j-hazard source and i-element of water source. The outcomes are in a well arranged way shown in Table 4. It is obvious from equation (1) and the definitions of frequency $f_j(\tau)$, sensitivity $S_{j,i}(\tau)$ and invariable $const'_i(\tau)$, that the values of risk point indexes $R_{i,j}(\tau) \in (0; 60\rangle \wedge R_{i,j}(\tau) \in Re^+$.

By comparing the data from Table 3 with the characteristics of intervals of risk index point values in Table 4 it may be discovered that all the identified risks resulting from the selected set of natural and anthropogenic hazard sources threatening the assessed ground water source are either negligible or acceptable.

The risk point index $R_{i,j}(\tau)$ of the increased radioactive background accompanied with the leak of radon is near the tolerable limit. This is caused by the origin of sedimentary material of rocks with the higher content of potassium and a number of mineral deposits of radioactive materials, which are still mined. While the radioactive background is almost constant in the area of infiltration and the source vicinity and its intensity decreases in time only due to the fission of radionuclides, the leakages of radon in the atmosphere fluctuate in dependence on the atmospheric pressure. The increased radioactive background accompanied by the leak of radon may deteriorate working conditions in non-ventilated water treatment facilities. The occurrence of radon in water does not represent risk in case of oral exposure. However, it represents not negligible carcinogenic risk due to the respiration exposure to radon volatilized from water in non-ventilated environment.

North of the assessed drill in the former stone quarry there is an illegal dump of solid household waste. The composition of waste dump as well as the migration of possible contamination are not known and more detailed information is not available. However, the extended analysis of water in the drill did not detect the leak of contaminants from the illegal dump into the hydrogeological col-

Table 2. Frequency $f_j(\tau)$ and sensitivity $S_{j,i}(\tau)$ point indexes of monitored water source.

Potential hazards	Frequency point indexes $f_j(\tau)$	Sensitivity point indexes $R_{j,i}(\tau)$				
		HGC	HR	WQ	WIS	WTP
1 Natural hazards						
1.1 Natural hazards caused by atmospheric changes						
Storms and other electric effects	4.55	–	–	–	0.30	0.40
Hailstorms and torrential rains	3.70	–	–	–	1.75	1.30
Floods	2.35	–	–	–	2.80	2.50
1.2 Natural hazards caused by other impacts	–	–	–	–	–	–
Increased radioactive background	4.60	–	–	1.45	–	–
2 Technological hazards						
2.1 Accidents						
Traffic accident with the leakage of fuels, oils, lubricants and other operational fluids	2.30	–	–	1.70	–	–
Traffic accident with the leakage of dangerous substances and wastes	1.10	–	–	2.90	–	–
The crash of agricultural machine during land cultivation	2.70	–	–	1.25	2.05	2.20
The crash of forestry machine during forest land cultivation	2.60			1.25	–	–
2.2 Common activities						
Illegal waste dump	5.00	–	–	1.25	–	–
Transport	5.00	–	–	0.60		
Agricultural production	4.40	–	–	1.40		
Forestry	4.50	–	–	0.40	–	–

* HGC—hydrogeological conditions; HR—hydrological regime, WQ—ground water quality; WIS—water intake structures; WTP—water treatment plant.

Table 3. Risk point indexes $R_{j,i}(\tau)$ for individual threatened elements of monitored water source.

Potential hazards	Risk point indexes $R_{j,i}(\tau)$				
	HGC	HR	WQ	WIS	WTP
1 Natural hazards					
1.1 Natural hazards caused by atmospheric changes					
Storms and other electric effects	–	–	–	2.46	2.60
Hailstorms and torrential rains	–	–	–	11.66	6.88
Floods	–	–	–	11.84	8.40
1.2 Natural hazards caused by other impacts	–	–	–	–	–
Increased radioactive background	–	–	17.00	–	–
2 Technological hazards					
2.1 Accidents					
Traffic accident with the leakage of fuels, oils, lubricants and other operational fluids	–	–	9.97	–	–
Traffic accident with the leakage of dangerous substances and wastes	–	–	8.13	–	–
The crash of agricultural machine during land cultivation	–	–	8.60	9.96	8.49
The crash of forestry machine during forest land cultivation	–	–	8.29	–	–
2.2 Common activities					
Illegal waste dump	–	–	15.94	–	–
Transport	–	–	7.65		
Agricultural production	–	–	15.71	–	–
Forestry	–	–	4.59	–	–

* HGC—hydrogeological conditions; HR—hydrological regime, WQ—ground water quality; WIS—water intake structures; WTP—water treatment plant.

Table 4. Characteristics of risks $R_{i,j}(\tau)$ for individual intervals of risk point indexes.

Interval of risk point indexes $R_{j,i}(\tau)$	Characteristics of risks
(0; 5⟩	Negligible. Water source may be immediately exploited without implementation of countermeasures.
(5; 18⟩	Acceptable. Water source can be immediately exploited with implementation of countermeasures, if need be, on the basis of a statement and decision made by top-management of source operator. The benefit of measure should be higher than costs.
(18; 30⟩	Tolerable. The exploitation of water source is heavily limited. If water source is to be used for the emergency supply of population, it is necessary to implement countermeasures in order to reduce the risk on the acceptable level. The costs of reducing the risk have to be adequate for the value of protected source element and the social benefit. In this case it is recommended to apply the Cost-Benefit Analysis method, possibly a multi-criteria assessment, which will enable us to assess the effectiveness of particular countermeasures being taken.
(30; 60⟩	Unacceptable. It is not recommended to exploit the water source for emergency supply.

lector. It may be caused by the fact that the waste is inert, the filtration coefficient of water source covering rocks is so low, or, in other words, the covering layers are so thick, that the contamination has not occurred. The latent risk may soon become acute, though.

The risk point index of agricultural production $R_{i,j}(\tau)$ is higher as well. Synthetic and natural fertilizers, mordants, seeds for sowing and pesticides are used in the field near the water source infiltration area and their leak into the hydrogeological collector may negatively affect the quality of water source. The covering layer of loess with good sorption capacity prevents larger contamination of ground water, though.

It should be added that the risk analysis considered also previous exploitation of the infiltration area and the source vicinity, which could signal a type of environmental burden. The area in the source vicinity was exploited solely for agricultural production, a part of the infiltration area was exploited also for forest production. Therefore agrochemicals were the only environmental burden expected in the area of interest. Due to the good bedrock the migration of contaminants into the saturated zone of water source has not been monitored though, which has been proved by an extended water analysis.

Therefore it may be stated that the assessed drill is sufficiently resistant to the identified natural and anthropogenic hazards, has a good water quality and is utilizable for emergency supply. It was necessary to assess also its availability, accessibility and richness in order to include it to the regional crisis plan. The findings of the assessment proved that the drill belongs to the category of water sources of regional importance capable of supplying 5×10^4 people during a crisis, i.e. almost the whole region. As the drill has been included into the system of group water supply it was not necessary to consider the costs connected with the process of putting it into operation.

At the same time the following measures have been proposed to increase the resistance of water source and operator's health safety, in case of which the cost-benefit efficiency is expected to be higher:

a. To analyze the composition of waste at the illegal waste dump and verify the migration of potential contamination. If there is an acute risk that the drill hydrogeological aquifer may be contaminated, the waste dump has to be immediately remediated;
b. To ensure that the building and the reinforced chamber are ventilated and the caught ground water is aerated.
c. To harmonize the exploitation of areas near the drill infiltration area according to area plans and in compliance with the drill water supply exploitation;
d. To carry out correct and sustainable activities in agriculture and forestry on the territory near the source infiltration area;
e. To control the technical condition of machinery in agriculture and forestry, including regular drivers' training.

5 CONCLUSION

The semi-quantitative risk analysis of ground water source earmarked for the emergency supply of population has been carried out. The analysis of water source hazards caused by natural events, breakdowns and ordinary anthropogenic activities proved that the risk is either negligible or acceptable with regard to all the identified hazard/sensitivity pairs and all the incorporated criticality elements

of the source hydrogeological structure and technical equipment. The source may be included into the regional crisis plan as it is resistant to the identified hazards, with good accessibility, availability and richness. It is assumed that the presented case study will become a guideline for risk assessment as a basis for the classification of ground water sources within the crisis planning system.

ACKNOWLEDGEMENT

The outcomes presented in this paper were acquired within the framework of the security research project of the Czech Republic on the Methodology of Assessing the Emergency Water Supply on the Basis of Risk Analysis, abridged as EWSSA. This project has been granted by the Ministry of Interior of the Czech Republic under No. VG20102013066.

REFERENCES

Amar, P.K. Ensuring Safe Water in Post-Chemical, Biological, Radiological and Nuclear Emergencies. *Journal of Pharmacy and Bioallied Sciences*. 2010, Vol. 2, No. 3, pp. 253–266.

American Water Works Association and Centers for Disease Control and Prevention. *Emergency Water Supply Planning Guide for Hospitals and Health Care Facilities*. [on line]. [2014-00-18]. URL: <http://www.cdc.gov/healthywater/pdf/emergency/emergency-water-supply-planning-guide.pdf>.

Bozek, F. et al. Classification of Ground Water Resources for Emergency Supply. *World Academy of Science, Engineering and Technology*, 2012, Vol. 71, pp. 1653–1656.

Bozek, F. et al. *Methodology of Assessing the Emergency Water Supply on the Basis of Risk Analysis*. [Security Research Project No. VG20102013066]. Brno: University of Defense, GEOtest, a. s., 2010–2013.

Bozek, F. et al. *Methodology of Assessing the Sources of Emergency Water Supply on the Basis of Risk Analysis.* Brno: University of Defence, 2013, 21 p.

Bozek, F. et al. Sources for Emergency Water Supply I. Hazard Identification. In: *Mathematical Methods and Techniques in Engineering & Environmental Science. Proceedings of the 4th WSEAS International Conference on Natural Hazards.* Catania: WSEAS Press, 2011, pp. 85–90. ISBN 978-1-61804-046-6.

Dalkey, N. & Helmer, O. An Experimental Application of the Delphi Method to the Use of Experts. *Management Science*, 1963, Vol. 9, No. 3, pp. 458–467.

Daniel, P.A. & Morley, K.M. Security and Preparedness. Postdisaster Water Supply: The Local-State-Federal Nexus and Recommendations for Speeding the Response. *Journal of American Water Works Association*, 2011, 103, (8), pp. 24–27.

European Council (EC). *European Security Strategy*. Brussels: EC, 2003, pp. 3–5.

Hubackova, et al. V. *Why the Protection of Critical Infrastructure in the Area of Emergency Water Supply?* [on line]. [2014-02-17]. URL: <http://www.smv.cz/res/data/054/006012.pdf?seek=6>.

Lantagne, D. Sodium Hypochlorite Dosage for Household and Emergency Water Treatment. *Journal of the American Water Works Association*, 2008, Vol. 100, No. 8, pp. 106–119.

Lantagne, D. & Classen, T. Point-of-Use Water Treatment in Emergency Response. *Waterlines*, 2012, Vol. 31, No. 1–2, pp. 30–52.

Ministry of Agriculture of the Czech Republic (MoA CR). Methodological Instructions of the MoA CR to Ensure the Standard Procedure to be followed by Regional and Municipal Authorities, the Authority of the Capital of Prague and its City Parts, in Emergency Water Supply provided by the Emergency Water Supply Service during the Extraordinary Events, Emergency and Crisis Situations. *Governmental Bulletin for Regional and Municipal Authorities*, 2011, Article 3, pp. 42–46.

Ministry of Agriculture of the Czech Republic (MoA CR). MoA Methodical Instructions for Selecting and Maintaining the Sources of Emergency Water Supply. Bulletin of MoA CR, 2002, Article 3, pp. 1–10.

National Institute of Public Health (NIPH). *Emergency Drinking Water Supply*. Methodical Recommendation of National Referential Centre (NIPH) for Drinking Water. Prague: NIPH, 2007, p. 5.

Osborn, A.F. *Applied Imagination: Principles and Procedures of Creative Problem Solving.* 3rd Ed. New York: Charles Scribner's Sons, 1963. 175 pp.

The Government of the Czech Republic. *Security Strategy of the Czech Republic*. Prague: The Government of the Czech Republic, 2011, p. 9–10.

US EPA. *Emergency Disinfection of Drinking Water*. [on line]. [2014-02-18]. URL: <http://water.epa.gov/drink/emerprep/emergencydisinfection.cfm>.

US EPA. *Planning for an Emergency Drinking Water Supply*. Washington D.C.: US EPA, 2011. 40 pp.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Study of volcanic Na-Tech risks in primary Waste Water Treatments

M.F. Milazzo & G. Ancione
University of Messina, Messina, Italy

E. Salzano
Consiglio Nazionale delle Ricerche, Napels, Italy

G. Maschio
University of Padova, Padua, Italy

ABSTRACT: Recently scientists focused their attention on Na-Tech risks (technological risks triggered by natural events). Among different Na-Tech risks, this paper aims at the study of those triggered by explosive volcanic eruptions, i.e. those caused by the fallout of volcanic ash. These events can directly endanger human health due to the inhalation of solid particles or indirectly compromise the safety of people due to damages on critical structures, infrastructures, chemical plants and lifelines. The main goal of this paper is to analyse volcanic Na-Tech risks in Waste Water Treatments (WWTs), with the respect to the phenomenon of volcanic ash emission. A preliminary research of the same authors highlighted the main modes of failure of the vulnerable components included in a WWT. By using the results of this survey, this work aims at the definition of the conditions leading to failures in the primary treatment (or mechanical treatment). The estimation of the threshold amounts of ash causing the equipment's damage has been made for a case study by using literature data.

1 INTRODUCTION

Due to some recent significant natural events (i.e. earthquakes, floods, tsunamis, landslides, volcanic eruptions, etc.), which caused several damages to industrial facilities (6.4% occurred in the oil industry in according to Fabiano and Currò (2012)) and lifelines (electrical power grids, water distribution systems, gas and oil pipelines), many scientists started to focus their research on the study of Na-Tech risks (technological risks triggered by natural events).

The last decades gave tangible evidence that natural disasters, together with technological disasters, may pose tremendous scenarios; this is not only due to the phenomena's simultaneity, but it is also determined by the lack of preparation in coping to such risks. Recently, De Rademaeker et al. (2014) have indicated some prioritised research topics according to process safety relevance, the category "Natural hazard triggering technological disasters" is amongst the emerging issues. In Europe there are many vulnerable installations located in areas subject to natural hazards, thus potentially prone to their impacts; it is also worth noting that the disruption of lifelines can affect whole cities or even entire countries (Cruz et al., 2004). In this framework, the need of specific tools quantifying the vulnerability of critical structures to Na-Tech risks, has emerged mainly to support risk managers in managing such events.

The literature shows some approaches estimating the failure probability of industrial facilities caused by many types of natural events, such as lightning, earthquake, flooding, etc. (Antonioni et al., 2007), but only few works investigate the effects of volcanic eruptions on industrial structures and infrastructures. Significant contributions are those due to the following authors: Spence et al. (2004) evaluated the vulnerability of buildings to pyroclastic flows; Baxter et al. (1982) analysed the reduction of functionality of water treatment systems (either industrial or civil installation); Milazzo and co-authors analysed the fragilities of atmospheric storage tanks (Milazzo et al., 2013a) and filtering systems (Milazzo et al., 2013b) to volcanic ash fallout, then, they also developed procedures for the vulnerability mapping (Milazzo et al., 2013c).

This paper focuses on the study of the Na-Tech events triggered by volcanic ash emissions. The main reason of such a study is that, after the recent eruption of the Eyjafjallajökull volcano (Iceland), the attention to the potential impacts of volcanic ash fallout, is growing. In particular this work deals with the analysis of the potential

damage on lifelines, more specifically, on Waste-Water Treatments (WWTs). Following an explosive volcanic eruption, thus causing ash fallout, the water quality of natural and man-made ponds in the surrounding the volcano can change. This is mainly correlated to the amount of ash, which enters both into the drainage system and wastewater treatments.

This paper is the prosecution of the study started by Ancione et al. (2014); the authors gave a survey of Na-Tech events in WWTs due to ash fallout. They identified the vulnerable equipment of a typical wastewater treatment; in that preliminary study, the causes of damage and the potential effects were also defined. The present work represents a further progress, since it contributes to the definition of the conditions leading to damages in primary treatments (or mechanical treatments). The focus in particular is on screenings.

This paper is structured as follows: in the first part, the characteristics of the natural phenomenon are described and a brief section has been devoted to the description of a typical wastewater treatment; in the second part a methodology for the quantification of the critical thicknesses of volcanic ash accumulated on the screens is proposed; finally the application to a case-study, which is the area surrounding Mt. Etna is shown.

2 VOLCANIC ASH EMISSION

Among several volcanic phenomena (e.g. lava flows, pyroclastic flows, etc.) which can potentially affect inhabitants and buildings, the volcanic ash emission is the most significant, due to its large impact area.

Volcanic ash is made up of tiny fragments of jagged rock, minerals and volcanic glass generated during volcanic eruptions. The size (diameter) of ash particles is equal or less than 2 mm. The quantities and the average grain-size of the volcanic ash emitted from the crater greatly vary for each eruption, but also during a single short explosive phenomenon (few hours or days).

Particles can travel downwind from about tens to thousands kilometres, depending on the following parameters: the wind speed, the volume of erupted ash, the height of the eruption column and the size of particles. The size of ash, falling to the ground, generally decreases exponentially with the distance from the crater (see Fig. 1, volcanoes.usgs.gov).

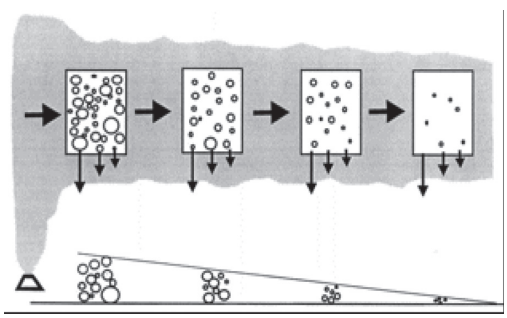


Figure 1. Trend of the size of the particles of ash with the distance from the vent.

3 WASTEWATER TREATMENT PLANT

The general principle in wastewater treatment is to remove pollutants from the water by getting them either to settle or float. Then this material must be removed. Some pollutants are easily removable, whereas others must be converted to settleable materials. The process of wastewater treatment is composed of subsequent steps, each one either removes particles from the sewage or changes dissolved and suspended material to a removable form. A wastewater treatment plant usually includes main phases. A schematic flow-chart of the process is given in Figure 2.

The first step is the primary treatment which provides a mechanical separation of most of the suspended and floating solids from the liquid stream (wastewater). In this phase, raw sewage passes through raked bar screens to remove large debris (such as rags, plastics, sticks and cans). Smaller inorganic material is removed by fine screens and grit removal tanks. Lighter organic solids remain suspended in the water and flow into large tanks, called primary clarifiers. Here, the heavier organic solids settle by gravity; the settled solids (named primary sludge) are removed and pumped to

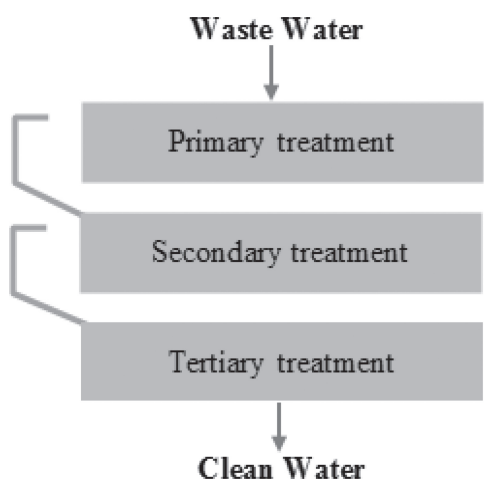


Figure 2. Flow-chart of a generic wastewater treatment.

anaerobic digesters for further treatment. Even if this phase is called mechanical treatment, a few chemicals are sometimes used to accelerate the sedimentation process.

Next step is the secondary treatment, also named biological treatment. It aims to remove the dissolved organic substance, escaped from previous treatments. The removal is achieved by bacteria, which consume the organic matter for their sustenance and convert it in carbon dioxide, water and energy for their own growth and reproduction. The biological process is then followed by additional settling tanks (secondary sedimentation). Secondary treatment technologies include basic activated sludge processes, the variants of pond and constructed wetland systems, trickling filters and other forms of treatment which use biological activity to break down organic matter.

The final step is the tertiary treatment. It is used for specific contaminants which cannot be removed by the secondary treatment. This phase is not always present in a WWT, it depends on the origin of the sewage and the final use of the water output. Individual treatment processes sometimes are necessary to remove nitrogen, phosphorus, additional suspended solids, refractory organics, heavy metals and dissolved solids. The technologies to be used depend on the contaminants which must be removed, i.e. filters and separation membranes, systems for dechlorination and disinfection, reverse osmosis systems, ion exchangers, activated carbon adsorption systems and physical-chemical treatments.

4 POTENTIAL FAILURES IN WASTEWATER TREATMENTS

A previous literature review allowed the identification of the main causes of damage in wastewater treatment plants associated with the volcanic ash fallout (Ancione et al., 2014).

Table 1 shows the modes of damage of some facilities and also points at the physical parameters causing the damage. It is possible to underline that the volcanic ash mainly causes mechanical screenings clogging (due to the overload of the lines because of the reduction of the flow-section caused by the particles), blockages and erosion of pumps and pH changes in biological and chemical treatment tanks. In the same table the potential effects associated with each failure are given.

This paper aims at the identification of the conditions leading to failures of screenings. Screens are included in the first step of the wastewater treatments. Next section analyses the events which could occur, after an explosive eruption, and defines how to correlate the damage to the amount of ash accumulated on the system.

4.1 *Screening*

Screens are the first equipment in a wastewater treatment plant. They are used to protect the following facilities by removing solids. Materials to be removed could be of different size and, therefore, screens can be composed by different mesh. There are usually coarse screens and fine screens.

Coarse screens remove large solids from sewage, and typically have openings ≥ of 6 mm. Coarse screens include mechanically and manually cleaned bar screens. Fine screens are typically used to remove material that could cause problems during the operations and the maintenance. Typical opening sizes for fine screens are in the range 1.5–6 mm, whereas very fine screens have openings from 0.2 to 1.5 mm; these sometimes are placed after coarse or fine screens to reduce suspended solids at levels close to those achieved by the primary clarification. Under normal operation, the velocity of water through the screen should be sufficient to avoid the sedimentation of particles, but not so high to produce an excessive pressure drop or a complete clogging of the equipment.

The degree of clogging depends both on the water quality and the system used to recover the waste from the screen. Taking into account the context outlines in the introduction, the potential clogging depends also on the characteristics of the volcanic ash, such as its size distribution.

The potential damage of screens, caused by volcanic ash fallout, is associated with the amount of particles accumulated on the grid. The main causes of failure are: (1) the partial or total blockage of the system and (2) the incomplete removal of the solid in waste stream. Malfunctions can also cause economic losses, mainly related to the energy consumption.

5 METHODOLOGY

In this section a methodology for the estimation of the threshold deposit of ash on a fine screen, which can cause certain damage, is described. The ash deposit can be considered as a granular bed and the sewage represents the fluid passing through it. The thickness of the accumulation can be estimated by means of the Darcy's equation for a streamline flow, or by the Carman's equation, if a transition or a turbulent flow occurs.

5.1 *Streamline flow regimes*

In 1856, Darcy gave a general relation to describe the flow rate of water through beds of sand of various thicknesses. He showed that the average velocity is directly proportional to the driving

Table 1. Main causes of damage in wastewater treatment and consequent effects.

Equipment	Cause of damage	Physical parameter	Effects	Reference
Pump	Blockage wear	Mass of the ash Ash concentration	Fluid is not pumped Unstable operating conditions (variability of flow-rate, water infiltration)	Day and Fisher, 1980; Blong, 1984
Primary sedimentation tank	Dispersion of particles	Ash concentration	Uncompleted separation	White et al. 2011.
Biological treatment tank	Dispersion of particles	pH of the ash	Bacteria death due to acidification followed by absence of organic matter removal	White et al. 1980
Grit removal, screen	Vibrations clogging	Mass of the ash Mass of the ash	Unstable operating conditions (variability of flow-rate, water infiltration) Flow rate reduction, flow absence	Blong 1984
Gearbox	Vibrations	Mass of the ash	Unstable operating conditions (variability of flow-rate, water infiltration)	White et al. 1980
Biofilters	Dispersion of particles	Ash concentration	Bacteria death due to acidification and asphyxiation followed by absence of organic matter removal	White et al. 1980
Metallic structures	Wear	Ash concentration	Damages depend on the equipment	Johnston 1997
Drainage system, stormwater system and pipe	Clogging/ blockage	Mass of the ash Mass of the ash	Flow absence	Blong, 1984; Blong, 2003; Barnard, 2004; Stewart et al., 2006
Electric system	Ash infiltration	Ash concentration	Power outage	Smithsonian-Institution 2000
Terminal disinfection tank (chlorination)	Dispersion of particles	Ash concentration	Higher turbidity levels which causes the protection of micro-organisms by the effects of disinfection	Stewart et al. 2009

pressure and inversely proportional to the thickness of the bed (Coulson et al., 2002), as follows:

$$Q = \frac{K}{\rho \cdot g} \cdot A_{tot} \cdot \frac{\Delta P}{l} \quad (1)$$

where: Q = volumetric flow rate of water [m^3/s]; A_{tot} = cross-sectional area [m^2]; ΔP = pressure drop [kg/m·s^2]; l = thickness of the porous medium [m]; g = acceleration of gravity [m/s^2]; K = constant, it depends on the characteristics of the porous medium (intrinsic permeability, B) and the fluid (viscosity and density) [m/s].

$$B = \frac{K \cdot \mu}{\rho \cdot g} \quad (2)$$

where: ρ = fluid density [kg/m^3]; μ = fluid viscosity [kg/m·s].

The equation (1) allows estimating the ash thickness l, which can cause certain damages. It is worth noting that this relation is not verified for transition and turbulent flows of the fluid. In these latter cases, the threshold of thickness must be estimated through another approach (see section 5.2).

5.2 *Transition and turbulent flow regimes*

If the flow is not streamline, the Carman's equation must be applied to estimate quantify the thickness of ash (Coulson et al., 2002):

$$\frac{R'}{\rho u_1^2} = \frac{e^3}{S \cdot (1-e)} \cdot \frac{(-\Delta P)}{l} \cdot \frac{1}{\rho \cdot u^2} \quad (3)$$

where: R' = component of the drag force per unit area of particle surface in the direction of motion; e = voidage or porosity, it represents the fraction of the volume of the bed which is not occupied by solid material [dimensionless]; S = specific surface area of the particles, it is the surface area of the particles divided by their volume [m^{-1}]; u_l = average velocity through the pore channels [m/s]; u = average velocity of the fluid [m/s].

Carman found that when the friction coefficient ($R'/\rho u_l^2$) is plotted against the Reynolds's number (Re), by using logarithmic coordinates, his data for the flow through randomly packed beds of solid particles could be correlated approximately by a single curve (curve A, Fig. 3).

The general equation of curve A is:

$$\frac{R'}{\rho u_1^2} = 5\,\mathrm{Re}^{-1} + 0,4\,\mathrm{Re}^{-0,1} \tag{4}$$

In equation (4):

$$\mathrm{Re} = \frac{Deq \cdot \rho \cdot u_l}{\mu} \tag{5}$$

where: D_{eq} = equivalent diameter of the pore space [m].

The equivalent diameter D_{eq} depends on the characteristics of granular bed, i.e. the specific surface area and the voidage:

$$Deq = \frac{e}{S \cdot (1-e)} \tag{6}$$

The average velocity through the pore channels is correlated to the average velocity of the flow:

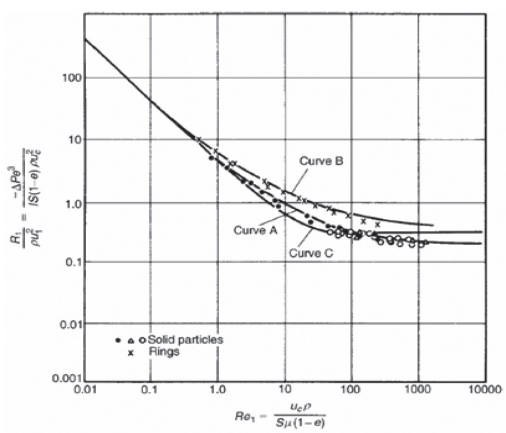


Figure 3. Carman's graph of $R'/\rho u_l^2$ against Re (Coulson et al., 2002).

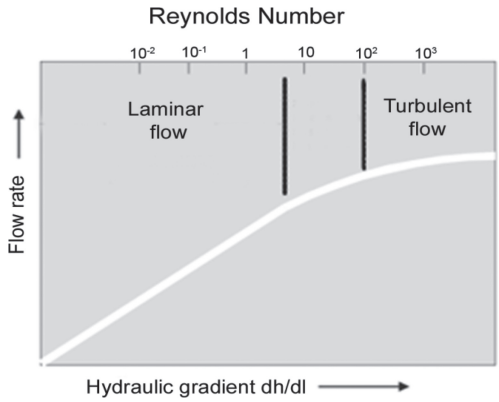


Figure 4. Flow regimes in granular beds.

$$u_l = \frac{u}{e} \tag{7}$$

Finally:

$$\mathrm{Re} = \frac{u \cdot \rho}{S \cdot \mu \cdot (1-e)} \tag{8}$$

5.3 *Determination of the regime of flow*

To choose the equation which better fit to the case under analysis, it is necessary the knowledge of the characteristics of the flow. In the fluid dynamic, the parameter, which permits to determine the flow's type for the fluid, is the Reynolds number (equation (5)). It is a dimensionless quantity. Figure 4 shows the ranges of number of Reynolds, where the various regimes occur. It refers to flow in granular beds.

The laminar (or streamline) flow occurs at low Re (<10), when viscous forces are dominant and is characterized by smooth, constant fluid motion; turbulent flow occurs at high Re (>2000) and is dominated by inertial forces, which tend to produce chaotic eddies, vortices and other flow instabilities (Coulson et al., 1999).

6 A CASE STUDY

The approach described above has been applied to a case study. A fine screen, which is included in a wastewater treatment plant, has been assumed. The WWT is located in the surrounding Mt. Etna (South Italy). The area close to the volcano is characterized by the presence of the city of Catania (300 thousand inhabitants), by many small urban centres and agricultural and industrial areas. Mt. Etna has recently changed its eruptive style

giving more frequent explosive eruptions with ash emissions (Palumbo 1988).

The first step of the methodology, given above, is the calculation of the Reynolds number for the wastewater stream, which flows in the granular bed (ash deposit). The value e and S for the volcanic ash are needed. In this preliminary analysis this data has been extrapolated from the literature as described in the following.

A sample of ash produced by an eruptions of Etna was taken in Giarre (coordinates: lat. 15°10′9″E, long. 37°44′5″N; distance 15.5 km). The average diameter of the particles has been calculated by means of an analysis of the size distribution. Then, by comparing the geometrical characteristics of the ash with those of different beds of particles, given by Coulson et al. (2002), some representative values of e and S have been assumed for the ash.

6.1 *Analysis of the size distribution*

The sieving has been used to determine the size distribution of the volcanic particles (Milazzo et al., 2014). The experimental determination makes use of special sieves arranged in a column; each of them retains the fraction of granules having larger dimensions compared with those of the holes of the sieve. The sieves must be stacked in such a way that the top has the larger mesh and the others have a gradually smaller mesh going down to the bottom. At the base of the column, there is a plate which is used to collect the granules with smaller diameters than the holes of the sieve with the lower mesh. The column is placed on a mechanical shaker for 20 min and, after the shaking, the solid fractions retained by each sieve is weighted. The weight of each solid fraction is then compared to the weight of the total solid to obtain the percentage of solid retained by each sieve.

The results (Fig. 5) are presented in a logarithmic graph of the retained percentage of solid versus the Krumbein parameter ϕ (Krumbein, 1934). Afterwards the weighted average diameter (d) of the particles has been calculated: $d = 5.3 \cdot 10^{-4}$ m.

6.2 *Properties of the granular bed*

Coulson et al. (2002) gave the properties of different granular beds. The particles are classified according to their geometric characteristics (dimension and shape) as shown in Table 2.

The following step has been to compare the geometrical characteristics of the ash with those of the particles of Table 2. The chosen values for e and S are those associated with the particles having similar dimensions. Table 3 gives the list of the samples considered in this study.

6.3 *Flow regime*

In order to choose the right approach to estimate the thickness of volcanic ash deposit on a fine screen, the Reynolds number of the wastewater through the granular bed has been calculated.

Re has been calculated by using equation (8); the values for e and S of the particles are shown in the previous section (Table 2). To take into account the variability of the characteristics of volcanic ash, several calculations have been made by referring to all the types of particles reported in the table.

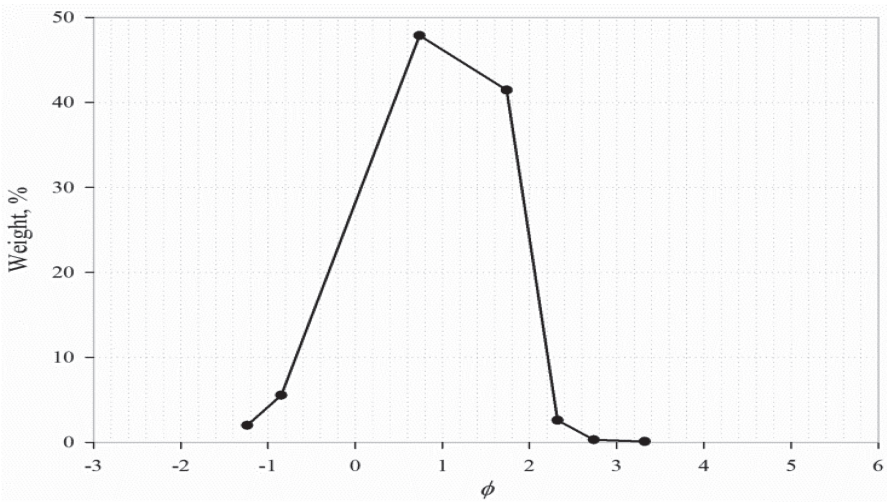


Figure 5. Size distribution for the sample of volcanic ash.

Table 2. Properties of beds of some regular-shaped materials (Coulson et al., 2002).

N	Sample	d [mm]	S [1/m]	e	B [m^2]
1	Spheres	0.794	7600	0.393	$6.2 \cdot 10^{-10}$
2	“	1.588	3759	0.405	$2.8 \cdot 10^{-9}$
3	“	3.175	1895	0.393	$9.4 \cdot 10^{-9}$
4	“	6.35	948	0.405	$4.9 \cdot 10^{-8}$
5	“	7.94	756	0.416	$9.4 \cdot 10^{-8}$
6	Cubes	3.175	1860	0.19	$4.6 \cdot 10^{-10}$
7	“	3.175	1860	0.425	$1.5 \cdot 10^{-8}$
8	“	6.35	1078	0.318	$1.4 \cdot 10^{-8}$
9	“	6.35	1078	0.455	$6.9 \cdot 10^{-8}$
10	Hexagonal prisms	4.76×4.76	1262	0.355	$1.3 \cdot 10^{-8}$
11	“	4.76×4.76	1262	0.472	$5.9 \cdot 10^{-8}$
12	Triang. pyramids	6.35×2.87	2410	0.361	$6.0 \cdot 10^{-9}$
13	“	6.35×2.87	2410	0.518	$1.9 \cdot 10^{-8}$
14	Cylinders	3.175×3.175	1840	0.401	$1.1 \cdot 10^{-8}$
15	“	3.175×3.175	1585	0.397	$1.2 \cdot 10^{-8}$
16	“	6.35×6.35	945	0.41	$4.6 \cdot 10^{-8}$
17	Plates	$6.35 \times 6.35 \times 0.794$	3033	0.41	$5.0 \cdot 10^{-9}$
18	“	$6.35 \times 6.35 \times 1.59$	1984	0.409	$1.1 \cdot 10^{-8}$
19	Discs	3.175×1.59	2540	0.398	$6.3 \cdot 10^{-9}$
20	Porcelain berl saddles	6	2450	0.685	$9.8 \cdot 10^{-8}$
21	“	6	2450	0.75	$1.73 \cdot 10^{-7}$
22	“	6	2450	0.79	$2.94 \cdot 10^{-7}$
23	“	6	2450	832	$3.94 \cdot 10^{-7}$
23	“	6	2450	832	$3.94\ 10^{-7}$
24	Lessing rings	6	5950	0.87	$1.71 \cdot 10^{-7}$
25	“	6	5950	0.889	$2.79 \cdot 10^{-7}$

Table 3. Reference samples for the study.

Sample	d [mm]	S [1/m]	e	B [m^2]
Spheres 1	0.794	7600	0.393	$6.2 \cdot 10^{-10}$
Spheres 2	1.588	3759	0.405	$2.8 \cdot 10^{-9}$
Hexagonal prisms 10	4.76×4.76	1262	0.355	$1.3 \cdot 10^{-8}$
Triangular pyramids 12	6.35×2.87	2410	0.361	$6.0 \cdot 10^{-9}$
Volcanic ash (Mt. Etna)	0.53	7600	0.393	$2.4 \cdot 10^{-12}$
“	“	“	0.4	“
“	“	“	0.5	“
“	“	“	0.6	“
“	“	“	0.7	“
“	“	“	0.8	“
“	“	“	0.9	“

Table 4. Reynolds numbers.

Sample	Re	Regime
Spheres 1	151.7	Transition
Spheres 2	313	Transition
Hexagonal prisms 10	860	Transition
Triangular pyramids 12	454.5	Transition
Volcanic ash (Mt. Etna)	151.7	Transition
“	153.5	Transition
“	184.2	Transition
“	230.3	Transition
“	307	Transition
“	460.5	Transition
“	921	Transition

Table 4 shows the value of the Re for the various cases. It can be noted that the flow is never streamline; this means that the thickness of the deposits must be quantified with the Carman equation.

7 RESULTS

As mentioned above, in this study a fine screen included in a wastewater treatment has been considered. Its characteristics are the following:

- $q = 0.8$ m^3/s
- u = 0.7 m/s
- $A_{tot} = 1.14$ m^2

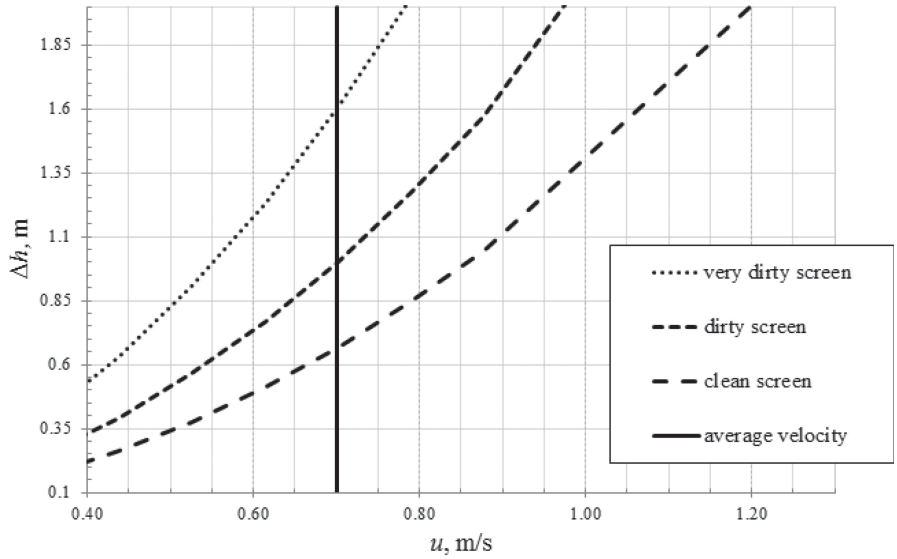


Figure 6. Head losses for fine screens vs. stream velocity.

– bar spacing = $0.5 \cdot 10^{-3}$ m
– bar thickness = $0.5 \cdot 10^{-3}$ m

The potential modes of failure, identified by Ancione et al. (2014) and investigated in this paper, are the partial clogging due to a dirty and a very dirty screen. The events, respectively, occurs when the following values of head loss are measured:

– $\Delta h_1 = 0{,}38$ m (for dirty screen),
– $\Delta h_2 = 0{,}8$ m (for very dirty screen).

These conditions lead to malfunctions and reductions of the stream flow rate. The extreme event is the total clogging; this condition has not been considered in this work, since we assumed that the cleaning operations are executed before the occurrence of a total blockage.

The previous values of head loss have been calculated by using the following equation, specific for fine screen (Metcalf et al., 2004):

$$\Delta h = \frac{1}{2 \cdot g \cdot C} \cdot \left(\frac{Q}{A} \right)^2 \tag{9}$$

where: Δh = hydraulic gradient (or head loss) [m]; C = coefficient of discharge for the fine screen (typically this value for clean screens is 0.60, for dirty screens is 0.4 and for very dirty screens is 0.25); A = effective open area of submerged screen [m^2].

Equation (9) has been plotted in a Cartesian axes system (Fig. 6), where the head loss is a function of the velocity of the upstream flow.

Table 5. Thicknesses of the volcanic ash deposit causing the values Δh_1 and Δh_2 of head loss.

Sample	Re	$R'/\rho u_1^2$	l_1 [mm]	l_2 [mm]
Spheres 1	151.7	0.27	0.3	0.8
Spheres 2	313.0	0.24	0.7	2.0
Hexagonal prisms 10	860.0	0.21	1.6	4.2
Triangular pyramids12	454.5	0.22	0.8	2.1
Volcanic ash (Mt.Etna)	151.7	0.30	0.3	0.8
“	153.5	0.30	0.3	0.8
“	184.2	0.28	0.7	2.0
“	230.3	0.27	1.7	4.5
“	307.0	0.25	3.7	10.0
“	460.5	0.24	8.9	23.7
“	921.1	0.21	27.8	74.0

Then, by using the Carman equation (4), the thicknesses of the ash deposit on the screen have been calculated. Results are shown in Table 5 (l_1 and l_2, respectively, are the thicknesses of the ash deposit causing the values Δh_1 and Δh_2 of head loss).

The results show that the increase of the index of the voidage for the granular bed determines an increase of the deposit thickness causing the values Δh_1 and Δh_2 of head loss. It must be noted that a minimum quantity of ash is enough to clog the screen.

8 CONCLUSION

In this paper the conditions leading to failures or malfunctions of screens, with the respect to the phenomenon of volcanic ash emission, have been determined. The estimation of the threshold amounts of ash causing the screens' damage has been made for a case-study (surrounding Mt. Etna) by using literature data. The results show that the increase of the voidage of the particles increases also the accumulation thickness, which causes a given head loss.

The study has provided the base for the construction of the vulnerability maps related to these facilities located in the area affected by the fallout of volcanic ash, according to the methodology presented by Milazzo et al. (2013c).

REFERENCES

Ancione, G., Salzano, E., Maschio, G. Milazzo, M.F. 2014. Vulnerability of Wastewater Treatment Plants to Volcanic Na-Tech events. *Chemical Engineering Transactions,* 36, 433–438. DOI: 10.3303/CET1436073.

Antonioni, G., Campedel, M., Spadoni, G., Cozzani, V. Development of a general framework for the quantitative assessment of risk related to Na-Tech accidents. Proceedings of ESREL 2007, European Safety and Reliability Conference. 4, 2749–2755, 2007.

Barnard, S.T. 2004. Results of a reconnaissance trip to Mt. Etna, Italy: The effects of the 2002 eruption of Etna on the province of Catania. *Bulletin of the New Zealand Society for Earthquake Engineering,* 37, 47–61.

Baxter, P.J., Bernstein, R.S., Falk, H., French, J., Ing, R. 1982. Medical aspects of volcanic disasters: An outline of the hazards and emergency response measures. *Disasters,* 6, 268–276.

Blong, R. 2003. Building damage in Rabaul, Papua New Guinea, 1994. *Bulletin of Volcanology,* 65, 43–54.

Blong, R.J. 1984. *Volcanic hazards: a sourcebook on the effects of eruptions/R.J. Blong,* Sydney, Academic Press.

Coulson, J.M., Richardson, J.F., Backhurst, J.R. 1999. Chemical Engineering: Fluid flow, heat transfer, and mass transfer (6th ed., 1999), Butterworth-Heinemann.

Coulson, J.M., Richardson, J.F., Backhurst, J.R. Harker, J.H. 2002. *Chemical engineering: Particle technology and separation processes*, *(5th ed.,2002),* Butterworth-Heinemann.

Cruz, A.M., Steinberg, L.J., Arellano, A.L.V., Nordvik, J.P., Pisano, F. 2004. State of the art in Natech risk management. *European Commission Directorate General Joint Research Centre, EUR,* 21292.

Day, T.G., Fisher, J.E. 1980. Mt. St. Helens: How a Wastewater Plant Coped with Its Aftermath. *Journal (Water Pollution Control Federation),* 52, 2082–2089.

De Rademaeker, E., Suter, G., Pasman, H., Fabiano, B. 2014. A review of the past, present and future of the European loss prevention and safety promotion in the process industries. *Process Safety and Environmental Protection*, http://dx.doi.org/10.1016/j.psep.2014.03.007.

Fabiano, B., Currò, F. 2012. From a survey on accidents in the downstream oil industry to the development of a detailed near-miss reporting system. *Process Safety Environmental Protection* 90: 357–367.

Johnston, D.M. 1997. *The physical and social impacts of past and future volcanic eruptions in New Zealand.* Unpublished PhD thesis, Massey University.

Krumbein, W.C. 1934. Size frequency distributions of sediments. Journal of Sedimentary Petrology 4: 65–77.

Metcalf, L., Eddy, H.P. Tchobanoglous, G. 2004. *Wastewater engineering: treatment, disposal, and reuse,* New York [etc.], McGraw-Hill.

Milazzo, M.F., Ancione, G., Basco, A., Lister, D., Salzano, E. Maschio, G. 2013a. Potential loading damage to industrial storage tanks due to volcanic ash fallout. *Natural Hazards,* 66, 939–953, doi: 10.1007/s11069-012-0518-5.

Milazzo, M.F., Ancione, G., Salzano, E., Maschio, G. 2013b. Risks associated with volcanic ash fallout from Mt. Etna with reference to industrial filtration systems. *Reliability Engineering & System Safety,* 120, 106–110. DOI: 10.1016/j.ress.2013.05.008.

Milazzo, M.F., Ancione, G., Salzano, E., Maschio, G. 2013c. Vulnerability of industrial facilities to potential volcanic ash fallouts. *Chemical Engineering Transactions,* 31, 901–906. DOI: 10.3303/CET1331151.

Milazzo, M.F., Primerano, P., Ancione, G., Salzano, E., Maschio, G. 2014. Potential damages of atmospheric storage tanks due to volcanic ash aggregations in presence of water. *Chemical Engineering Transactions*, 36, 487–492 DOI: 10.3303/CET1436082.

Palumbo, A. 1998. Long-term forecasting of the extreme eruptions of Etna. *Journal of Volcanology and Geothermal Research,* 83, 167–171.

Smithsonian-Institution 2000. Copahue. Bulletin of the Global Volcanism Network.

Spence, R.J.S., Baxter, P.J., Zuccaro, G. 2004. Building vulnerability and human casualty estimation for a pyroclastic flow: a model and its application to Vesuvius. *Journal of Volcanology and Geothermal Research,* 133, 321–343.

Stewart, C., Johnston, D.M., Leonard, G.S., Horwell, C.J., Thordarson, T., Cronin, S.J. 2006. Contamination of water supplies by volcanic ashfall: A literature review and simple impact modelling. *Journal of Volcanology and Geothermal Research,* 158, 296–306.

Stewart, C., Pizzolon, L., Wilson, T., Leonard, G., Dewar, D., Johnston, D., Cronin, S. 2009. Can volcanic ash poison water supplies? *Integrated Environmental Assessment and Management,* 5, 713–716.

Volcanoes.Usgs.Gov. *Ash properties & dispersal by wind* [Online]. Available: http://volcanoes.usgs.gov.

White, J., Stewart, C., Wareham, D., Wilson, T. 2011. *Treatment of volcanic ash-contaminated surface waters through the optimisation of physical and chemical processes,* Lower Hutt, N.Z., GNS Science.

White, W.T., Day, T.G., Berteck, D., Fisher, J. 1980. Mt St Helens Volcanic Ash vs. Yakima Wastewater treatment facility. Institute for water resources newsletter.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimum concept of management and trade-off with risks

D. Prochazkova
Faculty of Transportation Sciences, Czech Technical University in Prague, Czech Republic

ABSTRACT: The paper gives the results of expert's judgement of five basic procedures of management and trade-off with risks that are used in managerial and engineering disciplines in a present practice. The judgement is based on evaluation of procedures with regard to the public interest, i.e. according to their capability to ensure the security for humans through ensuring the safe buildings, safe infrastructures, safe territories and safe human communities considered as systems. The assessment respects that human system: is a system of systems having several incommensurable assets, which have sometimes different goals. Among assets there are interdependences of a different nature, which are sources of different conflicts. It is used: the multicriterial approach based on 14 criteria and quantity "criticality rate". Data for determination of criticality rates are obtained from experts from domains: public protection, territory protection, environment protection, public administration responsible for strategic development, protection of technological systems, and Integrated Rescue System. The optimum concept is determined by application of the theory of marginal assessment.

1 INTRODUCTION

For ensuring the live of humans in a safe space there is necessary to manage and trade-off with risks properly, i.e. measures and activities targeted to the existence, security and development of human system. In 1994 the UN (UN 1994) formulated the human society target as the human system safety and the EU (EU 2004) formulated it as the safe community in 2004. The basic tools of human society for achievement of these objectives are the human society governance and the correct application of knowledge and experiences connected with trade-off with risks respecting the public interests. In this respect the great role plays the management and engineering disciplines, the aim of which is to arrange the human security and sustainable development.

Present cognition shows that it means to take care on public assets: human lives, health and security; property and welfare; environment; critical technologies and infrastructures, Figure 1 (Prochazkova 2011a). The tool that is aimed to mentioned targets is an integral (complex) safety (Prochazkova 2011a). To reach above mentioned targets the problems on several levels: technical, functional (organisational, operative), tactical, strategic and political (Fig. 2) have been solved (Prochazkova 2011b) by a way that solutions on all levels have been interconnected.

Robustness and capacity on technical level are aspects that the under critical conditions guarantee the safety of objects and that are the important for

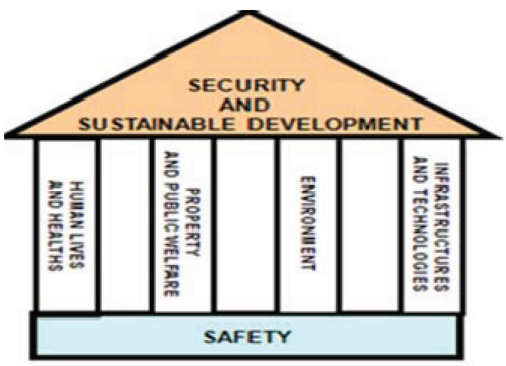


Figure 1. Human system public assets.

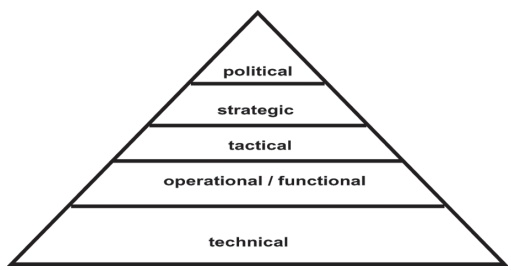


Figure 2. Levels on which security problems should be addressed.

ensuring the protection and survive of inhabitants (Prochazkova 2012).

2 STATE-OF-ART AND TERMS USED IN MANAGEMENT AND TRADE-OFF WITH RISKS

State of art of problems´ solution according to knowledge summarizes in works (Prochazkova 2011b, 2012) is:

– each object under consideration is a system, i.e. it is characterized by elements, linkages and flows,
– the system vulnerabilities are also caused by linkages and mainly by flows of energy, information, material, finances etc. among the system elements that cause couplings; mentioned couplings create often interdependences that are often the causes of failures and often by a cascade failure of several partial systems at occurrence of extreme (beyond design, severe) disasters, Figure 3 (Prochazkova 2011a, b, 2012, 2013). The nature of interdependences is physical, cyber, organisational and territorial (Prochazkova 2012).

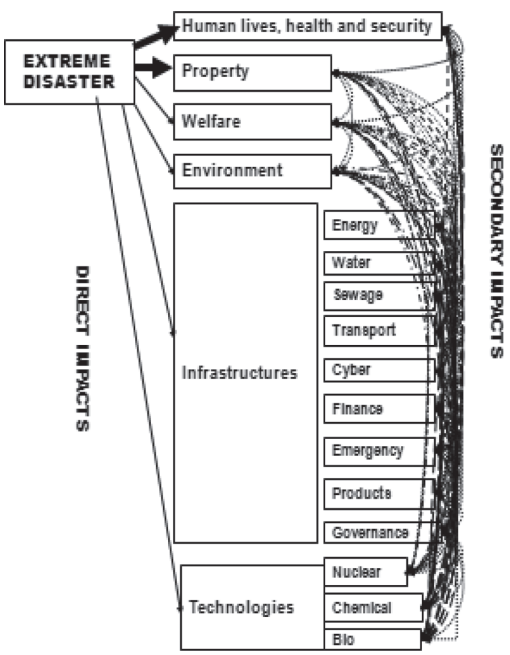


Figure 3. Impacts in the human system at extreme disaster; anthropogenic measures and activities ensure the protection of public assets only for disasters with size smaller than design disaster; only at defined nuclear facilities there are carried out measures and activities against selected beyond design disasters (Prochazkova 2011a).

The recent cognition shows that the present world and its objects are represented by a model denoted as a system of systems i.e. several overlapping systems that are open and fulfil certain functions (Prochazkova 2011a, b, 2012). They are interconnected by linkages and flows which create mutual interdependences that cause specific vulnerabilities (Prochazkova 2012).

A system according to its core means more than only a sum of parts (Prochazkova 2011b), and therefore, the stress is put on:

– a study of the interactions and associations,
– non-linear thinking,
– interactions,
– inductions;
– feedbacks,
– experiments or realistic simulations.

E.g. feedbacks cause non-linearity in the system behaviour and cause that the behaviour is not predictable, and therefore, it is not possible to use the common prognostic methods for the identification of the possible states of a system. The consequence is an occasional occurrence of unexpected situations that threaten the humans, and it is difficult to get over them.

The complexity of systems with which we work in practice is different. According to work (Prochazkova 2013) four types of system configurations are used; they are:

– simply organized units,
– composite systems,
– complex systems,
– set of overlapping systems.

Behaviour of simply organized units is clearly given by structure and properties of units and it is described by analytic functions. The composite systems are understood as a representation of elements that are organized and connected in a certain way and because of a proper structure they fulfil certain functions. Their behaviour is described by results of statistical solutions based on analytic functions, the parameters of which are variable in a certain interval, which are a reflection of various possible states/variants of the system behaviour. The complex systems have many components (often systems too) that interact together and are organized in several levels (Prochazkova 2013), which causes that we observe: suddenly emerged behaviour features that is not possible to obtain from the knowledge of components' behaviour, it is the so-called emergence; hierarchy; self-organization; and various management structures, which all together seems as a chaos, and therefore,

in their description there are random and epistemic uncertainties. Their behaviour is described by results of simulations taking note of existence of epistemic uncertainties. The System of Systems (SoS), i.e. a set of several overlapping systems (often complex systems), is very complicated, and therefore, its behaviour can be only obtained if a multidimensional and inter-dimensional approach is applied and it is based on simulation of variants by multi-criteria procedures.

Since the solution of many problems in practice means to consider the complex systems and the SoS, the system thinking is the fundamental principle of research if we deal with safety. The system thinking means: to see both, the whole and the details at the same time; ***to focus on the dynamics of processes;*** to pay attention to relations, associations and interactions; ***to take into account the roles of a feedback;*** to consider the relativity of possible situations; and to think in a long-term way (Prochazkova 2011b, 2012).

At management and engineering solution of complex systems and systems of systems it is then *necessary to use the multi-criteria approach and in a case of system of systems it is also* necessary to consider the cross-sectional risks that are the causes of emergent interdependences originating at certain conditions, and therefore, to their detection the attention of engineering disciplines is concentrated at system design. At their problems' solution the tools are based on: the theory of chaos; theory of fuzzy sets; complexity theory; and theory of possibilities—set of references to their derivation is in books (Prochazkova 2012, 2013). In case of management of SoS we must also respect basic requirements, i.e. co-existence of overlapping systems (Bossel 2004). For human goals fulfilment it is necessary to arrange the co-existence of important systems, minimally social, environmental and technological systems that create the human system.

Regarding to present view of the UN, EU and public interest (EU 2004, Prochazkova 2011a, UN 1994) the ground for human being is a conservation of existence, security and potential for development for humans. In this context in practice the following terms are used.

Security is the state of system at which the occurrence of harm or loss on system assets (protected public interests) has an acceptable probability (it is almost sure that harm and loss do not arise). It means that it ensures a certain stability of a system in time and space, i.e. a sustainable development which means that the system is well protected against internal and external disasters of all kinds.

Safety is a set of human measures and activities for ensuring the existence, security and sustainable development of system and its assets. Its measure is the effectiveness of appropriate measures and activities at ensuring the system assets security and sustainable development.

Secured system is the system that it and its assets are not threaten by disasters, the origin of which are inside and outside of system, including the human factor.

Safe system is the system that it and its assets are not threaten by disasters, the origin of which are inside and outside of system, including the human factor, and the system itself does not threaten its vicinity at its normal, abnormal and critical conditions.

Human system safety management is the management of human system directed to human system safety, the product of which is the security and sustainable development of all public assets.

The engineering is a set of disciplines that realise the tasks determined by management procedure into practice. The risk is for engineering practice expressed as probable size of losses, damages and harms on followed assets that are caused by a given disaster with specified size (size of normative hazard) and that are rescheduled for a certain time unit (usually 1 year) and a certain object or a certain site. The risk engineering was the 20th century phenomenon and on its base there was set up in developed countries the groundwork for human development that is quite resistant against to traditional disasters, namely natural ones; human, animal and plant diseases; technology failures; and social disasters.

According to definitions used by the UN, Swiss Re, World Bank etc. (summarized in Prochazkova 2011b) the risk engineering:

- is the systematic use of engineering knowledge and experiences for the optimization of the protection of human lives, environment, property and economic assets, i.e. for the optimum reach of security and sustainable development of human system,
- has a main purpose to reduce all types of harms and losses by the means of aimed and qualified trade-off with risk.

It is necessary to note that at present practice the risk engineering has not yet been interpreted by an explicit way and different concepts are not often distinguished.

It is necessary to consider that risk engineering is not a static discipline because it has been developed in time. ***The problem of present specialists, mainly oriented to calculations***, is that they do not distinguish different concepts, and in some cases such ignorance is a cause of incorrect solutions (e.g. if they used standards and norms for secured system and the correct solution of problem requires standards and norms for the safe system because the failure of system has a great potential

to damaged assets being in system vicinity); see lessons learned from recent important accidents (AIChE 1994, Prochazkova 2013).

3 PROCESS MODEL OF WORK WITH RISKS

According to present standards the risk expresses the probable size of undesirable and unacceptable impacts (losses, harms and detriment) of disasters with the size equal to a normative hazards on system assets or subsystems in a given time interval (e.g. 1 year) and a given site, i.e. it is always site specific (Prochazkova 2011b).

The typical risk properties are random and epistemic uncertainties (epistemic uncertainties = vagueness). If we want to manage risk, we must identify, analyse, assess it and after this to decide what we can do, in dependence on our possibilities—knowledge, staff, technical means and finance sources. For this, we must use a lot of different methods, tools and techniques and also principles of good practice (good engineering practice).

Work with risk is expressed by model shown in Figure 3 (Prochazkova 2013). It starts with definition of concept of work with risk (system characteristics, determination of assets, specification of aims), on the basis of which risks are identified, analysed, assessed, judged, managed, traded-off and monitored. Feedbacks denoted in this Figure 4 are used if risk level is not on required level (Prochazkova 2013).

For human safety and for human system safety (i.e. territory, organisation, plant) we must manage the integral risk including the human factor, i.e. to find the way of cross-section risks management and to concentrate the investigation on interdependences and on critical spots with a potential to start the system cascade failures, domino effects,

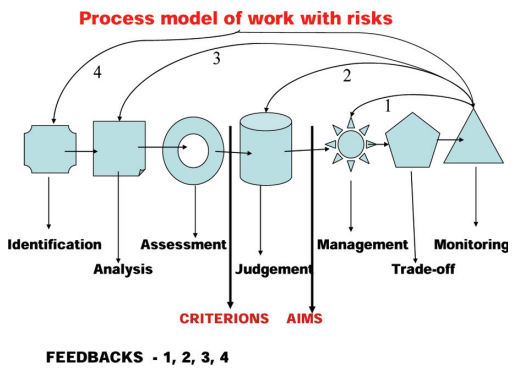


Figure 4. Process model of work with risks, numbers 1, 2, 3 and 4 denote feedbacks.

strange behaviour etc., and on the basis of such site knowledge to prepare measures and activities ensuring the continuity of limited infrastructure operation and of the human survival.

Evaluation of present knowledge shows that one of number of causes are interdependences inducing the cascade failures in the human system or in its part are the human errors (intentional or involuntary) in management and in deciding. Therefore, we must do all measures in managerial and engineering activities to avert human failures, namely at decision-making. Because consequences of errors originating at decision are often huge, the great attention is concentrated to work with risks at present (Prochazkova 2013, AIChE 1994).

The often used characteristic of engineering's work with the risks is:

- it considers multi-fields and cross-sectional disciplines that use both, the general and the specific methods, tools and techniques (specific ones are either simple or complex, complex ones represent well-ordered use of several general or simple methods, tools and techniques),
- it uses methods, tools and techniques logic, technological, financial, managerial and deciding because their integral part is a decision on technological problems, costs and time planning,
- it deals with tasks that connect the trade-off with risks for human system safety ensuring and the requirement of non-trivial solution of problems by use of multi-criteria methods, tools and techniques.

In all procedures it must be respected that assets and causes of risks have different natures that cause incommensurability of criterions and reasons, which only allows application of multi-criteria methods, tools and techniques that are suitable, i.e. correct and valid for a given problem target.

From the methodical viewpoint at selection of methods, tools and techniques they must be respected: data quality; structure of problem that is solved and requirements on quality of results; which means specially to test both, the data quality (accuracy, completeness, homogeneity, bearing witness to a given problem (Prochazkova 2011b)), and the qualification of experts if they are used (IAEA, OECD, World Bank etc. have strict criteria for judgement of expert qualification) (Prochazkova 2013).

4 PRESENT CONCEPTS OF MANAGEMENT AND TRADE-OFF WITH RISKS

The ground of human effort is to cope with (to tame) the risks. The term "*risk*" has the origin in

the middle Ages and our present knowledge on trade-off with risk has been collected since 30s of last century. Obtained knowledge and experiences have been influenced the management of risks and its measures and activities have been introduced step by step into practice by engineering disciplines (Prochazkova 2012).

At present work with risk, the risk is understood as the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). Now in practice there are used five types of risk management/engineering of systems, i.e.

– classical risk management and risk engineering,
– classical risk management and risk engineering including the human factor,
– security management and security engineering,
– safety management and safety engineering, i.e. risk governance/trade-off for security and sustainable development of system,
– safety management and safety engineering determined for System of Systems (SoS) (Prochazkova 2011b, 2012),

See Figure 5 and the detail description in the annex.

It is evident that each more advanced type keeps the higher demands on knowledge, tools, times, finance, personnel qualification etc. For each management and each engineering concept there has been developed a certain set of standards and norms for its use in practice (Prochazkova 2012).

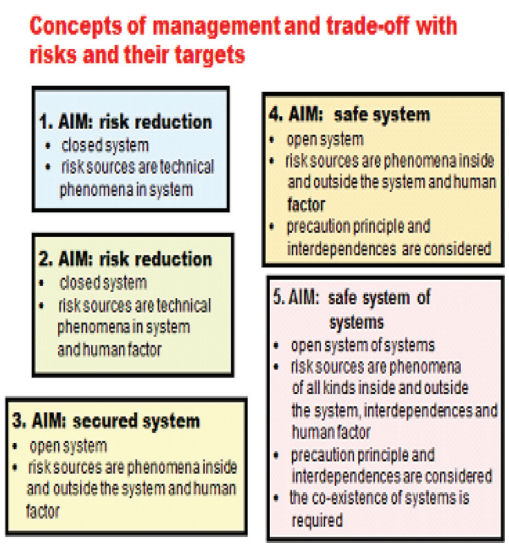


Figure 5. Concepts of management and trade-off with risks and their targets arranged chronologically according to introduction in practice.

For different assumptions of concepts the results of their applications in practice have not been the same. From these reasons in next paragraphs we compare mentioned concepts, especially in engineering disciplines and judge the validity of their use with regard to their capability to ensure human system safety, i.e. human security, existence and sustainable development.

5 DATA AND METHODS FOR DETERMINATION OF CRITICALITY RATES OF PROCEDURES FOR WORK WITH RISK

Object of our interest in which we test procedures for work with risks is the human system that is composed of assets: human health, property, welfare, environment, infrastructures and technologies that are incommensurable and some of their aims are conflicting (e.g. environment vs. technologies—exploitation of natural resources, contamination of air, water and rock); and linkages and flows among the assets. Therefore, for searching the best way of human work with risk the special tool must be used. As is given above we use five different concepts at present.

For comparison of concepts used in practice for system risk management and for trade-off with system risk from the viewpoint of their capability to ensure the human system security we use the quantity "criticality" and the procedure based on the Multiatribute Utility Theory (MUT) (Keeny & Raiffa 1976) with the statement "the higher, the worse". The criticality is given by level of integral risk in which the main role is played by level of cross-sectional risks (Prochazkova 2011b).

The assessment respects that human system: is a system of systems; and has several incommensurable assets, which have sometimes different goals and among them there are interdependences of a different nature, which are sources of different conflicts. Therefore, there are used: the multicriterial approach; 14 criteria directed to the public protection; quantity the criticality rate; and defined value scale.

The set of criterions used for judgement of capability of followed procedures is the following:

1. rate of capability of protection of human lives, health and security inside the system
2. rate of capability of protection of human lives, health and security outside the system
3. rate of capability of protection of property inside the system
4. rate of capability of protection of property outside of system
5. rate of capability of protection of welfare inside the system

6. rate of capability of protection of welfare outside of system
7. rate of capability of protection of environment inside the system
8. rate of capability of protection of environment outside the system
9. rate of capability of protection of live-giving infrastructures and technologies inside the system
10. rate of capability of protection of live-giving infrastructures and technologies outside the system
11. rate of capability of protection of human lives and health against disaster impacts caused by interdependences
12. rate of capability of protection of environment against disaster impacts caused by interdependences
13. rate of capability of protection of human society against disaster impacts caused by interdependences
14. rate of capability of protection of live-giving infrastructures and technologies against disaster impacts caused by interdependences

The used value scale that is used in many norms and standards for risk assessment (Prochazkova 2013) and in norms used by FEMA, Swiss Re etc. is the following:

0 point—criterion ensures extremely high capability of protection (expected damages are lower than 5%, concept application means no significant risk for assets, i.e. negligible concept criticality),
1 point—criterion ensures very high capability of protection (expected damages are in interval 5–25%, concept application means low risk for assets, i.e. low concept criticality),
2 points—criterion ensures high capability of protection (expected damages are in interval 25–45%, concept application means median risk for assets, i.e. median concept criticality),
3 points—criterion ensures median capability of protection (expected damages are in interval 45–70%, concept application means high risk for assets, i.e. high concept criticality),
4 points—criterion ensures low capability of protection (expected damages are in interval 70–95%, concept application means very high risk for assets, i.e. very high concept criticality),
5 points—criterion ensures negligible capability of protection (expected damages are higher than 95%, concept application means extremely high risk for assets, i.e. extremely high concept criticality).

Data for determination of criticality rates were obtained from experts from domains: public protection, territory protection, environment protection, public administration responsible for strategic development, protection of technological systems, and Integrated Rescue System. These experts fulfilled the criteria for expert competence used in the EU (Prochazkova 2013) and they evaluated 14 factors given above according to their knowledge and experience.

Table 1. Scale of values for determination of rate of criticality of concepts for work with risk.

Rate of concept criticality	Values in %	Number of points for factor
Extremely high	More than 95%	More than 66.5
Very high	70–95%	49–66.5
High	45–70%	31.5–49
Median	25–45%	17.5–31.5
Low	5–25%	3.5–17.5
Negligible	Less than 5%	Less than 3.5

The resultant value for each factor is determined as the median from data obtained from experts. Resultant assessment of capability of protection for all factors with assumption that all factors have the same weight can take on values from 0 to 70. If we again apply approach used in (Prochazkova 2013) we obtain values given in Table 1.

6 RESULTANT CRITICALITY RATES AND OPTIMUM CONCEPT OF WORK WITH RISKS

In work (Prochazkova 2014) there are described in detail results of evaluation obtained on the data from 6 experts who performed evaluation according to 14 criteria given above and directed to judgement of capability of followed concepts of risk management and engineering procedures for trade-off with risks to implement targets of humans that are existence, security and development of humans, i.e. it goes on public protection in the broadest context.

The author remarks that at other evaluation targets or at different assets' specification the different criteria and another threshold values must be used, which substantially affect the results. The results of evaluation under account are given in Table 2.

From Table 2 it follows that the criticality is:

– extremely high for the classical system risk management/engineering,
– very high for the classical system risk management/engineering considering the human factor,

Table 2. Rate of criticality of followed concepts of risk management/engineering.

Criterion	Classical system risk management and risk engineering	Classical system risk management and risk engineering considering the human factor	System security management and security engineering	System safety management and safety engineering	System of systems safety management and safety engineering
1	4	3	1	1	1
2	5	5	5	1	1
3	4	3	1	1	1
4	5	5	5	1	1
5	5	3	1	1	1
6	5	5	5	2	1
7	4	3	1	1	1
8	5	5	5	1	1
9	4	3	1	1	1
10	5	5	5	1	1
11	5	5	4	5	1
12	5	5	4	5	1
13	5	5	4	5	1
14	5	5	4	5	1
Total	66	60	41	31	14

– high for system security management/ engineering,
– median for system safety management/ engineering,
– low for system of systems safety management/ engineering.

It means that the system of systems safety management/engineering is the most effective concept of work with risk with regard to our present knowledge and experience directed to human system safety from the viewpoint of ensuring the human security and sustainable development. Taking into account the reality that the use of various concepts are differ by requirements on knowledge, data, personal qualification, material, finance and technical solutions, it is evident that the most effective concept is the most challenging. Therefore, it is necessary and important for strategic level of problems' solution. For tactical and functional levels of problems' solution is sufficient the concept ensuring the system safety management/engineering. The concept called as system security management/engineering is only suitable for technical level of problems' solution, i.e. in cases in which high damage on system vicinity are not probable.

It is also evident that at emergency management or at crisis management we have not time to determine the most suitable strategic solution, i.e. at emergency at simple case the risk management/engineering principles are sufficient, but at most of real cases the security management/engineering principles are applied if we *only* protect object under account and not its vicinity, ***otherwise*** the safety management/engineering principles or SoS management/engineering principles must be applied.

Because the system safety is complementary quantity to system criticality, i.e. safety + criticality = 1, we obtain from Table 2 the following values for safety rate: 0, 1, 2, 3, 4; and for safety rate the statement "the higher, the better".

To obtain the optimum concept for our aim we use the way used in the engineering disciplines, i.e. the theory of margin assessment (Sage & Rouse 2011, Savin 2010) which is often used in the engineering disciplines. By this way we obtain for safety rate the values: median $\mu = 2$ and standard deviation $\sigma = 0.63$; $\mu + \sigma = 2.63$; $\mu + 2\sigma = 3.26$; and $\mu + 3\sigma = 4.89$. From this it follows that ***the concept for system of systems safety management/engineering is the optimal for ensuring the EU security.***

The output also shows that at all fundamental decisions that have strategic significance and long-term consequence the work with risks must respect minimally a concept of work with risk for ensuring the safe system. Only by this way humankind might preserve a chance for long-term existence, security and development.

7 CONCLUSION

Five types of the risk management and risk engineering are used in a present practice. For each risk management and risk engineering type based on negotiation with risks there are standards and norms. Because the demands of various concepts are different, the standards and norms are

different, the results are different and requirements on data, knowledge, material, technology, finances etc. are different.

Owing to provident handle with sources, forces and means it is necessary in real cases to decide which concept is sufficient for a given problem solution. At deciding the role plays the risk size and the level of problem solution.

The results given above show that at:

- strategic level of problem solution it is necessary to use the system of systems safety management and system of systems safety engineering that fulfils demands of social engineers, technical engineers and environmental engineers,
- tactical and functional levels it is necessary to respect strategic concept recommendations and at site specific immediate problems' solution it is possible to use the system safety management and system safety engineering because character of solved problems is not so fundamental from the long term viewpoint,
- technical level it is necessary to respect recommendations of all higher concepts, i.e. strategic, tactical and functional ones and for site specific immediate problems' solution it is possible to use the system security management and security engineering if character of solved problems is not so fundamental from the time viewpoint,
- political problems solutions it might be respected strategic solutions if they want to respect public interests.

At solution of emergency situation there is lack of time, information and knowledge, and therefore, it is justified the reaction using the concept of management and engineering trade-off with risk directed to secured system and at critical cases only concept of management and engineering trade-off with risk directed to risk reduction considering the human factor.

REFERENCES

AIChE, 1994. *Guidelines for Preventing Human Error in Process Safety*, American lnstitute of Chemical Engineers, New York, NY, 1994.

Bossel, H. 2004. *Systeme, Dynamik, Simulation—Modellbildung, Analyse und Simulation komplexer Systeme*. Books on Demand, Norderstedt/Germany, ISBN 3-8334-0984-3, www.libri.de.

EU, 2004. *The Safe Community Concept.* Brussels: EU, PASR project.

Keeny, R.L. & Raiffa, H. 1976. *Decision Analysis with Multiple Conflicting Objectives*. New York: J. Wilex.

Prochazkova, D. 2011a. *Strategic Safety Management of Territory and Organisation*. ISBN 978-80-01-04844-3. Praha: ČVUT, Praha, 483p.

Prochazkova, D. 2011b. *Risk Analysis and Risk Management*. ISBN 978-80-01-04841-2. Praha: CVUT, Praha, 405p.

Prochazkova, D. 2012. *Critical Infrastructure Safety*. ISBN: 978-80-01-05103-0, Praha: ČVUT, 318p.

Prochazkova, D. 2013. *Principles of Critical Safety Management*. ISBN: 978-80-01-05245-7. Praha: ČVUT, 225p.

Prochazkova, D. 2014. Optimum concept of management and trade-off with risks—detail results. In: *Ochrana obyvatelstva 2014.* ISBN: 978-80-7385-142-2, ISSN: 1803-7372, SPBI, Ostrava, pp 181–190.

Sage, A.P. & Rouse, W.B. 2011. *Handbook of Systems Engineering and Management*. ISBN 978-0-470-08353-6. New Jersey: J. Wiley and Sons, 1504p.

Savin, D. 2010. *Control Systems Security Program—Transportation*. Washington: US Department of Transportation, www.dot.gov.

UN, 1994. *Human Development Report.* New York: UN, www.un.org.

Annex—description of types of risk management and risk engineering.

Type	Concepts of work with risks—characteristics, targets and procedures
Classical risk management/ engineering	Object is a closed system. Risk sources are internal technological phenomena in system. The target is to reduce the technological risks of a system to a certain level, given by standards and norms. It originated in 30s of last century. The risk is determined after the design of the system, and therefore, there is no possibility to reduce risks connected with an inappropriate solution for a given site and system. The reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones.
Classical risk management/ engineering considering the human factor	Object is a closed system. Risk sources are internal technological phenomena and human factor in system. The target is to reduce: the technological risks of a system to a certain level given by standards and norms; and risks connected with a human factor by safety instructions for danger works. It originated at the end of 70s of last century. The risk is determined after the design of the system, and therefore, for reduction of risks connected with an inappropriate solution for a given site and system may be removed only by organisational measures, the effectiveness of which is lower than effectiveness of technical ones.
System security management/ engineering	Object is an open system. Risk sources are external and internal phenomena including the human factor. The target is to reduce risks for a system: from external and internal phenomena, a human factor, and also failures of decision-makings at risk management/ engineering were to a certain level given by standards and norms; i.e. to ensure the security of a system and its assets. No interest on system vicinity. IT originated at the first half of 80s of last century. The protection of system vicinity is not solved. Unacceptable impacts on vicinity can be only mitigated by special off-site emergency plans, i.e. by organisational measures and activities if state enforces such legislation.
System safety management/ engineering	Object is an open system. Risk sources are given by all hazards approach. The target is to ensure the security of a system and its assets and the security of system vicinity. The advanced safety engineering uses at risk determination the following principles: risk is determined during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition; the risk determination is directed to user's demands and to the level of provided services; risk is determined according to the criticality of impacts on processes, provided services and on assets that are determined by public interest; and unacceptable risks are mitigated by tool for risk management, i.e. according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up. It originated at the second half of 80s of last century. The target is the safety, i.e. it is also necessary to trade-off with risks having low occurrence frequency if their impacts are unacceptable, and i.e. precaution principle is applied. The set of standards and norms exist especially for nuclear and chemical domain. To prepare groundwork, it is necessary to combine analytical methods with expert judgement by which we remove vagueness (epistemic uncertainties) in data. Except of technical measures respecting the precaution principle, special technical problems solution there are continuity plans containing the procedures for overcoming the critical conditions in system and system vicinity, emergency plans and crisis plans. The risk management viewpoint by these characters: sitting—designing—construction—project with risk reduction; operation with the integration of early warning systems and of procedures for the management of the acceptable level of risks; and defeating the abnormal, emergency and critical conditions at the operation and at putting out of the operation.
System of systems safety management/ engineering	Object is an open system of systems. The target is to ensure: the security of both, the system of systems including its assets and the system of systems vicinity; and the co-existence of individual systems creating the system of systems. Risk sources are given by all hazards approach and by interdependences among the partial systems and by those with vicinity. Formation at the beginning of third millennium. The set of standards and norms are under discussion and preparation.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Possibilistic risk analysis of failure in water supply network

B. Tchórzewska-Cieślak, K. Boryczko & I. Piegdoń
Department of Water Supply and Sewage Systems, Rzeszow University of Technology, Rzeszow, Poland

ABSTRACT: The paper proposes an alternative approach to the failure risk analysis of water supply network which includes random emergency events inaccuracy, diversity and a small amount of data. The presented method is based on the so-called theory of facts (Shafer) based on the concept of inaccurate probabilities and possibilities (Zadech), which combines the so-called distribution capabilities of the belonging function of fuzzy set. The main aim of this paper is to present the concept of failure risk analysis of water supply network. The proposed model was used for failure risk analysis of water supply system serving 63 thousand people in the east of Poland.

1 INTRODUCTION

The Collective Water Supply System (CWSS) as a complex technical system consisting of functionally interrelated objects, whose task is to provide safe drinking water for residents. It is one of the priority technical systems included in the basic infrastructure of urban agglomerations. Its importance to the public is unquestionable because water is a prerequisite for human existence. The World Health Organization (WHO) warns about the so-called global water crisis which is not only associated with a changing climate but also resulting from of the aquatic environment pollution, constantly increasing population (especially in poor regions) or armed conflicts.

The main element of this system is the water supply network, which supplies buildings with water. Reliability of water supply is to ensure stable conditions, enabling current and future water demand in accordance with the WHO and local standard. The water transported by the water network should be safe and should be provided in the required quantities and at the required pressure. The unreliability of the water supply system resulting mainly from various types of failures or the appearance of biofilm in the network. Those events can cause interruptions in water supply or polluted water provision. It is assumed that the measure of the loss of CWSS safety is risk related to system reliability. In terms of risk management in water supply systems spaces the European standard EN 15975-1-2011 Security of drinking water supply—guidelines for risk and crisis management—Part 1: crisis management. In Poland, they are respectively the PN-EN 15 975-2:2013-12 E and PN-EN 15975-1-2011.

It was assumed that the risk of failure of the water supply system is a function of the probability of failures occurrence, the consequences but also the degree of vulnerability to the hazard. Research conducted in this area by (Apostolakis & Kaplan 1981, Aven 2010, Christodoulous et al. 2008, Craun & Calderon 2001, Ezell et al. 2000, Haimes 1998, Zio 2007) cover a wide range of failure events cause and effect analyses related to the functioning and operation of water supply network. These studies demonstrate a significant effect of the material, the age of pipe, network pressure, the foundation but also chemical and biological stability of water (Christodoulous et al. 2003, Faber & Steward 2003, Grey-Gardner 2009, Hokstad et al. 2009, Hrudey & Hrudey 2004, Hubbard 2009 Very often hydraulic models are used (simulations using EPANET software) and various databases (e.g. GIS), which allow not only to evaluate the technical state of pipes, but also to forecast failure events (Boryczko et al. 2014, Maqsood et al. 2005). Such studies require appropriate methodology but also a detailed and structured database. It determines the correct statistical analysis of the data and the appropriate cause-effect model, e.g. event tree or fault tree, in terms of the analysis of various emergency scenarios that may cause the loss of water consumer safety (Ezell et al. 2000, Kołowrocki 2004, Rak 2003, Zio 2009, McGill et al. 2005).

The problem in the analysis occurs when the database is incomplete or uncertain. There is a need to rely on the knowledge and the experience of experts. In the literature it can be found a new issue of so-called risk analysis in uncertainty conditions. There are two approaches related to this issue. The first approach assumes that the risk is a kind of uncertainty. Taking into account the uncertainty data in risk analysis it is possible to make an analyse using the theory of subjective probability and neural Bayesian networks (Dempster 1967, Hahn et al. 2002, Haimes

et al. 2006, Kleiner & Rajani 2000). The second approach is based on fuzzy logic, neuro-fuzzy networks and genetic algorithms (Christodoulous & Deligianni 2010, Kleiner et al. 2004, Markowski & Mannan 2008, Sadiq & Tesfamariam 2009, Shang-Lien & Ruei-Shan 2002). This approach is used in a variety experts systems and in technical infrastructure management processes. In fuzzy models it is possible to use experts knowledge as a linguistic variables, which facilitates the analysis, primarily in the area with small data sets in which designated the combination of the probability distribution is significantly more difficult. In the absence of sufficient static database the parallel methods based on the so-called soft models including Bayes network, fuzzy modelling, were developed. The aim of this paper is to propose an alternative model of water supply system including failure risk analysis which uses a Dempster Shafer theory and fuzzy models for very unlikely events, but which may have serious consequences. The main applications of the model are analysis and risk assessment based on expert knowledge.

2 ASPECTS OF FAILURE RISK ANALYSIS OF WATER SUPPLY NETWORK

Failure risk analysis of water supply network is connected with (Ezell et al. 2000, Tchórzewska-Cieślak 2007, Souza & Chagas 2001, Mays 2005):

- failures of water pipes and fittings,
- secondary water pollution in the water supply system.

The consequences of these events are:

- lack of water supply to consumers or interruption of the supply,
- health risks of water consumers as a result of the consumption of poor quality water,
- waterworks company financial losses incurred as a result of failure removal, rinsing the network, the lack of water sales and compensating water consumers,
- water consumers financial losses related to the need to purchase bottled water, treatment costs, costs arising from difficulties with hygiene and sanitation.

The priority is to provide consumers with water of the right quality, at the appropriate pressure, at any time (Hrudey 2001, Johanson 2008). Water supply system failures are a major problem in the process of system operation (Hubbard 2009).

Failures of this type includes: the body of the pipe, joints or expansion joints, valves hydrants, vents, drains, etc. They may occur as a result of one-time random events or human intervention, or are the result of the combined action of time, excessive stresses and (or) local negative environmental conditions (Rak 2003). The causes of water supply network failures could also be a wrong concept of water supply network structure, wrong hydraulic operation (too high pressure, lack of protect valves against water hammer), the corrosiveness of the soil, temperature changes, etc. (Christodoulous et al. 2008, Craun & Calderon 2001, Sadiq et al. 2007).

T. Aven defines risk as a combination of three parameters: the probability of adverse events, their consequences and the uncertainty will those events will occur and what will be the consequences (Aven 1992, Haimes 2009, Rak & Tchórzewska-Cieślak 2006, Ezell et al. 2000, Zio 2007):

$$r = \{S, P, C\}$$

where:
S—failure events scenario,
P—probability of failure events scenario,
C—consequences (losses, effects) of scenario failure events occurrence.

In (Kaplan 1997) risk is described as a set of probabilities and consequences. Grouping them in terms of low probability, i.e. a vector of risk can be determined in the form of an equation that illustrates the so-called risk curve (Fig. 1) (Ezell et al. 2000, Haimes 2009, Hastak & Baim 2001, Kaplan 1997, Zio 2009):

The definition of water supply system failure risk should take into account both the possibility of the loss of water consumer safety as a result of lack of water or interruptions in water supply and consumption of poor quality water. Using the matrix method for Quantitative Risk Analysis (QRA), the following formula for determining the water supply system failure risk was proposed (Michaud & Apostolakis 2006, Tchórzewska-Cieślak & Rak 2006, Johanson 2008):

$$r = P \cdot C \cdot N \tag{1}$$

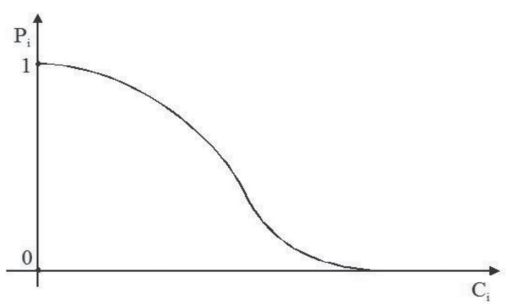


Figure 1. Risk curve.

where:
P—point weight related to the probability of failure event occurrence,
C—point scale related to the size of losses,
N—point weight associated with population at risk.

The process of risk analysis for water consumer safety occurs in the following phases of reconnaissance:

- determination of the number of residents using the CWSS,
- identification of the representative failure events and determination of scenarios to estimate losses,
- determination of the probability (frequency) of failure event occurrence.

Scales for point weights are as follow:

- a scale for the probability (frequency) of failure (*P*):
  - low—unlikely—once every 10÷50 years; $P = 1$,
  - average—quite likely—once for 1÷10 years; $P = 2$,
  - high—likely—1÷10 times a year, or more often; $P = 3$,
- a scale for the number of residents (N):
  - low—number of residents at risk up to 5 000, $N = 1$,
  - average—number of residents at risk from 5001 to 50 000, $N = 2$,
  - high—number of residents at risk more than 50 000, $N = 3$,
- consequences category (*C*):
  - small—noticeable organoleptic changes of water, individual consumer complaints, financial losses up to 5×103 EUR, $C = 1$,
  - average—a significant nuisance organoleptic (odour, colour change and turbidity), health indisposition of consumers, numerous complaints, the information in the regional public media, financial loss up to EUR 105, $C = 2$,
  - high—required hospital treatment, the results of indicator organisms revealed high levels of toxic substances, the information in the national media, financial loss above 105 EUR, $C = 3$.

Thus, the risk parameters: $P = \{1, 2, 3\}$, $C = \{1, 2, 3\}$, $N = \{1, 2, 3\}$. According to the formula (1) risk values are in the range [1–27]. The risk matrix has the form:

$$R_{PCN} = \begin{vmatrix} 111 & 121 & 131 & 112 & 122 & 132 & 113 & 123 & 133 \\ 211 & 221 & 231 & 212 & 222 & 232 & 213 & 223 & 233 \\ 311 & 321 & 331 & 312 & 322 & 332 & 313 & 323 & 333 \end{vmatrix} \quad (2)$$

The set of possible values for risk: $R = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 27\}$.

Risk assessment is the comparison of this value with criteria values:

- tolerable risk (rT) (1÷6>,
- controlled risk (rK) (6÷8>,
- unacceptable risk (rN) (8÷27>.

It should be noted that this assessment does not take into account the weights of the parameters, i.e. each parameter *P*, *C*, *N* is equally important in the risk assessment because the assessment is subject only to final risk value. For example, the risk may be equal 4 to the results of $P = 2$, $C = 2$, $N = 1$ or $P = 2$, $C = 1$, $N = 2$ or $P = 1$, $C = 2$, $N = 2$. Thus, such an analysis may be subject to some kind of uncertainty. The consideration of the possible weights for the respective risk parameters requires deeper analysis and expert knowledge.

3 POSSIBILISTIC RISK ANALYSIS

3.1 *Principles of the method*

The risk is very often equated with a kind of uncertainty. In this case, the risk is determined as a combination of the probability of failure events occurrence and consequences of these events, and uncertainties, whether those events will occur and what will be the consequences. Traditionally, failure risk modelling in CWSS is applied to the calculus of probability. It requires a statistically representative data set of faults. Often, in practice, this condition can't be met. Very often the data are derived from the experts whose knowledge is incomplete or uncertain. In this case, the use of arbitrary probability and its distributions leads to unreliable results (Tchórzewska-Cieślak 2010).

Probability can also be reported as a fuzzy, especially when it is estimated. In contrast to the classical set the boundary of fuzzy set is not precisely defined. This smooth transition is determined by the so-called membership function μA, where A denotes the set of fuzzy numbers. Fuzzy sets can be used to describe different linguistic terms associated with risk analysis (small, medium, large, very large). A linguistic variable is a variable that characterizes fuzzy, imprecise terms, expressed in words, for example: about number 1, high risk, low risk value. Before starting the process of fuzzification, the domain of discourse should be strictly defined, the so called X universe, which is an ordinary not fuzzy set. A fuzzy set is determined if all the membership functions for each element of the universe are given. The membership function (matching degree, compliance) assigns to each element x of the domain of discourse (space) a value within the range [0, 1], μ_A: X μ[0, 1], which means that every element x of the space X belongs to a fuzzy set A with certain degree of membership.

A fuzzy set A is defined as: $A = \{\mu_A (x), x\}$. The values of the membership function μ_A are real numbers in the interval [0, 1] (Braglia et al. 2003, Dubois & Prade 1980, Kleiner et al. 2006, Lee 1996, Sadiq et al. 2007, Tchórzewska-Cieślak 2010, Tchórzewska-Cieślak 2011, Zadeh 1965).

A possibilistic approach based on fuzzy set theory can be found in the so-called theory of possibility. The foundation of the theory of possibility is possibility distribution, which can be used to describe the data belonging to a particular fuzzy set. The distribution of possibility is equal to a defined membership function of fuzzy set (Johanson 2008, Klir & Folger 1988, Kluska 2009).

A special case is the so-called theory of possibility the Dempster-Shafer Theory (DST) called a mathematical theory of records (Alim 1988, Kacprzyk & Fedrizzi 1994, Shafer 1976). The Dempster-Shafer theory gives the possibility to combine different hypotheses (provided by experts) to determine the baseline probability. Different hypotheses assigns probabilities using the so-called Basic Probability Assignment (BPA) or mass function (the mass m (X) of X) function of belief m (Kacprzyk & Fedrizzi 1994).

The lower and upper boundary of the function of belief degree (m) of the truth of a hypothesis H with regard to X (or its components) define the measure (Kacprzyk & Fedrizzi 1994, Shafer 1976, Yager 1987, Luo & Caselton 1997):

belief degree: bel (X),
plausibility: pl(X),

belief ≤ *plausibility*

The belief degree has the following properties: $m(X_i) \rightarrow [0,1]$;

$$m(\varnothing) = 0 \tag{3}$$

$$\sum_{X_i \subseteq X} m(X_i) = 1. \tag{4}$$

where:
$m(X_i)$—belief degree,
$i = 1, 2, 3, ..., n$,
n—number of hypotheses concerning the set X,
$n = 2^j$; j—the number of elements of the set X,

The value of the function $m(X)$ refers only to the set X, and does not give any information about the subsets of X, for which individual belief functions are defined:

$$bel(X) \le P(X) \le pl(X) \tag{5}$$

$$bel(X_i) = \sum_{X_k \subseteq X_i} m(X_k) \tag{6}$$

$$bel(\varnothing) = 0,\ bel(X) = 1 \tag{7}$$

$$pl(X_i) = \sum_{X_k \cap X_i \neq \phi} m(X_k) \tag{8}$$

$$pl(\varnothing) = 0,\ pl(X) = 1 \tag{9}$$

$$pl(X_i) = 1 - bel(X_i) \tag{10}$$

where:
$bel(X)$—measure of belief (faith),
$pl(X)$—measure presumption (plausibility).

Combining rules (Dempster-Shafer Rule of Combination—DSRC). The result is a new distribution: $m(X) = (m1 \oplus m2 \oplus \cdots \oplus mi)(X)$

For two experts is as follows:

$$m_{1-2}(\varnothing) = 0 \tag{11}$$

$$m_{1-2}(X_i) = \frac{\sum_{X_a \cap X_b = X_i} m_1(X_a) \cdot m_2(X_b)}{1 - \sum_{X_a \cap X_b = \varnothing} m_1(X_a) \cdot m_2(X_b)} \tag{12}$$

In case of information conflict, i.e. the product of belief functions is an empty set, the conflict indicator K_f, is defined:

$$K_f = \sum_{X_a \cap X_b = \varnothing} m_1(X_a) \cdot m_2(X_b) \tag{13}$$

K_f is often interpreted as a measure of conflict between the different sources. The larger K is the more the sources are conflicting and the less sense has their combination. The factor K indicates the amount of evidential conflict. If $K = 0$, it shows complete compatibility, and if $0 < K < 1$, it shows partial compatibility. Finally, the orthogonal sum does not exist when $K = 1$ (Zadeh 1984).

To exclude information conflict the normalizing factor K_N is introduced:

$$K_N = (1 - K_f) \tag{14}$$

3.2 *The application case*

The water supply network in southeastern Polish city was analysed. The risk of failure of one of the major water mains, for the designated number of residents exposed to the lack of water supply due to failure was analysed (area A in Fig. 2).

The vast majority of the WDS works in the general supply pumping system without the expansion tanks. Most of the city is covered by a peripheral network. Only a small part of the network works as a branched network. Most of the WDS is built of steel and PVC. More than 40% of water supply pipeline is more than 20 years old. The second stage pumping station operates at a constant pressure at discharge (40 kPa). At present, urban water supply system serves about 63 thousand residents.

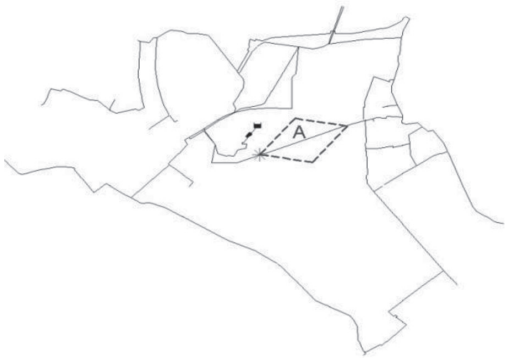


Figure 2. Diagram of the analyzed water supply system.

The state of metering of drinking water consumers is high, because it is 100% for the mass recipients and 98% for individual customers.

For risk the set of the possible risk levels were as follows: $R = \{rT, rK, rN\}$,

where:

– rT—tolerable risk,
– rK—controlled risk,
– rN—unacceptable risk.

The number of possible hypotheses Hn:

$n_j = 2^3 = 8, j = 1, 2, 3, 4, 5, 6, 7, 8.$

The characteristics of all possible hypotheses regarding the interpretation of risk values are presented in the form of a matrix. The matrix hypothesis is as follows:

$$M_{j,r} = \begin{vmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

The evaluation is made by two experts E1 and E2. Each expert assesses the risk analysis result in a fuzzy way. It was assumed that the adopted Fuzzy Risk Model (FRM) the membership functions take the form:

$$\mu_{(rT)} = \begin{cases} 1 \; dla \; x \le 6 \\ \dfrac{8-x}{2} \quad dla \; 6 < x < 8 \\ 0 \; dla \; x \ge 8 \end{cases} \tag{15}$$

$$\mu_{(rK)} = \begin{cases} 0 \; dla \; x \le 6 \\ \dfrac{x-6}{7{,}5} \quad dla \; 6 < x < 13{,}5 \\ \dfrac{18-x}{4{,}5} \quad dla \; 13{,}5 < x \le 18 \\ 0 \; dla \; x \ge 18 \end{cases} \tag{16}$$

$$\mu_{(rN)} = \begin{cases} 0 \; dla \; x \le 13{,}5 \\ \dfrac{x-13{,}5}{5} \quad dla \; 13{,}5 < x < 8 \\ 1 \; dla \; x \ge 18 \end{cases} \tag{17}$$

For determined risk value $r(x) = 7{,}2$

Risk assessment by experts is to estimate belonging to a specific set $r = \{rT, rK, rN\}$:

E1:

– the risk is certainly not unacceptable,
– the risk can be considered as tolerated to a higher degree (with weight) than the controlled,
– utilizing fuzzy membership functions the value of belief functions were estimated.

E2:

– the risk is certainly not unacceptable,
– the risk is tolerable with weight two times greater than the controlled risk,

$$M_{m(EiHj)} = \begin{vmatrix} 0 & 0{,}4 & 0{,}16 & 0 & 0{,}4 & 0{,}01 & 0{,}01 & 0{,}02 \\ 0 & 0{,}4 & 0{,}16 & 0 & 0 & 0{,}4 & 0{,}02 & 0{,}02 \end{vmatrix}$$

– utilizing fuzzy membership functions the value of belief functions were estimated.

The matrix of experts is as follows:

The next step is to make the process of combining the rules according to formulas (4) ÷ (11). For the opinion of two experts (E1, E2) the matrix is as follows:

$$M \prod_{i=1,j=1}^{i=2,j=8} m(EiHj)m(EiHj)$$

$$= \begin{vmatrix} 0{,}12 & \overline{0{,}048} & 0 & 0{,}12 & 0{,}003 & \overline{0{,}003} & 0{,}006 \\ \overline{0{,}104} & 0{,}0416 & 0 & 0{,}104 & \overline{0{,}0026} & 0{,}0026 & 0{,}0052 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}16 & \overline{0{,}064} & 0 & 0{,}16 & 0{,}004 & 0{,}004 & 0{,}008 \\ \overline{0{,}008} & 0{,}0032 & 0 & 0{,}008 & 0{,}0002 & 0{,}0002 & 0{,}0004 \\ 0{,}008 & 0{,}0032 & 0 & 0{,}008 & 0{,}0002 & 0{,}0002 & 0{,}0004 \end{vmatrix}$$

The overline values represent a conflict of information, i.e. it is not possible to assess the risk of

Table 1. The result values mE(1-2)(rn): belE(1-2)(rn), plE(1-2)(rn).

H_n	Description	$m_{E(1-2)}(r_n)$	$bel_{E(1-2)}(r_n)$	$pl_{E(1-2)}(r_n)$	AF
H_1	∅	0	0	0	0
H_2	rT	0,75	0,75	0,77	0,02
H_3	rK	0,23	0,23	0,232	0,02
H_4	rN	0,006	0,006	0,023	0,017
H_5	rT∨rK	0	1,0	1,0	0
H_6	rT∨rN	0,015	0,771	0,773	0,002
H_7	rK∨rN	0,001	0,237	0,253	0,016
H_8	rT∨rK∨rNA	0,001	1	1	0

failure in a defined scale. The degree of conflict was calculated using the formula (1):

The normalizing factor was determined by (13):

$$K_N = 0{,}7704.$$

Table 1 shows the main characteristics of the functions of belief m using the formulas (4) ÷ (11).

The highest values of the resulting belief function mE(1–2)(rn), the combination of two experts hypotheses indicates the level of failure risk analysis of water supply network. Measures of beliefs belE(1–2)(rn) and the presumption plE(1–2)(rn) characterized by the so-called interval of uncertainty as to the hypotheses interpretation. The uncertainty factor AF is the difference between belief and presumption in the case of hypothesis.

For the studied network (according to Fig. 2) the experts determined risk as tolerated with the uncertainty factor AF equal to 0.02, which proves the conformity of experts about hypotheses.

4 CONCLUSIONS AND DISCUSSION

If it is not possible to obtain accurate and complete statistical data which are required in the analysis and assessment of the risk of failure of the water supply network the necessary information can be obtained from experts. On the basis of their knowledge, experience and literature data they estimate the individual risk parameters.

Data obtained in this way are the basis of subjective evaluations, which are the basis for the fuzzy risk modelling. The theory of fuzzy sets allows to perform a risk analysis in natural language (e.g. low loss, risk tolerated) based on the experience of experts. It allows to model non-linearities, where the analytical, statistical or probabilistic description is difficult or impossible.

The model of fuzzy risk analysis can be combined with the Dempster-Shafer's model in the risk management process, particularly at the stage of obtaining, verification and grouping data and hypotheses posed by different experts. This allows the modelling of fuzzy evaluations of individual experts. The advantage of presented method is the ability to take into account the experts knowledge in case where there is no statistical database about adverse events in water supply system. Contrary to other experts methods which use Bayesian networks, Dempster-Shafer theory and fuzzy modeling does not require knowledge about probability distribution for every emergency events. The main limitation of presented method is uncertainty resulting from expert knowledge. Various experts opinions are eliminated through the use of normalization (so-called conflict information). There is why some informations might be not included in the final result. Application example demonstrates the usefulness of this method especially for events with incidental character (small statistical database) but which may have serious consequences. In the example a failure of one of the main pipeline in the city and its results in a lack of water supply was shown. That is why many times experts knowledge is the only method to determine the risk of failure on the main pipeline.

The proposed possibilistic model of failure risk analysis and assessment of water supply network is an alternative to the classical methods and models and should be used when possessed knowledge of risk factors is uncertain or incomplete.

REFERENCES

Alim, S., 1988. Application of Dempster-Shafer theory for interpretation of seismic parameters. *Asce, Journal of Structural Engineering,* 114(9): 2070–2084.

Apostolakis, G. & Kaplan, S., 1981. Pitfalls in risk calculations. *Reliability Engineering and System Safety*, 2: 135–145.

Aven, T., 2010. Conceptual framework for risk assessment and risk management. *Summer Safety & Reliability Seminars (Journal of Polish Safety and Reliability Association)*, 1: 15–27.

Boryczko, K., Piegdoń, I. & Eid, M., 2014. Water supply systems risk analysis model by means of RENO software. *Safety, Reliability and Risk Analysis: Beyond the Horizon*. Taylor & Francis Group, London, pp. 1987–1992.

Braglia, M., Frosolini, M. & Montanari, R., 2003. Fuzzy criticality assessment model for failure modes and effects analysis. *International Journal of Quality & Reliability Management*, 20(4): 503–524.

Christodoulous, S., Charalambous, C. & Adamou, A., 2008 Rehabilitation and maintenance of water distribution network assets. *Water Science and Technology, Water Supply*, IWA Publishing, 8(2): 231–237.

Christodoulous, S. & Deligianni, A., 2010. A neurofuzzy decision framework for the management of water distribution networks. *Water Resources Management*, 24: 1573–1650.

Christodoulous, S., Aslani, P. & Vanrenterghem, A. 2003. Risk analysis framework for evaluating structural degradation of water mains in urban settings using neuro fuzzy systems and statistical modelling techniques. World Water and Environmental Resources Congress, ASCE, Philadelphia, USA, 1–9.

Craun, G. & Calderon, R., 2001. Waterborne disease outbreaks caused by distribution system deficiencies. *Journal AWWA*, 9: 64–75.

Dempster A., 1967. Upper and lower probabilities induced by a multi-valued mapping. The Annals of Statistics, 28: 325–339.

Dubois, D. & Prade, H., 1980. Fuzzy sets and systems: Theory and application. *Academic Press*, New York.

Ezell, B., Farr, J. & Wiese, I., 2000. Infrastructure risk analysis of municipal water distribution system. *Journal of Infrastructure Systems*, ASCE, 6(3): 118–122.

Faber, M.H. & Steward, M.G., 2003. Risk assessment for civil engineering facilities: critical overview and discussion. Reliability Engineering and System Safety, 80:173–184.

Grey-Gardner, R., 2009. Implementing risk management for a water supplies: a catalyst and incentive for change. The Rangeland Journal, 30(1):149–156.

Hahn, M., Palmer, R. & Merr, M.S. 2002. Expert System for Prioritizing the Inspection of Sewers:Knowledge Base Formulation and Evaluation. Journal of Water Resources Planning and Management, 128: 121–129.

Haimes, Y.Y., 1998. Risk modelling, assessment and management. Wiley, New York.

Haimes, Y.Y., Moser, D. & Stakhin, E., 2006. Risk Based Decision Making in Water Resources. Journal of Infrastructure Systems, ASCE, 12: 401–415.

Haimes, Y.Y., 2009. On the complex definition of risk: a systems-based approach. *Risk Analysis*, 29(12): 1647–1654.

Hastak, H. & Baim, E., 2001. Risk factors affecting management and maintenance cost of urban infrastructure. *Journal of Infrastructure Systems*, ASCE, 7(2): 67–75.

Hokstad, P., Røstum, J., Sklet, S., Rosén, L., Pettersson, T.J.R., Linde, A., Sturm, S., Beuken, R., D. Kirchner, D. & Niewersch, C., 2009. Methods for risk analysis of drinking water systems from source to tap—Guidance report on Risk Analysis. TECHNEAU.

Hrudey, S.E., 2001. Drinking water quality—a risk management approach. Water, 26(1): 29–32.

Hrudey, S.E. & Hrudey, E.J., 2004. Safe drinking water. Lessons from recent outbreaks in affluent nations. IWA Publishing, New York.

Hubbard, D.W., 2009. The failure of risk management. Wiley, New York.

Johanson, B., 2008. Public Views on Drinking Water Standards as Risk Indicators. Risk Analysis, 28(6): 1515–1530.

Kacprzyk, J. & Fedrizzi, M., 1994. Advances in Dempster-Shafer theory of evidence. Wiley, New York, pp. 51–69.

Kaplan, S., 1997. The words of risk analysis. *Risk Analysis*, 7(4): 407–417.

Kleiner, Y., Rajani, B.B. & Sadiq, R., 2006. Failure risk management of buried infrastructure using fuzzy-based techniques. *Journal of Water Supply Research and Technology*, Aqua, 55(2): 81–94.

Kleiner, Y. & Rajani, B., 2000. Considering Time-dependent Factors in the Statistical Prediction of Water Main Breaks. AWWA Infrastructure Conference, Baltimore, MD, USA. 1–12.

Kleiner, Y., Sadiq, R. & Rajani, B., 2004. Modeling Failure Risk in Buried Pipes Using Fuzzy Markov Deterioration Process. Pipeline Engineering and Construction: What's on the Horizon?, ASCE, San Diego, CA, USA, 1–12.

Klir, G.J. & Folger T., 1988. Fuzzy sets, uncertainty, and information. Englewood Cliffs, Prentice-Hall, New York.

Kluska, J., 2009. Analytical Methods in Fuzzy Modelling and Control. Springer-Verlag, Berlin.

Kołowrocki, K., 2004. Reliability of Large Systems. Elsevier, New York.

Lee, H.M., 1996. Applying fuzzy set theory to evaluate the rate of aggregative risk in software development. *Fuzzy Sets and Systems*, 79: 323–336.

Luo, W.B. & Caselton B., 1997. Using Dempster-Shafer theory to represent climate change uncertainties. Journal of Environmental Management, 49(1): 73–93.

Markowski, A. & Mannan S., 2008. Fuzzy risk matrix. Journal of Hazardous Materials, 59(1): 152–156.

Maqsood, I., Jianbing, L., Guohe, H. & Uefei, H., 2005. Simulation-based risk assessment of contaminated sites under remediation scenarios, planning periods, and land-use patterns a Canadian case study. Stochastic Environ Research and Risk Asses, 19: 146–157.

Mays, L.W., 2005. The Role of Risk Analysis in Water Resources Engineering. Department of Civil and Environmental Engineering. Arizona State University, Arizona.

McGill, W.L., Ayyub, B.A. & Kaminskiy M., 2005. Risk Analysis for Critical Asset Protection. Risk Analysis, Wiley Blackwell, 27(5): 1265–1281.

Michaud, D. & Apostolakis, G.E., 2006. Methodology for ranking elements of water-supply networks. *Journal of Infrastructure Systems*, 12(4): 230–242.

Rak, J., 2003. A study of the qualitative methods for risk assessment in water supply systems. *Environment Protection Engineering*, Wydawn. Politechniki Wrocławskiej, z. 3–4: 123–134.

Rak, J. & Tchórzewska-Cieślak B., 2006. Five—parametric matrix to estimate risk connected with water supply system operating. *Environment Protection Engineering*, Wydawn. Politechniki Wrocławskiej, 2: 37–47.

Sadiq, R., Kleiner, Y. & Rajani, B., 2007. Water quality failures in distribution networks—risk analysis using fuzzy logic and evidential reasoning. *Risk Analysis*, 27(5): 1381–1394.

Sadiq, R., Tesfamariam, S., 2009. Environmental decision-making under uncertainty using Intuitionistic Fuzzy Analytic Hierarchy Process (IF-AHP). Stochastic Environmental Research and Risk Assessment, 23(1): 75–91.

Shafer G., 1976. A mathematical theory of evidence. Princeton University Press, USA, New York. ISBN 0-608-02508-9.

Shang-Lien, L. & Ruei-Shan, L., 2002. Diagnosing reservoir water quality using selforganizing maps and fuzzy theory. Water Reserch, 36: 265–2274.

Souza, R. & Chagas, P., 2001. Risk Analysis in Water Quality Problems. World Water andEnvironmental Resources Congress, ASCE, Orlando, FL, USA, 1–6.

Tchórzewska-Cieślak B., 2007. Method of assessing of risk of failure in water supply system. European safety and reliability conference (ESREL), *Risk, reliability and societal safety*, Taylor & Francis, (vol. 2): 1535–1539.

Tchórzewska-Cieślak, B., 2010. Model of risk of water mains failure using fuzzy logic. *Journal of Polish Safety and Reliability Association* (Summer Safety & Reliability Seminars), (vol. 1): 255–265.

Tchórzewska-Cieślak, B., 2011. Aplikacja matematycznej teorii ewidencji do analizy ryzyka awarii sieci wodociągowej. *Czasopismo techniczne—technical transaction,* Wydawnictwo Politechniki Krakowskiej, 1: 201–210.

Yager, R.R., 1987. On the Dempster-Shafer framework and new combination rules. *Information Sciences*, 41: 93–137.

Zadeh, L.A., 1965. Fuzzy sets. *Information and Control*, 8: 338–353.

Zadeh, L.A., 1984. Review of books: A mathematical theory of evidence. *The AI Magazine*, 5(3): 81–83.

Zio, E., 2009. Computational Methods for Reliability and Risk Analysis. Springer, Berlin.

Zio, E., 2007. An introduction to the basics of reliability and risk analysis. World Scientific Publishing, Singapure.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Multidimensional risk to networks of distributed systems

T.V. Garcez & A.T. de Almeida
Federal University of Pernambuco, Recife, Brazil

ABSTRACT: Managing risk in networks of distributed systems requires the analysis of large numbers of alternatives, hazard scenarios, consequences and uncertainties regarding the occurrence of an accident, mainly due to the wide diversity of characteristics in the areas surrounding the system. Therefore, the decision making process needs to be analyzed in a more complex way. If decisions are to be taken more rationally, the uncertainties inherent in the context of risk itself must be addressed as must how best to aggregate the decision maker's preferences, related to the possible consequences resulting from hazards. Decision theory jointly with a multidimensional view of risk (using Multi-Criteria Decision Making methodologies—MCDM) enables these issues to be dealt with. Hence, this paper puts forward the use of an additional assessment of risk in underground electrical distribution networks with a multidimensional view of risk that may be used as a decision aid tool in risk management.

1 INTRODUCTION

The system of underground cabling in the urban environment is an important part of the infrastructure of electricity which is the lifeblood of urban growth and therefore governments attach great importance to it. Societies are highly reliant on power systems for their energy needs (Castillo, 2014).

The infrastructure of such systems is critical because it is an asset that is essential so that society and the economy can function well. It shares a mutual dependence on numerous other critical infrastructures, including but not limited to the infrastructure that supports the supply of gas, water, and telecommunications, the financial services industry, public safety services, public health, agriculture, and transportation systems.

Any disruptions to these systems, from accidents, result in direct and indirect losses. The effects of power outages can include economic, social, physical and psychological impacts; such consequences on providers and customers include premature death, injury, and indirect and direct economic losses (Castillo, 2014).

In the case specific case of blackouts, widespread economic and non-economic losses on a large scale are not well-understood. This is compounded by the fact that private and public companies do not account for the hidden costs incurred as a result of the loss of reliability in their systems that might generate both other non-economic losses, such as premature human death and human injury, and indirect economic and social impacts (Castillo, 2014). Also, there is a concern about the possibility of terrorist attacks seeking to exploit the vulnerability of power components and the overall system and thereby seriously damaging them.

An aggravating factor in the analysis of the consequences and probabilities of failure is due to the great diversity of other forms of urban infrastructure that interact and interconnect with or are in the vicinity of the underground power grid. Interference from these may cause undesirable events such as accidents and disruptions. There are several factors that interfere with the safety and reliability of these systems amongst which are environmental conditions, technical matters, human errors, third-parties' actions, sabotage, terrorism, etc.

One of the main causes of incidents in underground networks is interference from a third party, which people may provoke by their direct or indirect actions. Examples of direct interference are excavation, cable ducts being crushed on building sites and during and road construction. The probabilities of these incidents occurring are aggravated by the lack of accurate mapping of power underground urban systems.

In technical conditions, errors that stand out include mistakes in design and specifying standards and in selecting inappropriate materials and forms of ventilation. Furthermore, there can be serious operational and maintenance errors that can cause major failures and consequently undesired events.

Among more important environmental conditions there may be the presence of groundwater, excessive humidity, damage caused by rain, sewage, seawater, salts (to thaw snow), excessively warm environments, and so forth. Such factors may lead to the accelerated corrosion of wires and

insulating materials, and therefore cause serious system failures. Furthermore, there are major natural adverse phenomena such as lightning, floods and earthquakes which can lead to serious levels of system failure.

These undesirable events can have various consequences, such as, fatalities and injuries to people, fires in nearby locations, disruptions in local vehicle traffic, loss of company image, financial loss, the local population being afraid (on account of the uncertainty of when and where an underground vault will explode), loss of reliability and safety and other consequences which cannot be measured financially (Garcez & Almeida, 2014; Garcez & Almeida, 2013).

What make risk management even more complex and uncertain are the facts of there being: a large number (hundreds or thousands) of underground vaults of different characteristics within a distributed system; the lack of historical data on failure modes; the rarity of the occurrence of some faults; the magnitude of their consequences and the involvement of a complex environment surrounding the hazard zone besides the need to evaluate different hazard scenarios (which represent different causes of accidents—i.e. failure modes) (Garcez & Almeida, 2014).

Moreover, if one consider the effects of the network, such analysis can become even more complex, and the use of appropriate computational tools and methodologies is necessary. There are instances of dependencies in the electricity network. These include: one node (subsystem) becomes overloaded due to the malfunction of adjacent nodes, and temporary blackouts which take place due to a malfunction in the path in the grid between the power plant and the subsystem (underground vault) (Garcez & Szufel, 2014).

According to Garcez & Almeida (2014), under a management approach to keep the system adequately safe, the Decision Maker (DM) needs to answer some questions: What underground vault is considered to have the highest risk? What is the intensity level of consequences that really is important to the DM? What underground vaults or set of vaults should be considered when allocating hazard prevention resources or scheduling mitigation actions?

Given that the power distribution system in operation meets all the minimum safety requirements required by regulatory and inspection safety agencies, in various situations DMs are faced with problems that are about needing to allocate or assign additional (financial, safety, time, staff, technology, etc.) resources of electric power companies to a given set of alternatives, when these resources are scarce and limited and may not have been distributed equitably. Hence, the DM faces a problem of choosing or prioritizing alternatives to determine which alternative will be chosen (prioritized) from the perspectives of the company's needs (Garcez & Almeida, 2014).

Therefore, a multidimensional approach to risk analysis is required to evaluate the consequences in different aspects. Another important point, which is rarely exploited in traditional models, is related to incorporating the preferences and values of the DM who manages the system. Therefore, aggregating the DM's preferences in modeling, by Multiple-Criteria Decision-Making (MCDM) methods is very important and the results are more complete, comprehensive and in particular consider the DM's desires (Garcez & Almeida, 2013).

Some applications of multidimensional risk and incorporating a DM's preferences can be verified in several papers on creating models for analyzing risk in gas transport and distribution in pipelines (natural gas and hydrogen) such as in studies by Brito & Almeida (2009); Alencar & Almeida (2010); Brito et al. (2010), and Lins & Almeida (2012).

This paper puts forward a multidimensional (multiattribute) assessment of the risk from vaults in underground electricity distribution systems, by generating a decision tool, which ranks risk values in a risk hierarchy.

2 HOW THE MODEL DIFFERS FROM TRADITIONAL RISK ANALYSIS

In traditional risk analysis, the risk is normally assessed under the dimension of human or financial loss. As to human loss of life, certainly the number of people close to an underground vault is directly linked to the possible human loss of life, but there may also be vaults in which there is a high probability of a hazard scenario occurring, but near which the presence of people (pedestrians) is low, and yet, they too must be considered. Which situation should be regarded as more dangerous and therefore treated as a priority? Are there vaults which have a lower probability of a hazard scenario occurring and yet, should an accident occur, a greater number of people than expected may be exposed to the consequences, or should any consideration be given to the possibility of some vaults having a high probability of a hazard scenario occurring and yet, a smaller than expected number of people being exposed to it? (Garcez & Almeida, 2014).

Thus, it is important to consider the DM's preference structure in order to make more rational decisions on allocating additional resources, on a priority basis, to underground vaults. By contrast, the approaches of traditional risk analysis do not

consider this issue. In other words, prioritization, under the approach we suggest, will depend on the DM's preference structure since this is considered to generate a better result in the expected value and to decrease the amount of risk when prevention or mitigation measures are implemented (Garcez & Almeida, 2014; 2013).

As Garcez & Almeida (2014) state, this proposed methodology does not obviate the need for a structured approach to traditional risk analysis to be carried out, whether this be done in a qualitative or quantitative way. In this context there are several approaches of qualitative and quantitative risk analysis widely that can be chosen which are accepted by academic and technical circles.

Hence, the methodology of risk analysis that we propose is complementary to other traditional forms of risk analysis, and thereby offers one more tool that will help the DM to determine which underground vaults should be prioritized.

3 MULTIDIMENSIONAL RISK MODEL

The decision making process is understood as an effort to try to solve problems of conflicting goals that require a "best compromise" between goals list for the best solution, see Keeney & Raiffa (1976). They further note that decision making is of several types e.g., it may be simple or complex, which may have specific or strategic consequences, local or comprehensive impacts, and immediate, short, middle or long term consequences, or any combination of these.

In order to allocate additional investments to manage risk effectively, consideration needs to be given to different issues, such as safety; the financial, operational and external characteristics of the system; the requirements of regulatory agencies; the stance of competitors; and the demands from society (Garcez & Almeida, 2013).

Therefore, it is necessary to ensure that the decisions taken are consistent with the goals of the company in different criteria, and that the DM's preferences are incorporated into it. Multi-Criteria Decision Analysis (MCDA) methodologies are well suited for such situations (Keeney & Raiffa, 1976).

Nowadays, the need to incorporate considerations related to financial, environmental and social matters into planning is associated with studies about sources of energy which makes experts use the multicriteria approach more frequently (Afgan et al., 2008).

Bishop et al. (2009) state that decisions are usually complex. Many criteria need to be satisfied. The consequences of the options to be evaluated present various spatial and temporal distributions, affecting different population and generation groups. Decisions are also made in a social context where perceptions can be as significant as facts. In this complex environment, a survey of the decision making area shows two aspects: commitment and serving the decision-making process.

MCDA is a set of models for operational research that deals with decision problems in the presence of (usually conflicting) multiple objectives, the main purpose of which is to make the problem clearer for the DM (Belton & Stewart, 2002; Vincke, 1992).

Among various issues, the problem of ranking emerges from the need for the DM to build a list of the most important alternatives in order of relevance (prioritization) which, in this particular case, is a risk hierarchy, such that the alternatives (the underground vaults of the system) most likely to be the source of a manhole accident are dealt with first of all by using the available additional resources and only thereafter other sections of the system by order of their ranking if resources are still available. Multiattribute Utility Theory (MAUT) achieves this ranking (Garcez & Almeida, 2013).

MAUT is used to aggregate preferences and consequence values amongst multiple dimensions taking into account the DM's preferences and his/her behavior considering cases with uncertainty in a clear measure of risk.

Specialists in this area consider methods belong to one of three large families: American school methods, outranking methods and interactive methods. Vincke (1992) affirms that MAUT, which started in North America, consists of combining different points of view in the same function that needs to be optimized. Studies linked to this family verify the mathematical conditions of aggregation, the shape of the particular aggregation function, and construction methods. The second family, inspired by the French school, first seeks aid by constructing a known relationship called outranking, which represents DMs' strong preferences. The third family is the newest, and presents methods which alternate calculations (thus producing successive commitment solutions) and dialogues (the source of extra information on decision preferences) (Alencar et al., 2009).

MAUT allows DMs to structure complex problems in a simple hierarchy, and to evaluate, in a subjective way, a large number of quantitative and qualitative factors where there are uncertainties. Utility is a measure of desirability or satisfaction, which makes it easier to use a uniform scale in order to combine and/or compare quantitative and/or qualitative factors. The utility function is an artifice that quantifies DMs' preferences through variations displayed in an index of the extent to which criteria have been satisfied (Belton & Stewart, 2002).

Even though these models are very useful, especially to improve the efficiency of the process of risk control by assigning the most appropriate risk-mitigating activities to be applied to underground vaults, the use of the model by Garcez & Almeida (2013, 2014) can improve the process of assigning such actions by providing a ranking of underground vaults that will be taken into account when defining the process of sorting priorities in order to mitigate risks to a system.

To define a hierarchy, under a risk context, a model of the consequences is needed. According to Aven (2012), the most appropriate definition of risk involves defining the consequences and uncertainties. The uncertainties come from different sources in the model. In this context, under Decision Theory, the uncertainties considered are those (Garcez & Almeida, 2014): (*i*) arising from the occurrence of a hazard scenario (because it is not known what hazard scenario actually will occur), (*ii*) arising from the consequence of a hazard scenario that has occurred (because there are probabilistic mechanisms that interfere in the magnitude of the consequences).

The first uncertainty can be dealt with by using a probability distribution that represents the expert's *a priori* knowledge and/or data gathered from accidents that have occurred. The second uncertainty is modeled by a probability distribution that defines the range of possible consequences that may result from an accident.

By Decision Theory, the loss (consequence) function can be defined as the negative of the utility function of the expected consequence ($L(c) = -u(c)$) (Berger, 1985). These consequences are the outcomes of the impact of an accident in a given dimension, and can be represented by a probability distribution function ($P(c|q, \theta)$), given knowledge of the hazard scenario (θ) (the final outcome of an accident), and the underground vault analyzed (q).

There are several causes of manhole events. The most important include: the aging process, use of inadequate facilities, inappropriate maintenance actions, thermo-mechanical stress of the cable and connections, thermal decomposition of the insulation, overloading the power grid, shared use of the underground space with other public and private utilities, the flooding of underground vaults, or drains and manhole covers being clogged or blocked (for further details see Garcez & Almeida (2014); Garcez & Almeida (2013); Koch and Carpentier (1992); Snodgrass & Black, (2005), and Walsh & Black (2002, 2005)).

These failures can cause internal and external explosions, fire, smoke, displacement of the manhole cover, intense light and noise, flash fires and shock and heat waves (Garcez & Almeida, 2013; 2014).

3.1 *Consequences*

Multidimensional risk has some advantages such as its providing a broader analysis, which makes it more realistic and complete, and it also deals with conflicting objectives, the different parties involved, and uncertainties. Some dimensions addressed are human safety, finance, the environment, property, the impact of stakeholders and the impact on a distribution company's external public image.

This study evaluates the consequences (c) from four dimensions: human impacts, financial impacts, operational impacts and disruptions to vehicular traffic. The human dimension (c_h) deals with the possibility of injuries caused by projection of manhole covers and where they crash land, and burns of at least the second degree due to exposure to incident energy from an arc flash. The financial dimension (c_f) is about any kind of monetary compensation related to an accident occurring. The operational dimension (c_o) corresponds to the impact on the supply operation of the electricity distribution company (downtime). Finally, the dimension of disruption to traffic (c_t) is evaluated by the process of how traffic jams form on the streets around the accident area. The consequence models are described in details in Garcez & Almeida (2013, 2014).

3.2 *Multidimensional decision model*

Multi-attribute utility theory, which lies within the concepts of MCDA, enables the values of the DM's preferences to be aggregated (through the utility function) from multiple attributes, together with the uncertainty inherent in their consequences $P(c|\theta, q)$ and hazard scenarios $\pi(\theta)$, in a unique synthesis criterion function.

As the loss function is defined as the negative of the utility function of the expected consequence, so the utility function is calculated by:

$$u(\theta,q) = \int_c u(c)P(c \mid \theta,q)dc \tag{1}$$

thus,

$$L(\theta,q) = -\int_c u(c)P(c \mid \theta,q)dc \tag{2}$$

The measurement of risk $r(q)$ in an underground vault is the expected value of loss function $L(\theta, q)$. This can be represented by:

$$\begin{aligned} r(q) &= \sum\nolimits_\theta \pi(\theta)L(\theta,q) \\ &= -\sum\nolimits_\theta \pi(\theta)\int_c u(c)P(c \mid \theta,q)dc + (-1)\pi(\theta_N) \end{aligned} \tag{3}$$

where $\pi(\theta)$ is the probability distribution over the states of nature (hazard scenarios); and, the state

of nature θ_N represents the scenario of the normality, in which there is no occurrence of an accident scenario and, consequently, no negative consequences in the system i.e., $\int_c u(c)P(c \mid \theta,q)dc = -1$ (the system is operating normally). The range of risk values is [–1, 0], where the value –1 is related to the "lowest risk" and the value 0 to the "highest risk".

With respect to the DM's preferences, he/ she may have different basic attitudes (behavior), such as: risk aversion, risk neutral or risk prone. If the DM is risk averse, then the expected utility value is greater than the value of the certainty equivalent ($u[E(\tilde{x})] > E[u(\tilde{x})]$). If the DM is risk-neutral, the expected utility value is equal to the certainty equivalent ($u[E(\tilde{x})] = E[u(\tilde{x})]$). Should the DM be risk prone, the expected utility value is less than the certainty equivalent ($u[E(\tilde{x})] < E[u(\tilde{x})]$).

By using MAUT concepts in the risk measure and by taking the probability independence of the consequences into account, the risk measure is expressed by (Garcez & Almeida, 2013):

$$r(q) = \sum_i \sum_\theta \pi(\theta)\left(-\int_c u(c)P(c \mid \theta,q)dc\right) + (-1)\pi(\theta_N) \quad (4)$$

where i represents the several dimensions of the analysis, i.e., the dimensions of the consequence (C_h, C_f, C_o, C_t), when a determined hazard scenario (θ) occurs. These risk measures form a top-down hierarchy of the risk from the underground vaults evaluated. Consequently, they serve as a support tool for decision making and risk management.

4 APPLICATION

This paper uses a numerical application based on the study by Garcez & Almeida (2013), in which a multicriteria decision model was presented, with a view to assessing and ranking the risks from underground vaults. That was a hypothetical study, albeit of a realistic situation, that was based on an underground system of an electricity distribution company.

The company's senior manager for safety and operations was considered the DM. Seven underground vaults were analyzed (q_1, q_2, …, q_7), which represent a wide range of possible scenarios typically found in electricity distribution companies. The main features of these vaults are summarized in Table 1 (for more details see Garcez & Almeida (2013).

Four main dimensions of consequence were considered: those of human impacts, financial impacts, operational impacts and traffic disruptions. Conservatively, only one hazard scenario was considered: an internal explosion caused by an arc flash, which is considered the greatest impact, and causes the manhole cover to be blown off and projected.

To estimate the projection (distance) of the manhole cover, the elicitation method, called Equiprobable Intervals, was used. Estimating the risk measures is made from the perspective of Decision Theory. At the same time, a multiattribute utility function $U(c_h, c_f, c_o, c_t)$ is elicited from the DM. As it is supposed that the DM's preference structure is additive independent between the criteria, the utility functions from the perspective of a one-dimensional utility ($U(C_h)$, $U(C_f)$, $U(C_o)$, $U(C_t)$) can be elicited separately. To do so, the procedures described in Keeney and Raiffa (1976) were followed. It was considered that the DM is risk averse in the human dimension and risk prone in the remaining dimensions. The values of the scale constants obtained were: $k_{c_h} = 0.3386$; $k_{c_t} = 0.1247$; $k_{c_o} = 0.0944$; and, $k_{c_f} = 0.4423$.

The multiattribute utility functions, by Eq. (4) are combined with the probability density function. Hence, the multidimensional risk measure is calculated. Results of the ranking of the multidimensional risk assessment are shown in Table 2.

Notice that the values of risks ($r(q)$) are close to –1. This is due to the greatest contribution being from the scenario of normal operation (θ_N), since the occurrence of manhole events is rare, the prob-

Table 1. Characteristics of the undergrounds vaults analyzed (Garcez & Almeida, 2013).

q	Description of the external vicinity	Location of the manhole cover	Dist. from the manhole cover center on sidewalk to street (m)	Dist. from the manhole cover center on street to sidewalk (m)	Diameter of the manhole cover (m)
q_1	Commercial area 2	Street	–	4.25	1.5
q_2	Commercial area 3	Sidewalk	2.25	–	1.5
q_3	Residential area 1	Sidewalk	2.50	–	1.0
q_4	Residential area 2	Street	–	3.5	1.0
q_5	Residential area 3	Sidewalk	3.25	–	1.5
q_6	Commercial area 4	Street	–	8.5	1.0
q_7	Commercial area 5	Street	–	8.5	1.0

Table 2. Results of ranking the risk.

Rank	q	Risk value $r(q)$	Risk difference $r_i(q) - r_{i+1}(q)$	Risk range $(r_i(q) - r_{i+1}(q)/ r_{first}(q) - r_{last}(q))$
1st	q_2	–0.99493	–8.86682E-05	3.268%
2nd	q_5	–0.99484	–2.9489E-05	1.087%
3rd	q_3	–0.99481	–0.000555485	20.474%
4th	q_4	–0.99426	–0.001284774	47.353%
5th	q_7	–0.99297	–0.000614308	22.642%
6th	q_1	–0.99236	–0.000140443	
7th	q_6	–0.99222		

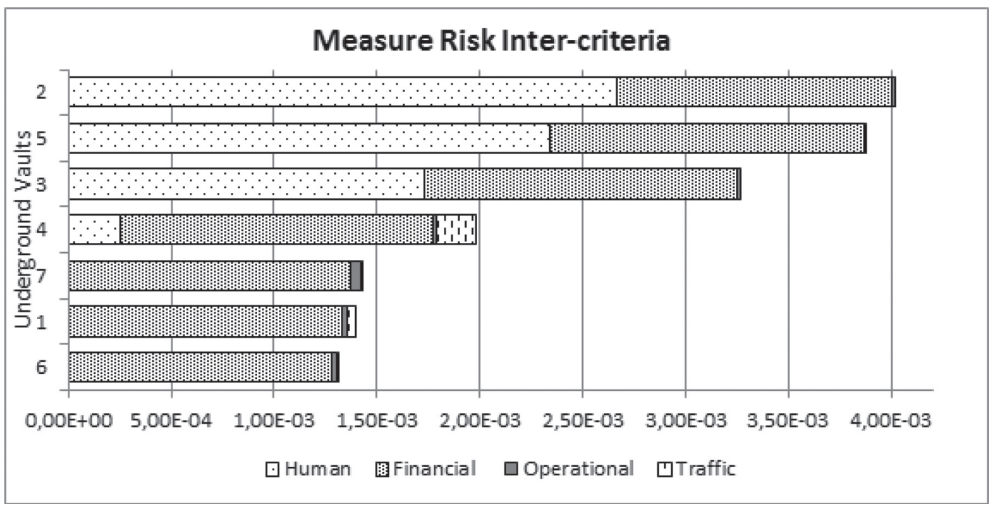


Figure 1. Analysis of the measures of inter-criteria risk.

ability of the scenario of normal operation $\pi(\theta_N)$ is close to 1, and its loss function is –1. The conclusion should be drawn that underground vault q_2 is at the top of the ranking; consequently, it should receive the greatest attention when additional resources are available for allocation to safety measures and system improvements.

By analyzing the differences between the risks and total risk range, the conclusion may be drawn that the difference between the risk values of vaults q_3 and q_4 corresponds to about 47% of the total range of risk $(r(q_3) - r(q_4)/ r(q_2) - r(q_6) \approx 47\%)$, which indicates a large increase in the risk between these vaults.

On analyzing the risk values under an inter-criteria approach graphically (Fig. 1), we conclude that: the first alternatives of the risk ranking show the human impact is major, while in the last-placed alternatives the human impact is nonexistent. The only major value of the impact of these last-placed alternatives is on the operational dimension.

Another source of strategic information comes from comparing the inter-criteria of the increments in risk (Garcez & Almeida, 2012). This analysis enables the criterion (dimension) that contributes the greatest difference in risk between alternatives to be identified. For example, on comparing the alternatives pair-to-pair under the inter-criterion approach, and on evaluating the alternatives q_2 and q_5 (see Fig. 2), these alternatives can be differentiated; there are major influences between the consequences of the financial and operational impacts and human loss (in descending order). Therefore, one can conclude that some preventive and mitigating actions that act on loss, for example, in disturbances to traffic, do not generate any change in the values of the difference in risk between these two alternatives. However, focusing on preventive and mitigating actions in the operational dimension of alternative q_2, would result in reducing the amount of risk compared to alternative q_5. Thus,

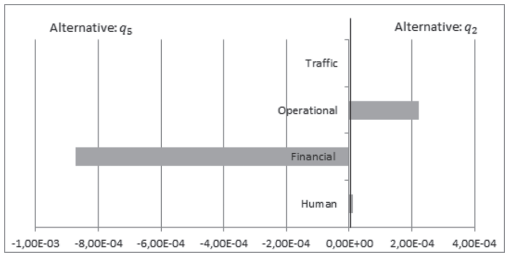


Figure 2. Analysis of the intra-criteria of the risk differences of alternatives q_2 and q_5.

resources can be redirected to manage risk more effectively.

5 CONCLUSIONS

Despite the underground system of electricity supply being safer than the overhead type, several accidents have occurred in these systems, and these have generated repercussions and consequences, not only for power distribution companies, but also for third-parties and society at large.

Thus, this study conducted a study of multidimensional risks in underground vaults in a power distribution system, taking into account several aspects of consequences, such as, the impacts on humans, financial impacts, operational impacts and impacts on the flow of local vehicular traffic.

The model supports a DM to prioritize alternatives in order to manage resources for risk management, plan maintenance for or to improve (upgrade) the system, first by allocating more resources to those that are the most critical among a large universe of alternatives. Furthermore, by analyzing the differences of risk inter-criteria, a better indication can be made of to what dimensions of the impact (loss) must preventive and mitigating actions be applied so as to guide how risk management can be undertaken more efficiently.

ACKNOWLEDGEMENTS

This paper is part of a research study funded by the Brazilian National Research Council (CNPq).

REFERENCES

Afgan, N.H., Carvalho, M.G., Pilavachi, P.A., & Martins, N. (2008). Evaluation of natural gas supply options for Southeast and Central Europe: Part 2. Multi-criteria assessment. Energy Conversion and Management, 49(8), 2345–2353. doi:10.1016/j.enconman. 2008.01.024.

Alencar, M.H., Almeida, A.T. de, Almeida-Filho, A.T. de, & Garcez, T.V. 2009. Multicriteria risk analysis application in a distribution gas pipeline system in Sergipe. In Reliability, Risk, and Safety, Three Volume Set. CRC Press. doi:10.1201/9780203859759.ch143.

Alencar, M.H., & de Almeida, A.T. 2010. Assigning priorities to actions in a pipeline transporting hydrogen based on a multicriteria decision model. International Journal of Hydrogen Energy, 35(8), 3610–3619. doi:10.1016/j.ijhydene.2010.01.122.

Aven, T. 2012. The risk concept—historical and recent development trends. Reliability Engineering & System Safety, 99(0951), 33–44. doi:10.1016/j.ress. 2011.11.006.

Belton, V., & Stewart, V.B.T.J. 2002. Multiple Criteria Decision Analysis: An Integrated Approach. Springer-Verlag GmbH.

Berger, J. 1985. Statistical Decision Theory and Bayesian Analysis (Springer Series in Statistics) (2nd ed.). Springer.

Bishop, I.D., Stock, C., & Williams, K.J. 2009. Using virtual environments and agent models in multi-criteria decision-making. Land Use Policy, 26(1), 87–94. doi:http://dx.doi.org/10.1016/j.landusepol. 2008.01.010.

Brito, A.J., & de Almeida, A.T. 2009. Multi-attribute risk assessment for risk ranking of natural gas pipelines. Reliability Engineering & System Safety, 94(2), 187–198. doi:10.1016/j.ress.2008.02.014.

Brito, A.J., de Almeida, A.T., & Mota, C.M.M. 2010. A multicriteria model for risk sorting of natural gas pipelines based on ELECTRE TRI integrating Utility Theory. European Journal of Operational Research, 200(3), 812–821. doi:10.1016/j.ejor.2009.01.016.

Castillo, A. 2014. Risk analysis and management in power outage and restoration: A literature survey. Electric Power Systems Research, 107, 9–15. doi:10.1016/j.epsr.2013.09.002.

Garcez, T.V., & de Almeida, A.T. 2014. A risk measurement tool for an underground electricity distribution system considering the consequences and uncertainties of manhole events. Reliability Engineering & System Safety, 124(0), 68–80. doi:10.1016/j.ress.2013.11.007.

Garcez, T.V., & Almeida, A.T. de. 2012. Multiple Dimension Manhole Explosion in an Underground Electrical Distribution System. In 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (Vol. 6, pp. 4893–4899). Helsinki, Finland: Curran Associates, Inc. (Dec 2012).

Garcez, T.V., & Almeida, A.T. de. 2013. Multidimensional Risk Assessment of Manhole Events as a Decision Tool for Ranking the Vaults of an Underground Electricity Distribution System. IEEE Transactions on Power Delivery, 1-1. doi:10.1109/TPWRD.2013.2273083.

Garcez, T.V., & Szufel, P. 2014. Multidimensional risk management for underground electricity networks. Studies in Logic Grammar and Rhetoric, 37(50), pp.

Keeney, R.L. & Raiffa, H. 1976. Decisions with multiple objectives: Preferences and Value Trade-Offs (p. 592). New York: John Wiley and Son. doi:doi.wiley.com/10.1002/bs.3830390206.

Koch, B., & Carpentier, Y. 1992. Manhole explosions due to arcing faults on underground secondary distribution cables in ducts. Power Delivery, IEEE Transactions on, 7(3), 1425–1433. doi:10.1109/61.141861.

Lins, P.H.C., & de Almeida, A.T. 2012. Multidimensional risk analysis of hydrogen pipelines. International Journal of Hydrogen Energy, 37(18), 13545–13554. doi:10.1016/j.ijhydene.2012.06.078.

Snodgrass, R.E., & Black, W.Z. 2005. Mitigating the Effects of Explosions in Underground Electrical Vaults. IEEE Transactions on Power Delivery, 20(2), 1767–1774. doi:10.1109/TPWRD.2004.834670.

Vincke, P. 1992. Multicriteria decision-aid. Bruxelles: John Wiley and Sons.

Walsh, B.P., & Black, W.Z. 2002. Thermodynamic and mechanical analysis of gas explosions in underground vaults. IEEE Transactions on Power Delivery, 17(1), 8–12. doi:10.1109/61.974181

Walsh, B.P., & Black, W.Z. 2005. Thermodynamic and Mechanical Analysis of Short Circuit Events in an Underground Vault. IEEE Transactions on Power Delivery, 20(3), 2235–2240. doi:10.1109/TPWRD.2005.848445.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Mathematics of PRA applied to Distributed Generation curtailment in saturated grids

P.E. Labeau, F. Faghihi & J.C. Maun
Université libre de Bruxelles, Brussels, Belgium

V. De Wilde & A. Vergnol
Elia System Operator, Brussels, Belgium

ABSTRACT: The share of distributed generation is steadily increasing in the field of electrical energy production. However, consequently to this shift, in rural areas mainly, grid operators are expecting more frequent line congestions and voltage problems. Active management of the distributed generation units is one of the possible solutions to keep the grid secure, while accepting more connections of this type of units to the existing grid infrastructure: (almost) real-time curtailment is applied to some generators in order to suppress congestion(s) on the grid. However, in the planning phase of the grid, the impact of active management, in terms of e.g. expected curtailed power per year, should be assessed before any possible new connection is allowed. This paper proposes a probabilistic risk assessment to estimate related risk indices, provides the mathematical formulation of the corresponding methodology and gives preliminary results on a simple test-case.

1 INTRODUCTION

The use of renewable energy for power generation has been steadily increasing these last years, as one of the candidate answers to the global warming issue. In addition, other types of Distributed Generation (DG), like e.g. CHP (Combined Heat and Power) units, are taking a significant share in the liberalized electricity market.

At the same time, the distribution grid infrastructure is still designed based on centralized production, i.e. for 'one-way flows' of electricity from large generation units and the transmission grid to local loads. Yet the increasing connection of DG units, mainly to the distribution grid, leads to 'two-way flows'. As a consequence, grid operators (both Transmission System Operators (TSOs) and Distribution System Operators (DSOs)) are expecting more frequent line congestions and voltage problems in many rural areas. To solve this problem, the network should be reinforced; nevertheless it is an expensive and time-consuming task, which cannot be seen as a short-term solution. Alternatively, Active Network Management (ANM) is introduced. An ANM scheme controls the injection of energy produced by DG units to the grid in (almost) real-time in case of congestion(s) on the grid (Davidson et al. 2010, Sansawatt et al. 2012). By this approach, the grid is retained secure.

The objective of an ANM scheme consists in connecting to the existing network infrastructure more DG units than what would be feasible based on their installed power and the strict application of the N-1 criterion. This allows also accepting to connect these DG units before envisioning any grid reinforcement, which is a costly process that spreads over several years. In this way, more energy is likely to be exported from these DG units to the transmission grid. However, the impact of ANM must be assessed before any possible new connection to the grid is allowed. Indeed, a possible investor in a new generation facility requests to obtain guarantees on the possible curtailment his/her unit could undergo. And the performance of the ANM scheme could determine contractual features with the system operator. Moreover, installing a new DG unit can affect the energy curtailment of the already connected DG units. In addition to this, the risk of congestion on the elements of the grid should also be analyzed.

Proper risk indices have therefore to be defined in order to characterize the ANM scheme performance. They also have to be estimated in a limited amount of time, as any request for a new DG unit connection must be answered in a limited amount of time. Deterministic methods (based on the N-1 criterion) used for network calculations in system planning are however not suitable to assess these indices, as DG units display an intermittent

production, contrarily to conventional generation facilities. This intermittency, combined with the variability of consumptions, corresponds to the sources of uncertainty affecting the system in this emerging context.

Analyzing a system whose inputs are stochastic variables, in the search for possible congestions and subsequent curtailment to eliminate them, calls for a probabilistic treatment. However, due to the large number of input variables (generations and loads) to be considered, and to the non-linearity of the electrical system, properly covering the state space of these stochastic variables turns out to be intractable. Moreover, for each variant, i.e. each possible combination of generations and loads, the N situation but also all N-1 situations should be analyzed, in the 3 seasonal regimes (winter, summer and inter-season) corresponding to different line ratings. Therefore, the number of network states to be treated dramatically increases.

In the literature, mainly two types of methods are proposed to deal with this problem, i.e. Monte Carlo Sampling (MCS) and the Multi-State Approach (MSA).

MCS consists in sampling variants from the joint probability density function (pdf) of the uncertain parameters (generations and loads, including correlations). Each sample serves as input data for an Optimal Power Flow (OPF) module to calculate the possible re-dispatching or curtailment of DG units. Based on the results of a large number of runs, MCS can provide an estimation of various quantities of interest, like e.g. the distribution of power flow on each grid element, the distribution of curtailed power for each DG unit, the annual energy produced by each DG unit (from which its utilization factor is straightforwardly derived) … However, it should be noted that the uncertainties of the high-dimensional variants are therefore propagated in a highly non-linear, multi-output model, in order to estimate non-point-wise indicators associated to rare events. Well-known acceleration techniques, like schemes based on a.o. importance sampling (e.g. Lux & Koblinger. 1991), splitting (e.g. L'Écuyer et al. 2009) or surrogate models (e.g. Li & Xiu. 2010), turn out to be irrelevant. A systematic coverage of the variant space is requested, and the resulting sample size is extremely large, even with a moderate accuracy in the estimation of the indicators.

In order to manage the number of variants to be analyzed, the MSA (Siano et al. 2010) rests on a discretization of the stochastic variables in significantly different combinations of discretized loads-generations, with respect to their likelihood to cause congestions. In order to keep the number of variants under control, some simplifications are made. For instance, correlation coefficients between all wind generations are taken equal to 1. The same assumption is made for the loads. These assumptions are likely to oversimplify the problem.

Given the limitations mentioned here above, this paper proposes a pragmatic methodology to handle the high dimensionality of the problem and estimate the impact of connecting a new DG unit. The latter is characterized by several relevant risk indices to be computed. A systematic, yet efficient, search of the variant space allows identifying all plausible congestion zones in a first stage, while an on-target sampling in these zones drives the computational effort towards the direction of interest, in a second stage. This combined approach allows managing the computation time.

This paper is organized as follows. First the steps of the proposed methodology are explained. Then the mathematical formulation of the methodology is exposed. Next, typical results obtained on a test case are presented. The final section is dedicated to the conclusions.

2 METHODOLOGY

The flowchart of the methodology is shown in Figure 1 (Faghihi et al. 2013).

As highlighted in this flowchart, the methodology rests on an attempt at decoupling as much as possible the electrical problem (congestion identification and curtailment analysis) from the probabilistic assessment (modeling of uncertain input variables and likelihood of the challenging situations). The main steps of the methodology are further presented in the next subsections.

2.1 *Modelling uncertainties*

Modeling the stochastic behavior of the generations of all DG units and the loads at all substations of the grid under study rests on eliciting the joint pdf of all these inputs this is based on inference from collected field data and on some assumptions.

Among the latter, correlations between random variables have to be considered:

- Loads at the different nodes are correlated due to either similar weather conditions or same daytime;
- Powers generated by wind farms are also correlated due to dependency on the wind speed in the area;
- Other possible correlations are neglected at this stage of the methodology development.

The joint pdf for each group of correlated variables is built by resorting to a Copula (Sklar 1959, Nelsen 2006).

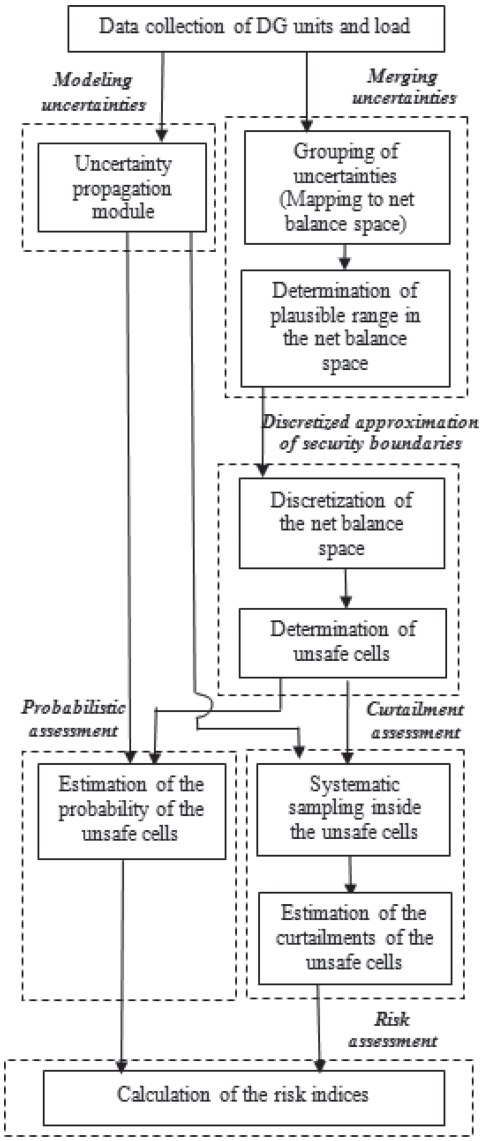


Figure 1. Flowchart of the methodology.

2.2 *Merging uncertainties*

As mentioned in the introduction, the proposed methodology should overcome the shortcomings of both MCS and MSA. The description of the input data, as summarized in the previous subsection, avoids the simplifications introduced in MSA. Now, in order to reduce the dimensions of the problem that affects strongly the efficiency of MCS, the uncertainties are first grouped in *net balances*, i.e. the algebraic sum of all productions minus the total load in each substation. Indeed, from the perspective of causing congestion on the grid elements, multiple variants corresponding to the same set of net balances will have the same effect. Identifying regions of the net balance space (i.e. a much less dimensional space than the variant space) where congestions are possible allows focusing the curtailment analysis on those full variants of interest that correspond to these regions, while avoiding a very large number of analyses of variants not contributing to the curtailment indicators.

In order to achieve this goal, a plausible domain of interest for the study is first determined in the net balance space, by considering on which range generations and load vary at each node. This domain naturally splits into a *safe* and an *unsafe* region, in terms of combinations of net balances making congestion on the grid.

As shown in Figure 2, a security boundary divides the net balance space into these two regions. A huge part of the net balance space belongs to the safe region, for current unsaturated grids in which a new DG unit could be connected. This safe region can therefore be skipped in further analysis. On the contrary, the sampling of variants should be forced into the unsafe region where curtailment is required.

It should be noted that for the N and each N-1 situation, security boundaries are different, due to different possibilities of congestion in each topology. The same remark can be made for different seasonal conditions, for which the line ratings take different values.

The next section deals with how these security boundaries can be approached.

2.3 *Discretized approximation of safety boundaries*

The unsafe region boundaries cannot be easily obtained. This region can take unpredictable

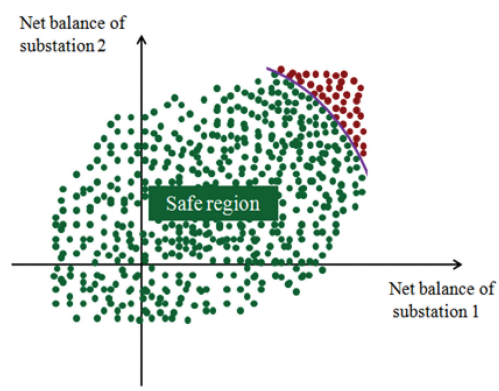


Figure 2. Safe and unsafe regions in the net balance state space.

shapes, mainly in already quite saturated grids, due to the non-linearity of the electrical system behavior. Sampling points in the net balance space, despite the lower dimensionality of the latter, would turn out to be time consuming. Therefore, a mesh is defined in this space (Fig. 3). Cells are labelled as safe or unsafe according to the following criterion: a Load Flow (LF) calculation is applied on the variants located at the corners of the cells; if all the corners of a cell are safe (i.e. cause no congestion), then the cell is considered as safe, otherwise it is assumed to be unsafe (Fig. 4).

This discrimination between safe and unsafe cells is repeated for each topology and each seasonal regime. In each case, only unsafe cells will have to be considered in the sequel of the analysis.

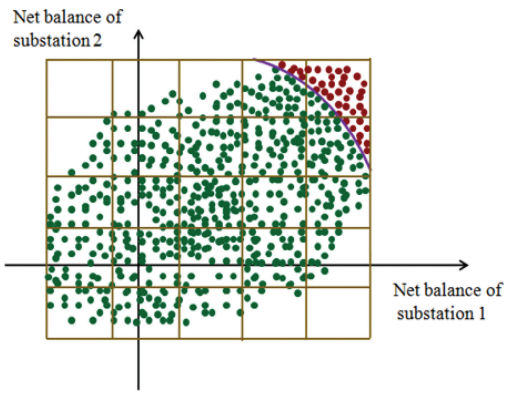


Figure 3. Discretization of the net balance state space.

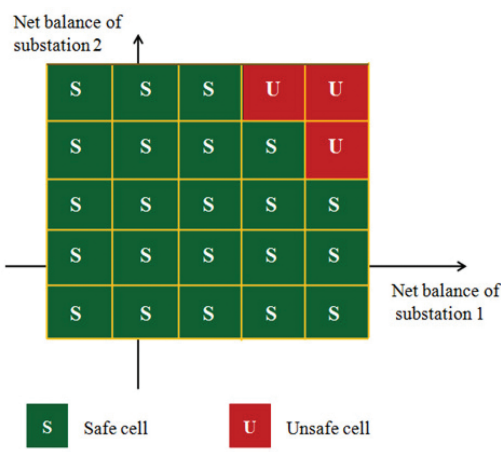


Figure 4. Approximation of the safe and unsafe regions by safe and unsafe cells.

2.4 *Curtailment assessment*

Variants likely to cause congestion on grid elements are thus only those corresponding to combinations of net balances lying inside unsafe cells, for given topology and season. MCS is therefore applied, by systematically sampling inside the unsafe cells. This allows

- Focusing the computational effort on those variants likely to lead to curtailment;
- Assessing conditional risk indicators, given each unsafe cell, before assessing the corresponding global indicators (see next subsections);
- Applying a cut-off criterion for too low-probable unsafe cells, having a negligible contribution to the total risk indices.

Different costs of curtailment can be assigned to the different (types of) DG units via the objective function of an OPF tool. The curtailments of all DG units, for each sampled variant, are calculated by such a tool, while accounting for the Principle of Access (PoA) of each DG unit. PoA defines the priority of curtailment of the different DG units contributing to the same congestion: some can export the power they produce at any time, others are guaranteed to do so only in the N situation, while others are likely to be curtailed in any topology, depending on the contractual characteristics of their connection.

Different PoA's can be defined depending on the location of the congestion, i.e. whether it appears on the HV grid and/or at the HV/MV substation. For instance, a technical optimum can be chosen to handle the overloads on the HV grid and a LIFO (Last in First Out) scheme could be applied at the substation level, in order to distribute the amount of required curtailment (due to overloads on HV grid on one hand and to HV/MV transformers on the other hand).

2.5 *Probabilistic assessment*

In order to calculate the global risk indices of the problem, the probability of the unsafe cells in the net balance space has to be estimated. However, this operation is not straightforward, as the joint pdf of all variants is complex and is not easily integrated on a volume in the net balance space. Therefore, a pragmatic approach is followed. First, a large number of samples are generated by MCS from the joint pdf of the correlated uncertainties (i.e. variants). Those correlated samples correspond to the power produced by the wind farms as well as to the loads at the different substations. However, the possible number of states obtained by combining the production of DG units and the loads may lead to a non-manageable

sample size due to combinatorial explosion. Therefore, a MSA-related technique is applied: the space of each group of correlated variables is discretized on a mesh in order to create a limited (but appropriate) number of states. The center of each cell in the mesh represents all the samples inside this cell, and the ratio of the number of samples inside the cell over the total number of samples determines the cell probability estimation. This is done for the different groups of correlated uncertainties, before combining the corresponding discretized states by a simple rule of product and converting them to the corresponding net balance value. Finally, the probability of each unsafe cell in the net balance space is calculated, considering the sampled variants that can be mapped to this cell and the probabilities of the discretized states associated to each group of correlated uncertainties.

2.6 *Risk assessment*

In the previous subsections, the unsafe cells were identified, the expected curtailments given each unsafe cell were assessed, and the probabilities of the cells were estimated. Having all these ingredients, the total risk of curtailment for each DG unit is obtained by summing on the unsafe cells, the expected curtailment associated to each cell weighed by the corresponding probability. This has to be summed up on all possible topologies and seasonal regimes considered, by considering the probability of each combination 'topology-season'.

Based on the risk of curtailment for each DG unit, its Utilization Factor (UF) can be calculated. The UF of a DG unit is the ratio of the actual energy produced in one year over the corresponding theoretical maximum, based on its installed power. The UF of a DG unit is an economic characteristic of the relevance of the investment for a producer. This UF can also be compared to its Capacity Factor (CF), i.e. the ratio of the energy that could have been produced in a year, without any curtailment, over the maximum energy produced on the basis of the installed power.

In addition to these indices that characterize the expected curtailment in a year, the curtailment distribution can also be provided. The distribution of the congestion on each element of the grid can also be estimated.

3 MATHEMATICAL FORMULATION

The present section aims to express in mathematical terms the methodology summarized in Figure 1 and presented in details in Section 2.

3.1 *General definition of the risk indices*

Consider the risk assessment of an ANM scheme under the following assumptions. The grid under study displays n nodes. To each node i, a load L_i is connected as well as DG units having a production P_{ij}, $j = 1 \ldots n_j$, respectively.

The grid is studied in all configurations N and N-1, with a probability p_k to lie in configuration k, $k = 1 \ldots n_c$, and in the various seasons defined (summer, winter, inter-season), with a probability q_l to be in season l, $l = 1 \ldots n_s$.

Let us define:

- $\overline{L} \equiv \{L_1 \ldots L_n\}$, vector of the loads;
- $\overline{P} \equiv \{P_{11} .. P_{1n}, P_{21} .. P_{2n}, \ldots P_{n1} .. P_{nn}\}$, vector of the productions;
- $\varphi_{kl}(\overline{L}, \overline{P})$, joint pdf of the variants $(\overline{L}, \overline{P})$ in configuration k and season l;
- $f_{kl}(\overline{L}, \overline{P})$, performance function associated to a given risk index RI in configuration k and season l.

This performance function could be for instance an indicator function (equal to 1 when there is a congestion, and 0 else—the result of a Load Flow calculation) for the congestion probability, or the curtailment at a given DG unit if the corresponding expected curtailment is the measure of interest (the result of an Optimal Power Flow calculation).

The risk index RI can then be expressed as:

$$RI = \sum_{k=1}^{n_c} \sum_{l=1}^{n_s} \int\int f_{kl}(\overline{L}, \overline{P}) \varphi_{kl}(\overline{L}, \overline{P}) d\overline{L} d\overline{P} \quad (1)$$

where the integrals on the loads are limited to the ranges (minimum load, maximum load) for all nodes, and those on the productions extend from 0 to the installed power of each DG unit.

As the double summation does not bring any additional complexity in the calculation, we will assume in the following $n_c = n_s = 1$. Therefore:

$$RI = \int\int f(\overline{L}, \overline{P}) \varphi(\overline{L}, \overline{P}) d\overline{L} d\overline{P} \quad (2)$$

3.2 *Mapping to the net balance space*

Let

$$NB_i = \sum_{j=1}^{n_i} P_{ij} - L_i \quad (3)$$

be the net balance seen by the grid at node i, $i = 1 \ldots n$. The Jacobian of the corresponding change of variables being equal to 1, we can rewrite eq. (2) as follows:

$$RI = \int\int f(\overline{L}(\overline{NB}, \overline{P}), \overline{P}) \varphi(\overline{L}(\overline{NB}, \overline{P}), \overline{P}) d\,\overline{NB} d\overline{P} \quad (4)$$

where the integrals on the net balances are to be calculated on a domain (called *search space*) resulting from the possible values of the loads and productions mentioned above.

The performance function can only take non-zero values for variants causing congestion on the grid. Since the latter situation corresponds only to given net balance variants $\overline{NB}$, we can multiply the performance function f by an indicator function $\theta(\overline{NB})$ such that

$$\theta(\overline{NB}) = \begin{cases} 1 & \text{if } \overline{NB} \text{ causes a congestion on the grid} \\ 0 & \text{else} \end{cases} \tag{5}$$

All net balance variants $\overline{NB}$ belonging to the search space and for which $\theta = 1$ compose the so-called unsafe region UR of the search space. Consequently,

$$\begin{aligned} RI &= \int\int f(\bar{L}(\overline{NB},\bar{P}),\bar{P})\theta(\overline{NB})\varphi(\bar{L}(\overline{NB},\bar{P}),\bar{P})d\overline{NB}d\bar{P} \\ &= \int_{UR} d\overline{NB}\int f(\bar{L}(\overline{NB},\bar{P}),\bar{P})\varphi(\bar{L}(\overline{NB},\bar{P}),\bar{P})d\bar{P} \end{aligned} \tag{6a,b}$$

3.3 *Discretization of the search space*

Let us now discretize the search space in n_{cel} cells. Then we have:

$$\int d\overline{NB} = \sum_{c=1}^{n_{cel}} \int_{cell\,c} d\overline{NB} \tag{7}$$

In addition to this, each cell c on which $\theta(\overline{NB}) = 0$ everywhere is called *safe* and the integral over it is 0. Therefore

$$RI = \sum_{\substack{unsafe \\ cells\,c}} \int_{cell\,c} d\overline{NB}\int f(\bar{L}(\overline{NB},\bar{P}),\bar{P})\varphi(\bar{L}(\overline{NB},\bar{P}),\bar{P})d\bar{P} \tag{8}$$

Let

$$\alpha_c \equiv \int_{cell\,c} d\overline{NB}\int d\bar{P}\varphi(\bar{L}(\overline{NB},\bar{P}),\bar{P}) \tag{9}$$

be the probability to be in cell c, and

$$\varphi_c(\bar{L}(\overline{NB},\bar{P}),\bar{P}) \equiv \begin{cases} \dfrac{\varphi(\bar{L}(\overline{NB},\bar{P}),\bar{P})}{\alpha_c} & \text{if } \overline{NB} \in cell\,c \\ 0 & \text{else} \end{cases} \tag{10}$$

be the truncated pdf of the variants belonging to cell c. Then, we obtain:

$$RI = \sum_{\substack{unsafe \\ cells\,c}} \alpha_c \int_{cell\,c} d\overline{NB}\int f(\bar{L}(\overline{NB},\bar{P}),\bar{P})\varphi_c(\bar{L}(\overline{NB},\bar{P}),\bar{P})d\bar{P} \tag{11}$$

We can finally remap this result to the original variant space by writing:

$$RI = \sum_{\substack{unsafe \\ cells\,c}} \alpha_c \int_{\substack{\Sigma\bar{P}-\bar{L} \\ \in cell\,c}} d\bar{L}\int f(\bar{L},\bar{P})\varphi_c(\bar{L},\bar{P})d\bar{P} \tag{12}$$

Each integral in eq. (12) is estimated in our methodology by a MCS approach restricted to each unsafe cell (see Subsection 2.4), while α_c is assessed by the MSA-like technique explained in Subsection 2.5.

4 RESULTS

Our methodology has been applied, for the sake of illustration, on a test case (Faghihi et al. 2014) displaying 3 substations, 5 wind farms (for a total installed capacity of 52 MW), 3 CHP units (total capacity: 35 MW) and one load in each substation (Fig. 5).

For the purpose of our test case, all DG units are assumed to be connected to the MV side. However,

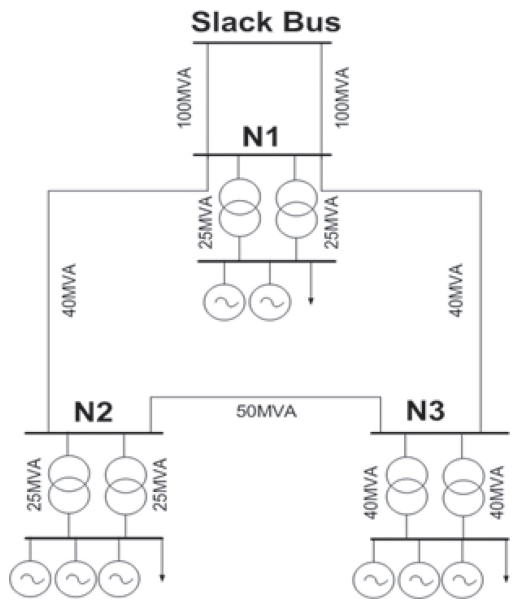


Figure 5. Test grid.

the methodology can be adapted to a mix of connections on both HV and MV sides. Although the network is simply made of 3 lines and 3 substations, the load and production profiles are chosen plausible, since they are inspired from a real case. Risk indices are estimated for the N and all N-1 situations (i.e. outages of HV/MV transformer in substation no. 2 and each HV line), as well as for the 3 seasons considered in a year and characterized by different line ratings. The probabilities to be in summer, inter-season and winter are 0.25, 0.5 and 0.25, respectively. A probability of outage of each line and each HV/MV transformer is assumed as well.

The distributions of the curtailment in one of the wind farms due to outage on the HV grid and in a HV/MV transformer are shown in Figures 6 and 7, respectively. A separate analysis of the distribution of the curtailment of each DG unit in N and each N-1 situation in each season can also be provided. As an example, the distribution of the congestion on a line in a N-1 situation on the HV grid in summer is displayed in Figure 8. Such a detailed analysis can be obtained for each asset in N and all N-1 situations in each season.

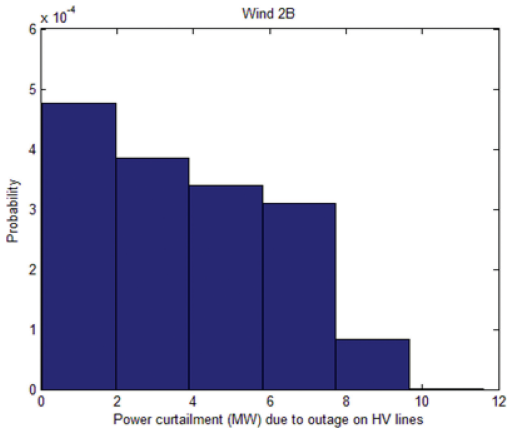


Figure 6. Distribution of the curtailed power in a wind farm due to outage on HV lines.

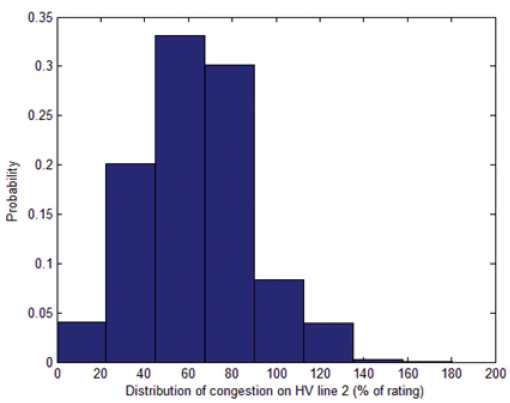


Figure 7. Distribution of the curtailed power in a wind farm due to outage on a HV/MV transformer.

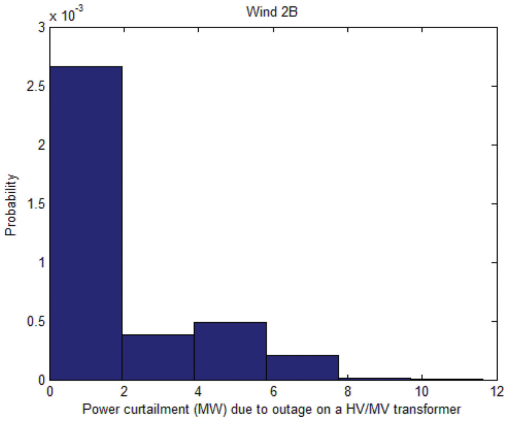


Figure 8. Distribution of the congestion on a line in a N-1 situation on the HV grid in summer.

5 CONCLUSIONS

The share of DG in electricity generation is increasing, at a rate faster than that of possible grid reinforcements, which in addition are very expensive. Both TSOs and DSOs are likely to face more congestion and voltage problems, due to 'two-way flows' at the distribution level. Modern grids should evolve to handle these challenges, before reinforcing their current infrastructure. ANM, in the context of smart grids, allows controlling the injection of energy produced by DG units in case of security problem on the network, and is therefore a possible solution to this challenge.

However, in the planning phase, the performance of an ANM scheme should be assessed when considering the impact of any possible new connection to the grid. Indeed, any new DG unit is likely to modify the current expected curtailment of the other DG units installed in the area. Therefore, proper risk measures related to the curtailment of each producer (in N and N-1 situations) have to be assessed.

Considering the intermittent production of DG units, as well as the variability of the load, probabilistic approaches are developed to handle the problem. However, even for medium-size grids, the

number of random input variables of an OPF tool estimating the curtailment level, soon becomes important. Due to the non-linearity of the electrical system, classical techniques to improve the efficient of a MCS approach turn out to be irrelevant.

This paper proposed a pragmatic methodology to assess risk indices characterizing the performance of an ANM scheme in a systematic way. The method rests on the grouping of uncertainties, based on their similarity in making congestion on the grid. A new, much less dimensional state space, i.e. the net balance space, is then introduced. The unsafe region in this space is identified, and MCS is then limited to variants corresponding to this unsafe domain.

The main advantage of this approach is to drive the sampling towards regions of interest in the search space, while skipping numerous variant analyses that do not contribute to the risk indicators of interest. The results are categorized into two main groups, i.e. risks related to the curtailment of DG units and the risk associated with congestions on grid elements.

REFERENCES

Davidson, E.M., Ault, G.W. & McArthur, S.D.J. 2010. AuRA-NMS: An autonomous regional active network management system for EDF energy and SP energy networks. *In Proceedings of the Power and Energy Society General Meeting, Minneapolis (USA)*.

Faghihi, F., Labeau, P.E., Maun, J.C., De Wilde, V. & Vergnol, A. 2013. Probabilistic risk analysis of distributed generation curtailment in a saturated grid. *In Proceedings of Esrel2013, Amsterdam (The Netherlands): Balkema*.

Faghihi, F., Labeau, P.E., Maun, J.C., De Wilde, V. & Vergnol, A. 2014. Towards a probabilistic risk assessment of distributed generation curtailment in saturated TSO/DSO networks. *In Proceedings of CIRED 2014, Rome (Italy)*.

L'Écuyer, P., Le Gland, F., Lezaud, P. & Tuffin, B. 2009. Splitting methods. In G. Rubino & B. Tuffin (eds.), *Monte Carlo methods for rare event analysis*: 39–61. Chichester: John Wiley & Sons.

Li, J. & Xiu, D. 2010. Evaluation of failure probability via surrogate models, *Journal of Computational Physics* 229: 8966–8980.

Lux, I. & Koblinger, L. 1991. *Monte Carlo particle transport methods: neutron and photon calculations*. Boca Raton: CRC Press.

Nelsen, R.B. 2006. *An introduction to copulas*, New York: Springer.

Sansawatt T., Ochoa, L.F. & Harrison, G.P. 2012. Smart decentralized control of DG for voltage and thermal constraint management. *IEEE transactions on power systems* 27: 1637–1645.

Siano, P., Chen, P., Chen, Z. & Piccolo, A. 2010. Evaluating maximum wind energy exploitation in active distribution networks. *IET generation, transmission and distribution* 598–608.

Sklar, A. 1959. Fonctions de répartition à n dimensions et leurs marges. *Publ. Inst. Statist. Univ. Paris* 8: 229–231 (in French).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Priorities assignment for actions in a pipeline: A decision model to evaluate multiple objectives

M.H. Alencar, M.F. Marsaro & A.T. de Almeida
Universidade Federal de Pernambuco, Recife, Pernambuco, Brazil

ABSTRACT: Pipelines are considered one of the safest means of transport of natural gas. However, when an accident occurs, can generate catastrophic consequences in terms of human, environmental and financial aspects. In this context, this paper presents a quantitative analysis, based on the application of a multicriteria decision model for risk assessment in natural gas pipelines, prioritizing pipeline sections according to the risk value obtained.

1 INTRODUCTION

Shahriar et al. (2012) state that Oil and Gas (O & G) are the major fuel sources consumed in the world. Many of these fuels are transported from origin to destination through pipelines. Jo and Crowl (2008) point out that these distances cover hundreds or even thousands of miles. Long pipelines pass through distinct locations, each with different characteristics e.g. industrial, agricultural or residential areas, commercial districts, preserved environmental sites, etc).

The integrity of pipelines is very important to companies, government agencies, consumers, and other stakeholders, due to the potential adverse consequences related to public health, safety, the environment and financial expenditure on correcting whatever type of system failure may occur. However, a pipeline is subject to deterioration due to age, aggressive environmental factors, inadequate design and improper maintenance and protection. In this context it is observed that some accidents have occurred over the years, which have often generated critical consequences.

Han and Weng (2011) consider that accidents caused by gas pipelines rupturing bring about major threats to public safety. Due to the physical and chemical characteristics of natural gas and the complexity of the topology of pipeline networks, the occurrence of accidents in pipelines are completely different from any other kind of industrial accident.

Marhavilas et al. (2011) describes that different studies on risk in the natural gas pipeline environment have been conducted using different methods of evaluation which have included qualitative and quantitative approaches. More specifically, given these aspects, this paper presents quantitative analyses, based on the application of a multiple criteria decision model for risk assessment of a natural gas pipeline, prioritizing pipeline sections according to the risk value obtained. Multi-Attribute Utility Theory (MAUT) is applied to incorporate the decision maker's risk behavior. MAUT takes into account the probabilistic context in which pipeline risk analysis is inserted, presenting a very well defined axiomatic structure, based on the axioms of utility theory.

The paper presents the following sections: Section 2 presents some aspects associated with the decision context; Section 3 sets out the decision model; Section 4 describes an application of the model; and the last section draws some conclusions.

2 DECISION CONTEXT

According to Alencar and Almeida (2010), segments of pipelines that have homogeneous characteristics can be divided into sections. Age of piping, soil type, pressure and pipeline diameter are some of the homogeneous characteristics that can be considered.

Each section from Figure 1 presents different characteristics, which cover residential areas, industrial areas, commercial areas and a tourist complex. The layout of these sections is shown in Figure 1.

To evaluate the gas pipeline sections, it is interesting to evaluate the decision maker's objectives. Keeney (1992) proposed important steps which point out that values are the basis of interest for any decision, and these become clear after the objectives have been identified. In the same way, consequences are descriptions of alternative impacts described in terms of the degree to which objectives were achieved. Thus, in this multicriteria

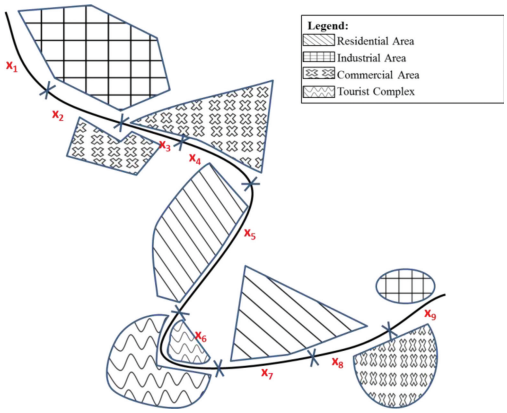


Figure 1. Layout of the arrangement of the sections considered.

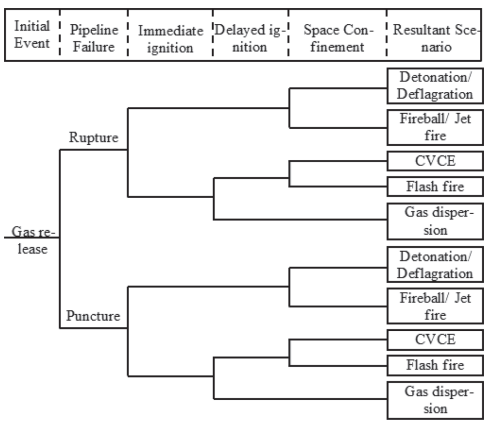


Figure 2. Event tree for a natural gas pipeline (adapted from Brito et al. (2010)).

decision, the consequences of the human (h), environmental (v) and financial (m) dimensions are what the model considers.

While considering that the complexity of operational decision situations can lead to accidents occurring, Crowl and Jo (2007) point out that incidents may also provoke accidents. Many incidents are followed by a series of events that result in an accident. This may include explosions, leaks and fire. In this paper, hazard scenarios are defined for natural gas pipelines based on Brito et al. (2010), as presented (Fig. 2).

3 MULTICRITERIA DECISION MODEL

According Vincke (1992), Multiple Criteria Decision Making (MCDM) is a set of methods and techniques developed to support individuals and organizations in resolving decision problems.

The multi-attribute decision model considered (see Fig. 3) in this paper uses a multiple risk dimension based evaluation for each section of a pipeline network, providing an idea of the risk hierarchy between each pipeline section by comparing these sections.

This information can be used as input for managerial purposes with regard to maintenance and operational decisions, especially to priorities for allocating resources amongst gas pipeline sections, taking human, environmental and financial risks into consideration. This model uses only one decision maker.

As used in Brito et al. (2010), "A" is defined as the set of all possible outcomes from a given accident in a dimension amongst the set of dimensions considered. As described in Brito et al. (2010), states of nature "θ" related to potential accidents in natural gas pipelines express the uncertainty associated to this problem.

To deal with uncertainties in "A", a probabilistic approach is applied by using a probability distribution over consequences and by elicitating utility functions for these consequences. Considering descriptions by Berger (1985), "$\pi_i(\theta)$" sets the probability of each state of nature or accidental scenario.

Each pipe section is denoted by "x_i". The utility when the scenario is "θ" and the section "x_i" is established by "$U(\theta,x_i)$". "q" represents the consequences. The utility is obtained through the combination of the probabilities of deterministic

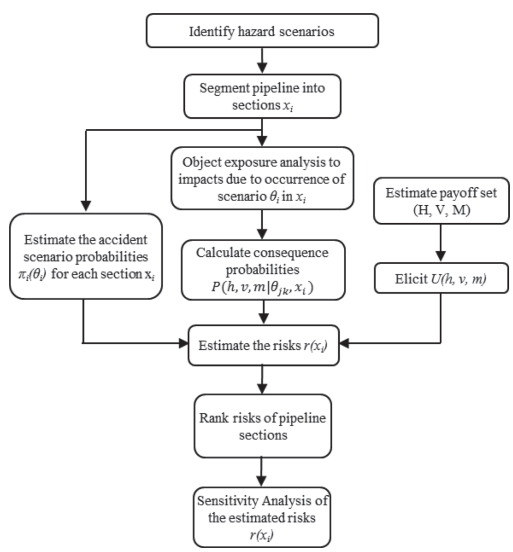


Figure 3. Model structure (adapted from Brito and Almeida (2009)).

consequences "q" in "A" (consequence function, "$P(q|\theta, x_i)$"). Additionally, it is considered that consequence functions are represented by the probability density function "$f(q|\theta, x_i)$".

According to Keeney and Raiffa (1976), the values of the utility function are defined in interval scales between the extremes [0,1], where "0" is associated with "least preferable" and "1" with "most preferable". The utility function of these consequences (represented by "$U(q)$", where "q" Є "A") is defined by the following equation:

$$U(\theta, x_i) = \int_q P(q|\theta, x_i)U(q)dq \quad (1)$$

According to Berger (1985), the loss function is calculated through the negative of the utility function "$L(\theta, x_i) = -U(\theta, x_i)$". The loss is estimated for sections of the pipelines and for the accident scenarios in question as shown below:

$$L(\theta, x_i) = -\int_H \int_V \int_M f(h,v,m|\theta, x_i)U(h,v,m)dhdvdm \quad (2)$$

Brito et al. (2010) argue that the expected value of loss, defined as the risk, should be established for each pipeline section and for each criterion, and enables the decision maker's attitude in relation to risk to be incorporated by eliciting the utility function. In this context, the interval scale for "$L(\theta, x_i)$" and "$r(x_i)$" is defined as [–1,0], where "–1" is associated with "lowest risk" and "0" with the highest risk.

For each criterion related to a pipeline section and for each accident scenario, the risk is defined as the expected value of losses, as per the definitions found in Berger (1985) and Keeney and Raiffa (1976). In this statement, the risk is considered to be the result of summing the losses associated with each specific scenario "θ" and each section "x_i" for the three consequence dimensions considered, multiplied by the probabilities of accident scenarios "$\pi_i(\theta)$" added to the losses indexed to the scenario "θ_N". In this context, "θ_N" represents the scenario of normality of the system, "$r(\theta_N)$" assumes the value of (–1) which multiplies "$\pi_i(\theta_N)$", the loss associated with the scenario "θ_N" without the occurrence of any damage. Thus, the risk is established by the following equation:

$$r(x) = \left\{ \Sigma_j \Sigma_k \left\{ - \left[\begin{array}{l} +k_h \int_h f(h \mid \theta_{jk}, x)u(h)dh \\ +k_v \int_v f(v \mid \theta_{jk}, x)u(v)dv \\ +k_m \int_m f(m \mid \theta_{jk}, x)u(m)dm \end{array} \right] \right\} \cdot \pi_i(\theta_{jk}) \right\} + (-1) \cdot \pi_i(\theta_N) \quad (3)$$

4 APPLICATION

A numerical application is presented. The objective is to illustrate the proposed model for assessing risk in a natural gas pipeline using the multiple criteria decision model developed.

The hazard scenarios were defined from the event tree presented in Figure 2. Simulations were developed for analyzing accident scenarios "θ" and sections throughout the considered pipeline by using computational tools. The probability density functions $f(h|\theta, x_i)$, $f(v|\theta, x_i)$ and $f(m|\theta, x_i)$ are used to estimate probabilities.

Using the structured elicitation protocol described in Keeney and Raiffa (1976), the multi-attribute utility function $U(h,v,m)$ is achieved by choosing from among consequences associated with accidents in pipelines.

Another step of the model includes estimating the risks and ranking them as presented in Table 1. To estimate the risk assigned to each section of the pipeline, the multi-attribute utility function is associated with the probability density function of the consequences.

Further analysis, in addition to ranking, is to compare the increments of risk in relation to pipeline sections. According to Keeney and Raiffa (1976), this is possible due to the interval scale of utility functions.

A descending ranking of values is used for risk assessment. From this result some considerations can be made.

One of these considerations is that an Absolute Difference Index (ADI) for each section should be defined from the ratio "$r(y_i) - r(y_i + 1)$" where "y_i" and "$y_i + 1$" represent the positions in the ranking of given sections of the pipe. Another index for the risk analysis is the Difference Ratio Index (DRI), expressed by Equation (4):

$$DRI = \frac{r_y(x_i) - r_{y+1}(x_j)}{r_{y+1}(x_j) - r_{y+2}(x_j)} \quad (4)$$

Table 1. Result of ranking the risks to sections of the pipeline.

Ranking position (y)	Section (x_i)	ADI	DRI
1	x_8	0.6681	0.2062
2	x_4	3.2395	0.9881
3	x_5	3.2782	6.0895
4	x_9	0.5383	0.3724
5	x_6	1.4455	0.3781
6	x_3	3.8225	1.9350
7	x_2	1.9754	11.6310
8	x_1	0.1698	–
9	x_7	–	–

In this way, is possible to verify in Table 1 that section 8 presents the highest value of risk among the sections that were analyzed, when all three risk dimensions are considered: human, financial and environmental. The highest losses related to the likely consequences of accidents are expected for the section 8. Additionally, it is verified that the increment in the risk values from section 5 to section 9 is 6 times greater than that from section 9 to section 6. In the same way the increment in the risk values from section 2 to section 1 is almost 12 times greater than that from section 1 to section 7.

This evaluation of risk increment allows the decision-makers make better decisions about resource allocation, especially when it comes to scarce resources for the maintenance and management of pipelines designed to risk mitigation. Well as identifies the sections more prone to severe consequences when an accident occurs, the decision maker can identify those most vulnerable sections and requiring more resources.

According to Alencar and Almeida (2010), the last stage refers to verify the consistency of results, from the variation of some parameters. Due the uncertainty related with model parameters, this phase can identify the impact of the results by using a sensitivity analysis.

5 CONCLUSION

The use of a multiple criteria approach to evaluate risk from a natural gas pipeline allows a multidimensional risk analysis to be conducted, as presented in this paper. More specifically, the use of MAUT (Multi-attribute Utility Theory) adds important aspects to this problem such as: taking into consideration the decision makers' preferences; the decision makers' behavior in relation to risk; and using the interval scale for assessing the risk increment through increment ratios.

Obtaining a ranking of risk values allows managers to visualize the existing context better, which should lead the company to consider these aspects of mitigating risks and to adopt preventive actions related to risk mitigation. For future studies, the involvement of stakeholders may be an interesting point to include in the decision making process of risk analysis in natural gas pipelines, and would add the context of group decision making to this approach.

ACKNOWLEDGEMENTS

This work was supported by the Brazilian National Research Council (CNPq) and CAPES (a Brazilian Research Agency under the Ministry of Education of Brazil).

REFERENCES

Alencar, M.H., Almeida, A.T. 2010. Assigning priorities to actions in a pipeline transporting hydrogen based on a multicriteria decision model. *Int. J. Hydrogen Energy*. 35, 3610–3619.

Brito A.J. & Almeida A.T. 2009. Multi-attribute risk assessment for risk ranking of natural gas pipeline. *Reliability Engineering and System Safety* 94: 187–198.

Brito, A.J., Almeida, A.T., Mota, C.M.M. 2010. A multicriteria model for risk sorting of natural gas pipelines based on ELECTRE TRI integrating Utility Theory. Eur. *J. Oper. Res.* 200, 812–821.

Crowl, D.A., Jo, Y.D. 2007. The hazards and risks of hydrogen. J. Loss. Prev. Process Ind. 20, 158–164.

Han, Z.Y., Weng, W.G. 2011. Comparison study on qualitative and quantitative risk assessment methods for urban natural gas pipeline network. *J. Hazardous Mat.* 189, 509–518.

Jo, Y.D., Crowl, D.A. 2008. Individual risk analysis of high-pressure natural gas pipelines. *J. Loss Prev. Process Ind.* 21, 589–595.

Keeney, R.L. 1992. Value-focused Thinking: a path to creative decision making. *Harvard University Press*, London.

Keeney, R.L., Raiffa H. 1976. Decisions with multiple objectives: preferences and value trade-offs. *John Wiley & Sons*, New York.

Marhavilas, P.K., Koulouriotis, D., & Gemeni. 2011. V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009, *Journal of Loss Prevention in the Process Industries*. 24, 477–523.

Shahriar, A. Sadiq, R. Tesfamariam, S. 2012. Risk analysis for oil & gas pipelines: A sustainability assessment approach using fuzzy based bow-tie analysis. *J. Loss Prevention Process Ind.* 25, 505–523.

Vincke, P. 1992. Multicriteria Decision—aid. *John Wiley & Sons,* Bruxelles.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk assessment in heat supply system

B. Babiarz
Rzeszow University of Technology, Rzeszow, Poland

ABSTRACT: The task of a heat supply system is to provide the consumer with the required quantity of the energy in the form of the "usable energy"- heat. Both risk and uncertainty are connected with the functioning of communal systems involving heat supply systems. The issue of risk assessment in heat supply systems requires considering their specific character. Heat supply systems characterize changeable heat load during the year. The delivery of heat to consumers depends on changeable external conditions.

These conditions affect energy security, security of energy supply and safety of people as users or operators of system. The paper presents an approach to risk assessment in the heat supply system, as a system consisting of three sub-systems, taking into account the location of the risk, identification, hazard classification, estimation of risk and risk responses. The proposed approach to risk analysis has been summarized with the requirements of the current legislation concerning heat engineering.

Method of risk assessment using an event tree method, possible to application in heat supply system considering changeable atmospheric conditions have been presented in this work.

1 INTRODUCTION

The task of a Heat Supply System (HSS) under the relevant legislation is a current, continuous and reliable heat supply to the needs of local communities through the provision of services, which are commonly available. Ensuring continuity and reliability of HSS must meet the requirements to ensure:

- energy security—as a condition of the economy which enables full coverage of the customers' ongoing and prospective demand for fuels and energy in a technically and economically justified manner, with the observance of the environment protection requirements;
- security of energy supply, forming an ability of the system to ensure the security of the operating network and balancing energy supply with demanding for this energy;
- safety of people, as users or operators of a system.

The measure of the loss of security is the risk, resulting from the likely sequence of events affecting the level or from the possible consequences of the decisions taken. Risk is characterized by the quality of the fulfillment of the system task. Taking into consideration, that risk is inherent in the businesses of heating, and the quality of services provided is a measure of competitiveness, we can conclude, that these companies should strive to eliminate or minimize the hazards, which may affect the level of risk.

It is possible to achieve through improving operating process of the subsystems, objects or elements that are components of the entire heat supply system by introducing into traditional management system methods aimed at identifying hazards, eliminating or reducing their potential effects in order to estimate the risk and to take action with the aim of responding to risk. The results of the risk assessment process should serve as an important basis to determine the strategy of actions to meet the safety requirements in the area of economically reasonable as well as draft a plan for responding to risk.

2 THE TERM AND KINDS OF RISK

Risk is the basic category of security issues. It is derived from the theory of reliability and safety of systems. This is connected with situations of slight, uncertain or problematic effect of exposing to danger, loss or harm—with the likelihood that something will bring negative results. In this perspective, the risk is identified with the loss of safety (Babiarz & Rak 2001).

The risk is at least two-dimensional, complex concept involving the possibility of an adverse outcome or uncertainty about disadvantageous events, which are the occurring time, kind of event, its duration, the size of an adverse outcome. In addition to the term risk is used term hazard, which is more than the risk associated with a sense of danger. The concept of risk, in turn, is more associated with the estimate of uncertainty and possible losses related to this.

Risk characteristics are uncertainty, probability, the dispersion of results (adverse effects). There are two ways to define risk. The first of these combines the risk with possible distribution of results—the risk is a possible variance of the expected results. In this perspective, risk is a function of the variability of possible outcomes. A second look at risk refers to the probability of losses and their sizes. The more probable that an event causing losses occur, the greater risk is. According to this definition, the size of the risk can be defined as the frequency of obtaining undesirable results. Then you can bind the level of the risk with the sizes of possible losses. In this perspective, the greater the loss suffered may be the greater risk occurs. There is also a definition of risk as the product of the probability of occurrence of an adverse event and the size of the losses caused by event.

From the mathematical point of view the basic definition is obligatory:

$$r = P \cdot C \tag{1}$$

where:
P—a measure of the system functioning unreliability, corresponding to the category of probability—frequency;
C—a measure of the consequences, corresponding to the category of effects—damage, expressed in units of financial resources.

3 THE APPROACH TO RISK ANALYSIS IN HSS

Risk and safety analysis in HSS is the basis for the proper conduction of the process of exploitation and prevention the occurrence of serious failures that can lead to economic, social and environmental losses. Heat supply systems characterize changeable heat load in the year (Babiarz 2006). The delivery of heat to consumers depends on changeable external conditions.

Risk analysis in HSS requires taking action on its:

- location (determining the place of occurrence, the type of subsystem, coverage, risk groups);
- identification (identifying the types of risks, factors of uncertainties, kinds of hazards);
- designation (estimation of risk measures, using appropriate quantitative or qualitative methods);
- respond to risk and management of it (controlling and exploration of activities aiming to reduce it).

Identification of risk requires the identification of hazards as factors, that may cause dangerous situations to the users of object, the object itself or its environment.

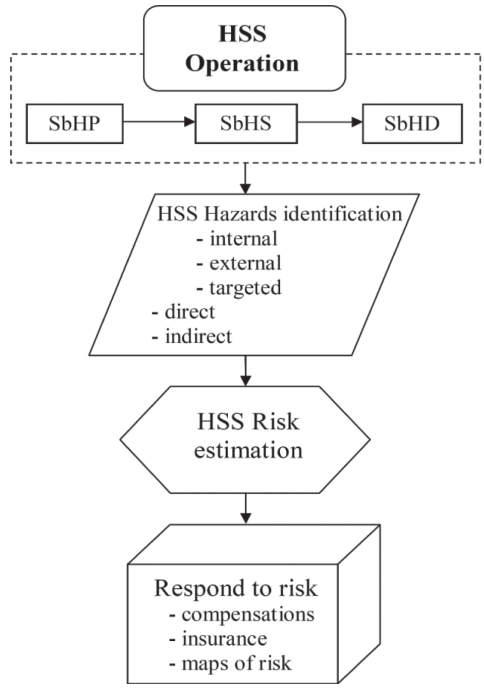


Figure 1. The approach to HSS risk assessment.

From the point of view of the source of danger in HSS, hazards can be distinguished as: internal, external and intentional (targeted).

Internal hazards arise from the nature of the system, its specific character and they are based on the kind of technological processes, which are, depending on the degree of system decomposition, production, supply and distribution of heat to the public via the heating medium with appropriate parameters. In particular, these are:

- deviations from the established parameters, required in given operating conditions: temperature, pressure, flow, thermal power;
- failures of the heat production subsystem components: boilers, pumps, control and measurement devices, etc.;
- failure of heat supply subsystem components: district heating pipes, fittings, alarm devices, etc.;
- failure of the heat distribution subsystem elements: heat distribution pipes in heating stations, fittings, internal system components, etc.;
- error of human—as an operator or conservator of system—maintenance and inspection mistakes;
- unreliability of the system supplying the media needed to execute the HSS tasks, in particular: electricity, water, steam, air, oil, etc.

External hazards are mainly determined by unfavorable weather conditions, or they may be caused by the proximity of communication tractions, and other objects having influence on the state of the object and the consequences of limitations, or the lack of heat supply to consumers. These can be distinguished as:

- natural, extreme climatic events such as floods, earthquakes, landslides, strong winds, lightning;
- serious failures in electric power systems, causing interruptions in the power supply, which can cause even blackout failure;
- other installations or technical facilities located in the vicinity, which could adversely affect the elements of HSS;
- transport routes located nearby, which are the source of stray currents that may cause damage to the network elements.

Intentional (targeted) hazards are those connected with the operation of unauthorized persons, terrorist attacks. Moreover, the political situation has also the impact on the security of fuel supplies needed for energy production.

Considering the impact of adverse events, hazards can be divided into: direct, arising as a result of failures (the direct impact factor of high temperature and pressure) and indirect hazards, which are results of HSS component failures. Direct hazards in the above sense is any factor's impact on the surrounding environment, people, equipment and buildings. Steam and hot water under high pressure are particularly dangerous in the event of damage in the heating network located in street lane or in its close proximity.

Direct hazards are:

- failure posing a threat to human life and health: the possibility of burns as a result of the impact of hot water and steam, scouring the streets, foundations of buildings, caused by leaching of soil by flowing a heating medium;
- failures causing property damage: damage in material objects (buildings, cars, etc.) caused by leaching the soil, damage to existing utilities (sewerage system, water supply and electricity network).

Indirect hazards are caused by HSS element failures and, consequently, by the lack or limitation of heat supply to consumers. Depending on the design of buildings, sealing of windows and doors can cause a significant decrease in temperature in rooms inside buildings. Force of the wind and temperature outside, which prevails at the time of damage are measures of an indirect hazard degree. These threads can be distinguished as:

- lowering indoor room temperatures, which in consequence leads to closure of nurseries, schools, kindergartens, offices, security or evacuation of hospitals, which do not have an emergency heat sources;
- the necessity to drain the internal installations of the water—lack of these activities might result in the possibility of damages in the installation elements, caused by freezing water in it;
- the necessity to stop production and the possibility of occurring serious losses as a result of failure to meet the technological parameters in industrial companies, greenhouses, etc. (Babiarz & Rak 2002).

Failures occurring in the HSS cause lowering of qualitative parameters of generated heat. This usually makes a thermal power balance not sustainable. The balance of thermal power in the heat supply system $\Delta\Phi$ may be expressed by a difference between the thermal power supplied to the system Φ_s and thermal power required (ordered) by the system Φ_o. In the case of optimal cooperation between the heat source and the entire system, the balance is sustainable and it can be described as follows:

$$\Delta\Phi = \Phi_s - \Phi_o = 0 \tag{2}$$

In case of irregularities, the balance equation can take two forms:

$$\Delta\Phi = \Phi_s - \Phi_o < 0 \tag{3}$$

or

$$\Delta\Phi = \Phi_s - \Phi_o > 0 \tag{4}$$

The case defined by the relation (3) occurs, when the thermal power output by the source to the district heating network is less, than the demand of consumers. Then the thermal power deficit occurs. On the other hand, a case described by formula (4) takes place when the network parameters control is not correct and returning water from the district heating network has a higher temperature than it should be according to the thermal power control charts (Babiarz B. 2014). This involves an indirect threat, which, in the case of simultaneous occurrence of several factors having influence on the heat load, can cause significant social and economic losses.

Identification and analysis of hazards give an overview to the characteristics and operating conditions of the system. They are useful in the estimation of risk.

Specialized techniques known as risk assessment are created as part of the developing science of safety. They are based on the qualitative, quantitative, semi-quantitative and simulation methods, using control and data acquisition as well as computer databases, operating system based on GIS.

Risk assessment may be qualitative, quantitative or semi-quantitative. Qualitative risk assessment is

applicable when the risk is small and well known. Simple description of the types of major accidents, their consequences and their likelihood and review of compliance with standards are sufficient. Quantified risk assessment is only appropriate where it is both reasonable and practicable in term of the availability of information and data (Arunraj & Maiti 2007).

Among the qualitative risk assessment methods there should be distinguished:

- CHL—Check Lists;
- FMEA—Failure Mode & Effects Analysis;
- HAZOP—Hazard & Operability Studies;
- PHA—Preliminary Hazard Analysis;
- PSA—Process Safety Analysis;
- Relative Ranking;
- What-If Analysis.

Quantitative methods of risk assessment are:

- ETA—Event Tree Analysis;
- FTA—Fault Tree Analysis;
- CCA—Cause & Consequence Analysis;
- HRA—Human Reliability Analysis;
- Monte Carlo Methods;
- Markov Methods;
- Matrix Methods.

Semi-quantitative risk assessment methods are:

- Domino effect analysis;
- LOPA—Layers of protection analysis.

The choice of the method depends mainly on the complexity of the system, the type of hazard and the probability of their occurrence. In addition, there should be considered: specific character of system, the type and scope of functions, the kinds of hazards and the likelihood of their occurrence, technology and types of databases, etc.

Examples of the application of risk assessment methods are presented in many publications (Werbińska, 2006, Zio 2009, Vališ & Zając 2010, Młyńczak et al. 2011, Aven 2012).

The next step in the risk analysis is responding to the risk. Result of the risk assessment process is used to make a decision on acceptance, minimization, avoidance or reducing risk. On this basis cost and benefits analyzes and strategies as well as responding to the risk plans are created.

According to current law regulations, heating companies should create action procedures, when hazards occur.

Restrictions in the heat supply can be introduced in the case of occurrence:

- a threat to the energy security of the country consisting in a long term lack of balance on the fuel and energy market;
- a threat to the safety of people;
- a threat of significant material loss.

Restrictions consist in a reduction or an interruption of the heat supply.

Supplier of heat introduces restrictions on the provision of heat by:

- reduction of the quality and/or quantitative parameters of heating medium to a level enabling maintenance of temperature 10 degrees Celsius in dwellings and 5 degrees Celsius in other facilities heated;
- the adjustment of parameters in customers' systems by changing the controller settings on particular thermal nodes.

Supplier can reduce the supply of heat to the limit, which guarantees only maintaining the circulation of the heating medium in the district heating network, which prevent it from freezing in the case of restrictions on sale of coal and electricity consumption.

Under the current provisions, in case of default by heating company established customer service quality standards, the recipient is entitled to a decrease of costs. These issues have been regulated in the Ordinance of the Minister of Economy of 17 September 2010 concerning the detailed principles of the establishment and calculation of tariffs and billing principles for heat supply (Journal of Laws No. 194, item. 1291). Recipients are entitled to a decrease of heat costs in case of default by the energy company terms and conditions of sale of heat in terms of start and end dates of heat supply for heating and planned interruptions in the supply of heat in the summer. In accordance with § 40 of the Ordinance, the amount of discounts, referred to above, shall be determined as follows (if the sales contract does not provide differently):

- if the start or end of the heat supply for heating were delayed in relation to established quality standards of customers' service, discount is 1/30 of the monthly fee for the ordered thermal power for plants in which there was a delay—per each day of delay;
- if the planned interruption in the supply of heat in the summer was longer than the established quality standards of customers' service, discount is 1/30 of the monthly fee for the ordered thermal power for plants, in which there was an extension of a break in the heat supply—per each day extension of the break.

Furthermore, in accordance with § 44 of the tariff regulation, when due to breach by the energy company quality standards of customers' service, thermal power has been reduced (if the sales contract does not provide differently), the recipient

is entitled to a discount, the amount of which is calculated as follows:

- if the thermal power limit is up to 40%, the discount is calculated by the formulas:

$$S_{u40} = S_{um40} + S_{uc40} \quad (5)$$

$$S_{um40} = 0,25 \cdot (\Phi_t - \Phi_r) \cdot 3,6 \cdot 24 \cdot C_n \cdot h_p : 365 \quad (6)$$

$$S_{uc40} = 0,4 \cdot (\Phi_t - \Phi_r) \cdot 3,6 \cdot 24 \cdot h_p \cdot C_c \quad (7)$$

- if the thermal power limit is above 40%, the discount is calculated by the formulas:

$$S_{u40u} = S_{um40u} + S_{uc40u} \quad (8)$$

$$S_{um40u} = 0,5 \cdot (\Phi_t - \Phi_r) \cdot C_n \cdot h_p : 365 \quad (9)$$

$$S_{uc40u} = 0,8 \cdot (\Phi_t - \Phi_r) \cdot 3,6 \cdot 24 \cdot h_p \cdot C_c \quad (10)$$

where:

S_u—the total discount for restrictions in heat providing,
S_{um}—crediting (decrease of cost) for limiting of thermal power,
S_{uc}—crediting for undelivered heat,
Φ_t—thermal power determined on the basis of calculating flow rate and heat carrier parameters specified in regulatory table [MW],
Φ_r—the actual thermal power, determined on the basis of the flow rate and actual parameters of the heat carrier [MW],
24—multiplier, meaning 24 hours a day [h],
h_p—the number of days in which there were lrestriction in the supply of heat, due to breach by the energy company service quality recipients' standards,
C_n—the price for the ordered thermal power for the tariff group [PLN/MW],
C_c—the price of heat for a given tariff group [PLN/GJ].

4 AN EXAMPLE OF DETERMINING THE RISK USING EVENT TREE METHOD

The purpose of the risk, hazards and level of safety assessment in HSS is to create a database of relevant, criterial information, necessary in decision-making, optimization of processes, exploitation and control of systems, as well as in taking protective measures to prevent the occurrence of adverse effects of events. There are many methods of determining the risk. Event tree method is often used in analyzes of technical systems. The concept of the event tree method is to consider the consequences of adverse effect as the result of adverse events during or erroneous evaluations and decisions (Babiarz & Rak, 2002). Then all possible sequences of events, being a consequence of

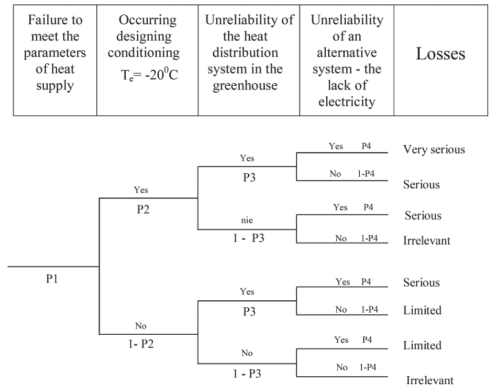


Figure 2. Illustration of event scenario providing greenhouse with heat using event tree.

adverse events in the scenario and their effects are defined. The essence of the method is illustrated in the following example.

A greenhouse is a recipient of technological heat to maintain the proper temperature of the vegetables production process. Alternative heat source is the possibility to use electric power to the provisional, localized heating of the greenhouse capacity. The only security of certainty of heat supply to the greenhouse is reservation of the heating network, supplying heat to heat the greenhouse. The heating medium is supplied to the object by three-wired heating network. One of these three wires is a reserve in the case of failure of any of the two others. Estimation of the risk of incurring identified losses by the owner of the greenhouse is presented is the following example.

Figure 2 presents example of event tree representing a risk for greenhouse facilities, to estimate the loss of the owner. Initiating event is a failure to meet the parameters of heat supply or non-delivery of heat. Then the sequence of possible adverse events is considered in case of occurrence or absence of the computational, design conditions. The one, shown in Figure 2, allows calculating the risk of very serious losses r_{vs}, according to the formula:

$$r_{vs} = P1 \cdot P2 \cdot P3 \cdot P4 \quad (11)$$

In turn, the risk of serious loss r_s is:

$$r_s = P1 \cdot P2 \cdot P3 \cdot (1 - P4) + P1 \cdot P2 \cdot (1 - P3) \cdot P4 + P1 \cdot (1 - P2) \cdot P3 \cdot P4 \quad (12)$$

5 SUMMARY

Risk assessment in HSS is connected with the energy security of the country. Current law

legislations define issues related to energy security, determining the necessity to develop procedures of limitations restrictions in the heat supply by the company in case of emergency. Existing regulations, shaping the issues of decrease of costs, require energy companies to give a discount in the case of occurring certain events failure to meet the quality standards in heat supply service to customers. Very important things in the heat supply management are to assess the risks, inform others of its sizes and initiate actions that must be taken in the face of risk occurring.

The approach to risk assessment, presented in the paper, takes into account the decomposition of HSS system in the analysis of the degree of fulfillment of tasks in the exploitation process. The comprehensive approach to risk assessment in HSS requires its location, identification and classification of hazards, estimation of risk and response to risk, including setting priorities for risk management by comparing the level of risk with pre-established targeted levels of risk. Moreover, monitoring of risk and checking of compliance with established procedures are also necessary. The final product of identification, assessment and measurement of risk in HSS may be risk maps, which are a useful tool in the effective management of centralized heat supply to consumers.

Assessment of risk using the event tree can be useful in countering threats resulting from damage to system components, taking into account the variability of weather conditions affecting the thermal load. It may be an additional element in the conduction of preventive activities, related to prevention of damage, standardization of repairs, as well as in the development of emergency scenarios.

The subject of risk in HSS requires further in-depth analysis, based on the available tools and methods, and particularly determining the required level of risk.

REFERENCES

Arunraj N.S. & Maiti J. 2007 Risk—based maintenance—Techniques and applications. *Journal of Hazardous Materials* 142/2007.

Aven T. 2012 Foundational Issues in Risk Assessment and Risk Management. *Risk Analysis, Vol. 32, No. 10.*

Babiarz B. 2006. An introduction to the assessment of reliability of the heat supply systems. *International Journal of Pressure Vessels and Piping,* Volume 83, Number 4/2006, 230–235 Elsevier.

Babiarz B. 2014: Heat supply system reliability management. *European Safety and Reliability Conference ESREL*, Wroclaw 2014.

Babiarz B. & Rak J. 2002. The preliminary analysis of risk evaluation in a heat supply system. International Conference of Air Conditioning & District Heating. Szklarska Poręba.

Młyńczak M., Nowakowski T. & Vališ D. 2011. How to manage risk? An approach based on standards. Maintenance problems, 2011, vol. 1, no. 80, p. 137–148.

PN-EN-1050. Zasady oceny ryzyka, 1999.

PN-IEC 60300-3-9. Analiza ryzyka w systemach technicznych, 1999.

Rak J., Babiarz B., Tchórzewska-Cieślak B. & Studziński A. 2005: O podstawowych uwarunkowaniach analiz i ocen ryzyka. *Gaz Woda i Technika Sanitarna* nr 11/2005.

Smith D.J. 2001 Reliability, Maintainability and Risk. Practical methods for engineers. Butterwort Heinemann.

The Act of 10 April 1997 on the Energy Law. *Journal of Laws* No. 54, item. 384, as amended.

Vališ, D. & Zając M. 2010: Fundamental risk assessment in example of transshipment system. *Reliability & risk analysis: theory & applications; Electronic journal of international group on reliability*, No. 4.

Werbińska, S. 2006: Risk analysis of logistic customer service—case study of Nashuatec products distribution network. Safety and reliability for managing risk. Vol. 2, Eds. C. G. Soares, E. Zio. Leiden: Taylor and Francis, pp. 1127–1135.

Zio, E. 2009. Computational Methods for Reliability and Risk Analysis. *World Scientific Publishing* Co., London.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Vulnerability of Energy Infrastructure to intentional attacks—the interplay of resource, conflict and security

P. Burgherr
Laboratory for Energy Systems Analysis, Paul Scherrer Institute, Villigen PSI, Switzerland

J. Giroux
Center for Security Studies, ETH Zürich, Zürich, Switzerland

M. Spada
Laboratory for Energy Systems Analysis, Paul Scherrer Institute, Villigen PSI, Switzerland

ABSTRACT: Attacks against critical energy infrastructures have recently become an increasingly important factor in energy security discussions. Studies examining such threats often focus on particular aspects like terrorist threats or resource conflicts. Therefore, the recently established Energy Infrastructure Attack Database (EIAD) has a much broader scope by considering attacks towards energy infrastructures that are carried out by a broad range of Violent Non-State Actors (VNSAs). The current study analyzed energy infrastructure attacks with regard to their spatial and temporal clustering patterns to identify and describe differences between countries as well as temporal shifts within a specific country. In this way the observed patterns could be conceptualized as a type of tactical contagion.

This paper presents an analysis of EIAD, which contains about 8600 entries of intentional attacks worldwide for the period 1980–2011. In this study we found that "linear infrastructures" such as transmission lines and pipelines are predominantly targeted because they often run through rather remote areas and are thus difficult to protect compared to "point" sources (e.g. refineries, power plants). Geo-referencing of EIAD data allowed for identifying distinct country/region hotspots, which we conceptualize as attack clusters. Furthermore, the temporal patterns and underlying mechanisms (e.g. tactical contagion) creating these clusters were analyzed. In summary, EIAD offers a comprehensive basis for the quantitative evaluation of energy infrastructure attacks by VNSAs, and provides decision and policy makers with objective facts and recommendations, which are an essential component for contemporary debates on energy security.

1 INTRODUCTION

In an age of increasing complexity and uncertainty risk management has become a default component and practice of many different organizations, assets, processes, etc. Consequently a variety of theoretical concepts, approaches and methodologies have been developed (Aven and Zio, 2012). However, in general, risks are often analyzed in the context of their potential impacts on human health and the environment as well as economic losses (Jonkman et al., 2003), and assessments are used as tool to provide an objective and transparent evaluation that enables informed decision-making. For this purpose, the choice of adequate and understandable risk metrics is indispensable (Johansen and Rausand, 2014). In general, three basic risk management strategies, or risk-based approaches, can be distinguished, including: threshold levels, risk reduction activities using the precautionary principle, and standards derived from discursive processes (Klinke and Renn, 2002, Stirling, 1999). Furthermore, risk and sustainable assessment are partially linked and complementary concepts because in practice they are both often measured by means of indicators, and are concerned about the future. (Gray and Wiedemann, 1999).

The need for a comprehensive risk assessment framework in the energy sector has been expressed by different authors since the 1980s (Fritzsche, 1989, Inhaber, 2004, Rasmussen, 1981). In the 1990s, the Paul Scherrer Institut (PSI) laid the foundations for a methodological approach that allows a transparent and objective quantification of accident risks and their comparison across different energy technologies (Hirschberg et al., 1998). The Energy-related Severe Accident Database (ENSAD) constitutes its core component, and since its initial release it has been regularly updated and extended (e.g., Burgherr et al., 2014). Therefore, the risks of technological accidents in the energy sector and their potentially disastrous consequences are

nowadays included in a comprehensive assessment of sustainability and energy security concerns (Burgherr and Hirschberg, 2014, Burgherr et al., 2013).

In contrast, intentional attacks against critical energy infrastructures have only recently emerged as an increasingly important factor in energy security discussions. This is primarily due to the growing dependence on oil and gas imports from regions considered less reliable and stable, but also large-scale imports of new renewables could lead to increased energy security vulnerabilities (Lacher and Kumetat, 2011, Lilliestam, 2014). Despite growing interest, intentional attacks against energy infrastructures have yet to receive the same analytical treatment as accident risks. Studies examining such threats often focus on particular aspects like terrorist threats (Luft and Korin, 2003, Toft et al., 2010), maritime piracy (Pristrom et al., 2013) or resource conflicts (Rodgers and O'Neill, 2012), and thus do not address the entire picture nor complexity of the topic and hence miss a big part of the risk picture, which in turn impacts assessments. To fill this gap, the present study aims to provide a much broader perspective by considering attacks towards energy infrastructures that are carried out by Violent Non-State Actors (VNSAs), spanning the full motivational and tactical spectrum. For this purpose, the Energy Infrastructure Attack Database (EIAD) was developed, ensuring a consistent data basis.

The main objectives of this article are threefold, namely (1) to introduce and describe this new dataset, (2) to present an initial analysis of the data between 1980–2011, and (3) to discuss potential future research directions.

2 METHODS

2.1 *EIAD database*

The EIAD database is a joint effort of the Center of Security Studies (CSS) of the Swiss Federal Institute of Technology (ETH) and the Technology Assessment (TA) group at the PSI. It has been initiated in 2010, and by now it can be considered a fully matured and comprehensive information source on Energy Infrastructure (EI) attacks that are executed by Violent Non-State Actors (VNSA). Although EIAD is not completely different from other databases, it has some unique features. Databases such as the Global Terrorism Database (GTD) (LaFree and Dugan, 2007) or the Worldwide Incidents Tracking System (WITS) (Wigle, 2010) are focused on the terrorist threat only, but include attacks from all types of sectors and activities. In contrast, EIAD considers all kinds of criminal and politically motivated attacks that are targeted at energy infrastructures. Other outstanding characteristics of EIAD are that it contains successful, failed and foiled attacks, and that it does not code for motivation that is often difficult to accurately determine, but rather for attack type (e.g. bombing, assault, hijacking, etc.).

EIAD has a modularized and standardized data record structure that comprises the following elements:

- EIAD ID: uniquely identifies each database record
- Incident Date
- Incident Location: country, location description (e.g. city name), latitude and longitude coordinates
- Incident information: event type, multiple attack (Y/N), free text summary
- Attack information: primary attack type, secondary attack type (if applicable), instruments used (e.g. explosive, firearms, arson, etc.), combination attack (Y/N)
- Target information: energy sector (e.g. petroleum, gas, etc.), energy infrastructure (e.g. pipeline, refinery, etc.), specific target (free text), second target (if applicable)
- Perpetrator information: group/actor, claim responsibility (Y/N), motive (free text)
- Incident consequences: fatalities, casualties, reported downtime, infrastructure impact (ordinal scale), hostage situation (Y/N), number of hostages, ransom paid (amount)
- Additional information; further event details (free text)
- Source information (up to three primary data sources)

For a more extensive description of EIAD see Giroux et al. (2013).

2.2 *Characterization of data set*

EIAD covers the period 1980–2011, which formed the basis for the analyses performed in this study. It should be noted that in the past months the contents of EIAD has been completely reviewed, and where necessary modified and updated. Therefore, the current analysis can partially differ from previous ones (e.g., Giroux et al., 2013), reflecting the continuous improvements of the database. Data for years 2012 and 2013 were not included because the validation and verification has not yet been fully completed.

First, a general overview and basic characterization of the EIAD data set was performed. This included an evaluation of temporal trends in the annual attack numbers, using the non-parametric Mann–Kendall test (Mann, 1945). A positive (negative) value of the Z-statistic identifies

an upward (downward) trend at the chosen significance level $\alpha = 0.05$.

Calculations were performed with the MS Excel application MAKESENS (Salmi et al., 2002).

2.3 *Frequency distributions of attacks*

In a second step, different distributions were fitted to the data (full data set and individual countries that contribute at least 2.5% to all attacks) to determine the model that best describe the attack frequencies.

2.3.1 *Fitting the frequency distribution*

A Maximum Likelihood Estimation (MLE) method was used to fit models on the frequency dataset. MLE is a common statistical technique for es-timating model parameters (e.g., Cousineau et al., 2004). The MLE proceeds to maximize a likelihood function, which in turn maximizes the agreement be-tween the model and the data. In this study the MLE algorithm proposed by Rigby and Stasinopoulos (1996) was applied. This algorithm is converging to the model and it stops once the change in the likelihood is sufficiently small, that is the Global Deviance (GD) reaches the minimum.

When fitting models, the MLE is used to find the optimal fit to the dataset. However, maximizing the log likelihood often results in fitting noise and parameter estimates that are unstable, particularly when the data set is relatively small. This is because MLE trusts too much the observed trends in the, often limited, data (Moons et al., 2004). In order to avoid possible over-fitting, the Bayesian Information Criterion (BIC) was utilized (Schwarz, 1978). BIC is a criterion for model selection, and includes a penalty term for the number of parameters in the model. The BIC is given by the following equation:

$$BIC = -2 * \text{loglikelihood} + d * \log(N)$$

where N is the sample size of the training set and d is the total number of parameters. Thus, similar to the Generalized Akaike Information Criterion (GAIC) (Akaike, 1983), the BIC score gives an estimate of the goodness of fit of the model performance to the dataset. A lower BIC score indicates a better model fit. The BIC was used, since it penalizes complexity more than GAIC (Hastie et al., 2009).

2.4 *Distribution family*

A set of discrete distributions described by a maximum two parameters was chosen to avoid overfitting due to high number of parameters used in the model. The following probability distributions were fitted to the EIAD data:

- Negative Binomial distribution (NBI)
- Geometric distribution (GEO); a special case of the NBI
- Poisson distribution (POI)
- Zero-inflated Poisson model (ZIP); allows for frequent zero-valued observations
- Zero-adjusted Poisson model (ZAP); useful when count data with too few or too many zeroes are encountered

2.5 *Spatial distribution of EIAD data*

Geo-referenced EI attacks were imported into ArcGIS (ESRI, 2006) to produce a world map that visualizes and explores specific aspects of the data. Additionally, Kernel density estimation was used to calculate the density of features (e.g. points) in a neighborhood around those features, i.e. a smoothly curved surface is fitted over each point (Silverman, 1986). Lastly, spatial statistics were used to determine if energy infrastructure attacks were clustered or dispersed (randomly distribution) in space. The Average Nearest Neighbor Distance measures the distance between each point (EI attack) and its nearest neighbor's centroid location. All these nearest neighbor distances are then averaged, and if the average distance is less than the average for a hypothetical random distribution, the distribution is considered clustered (Ebdon, 1985). Moran's I calculates spatial autocorrelation (feature similarity), based not only on feature locations (EI attacks) or attribute values (e.g. decade, attack type, perpetrator group, etc.) alone, but on both feature locations and attribute values simultaneously. Given a set of features and an associated attribute, it evaluates whether the pattern expressed is clustered, dispersed, or random (Moran, 1948).

2.6 *Energy infrastructure attack hotspots*

Temporal peaks or hotspots were evaluated using data of individual countries that at least contributed 2.5% to the total of all (see chapter 2.3) to ensure that sufficient data was available. Three peak levels were defined, i.e. a high peak is a year with 200 or more attacks, a medium peak is between 100 and 199 attacks, and a low peak is between 50 and 99 attacks.

3 SELECTED RESULTS

3.1 *Overview and contents of EIAD*

In total, EIAD contains 9432 energy infrastructure attacks, covering the period 1980–2011.

Figure 1 shows the number of attacks per year (blue bars), the cumulated attacks over the observation period (red line), and averages per decade (black line). In the 1980s and 1990s the average number of attacks per year increased only slightly from 184 to 197, whereas in the 2000s it more than doubled (471). The two years available for the 2010s (526) indicate that a further increase could be expected if no drastic changes in the overall situation and/or boundary conditions will occur in the next few years. The apparent overall upward trend in EI attacks was also statistically confirmed by a non-parametric Man-Kendall test ($n = 32$, $Z = 3.84$, $p = 0.001$).

It is worthwhile to note that the year 1993 seems to be a substantial outlier to this trend with only 15 attacks; however it does not affect the prevailing pattern. This can be illustrated by replacing the 1993 value by the average of 1992 and 1994, which increases the decade average by a modest 8%, and which is reported above and shown in Figure 1. The very low 1993 value can be explained by the fact that the Global Terrorism Database (GTD) is one of the major primary information sources used for EIAD. The data for 1993 were unfortunately lost prior to the compilation of the GTD from various data collection efforts, and several attempts to recover the data did not succeed (GTD, 2012). However, cumulated country level statistics in the same GTD document suggest that GTD should contain almost 5000 incidents for 1993. Although a dedicated effort within the EIAD framework was carried out, it was not possible to obtain a better coverage of individual EI attacks for 1993, which is why EIAD currently has the same data gap for 1993 like GTD.

The vast majority of attacks was classified as successful (95.3%), distantly followed by failed (3.7%) and foiled (0.8%) attacks. The remaining 0.2% are plots, threats or unknown. A rather large amount of 43.7% was considered multiple attacks.

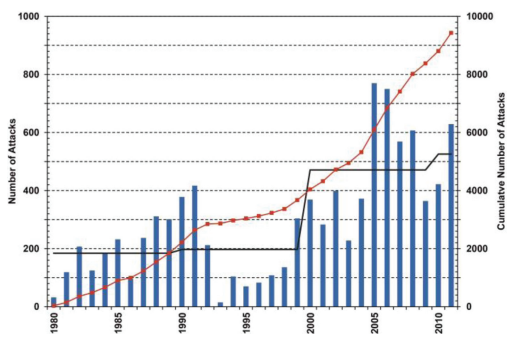


Figure 1. Annual number of EI attacks (blue bars), cumulated attacks (red line), and decadal averages (black line) over the period 1980–2011.

Bombings (82.3) are the dominant attack type, followed by several other attack types that cumulatively amount to 13.6%, of which assault, hostage taking/kidnapping, sabotage, hijacking, assassination and looting/theft were between 1% and 5%. The remaining categories were practically negligible with a share of 0.5%. Finally, 3.6% of all attacks could not be assigned to a specific category because of incomplete information in the available incident summary, and thus were classified as unknown.

The electricity and petroleum sectors account for 54.4% and 36.6%, respectively. The natural gas sector makes up only 7.4%, and all other sectors are almost negligible. A possible reason for this pattern could be that attacks predominantly target "linear" energy infrastructures (e.g. pipelines and transmission lines) that are difficult to protect, and also often pass through remote areas. In contrast, "point sources" such as power plants or refineries can be more easily controlled and secured.

3.2 *Frequency distributions of attacks*

Table 1 shows the BIC scores for the five probability distributions that were fitted to all attacks, and to those countries that have a share of at least 2.5% of all attacks. The Negative Binominal distribution (NBI) fits clearly better than the Poisson distribution, as indicated by the substantially lower BIC scores. The Geometric distribution (GEO), which is a special case of the NBI, performs practically the same. Similarly, the Zero-Inflated (ZIP) and Zero-Adjusted (ZAP) Poisson models are only marginally different from the POI. The NBI has the following advantages compared to the POI:

– The NBI has two parameters unlike the POI with one parameter, which allows adjustment of the variance independently of the mean value.

Table 1. BIC scores of the five probability distributions fitted to the entire EIAD dataset (1980–2011) and the eight countries in which at least 2.5% of all attacks occurred. # Att = number of attacks; see chapter 2.4 for abbreviations of distributions.

Country	# Att.	**NBI**	GEO	POI	ZIP	ZAP
All countries	9432	**418**	429	2584	2587	2587
Colombia	2490	**410**	421	2378	2382	2382
Iraq	1188	**350**	353	1501	1505	1505
Pakistan	1070	**344**	346	1353	1357	1357
El Salvador	840	**401**	400	3422	3425	3425
Peru	532	**316**	323	909	912	912
Nigeria	307	**350**	353	1501	1505	1505
Afghanistan	262	**418**	429	2584	2587	2587
India	240	**374**	375	2395	2399	2399
Chile	234	**414**	424	2481	2484	2484

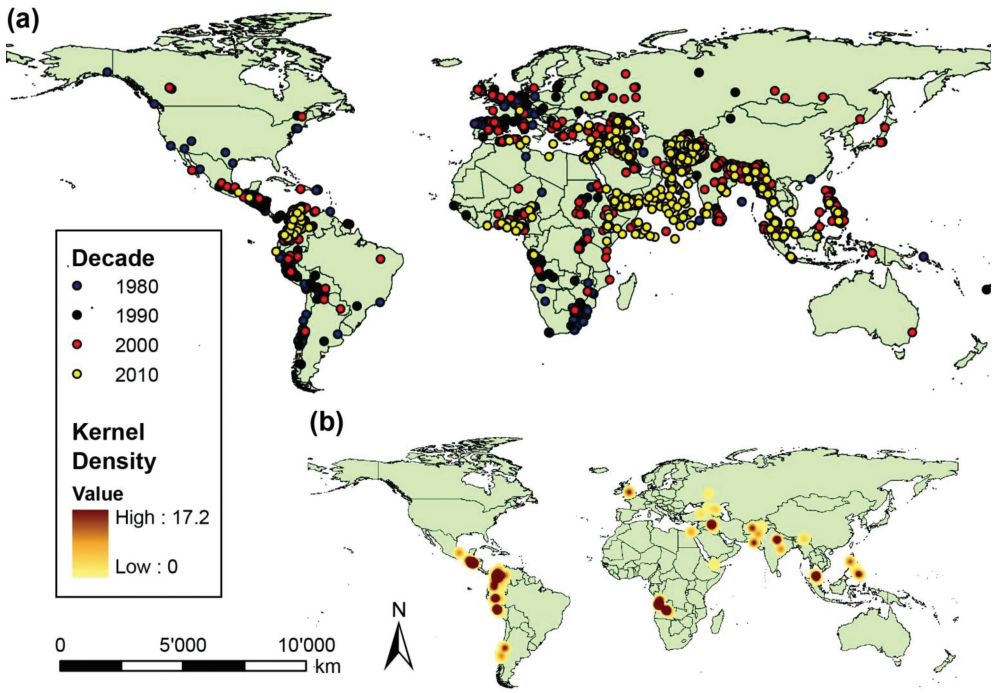


Figure 2. Spatial distribution of EI attacks in the period 1980–2011 (n = 8549). The upper panel (a) shows attacks by decade, and the lower panel (b) displays hotspots areas based on point Kernel density estimation.

Table 2. Results of average nearest neighbor and Moran's I.

	All	Petroleum	Electricity
Average Nearest Neighbor	Clustered Z = –158.72 p < 0.01	Clustered Z = –18.37 p < 0.01	Clustered Z = –50.78 p < 0.01
Morans's I (attribute: Decade)	Clustered I = 0.36 Z = 14.75 p < 0.01	Random I = 0.03 Z = 0.99 p > 0.1	Clustered I = 0.41 Z = 16.13 p < 0.01

– The NBI is especially useful for discrete data with a finite number of confounded positive values whose sample variance exceeds the sample mean.
– Therefore, values of the NBI are more dispersed compared to values of POI.

3.3 *Spatial distribution of EIAD data*

The spatial distribution of EI attacks by country for the years 1980–2011 is given in Figure 2. Only events that could be accurately geo-referenced were considered, which is why only 8549 out of all 9432 EI attacks were included.

The color coding scheme in Figure 2a distinguishes attacks by decades. Already a quick visual inspection suggests that data are clustered. A Kernel density estimation was used to produce a smoother distribution of values to better designate potential hotspot areas (Fig. 2b). Results of spatial statistics are summarized in Table 2. Average nearest neighbor analysis confirmed a clustered pattern for all EI attacks as well as for the dominant petroleum and electricity sectors. Spatial autocorrelation (Moran's I) with decade as the attribute value, indicated clustering for all EI attacks and electricity, whereas for petroleum a random pattern was found.

3.4 *Energy infrastructure attack hotspots*

Figure 3 shows attack patterns for individual countries that at least contributed 2.5% to the total number of attacks in the period 1980–2011. High peaks (≥200 attacks) were only found in the top three countries (Fig. 3a), and medium peaks (≥100) were also quite common. For countries ranked positions four to nine only few medium peaks occurred, but low peaks (50–99 attacks) were more common. In the following individual patterns for the top three countries are briefly described.

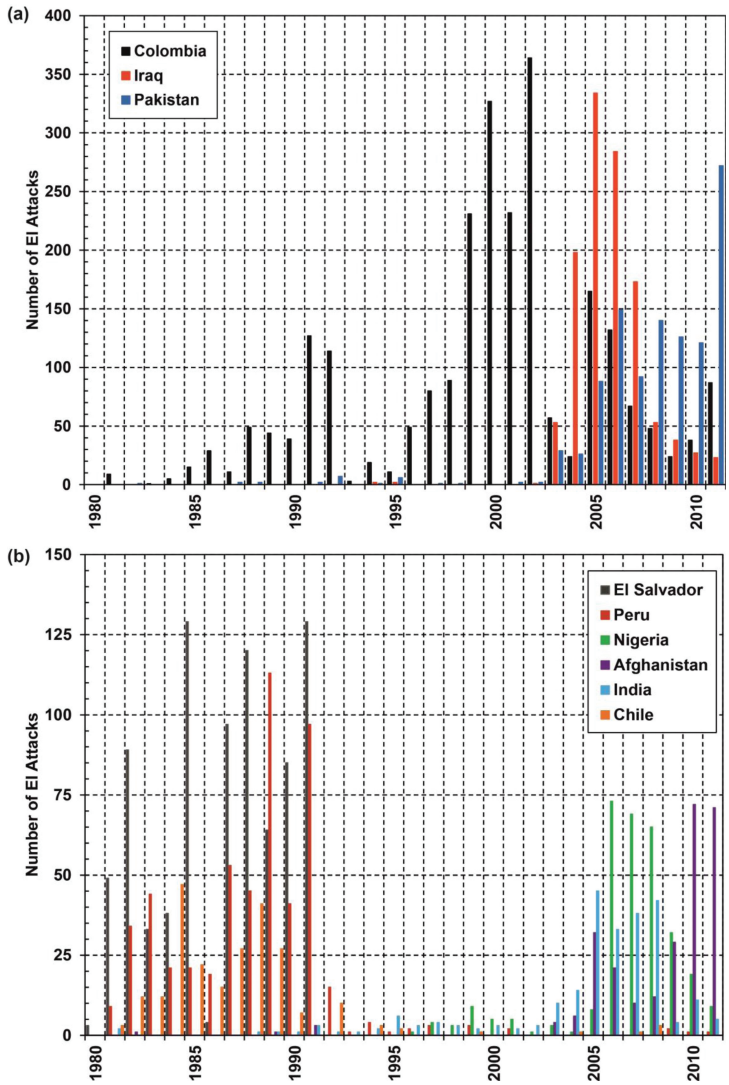


Figure 3. Annual numbers of EI attacks for (a) the top three countries, and (b) the countries ranked fourth to ninth (all contributing at least 2.5% to the total of EI attacks in the period 1980–2011).

For Colombia, three distinct peaks of EI attacks can be observed, i.e. 1991–1992 (medium peak), 1999–2002 (medium to high), and 2005–2007 (low-medium). It is worthwhile to note that annual attacks after the third peak generally remained at higher levels than before the first peak, indicating that the situation is still fragile. The first peak is predominantly attributable to the petroleum sector and attacks on the Cano Limon pipeline. The second peak phase was targeted towards transmission lines in the energy sector, and to a lesser extent this was also the case for the third peak. In Iraq, the medium-high peak from 2004–2007 was mostly due to attacks on oil pipelines. In Pakistan a shift from attacks on transmission lines (2004–2005) to natural gas pipelines (2006–2009), and most recently oil transport by road tanker (2010–2011) was observed.

4 CONCLUSIONS

Overall, EIAD provides a comprehensive foundation for the analysis of energy infrastructure

attacks by VNSAs. Framed within the risk analysis, it was found that while technological accidents in the energy sector are normally rare and independent events, EI attacks are often multiple events and concentrated both in time and space, resulting in distinct hotspots.

The current study evaluated the spatial and temporal clustering patterns of EI attacks in the context of affected energy sectors and infrastructure types. In this way differences between countries as well as temporal shifts within a specific country were identified, and thus the observed patterns could be conceptualized as a type of tactical contagion.

The majority of attacks targeted "linear" energy infrastructures (e.g. pipelines and transmission lines) which are difficult to protect and often pass through remote areas. Therefore, consequences in terms of fatalities and casualties were mostly minor, although when attacks occur frequently (in terms of multiple and connected events), they can result in substantial business and supply disruptions.

The analysis of EIAD data at a macro level has already led to interesting and useful insights and conclusions. However, detailed case studies at the community or micro-level as well as predictive modeling to forecast likely future hotspots could support adapting existing or developing new strategies and policies to contain or mitigate emerging conflict situations.

REFERENCES

Akaike, H. 1983 Information measures and model selection. *Bull. Int. Statist. Inst.,* 50, 277–290.

Aven, T. & Zio, E. 2012 Foundational issues in risk assessment and risk management. *Risk Analysis,* 32, 1647–1656.

Burgherr, P., Eckle, P. & Hirschberg, S. 2014 Comparative risk assessment of severe accidents in the energy sector based on the ENSAD database: 20 years of experience. IN Steenbergen, R.D.J.M., Van Gelder, P.H.A.J.M., Miraglia, S. & Vrouwenvelder, A.C.W.M. (Eds.) *Safety, Reliability and Risk Analysis: Beyond the Horizon.* London (UK), Taylor & Francis Group.

Burgherr, P. & Hirschberg, S. 2014 Comparative risk assessment of severe accidents in the energy sector. *Energy Policy,* (in press, available online).

Burgherr, P., Hirschberg, S. & Spada, M. 2013 Comparative assessment of accident risks in the energy sector. IN Kovacevic, R.M., Pflug, G.C. & Vespucci, M.T. (Eds.) *Handbook of risk management in energy production and trading.* New York (USA), Springer Science+Business Media.

Cousineau, D., Brown, S. & Heathcote, A. 2004 Fitting distributions using maximum likelihood: Methods and packages. *Behavior Research Methods Instruments & Computers,* 36, 742–756.

Ebdon, D. 1985 *Statistics in Geography. 2nd eEdition*, London (UK), Blackwell.

ESRI 2006 *ArcGIS 9.2,* Redlands (CA), USA, Environmental Systems Research Institute Inc. (ESRI).

Fritzsche, A.F. 1989 The health risks of energy production. *Risk Analysis,* 9, 565–577.

Giroux, J., Burgherr, P. & Melkunaite, L. 2013 Research Note on the Energy Infrastructure Attack Database (EIAD). *Perspectives on Terrorism,* 7, 113–125.

Gray, P.C.R. & Wiedemann, P.M. 1999 Risk management and sustainable development: mutual lessons from approaches to the use of indicators. *Journal of Risk Research,* 2, 201–218.

GTD 2012 Global Terrorism Database codebook: inclusion criteria and variables. National Consortium for the Study of Terrorism and Responses to Terrorism.

Hastie, T., Tibshirani, R. & Friedman, J. 2009 *The elements of statistical learning: Data mining, inference, and prediction*, Springer.

Hirschberg, S., Spiekerman, G. & Dones, R. 1998 Severe accidents in the energy sector—first edition. PSI Report No. 98-16. Villigen PSI, Switzerland, Paul Scherrer Institut.

Inhaber, H. 2004 Risk analysis applied to energy systems. IN Cleveland, C.J. (Ed.) *Encyclopedia of Energy, Volume 5.* Amsterdam, The Netherlands, Elsevier.

Johansen, I.L. & Rausand, M. 2014 Foundations and choice of risk metrics. *Safety Science 62,* 62, 386–399.

Jonkman, S.N., van Gelder, P.H.A.J.M. & Vrijling, J.K. 2003 An overview of quantitative risk measures for loss of life and economic damage. *Journal of Hazardous Materials* 99, 1–30.

Klinke, A. & Renn, O. 2002 A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Analysis,* 22, 1071–1094.

Lacher, W. & Kumetat, D. 2011 The security of energy infrastructure and supply in North Africa: hydrocarbons and renewable energies in comparative perspective. *Energy Policy,* 39, 4466–4478.

LaFree, G. & Dugan, L. 2007 Introducing the Global Terrorism Database. *Terrorism and Political Violence,* 19, 181–204.

Lilliestam, J. 2014 Vulnerability to terrorist attacks in European electricity decarbonisation scenarios: Comparing renewable electricity imports to gas imports. *Energy Policy,* 66, 234–248.

Luft, G. & Korin, A. 2003 Terror's next target. *The Journal of International Security Affairs,* http://www.iags.org/n0111041.htm.

Mann, H.B. (1945) Nonparametric test against trend. *Econometrica* 13, 245–259.

Moons, K.G.M., Donders, A.R.T., Steyerberg, E.W. & Harrell, F.E. 2004 Penalized maximum likelihood estimation to directly adjust diagnostic and prognostic prediction models for overoptimism: a clinical example. *Journal of Clinical Epidemiology,* 57, 1262–1270.

Moran, P. 1948 The interpretation of statistical maps. *Journal of the Royal Statistical Society B,* 10, 243–251.

Pristrom, S., Li, K.X., Yang, Z. & Wang, J. 2013 A study of maritime security and piracy. *Maritime Policy & Management,* 40, 675–693.

Rasmussen, N.C. 1981 The application of probabilistic risk assessment techniques to energy technologies. *Annual Review of Energy,* 6, 123–138.

Rigby, R.A. & Stasinopoulos, D.M. 1996 A semi-parametric additive model for variance heterogeneity. *Statistics and Computing,* 6, 57–65.

Rodgers, D. & O'Neill, B. 2012 Infrastructural violence: Introduction to the special issue. *Ethnography,* 13, 401–412.

Salmi, T., Määttä, A., Anttila, P., Ruoho-Airola, T. & Amnell, T. (2002) Detecting trends of annual values of atmospheric pollutants by the Mann-Kendall test and Sen's slope estimates—the Excel template application Makesens. Helsinki (Finland), Finnish Meteorological Institute.

Schwarz, G. (1978) Estimating the dimension of a model. *Ann. Statist.,* 6, 461–464.

Silverman, B.W. 1986 *Density Estimation for Statistics and Data Analysis,* New York (USA), Chapman and Hall.

Stirling, A. (1999) On science and precaution in the management of technological risks. Final report for the EC Forward Studies Unit under auspices of the ESTO network. Report EUR 19056 EN. Brussels (Belgium), European Commission.

Toft, P., Duero, A. & Bieliauskas, A. 2010 Terrorist targeting and energy security. *Energy Policy,* 38, 4411–4421.

Wigle, J. (2010) Introducing the Worldwide Incidents Tracking System (WITS). *Perspectives on Terrorism,* 4, 3–23.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Solar storm impact on critical infrastructure

O. Sokolova
Reliability and Risk Engineering Laboratory, ETH Zurich, Zurich, Switzerland

P. Burgherr
Paul Scherrer Institute, Villigen, Switzerland

W. Collenberg
Swiss Reinsurance Company Ltd., Zurich, Switzerland

ABSTRACT: Natural hazards can trigger disasters resulting in large numbers of fatalities and billions of economic losses. In the last decades, critical infrastructures were developed in the way to ensure their stability against natural hazards. Consequently, long, divaricated, interconnected systems were constructed. Hence, such diversification increases systems vulnerability against solar storm. Hydro-Quebec blackout in 1989 was the tipping point for space weather research, shifting status from curiosity to necessity. Despite dedicated research, the widespread outages and economic losses resulting from the relatively strong Halloween blackout in 2003 could not be prevented. The analysis of solar storm impact on critical infrastructure consists of two main parts: the geoelectric field determination associated with geomagnetic storm variations; and the determination of the network vulnerability with known topology. The quantitative assessment of possible solar storm impact on the Scandinavian power system and comparison of geographical areas will be given in the paper.

1 INTRODUCTION

Solar storms are known to affect critical infrastructure, especially power systems by causing voltage blackouts and equipment outage. The first registered impact on galvanic systems is Carrington Event in 1859. The solar storm lasted for six days: 28th August—2nd September 1859, and interrupted normal telegraph operation on large geographical area (UK, France, USA, and Canada). Mr. Wood, superintendent of Canadian Telegraph lines, described the event as follows: so completely were the lines under the influence of aurora borealis, that it was found impossible to communicate between the telegraph stations, and the line was closed for the night. It is still the strongest ever registered solar storm. The event of such strength is called nowadays "Super solar storm".

An extensive research of solar storm phenomena concurred with space exploration era after the launch of first satellite in 1957. Even though the principle of solar storm coupling with Earth magnetic field is evident, the variety of heliophysics questions are in nowhere. The questions are following: what drives the solar wind and where does the coronal magnetic field originate from? how do solar transients drive heliospheric variability? how do solar eruptions produce energetic particle radiation that fills the heliosphere? and others.

Geomagnetically Induced Currents (GIC) which are studied in this paper are so-called echo of solar storm on Earth. The varying Earth's magnetic field associated with geoelectric field induces currents due to Faraday's law. In accordance to Ohm's law, currents lead to transmit over the system of conductors with the lowest resistivity. Power grid can be considered as the sample of such a system. The source of GIC in power grid is the grounding points of power system equipment. By entering the power grid, GIC are distributed over the transmission lines, which might cause equipment outage. A power grid performs like an antenna in the presence of GIC by amplifying the negative impact. The majority of power system equipment is no barriers for GIC distribution.

Not all solar storms affect the power grids. The National Oceanic and Atmospheric Administration (NOAA, USA), European Incoherent Scatter Scientific Association and other agencies provide storm forecasting products in an index-style severity classification. The most familiar one is the K-index, a logarithmic scale from 0 to 9 that classifies the severity of solar storms in a similar way to the Richter scale. All "super solar storms" correlate with K equal to 9. Nevertheless, weaker

solar activity may also interrupt normal power system operation.

The structure of this paper is as follows. First in Section 2, we describe the principles of GIC determination and the studied model. In Section 3, the impact of GIC on power system equipment and on the network as a whole is discussed. Finally in Sections 4 and 5, we discuss possible mitigation actions and do the comparison of power grid vulnerability in different geographical areas.

2 MODELLING TECHNIQUE

2.1 *Calculation scheme*

In general, the following set of factors determines solar storm impact on power systems (Marusek 2007):

- geomagnetic latitude;
- ground conductivity;
- power grid topology and characteristics;
- installed power equipment characteristics.

Scandinavian power grid is located in the northern geomagnetic latitude (aurora region), which makes it liable to space weather impact. In the past years, disturbances of normal power system operation as the result of solar storms were registered in Scandinavian grid. The most famous one is Halloween blackout in 2003. Also one of the highest ever determined GIC (200 A in power transformer neutral) was registered in Finish power grid a part of Scandinavian grid. Thereby, equivalent High Voltage (HV) Scandinavian power grid is studied.

Detailed power system characteristics are not available in the open source because of security reasons. The interconnected ENTSOE network model was used. The final model has a realistic number of nodes and lines and emulates the real processes. The total number of nodes is 150. The simplified calculation scheme is represented on Figure 1.

In (Viljanen et al. 1999) was shown that the reasonable understanding of GIC flow can be achieved

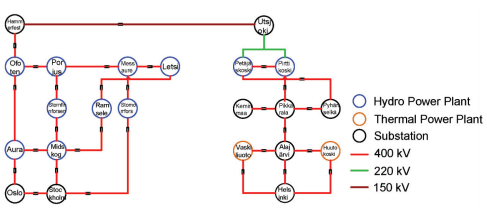


Figure 1. Simplified equivalent Scandinavian power grid model.

even with incomplete data. The final model is described by the following set of characteristics:

- Not all network elements are included.
- The nodes locations are given with varying accuracy up to 20 km.
- All transmission lines are assumed to be straight if no detailed information was found.
- All nodes are far enough from each other to prevent them from bearing each other (Pirjola 2008).

The resistivity of 400 kV lines is taken equal to 0.008 Ω per km (Viljanen et al. 2012). Thereafter the resistivity values of 220 and 110 kV lines were taken as 0.012 Ω per km and 0.016 Ω per km in accordance with the physical dependences between the voltage level and conductor resistivity.

The calculation model was represented as the direct current scheme because the GIC are considered to be the quasi Direct Currents (DC) since their frequency is much lower than the nominal operational frequency (50 or 60 Hz). In the same manner, transmission lines with installed series compensators were neglected, since they perform as barrier to GIC.

2.2 *Geomagnetically induced currents determination*

The analysis of geomagnetic storm impact on power systems consists of two parts:

- Location determination. The geoelectric field determination associated with geomagnetic disturbances.
- Technical arrangement. The GIC determination in the known conductor system due to the geoelectric field variation.

The determination of quantitative dependences between GIC and the electro physical characteristics of structural elements of the Earth's crust is one of the most important and complicated tasks of modern geophysics. The geophysical part does not depend on network configurations and parameters. The input data consists of knowledge concerning ground conductivity and geomagnetic variations at the Earths surface. The used geometrical model for geoelectrical field calculation is shown on Figure 2.

Reflected magnetic field B_x is directed in east-west direction since it is the preliminary direction for geomagnetic field distribution (Marusek 2007). Magnetic permeability is equal to the one in vacuum $4\pi 10^{-7}$ H per m. Ground conductivity is constant. Exact value was taken from the results of European Resistivity Ohm Model (EUROHOM) project. On the basis of Maxwell equations, the analytical dependence between the geolectirc field

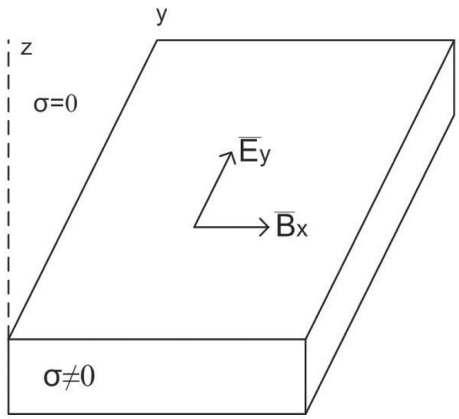


Figure 2. Geometrical model for geoelectric field calculation.

on Earths surface and measured geomagnetic field variation is following:

$$E_y = \frac{(1+j)B_x}{\mu_0 \sigma \delta_e}, \tag{1}$$

where μ_o = magnetic permeability in vacuum; σ = ground conductivity; and δ_e = penetration depth.

Geoelctic field variations are calculated for five geomagnetic severities (from minor to extreme) and six frequencies (10–5–1 Hz). The voltage difference over the branch is calculated by integrating the projected electric field across the path. Since all the HV equipment is grounded, the voltage node difference method is used for GIC determination.

$$GU = J, \tag{2}$$

where G = node conductivity matrix; U = voltage node vector; and J = current source vector.

Obtained results showed that GIC distribution significantly depends on grids topology and characteristics. This dependence is more expressed than the dependence on geomagnetic latitudes in the regions with constant ground conductivity e.g. Scandinavia. This allows us to postulate that mid latitude power systems may also experience negative solar storm impact if they were designed without considering space weather impact.

3 POWER SYSTEM OPERATION RISK ASSESSMENT

3.1 *Power transformer performance*

Power transformer is the key element of reliable power system operation. The power transformers differ from other types of power system equipment as their design, production and operation involve high cost and long time period. In terms of solar storm, the power transformer replacement period is longer than for any other types. Power transformers are designed for normal operation under sinusoidal Alternative Current (AC). The principle of transformers operation is based on the Faradays law, which states that the electromotive force is proportional to the rate of change of the magnetic flux. GIC as the DC component can cause power transformers saturation. Only few amperes and seconds can disrupt normal operation. For example, the interval between the time when electromagnetic impulse interrupted Earths magnetic field and Hydro Quebec blackout was only 92 seconds.

The features of power transformers saturation process depend on construction type. Two common power transformer types exist: shell and core type. Generally, transformers of both types can be constructed for any nominal power or voltage level and from any magnetic material. Nevertheless, the construction type does not influence the functional principle, electromagnetic processes or the ability to ensure required outputs. The set of following characteristics determines the transformers saturation capability: DC flux path, moment of GIC appearance and insulation characteristics.

3.1.1 *Direct current flux path*

Power transformers magnetic characteristics are determined by following parameters: steel type, mark-to space ratio, magnetic conductivity, coil dimensions, specific power losses at the nominal frequency and dependence between power losses and frequency. These parameters specify winding turn leakage inductance L_S, which in turn determines the length of DC flux path. Winding turn leakage inductance is described by equation (3).

$$L_S = \frac{\mu_0 c_t L_t w^2}{3h_t}, \tag{3}$$

where μ_o = magnetic permeability in vacuum; c_t = winding turn thickness; L_t = winding turn length; h_t = winding turn height; and w = winding number.

In other words, wider is the section for reversal magnetic power flow, higher is the transformers vulnerability. The relative comparison of transformers vulnerability is represented in Table 1.

In three-phase three-limb transformer, DC fluxes compensate each other in the main limbs and connecting yokes. Thereby, this transformer type has the highest resiliency. Test results showed that even in case of impact of GIC equal to 50 nominal magnetization current ($\approx 50A$), the transformer current

Table 1. Relative susceptibility of power transformers.

Transformer type	Relative susceptibility
Single phase	1.0
Three phase seven limb	0.67
Three phase five limb	0.33
Three phase three limb	0.05

will be increased less than two times. Single phase trans-former is the most prone type. The magnetic flux inducted by GIC is closed in the power transformers core on the way of the main magnetic flux (inducted by nominal sinusoidal current). The simulation showed that the impact of GIC equal to nominal magnetization current (1 A in studied case) significantly increases transformer current. The current was increased up to 76 A in condition of base-load current equal to 0.8 A. The comparison of magnetization currents for singlephase and three-phase three-limb power transformers is shown on Figure 3. Since power transformers have complex three-dimensional geometry and consist of linear and non-linear components, the assumption of phase symmetry was accepted for the detailed analysis (Mousavi et al. 2013).

Hence, the passport parameter, which determines power transformers susceptibility to saturation, is no-load current. Higher is the value, higher is the saturation risk under GIC impact.

3.1.2 *Moment of GIC appearance*

The second parameter specifying severity of GIC impact is the current phase at the moment of GIC appearance. The power system steady state is described by the following equation set (4) in case of sinusoidal AC. The sinusoidal phase voltages are:

$$\begin{aligned} e_a &= E_m cos(\omega_n t + \psi) \\ e_b &= E_m cos(\omega_n t + \psi - \rho) \\ e_c &= E_m cos(\omega_n t + \psi + \rho), \end{aligned} \tag{4}$$

where E_m = voltage level; ω_n = nominal grid frequency; ψ = initial phase; and ρ = phase angle.

By knowing the phase voltage, the phase current can be found. Due to phase symmetry, one phase model can be analyzed. Thereby, the steady state phase current is:

$$i_a = I_{nmo} cos(\omega_n t + \psi - \phi), \tag{5}$$

where I_{nmo} = current level in steady state; and ϕ = angle between voltage and current of the same phase.

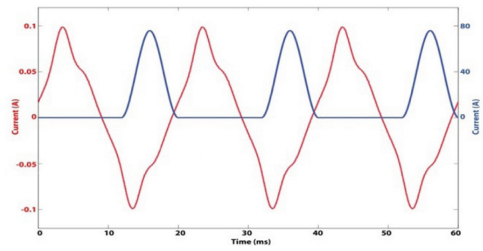


Figure 3. Magnetization current of single phase transformer with GIC equal to nominal magnetization current (red curve) and three-phase thee-limb power transformer with GIC equal to 50 nominal magnetization currents (blue curve).

The phase current under the GIC impact is the solution of following differential equation:

$$e_a = L\frac{di_a}{dt} + ri_a, \tag{6}$$

where L and R = power grid parameters.

Thereby, analyzed current is:

$$\begin{aligned} i_a &= i_{ap} + i_{au} \\ &= I_{nm} cos(\omega_n t + \psi - \phi) - Ae^{\frac{-t}{T_a}}, \end{aligned} \tag{7}$$

where i_{ap} = forced component; $i_a u$ = free component; A = integration constant; and T_a = time constant.

Integration constant can be found as:

$$A = I_{ao} - I_{nm} cos(\psi - \phi), \tag{8}$$

Thereby, criteria for maximum GIC impact are:

1. $\psi = \pi/2$
2. $\omega_n t = \pi$. This corresponds to a moment equal to 0.01 s. in case of power system frequency of 50 Hz.
3. $i_{ao} = 0$ i.e. pre-fault conditions correspond to no-load mode.

3.1.3 *Insulation characteristics*

Inspections of the failed power transformers revealed heat failure, mostly because of paper insulation degradation. GIC can cause immediate or delayed power transformer outage. In the second case, power transformer outage is the result of several solar storms impacts. The diagnostics mechanism with the means of Duval triangle is described in (Gaunt, Charles Trevor 2014).

3.2 *Direct current substations*

Direct current transmissions have several advantages contrary to AC systems. Firstly, the maximum

transmitted power is limited only by equipment characteristics and not limited by voltage stability angle. Secondly, the decomposition of power grid with DC nodes allows reducing the short-circuit injection current. Thirdly, DC transmissions are characterized by higher than AC transmissions controllability. In terms of transmission construction and design, DC transmissions of the length less than 500–700 km are cheaper. The combined factors make the idea of wide DC transmissions usage attractive. Nevertheless, in terms of GIC, DC transmissions have no benefits over AC systems.

The operation principle of DC systems is based on 2–3 rule, meaning that the valves of two phases are burning in normal state and valves of three phases are burning in transient state. This brings the asymmetry to the power system state which leads to decrease its robustness against solar storm.

3.3 *Voltage collapse*

Power transformers under half-cycle saturation pose threat to power system stability. Power transformers saturation intends cores magnetic permeability to lead to the one in vacuum $4\pi 10^{-7}$ H per m. This causes the growth of reactive power consumption as the result of reactance drop and magnetization current growth. Common cause of voltage avalanches is the reactive power deficit especially for networks constructed from long HV transmission lines. The voltage avalanche risk is higher during space weather events, since the power systems are rarely designed for operation under these circumstances.

The disturbance conditions for the network have to be summarized as a whole. The N power system states have to be analyzed. Under saturation, power transformers reactive power consumption Q is described by the equation (9).

$$Q = U(I_{exc} + KI_{GIC}), \tag{9}$$

where U = voltage level; I_{exc} = excitation current; K= empirical coefficient. Experiment results showed out that K is equal to 2.8 for single phase power transformers and 0.4 for three-phase three-limb power transformers.

The system impact depends not only on the power transformer type but also on the exposed node location. The transmission grid can be represented as the generation-transmission-distribution chain (Fig. 4).

Two cases were studied: saturation of step-up power transformer (Fig. 5) and saturation of grid transformer (Fig. 6). In both of the cases, impact of saturated single phase power transformer was analyzed.

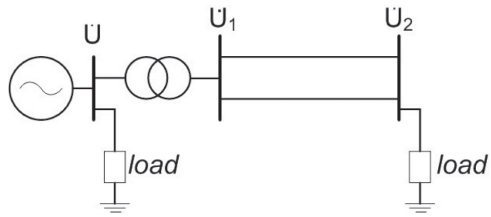


Figure 4. Generation—transmission—distribution chain.

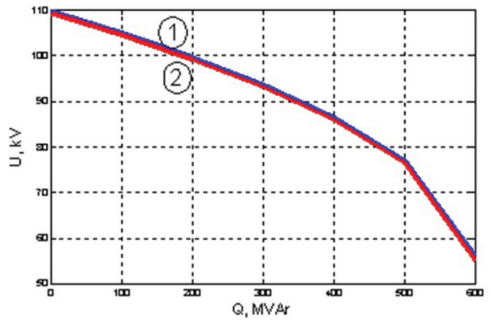


Figure 5. Voltage level as a function of reactive power deficit in case of step-up transformer saturation: 1—voltage at the beginning of transmission line U_1; 2—load voltage U_2.

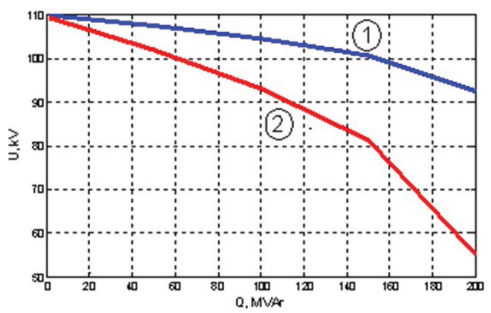


Figure 6. Voltage level as a function of reactive power deficit in case of grid transformer saturation: 1—voltage at the beginning of transmission line U_1; 2—load voltage U_2.

The comparison showed out that grids transformer saturation weakens the grid mode more. The reason of the higher resilience of step-up power transformer is the support of generator excitation system.

Another threat exposed by power transformers saturation is harmonics spectrum change. Thereby, the total reactive power consumption Q_Σ has to be calculated (10).

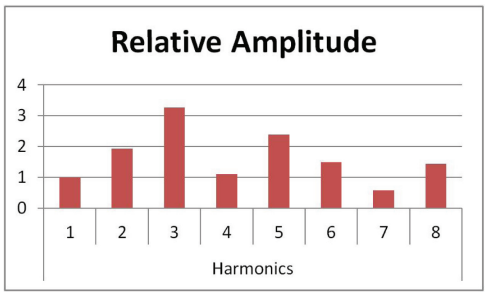


Figure 7. High harmonics spectrum under GIC impact.

$$Q_{\Sigma} = U\left(\sum_{i=1}^{n} I_i^2\right)^{\frac{1}{2}}, \tag{10}$$

where I_i = current level of i-harmonic.

For harmonics spectrum determination, data from measurement instruments installed on 330 kV substation Louhi, Russia (Efimov and Selivanov 2013) is used. The Fourier analysis turned out that high harmonics significantly exceed admissible values (Fig. 7).

The Standard EN50160 puts the limits on maximum harmonics amplitude. For example, the third harmonic has to be not bigger than 5% of the main one. As it is seen on Figure 7, under GIC impact third harmonic is about 3 times bigger than the main one. Such distribution makes challenging the relay protection system operation. Thereby, emergency control system for power system stability ensuring designed for operation under normal harmonic spectrum is ineffective. The power system response time is too short for implementing any meaningful actions. This poses one more threat to reliable and quality power energy supply.

4 MITIGATION ACTIONS

The mitigation actions can be implemented both on network element and system level. On network element level, following actions are possible:

- power transformer change by more resilient types;
- implementation of power transformers with special compensation windings;
- implementation of power transformer with clearance gap in the core;

The lengthwise compensated transmission lines prevent GIC distribution in power grid. The grid redesign with implementation of lengthwise compensated transmission lines was performed in Hydro Quebec system after the blackout in 1989. The project was finalized in 1996. Despite of high effectivenesss in terms of GIC, this mitigation action has to be implemented only after detailed analysis of N normal power system states and N' emergency states. The mitigation actions against GIC impact cannot weaker ordinary power system operation. The same aspect has to be considered while relay protection algorithms change. Technological mitigation measures need to be combined with organizational ones. Operational manuals need to be revised and corrected. Possible list of operational actions is following:

- Decreasing power flows over the transmission lines both AC and DC;
- Switching on neutral blocking devices;
- Switching on series compensators;
- Switching off shunt reactors;
- Switching off vulnerable power transformers;

5 VULNERABILITY COMPARISON

5.1 *Scandinavian power grid*

In 2008, Swedish transmission system operator, Svenska Kraftnat, accepted the project for gradually change of HV power transformers to three-phase three-limb type (Kraftnat 2008). As it is shown in Table 1, this is the most resilient to GIC power transformer type. Currently, 60% of power transformers fulfill the requirements, the rest are either single-phase or three-phase five limb power transformers. The distribution principle is following: single phase transformers are normally used as step-up ones; three-phase five-limb as grid installations. Even though, the impact on grid stability is bigger from saturation of grid transformer, their robustness to GIC is higher, because they are normally three phase five limb or three phase three limb types. The most likely scenario for Scandinavian grid is the voltage avalanche without power equipment loss. Voltage avalanche might happen in case of solar storm impact with severity higher than following: $K = 8$ and $f = 10^{-3}$.

5.2 *US power grid*

The full-scale analysis of installed power transformers is done in (Kappenmann 2010). US power grid is characterized with the presence of the higher voltage levels than in Scandinavian grid. The network consists of three voltage classes: 765 kV, 500 kV and 345 kV. The most common one is 345 kV, which makes up 64% of the transmission network. Nevertheless, the wider usage of single phase equipment is presented in US power grid, because of ultra high voltage networks (Fig. 8).

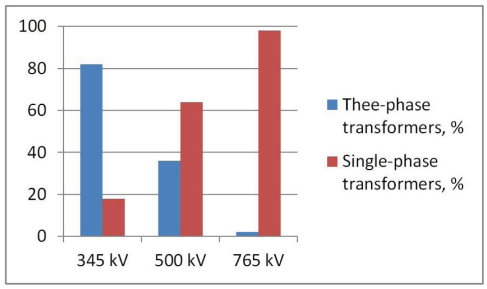


Figure 8. Demographic estimates of power transformers as a function of voltage level (kV rating).

The accumulated power transformer outage in Carrington like event (magnetic field variation equal to 4800 nT) is 368 units (Kappenmann 2010). In other words, 20% of 345 kV, 28,4% of 500 kV and 31,8% of 765 kV power transformers might be damaged.

6 CONCLUSIONS

Solar storms can develop simultaneously over large areas, potentially causing cascade outage of critical infrastructure systems. Power system reliable and high quality operation as the key element of critical infrastructure is of highest importance. Historical examples showed that power system operation algorithms have to include actions not only from known threats ("N-1" principle), but also from solar storm impact in the form of GIC. By entering power system, GIC might cause:

- Voltage avalanche due to reactive power deficit and relay protection system missoperation with equipment outage.
- Voltage avalanche due to reactive power deficit and relay protection system missoperation without equipment outage.
- Power equipment outage without widespread voltage blackout.

Impact on power transformers as the principle elements of power system were analyzed in this paper. The analysis showed that the impact level depends on DC flux path, moment of GIC appearance and equipment isolation. Power transformers vulnerability depends, primarily, on the size of core's section admissible for reversal magnetic flow. The most vulnerable type is the set of single phase transformers. Contrary, the most resilient ones are three-phase three-limb power transformers, in which DC fluxes compensate each other in the main limbs and connecting yokes. The analysis was done on equivalent scheme of Scandinavian power system. The results were compared with the solar storm impact on US power grid. The main conclusion is following: solar storm impact severity is determined mainly by power system technological parameters. For instance, power grid of US might experience higher impact than Scandinavian grid even though it is located in more southern geomagnetic latitude.

REFERENCES

Efimov, B. and Sakharov, Y. & V. Selivanov (2013). Geomagnetic storms: study of the impacts on power system of karelia and the kola. *Electrotechnik news 2*, 30–33.

Gaunt, Charles Trevor (2014). Reducing uncertainty responses for electricity utilities to severe solar storms. *J. Space Weather Space Clim. 4*, A01.

Kappenmann, J. (2010). Geomagnetic storms and their impacts on us power grid. Technical report, Metatech Corporation, 358 S. Fairview Ave., Suite E, Goleta, CA 93117.

Kraftnat, S. (2008). Standard power transformers 2 mva and above. Technical report, Svenska Kraftnat, Sundbyberg, Sweden.

Marusek, J.A. (2007). *Solar storm threat analysis.* Impact.

Mousavi, S.A., C. Carrander, & G. Engdahl (2013). Comprehensive study on magnetization current harmonics of power transformers due to gics.

Pirjola, R. (2008). Effects of interactions between stations on the calculation of geomagnetically induced currents in an electric power transmission system. *Earth Planets and Space (EPS) 60*(7), 743.

Viljanen, A., O. Amm, & R. Pirjola (1999). Modeling geomagnetically induced currents during different ionospheric situations. *Journal of Geophysical Research: Space Physics (1978–2012) 104*(A12), 28059–28071.

Viljanen, A., R. Pirjola, M. Wik, A. Ádám, E. Prácser, Y. Sakharov, & J. Katkalov (2012). Continental scale modelling of geomagnetically induced currents. *Journal of Space Weather and Space Climate 2*, A17.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Accident risk assessment for deep geothermal energy systems

M. Spada, E. Sutra, S. Wolf & P. Burgherr
Laboratory for Energy Systems Analysis, Paul Scherrer Institute, Villigen PSI, Switzerland

ABSTRACT: Deep geothermal energy systems are, like all energy technologies, not fully risk free. The primary risk identified in the domain of deep geothermal is induced seismicity. However, a comprehensive risk assessment needs to take into account additional aspects such as potential borehole blowout. In this study the different technological risks associated with deep geothermal energy systems are identified, characterized and quantitatively analyzed. First, a literature review is performed to compile a set of risk indicators that has either the potential to affect human health or impact the environment. In a second step, damage rates are calculated for different consequence types (e.g., fatalities, injured persons) for accident risks related to blowouts in the drilling phase and the use of hazardous substances in both drilling and operational phases. Finally, a comparison between identified risks is carried out showing that one of the main sources of accident risk is related to blowout.

1 INTRODUCTION

Geothermal energy is an abundant, clean (low greenhouse gas emissions) and reliable natural resource. The main part of the heat (~80–85%) is generated by the natural decay over millions of years of radiogenic elements from the continental crust and the earth's mantle, such as uranium, thorium and potassium (e.g., Tester et al., 2006).

Geothermal resources nowadays are mainly utilized for electricity generation, although direct-use applications are also significant. Globally, geothermal energy use is projected to more than double over the outlook period to 2035 according to the IEA's New Policies Scenario (e.g., IEA, 2012).

Until recently, geothermal energy was considered to have significant economic potential only in areas with hydrothermal systems, such as active volcanoes (e.g., WEC, 2013). However, in the last few years, new technologies, such as Enhanced Geothermal Systems (EGS) (e.g., Tester et al., 2006), have permitted to use geothermal resources in deeper geological layers and at lower temperatures.

Deep geothermal systems can be subdivided in two main families, hydrothermal and petrothermal systems, (e.g., Goldstein et al., 2011). The former is similar to the common geothermal system, where the warm water in the underground is used to produce electricity and/or heat. In petrothermal systems, on the other hand, the reservoir is created by hydraulic stimulation and the water is pumped in the underground and afterwards circulates in a closed circle. Therefore, considering the latter, all countries have theoretically a clean and abundant energy source in the underground, which could be used for district heating as well as electricity generation (e.g., Breede et al., 2013).

In this context, stakeholder interest has increased for deep geothermal energy systems. However, the exploitation of underground energy resources is, like all energy technologies, not risk free. Studies on deep geothermal risks often primarily focus on induced seismicity, since it has been shown to be one of the biggest issues for deep geothermal energy (e.g., Tester et al., 2006). Furthermore, few studies addressed other possible issues, such as groundwater contamination (e.g., Aksoy et al., 2009), or including an overview of possible associated hazards (e.g., Tester et al., 2006). Therefore, a comprehensive risk assessment is needed in order to take into account additional aspects with respect to induced seismicity, such as borehole blowout and use of hazardous substances, among others. Furthermore, it is important to consider both the drilling and operational phases of a deep geothermal system in order to analyze the two main phases separately.

In this study, different technological risks, with focus on human health effects and environmental impacts, associated with deep geothermal energy systems are identified, characterized and, possibly, quantitatively analyzed. In order to assess the accident risk for deep geothermal systems the current study is divided into two main parts. At first, a summary of possible sources of accident risks is provided. Afterwards, risk indicators relevant for deep geothermal systems with regard to accidents causing damage to human health and the environment are defined for two of the major sources of possible consequences, which are blowouts in the

drilling phase and the use of hazardous substances in both drilling and operational phases. Finally, the risk indicators are quantified and compared for the aforementioned sources of risk.

2 OVERVIEW OF THE POTENTIAL RISKS OF DEEP GEOTHERMAL SYSTEMS

In order to assess the accident risks in deep geothermal systems, a comprehensive literature research is carried out. Different types of potential risks are identified and described for both drilling and operational phases. These are related, for example, to the use of hazardous substances, although most of them in relatively small quantity. In the following, an overview of the different risks is given.

2.1 *Kicks*

A kick is a well control problem in which the pressure found within the drilled rock is higher than the mud hydrostatic pressure acting on the borehole or rock face. When this occurs, the greater formation pressure has a tendency to force formation fluids into the wellbore. This forced fluid flow is called a kick. If the flow is successfully controlled, the kick is considered killed. An uncontrolled kick that increases in severity may result in what is known as a "blowout."

Kicks can be labeled in different ways depending on the material entering the borehole (oil, sand, carbon dioxide, etc.). The accident that happened in 2013 at the deep geothermal site in St. Gallen (Switzerland) is an example of gas kick (Sonderegger, 2014). Furthermore, the kick can be dangerous if it is caused by flammable natural gas or poisonous hydrogen sulphide gas.

Three main parameters play a role in a kick development. Two are related to the type of rocks in which drilling is performed: permeability and porosity. The third parameter is the difference between the formation fluid pressure and the mud hydrostatic pressure. If the formation pressure is much greater than the hydrostatic pressure, a large negative differential pressure exists.

2.2 *Blowouts*

Geothermal drilling relies on the same kind of technology used in the oil and natural gas industry, modified for high temperature applications and larger well diameters (e.g., Finger and Blankenship, 2010). Deep geothermal systems and oil/natural gas also differ in temperature (higher in deep geothermal systems), production pressure (lower in deep geothermal systems), and production rates (higher for deep geothermal systems) on the drilling phase (e.g., Tester et al., 2006).

Therefore, we assume that the blowout risk in the drilling phase for deep geothermal systems can be roughly approximated from the corresponding risks in the natural gas and oil chains.

2.3 *Drilling mud*

In geothermal systems in general, during the drilling phase, the used mud is a composition of water and some additives, such as barite. The additives are added to the fresh water in order to increase the viscosity, the weight and to control the pH, and must be adapted to the geology of the site.

The addition of active solids, clays (bentonite) and polymers to water allows producing a colloidal suspension and are known as viscosifiers. Inert solids are those added to the mud either by drilling (formation particles) or by using barite as a weighting material without significantly affecting the global viscosity (e.g., Chemwotei, 2011).

The alkalinity of the fluid is also essential for corrosion control, rheological properties in bentonite mud, and for its reaction with some formation constituents. Water-based drilling mud (Spud Mud) commonly consists of bentonite clay (gel) accounting for around 10% of the mixture, with additives such as barium sulphate (barite), calcium carbonate (chalk) or hematite (e.g., HSL, 2000). In some cases (Natural Bentonite Mud), caustic soda (ca. 1% of the mud mass) is added to water and bentonite (ca. 9% of the mud mass) to stabilize the pH. The pH usually ranges between 9.5 and 10.5, but higher values are not uncommon (e.g., Finger and Blankenship, 2010).

In general most of the chemical additives are not dangerous for the environment and human health. However, for example, the caustic soda is an extremely corrosive substance for metals, even more for the humans and could cause fatalities primarily in case of ingestion (e.g., ATSDR, 2002).

2.4 *Hydraulic stimulation*

To improve the well productivity, the main stimulation technique generally used in Enhanced Geothermal Systems (EGS) activities is the "hydraulic stimulation" largely associated with the "chemical stimulation" (Aqui and Zarrouk, 2011). Developed and mainly employed in the oil/gas industry, recent studies highlight the use of chemical substances in numerous deep geothermal systems stimulation (Clark et al., 2013). Even if the use of gel and proppant in geothermal wells is not expected, their usage are reported from different sites, e.g., Fjallbacka (Sweden) (e.g., INL, 2006).

In general, during chemical stimulations, the process of acidification implies solutions of HCl, HF, KCl, or NH4Cl, with concentrations around

0.1% to 15%, injected in three main steps (Clark et al., 2013). These acid treatments seem also to be also supplemented with some additives as corrosion inhibitor and inhibitor intensifier, as well as chelating agents in order to minimize iron precipitation (Schulte et al., 2010).

2.5 *Working fluids used in the power plants*

The binary cycle power plant type appears as the more efficient system for deep geothermal energy (e.g., Gerber and Maréchal, 2012). In the binary process, geothermal water is used to heat another liquid, such as benzene, which boils at a lower temperature than water. The two liquids are kept completely separate through the use of a heat exchanger, which transfers the heat energy from the geothermal water to a secondary fluid (also known as the "working fluid"). The secondary fluid vaporizes into gaseous vapor and the force of the expanding vapor turns the turbines that power the generators. Finally, the fluid is air cooled or condensed with water. In the meantime, the geothermal fluid is re-injected into the borehole (e.g., Goldstein et al., 2011).

Within this system, two power plant types exist: a) Kalina cycle, and b) Organic Rankine Cycles (ORC). These types of power plants are commonly used in low-temperature environments (≤ 120ºC).

In the Kalina cycle, the working fluid is a composition of water and ammonia (NH3). Although in wide use (e.g., as a fertilizer), ammonia is toxic and corrosive for humans and in general dangerous for the environment (e.g., Roy et al., 2011). In the ORC cycle, the most common organic fluids used are n-pentane, iso-butane, iso-pentane, benzene, toluene, n-butane and R134a. Most of these fluids are highly inflammable, toxic and dangerous for the environment as well as for human health.

In this context, the transportation of these substances and their use in the power plant pose the main accident risk.

2.6 *Dry and wet cooling systems*

In a geothermal power plant cooling is necessary to condense the vapor feeding the turbine, lower the heat rejection temperature, raise power output and increase heat to power conversion efficiency (e.g., Mendrinos et al., 2006). The process of cooling can be assessed using air (dry cooling) or water (wet cooling). The dry cooling is the most adopted option in geothermal energy systems, ca. 80% (e.g., Mishra et al., 2011). In a binary cycle power plant the cooling of the working fluid is achieved by using a second heat exchanger (e.g., Kutscher and Costenaro, 2002). Thus, the fluids never make contact with the atmosphere (air-cooling) or the water (dry-cooling). However, for example, a failure of the pipe that transports the working fluid into the second heat exchanger could produce a contact between the water/air and the former. As a consequence, based on the working fluids commonly used (see section 2.5), the environment and the human health could be severely affected.

2.7 *Geofluids*

In both drilling and operational phases a potential risk is connected to the chemical composition of the geofluids (or brine). The brine, a highly saline solution mixed with various chemicals and gases, could cause operational limitations due to their severe scaling and corrosion effects that can occur in wells, lines and equipment.

If not handled responsibly, geofluids are a potential source of water and soil contamination due to presence of toxic minerals, such as arsenic, barium, antimony, and elevated dissolved solid elements, such as sodium chloride, bicarbonate, sulphate, silica, calcium and potassium (e.g., Clark et al., 2011). Arsenic is highly toxic for the environment and human health; thus it could be seriously dangerous in case of geofluids release (e.g., due to pipeline leakage), into the environment.

Among all these elements (e.g., Parmaksiz, 2013), radionuclides also appear to occur commonly in geothermal fluids samples (e.g., 238U, 232Th, 40 K and 226Ra). The accumulation of radionuclides in the inner parts of the drilling equipment, in pipes, valves, tanks, or in cooling systems, can represent, at first, a risk for the workers at a deep geothermal system site. However, studies carried out in USA (e.g., EPA, 2013) and Germany (Köhler and Degering, 2010) show that the total expected quantity of radioactive material at geothermal power plants is not harmful for human health, unless water samples are used as drinking water. Actually, the radioactive exposure level is expected to satisfy the limit of 1 mSv/yr valid for the population (e.g., Köhler and Degering, 2010), while the limit for workers is higher, 20 mSv/yr, with which the results of these studies seem to comply.

2.8 *Induced landslides*

In the past, landslides have occurred at not deep geothermal systems, but the cause is often unclear (e.g., Tester et al., 2006). Many geothermal fields are in rugged terrain that is prone to natural landslides, and some fields actually have been developed atop ancient landslides.

The worst disaster attributable to induced landslide, due to the presence of a geothermal field, is still under debate (e.g., DiPippo, 2012). The accident happened at the Zunil geothermal field

(Guatemala) in 1991, where at least 23 people were killed.

2.9 *Induced seismicity*

Induced seismicity is currently the most discussed risk aspect of deep geothermal systems. Drilling through and pumping fluids under high-pressure into an underground formation layer under shear stress conditions can potentially induce seismicity by releasing the stress (e.g., DiPippo, 2012).

In case of deep geothermal systems, seismicity could be induced in two ways. During the hydraulic fracking step, fluids at higher pressure than in the operational phase are injected into the underground to expand existing fractures in the formation. This high pressure could increase the stress in the formation and create induced seismic events. The second possible cause of induced seismicity is related to the reinjection of the geofluids (see section 2.7), which requires high pressure (e.g., DiPippo, 2012).

In the short history of deep geothermal systems, induced seismicity affected the decision to continue or stop a project in several instances. For example in Basel (Switzerland), a petrothermal project was aborted due to an induced seismic event with a magnitude of 3.3 (e.g., Bachmann et al., 2011). Finally, at the ongoing test plant in Soultz (France) a maximum magnitude of 2.9 was registered without consequences for the project (e.g., Genter et al., 2010). Therefore, no clear magnitude limit can be identified, at which a project should be stopped. Furthermore, preventive measures and mitigation plans to reduce the impacts of induced seismicity have been proposed and developed (e.g., DiPippo, 2012).

3 DATA

In this study, historical accidents related to the use of hazardous substances and to blowouts, causing at least one consequence (e.g., 1 fatality, 1 injury, etc.), are collected for the time period 1990–2012 for countries belonging to the OECD (Organization for Economic Co-operation and Development). The latter choice is done in order to assess the accident risk based on data from countries with similar management, regulatory and safety frameworks. Furthermore, the time period is chosen since deep geothermal energy is a new technology. We believe that 1990 as starting year better reflects the historical information relevant for our purpose, since starting from more recent years, for example in 2000, would result in a weaker statistical basis. In this study, different industrial accidents databases are surveyed to find information about accidents related to both the use of hazardous substances and blowouts. Finally, the collected data are homogenized prior to analysis, in order to avoid possible double counts. The examined databases are the following: The Emergency Response Notification System (ERNS) is a database of incidents reported to the National Response Center (NRC) of the USA.

- The Major Hazard Incident Data Service (MHIDAS) developed on behalf of the Major Hazards Assessment Unit of United Kingdom Health and Safety Executive.
- The Analysis, Research and Information on Accidents (ARIA) database is operated by the French Ministry of Ecology and Sustainable Development.
- The UK Health and Safety Executive (HSE) Information Services create HSELINE. Since 1977, HSELINE collects references to documents relevant to health and safety at work.
- The MHAID (Major Hazards Accidents and Incidents) database contains information on worldwide accidents or incidents involving hazardous materials.
- The Failure and Accidents Technical information System (FACTS) is an accident database, which contains information on more than 25200 (industrial) accidents (incidents) involving hazardous materials or dangerous goods that have happened all over the world during the past 90 years.

In addition to the aforementioned, two extra databases are considered to collect data on the risk of blowout accidents:

- PSI's ENergy-related Severe Accidents Database (ENSAD), comprehensively covers energy related severe accidents worldwide (e.g., Burgherr et al., 2013).
- Alberta Oil Spill open data compiled by the Alberta Energy Resources Conservation Board (ERCB).

3.1 *Hazardous substances*

In the drilling phase, the mud is based mainly on water with low percentage of chemical additives. Among the additives considered as "environment and human friendly", acids, such as caustic soda, could be used in order to preserve the pH. Caustic soda is a highly caustic metallic base and alkali salt and is extremely corrosive for humans (as well as metals). Therefore, the risk related to the use of caustic soda as additive in the drilling phase is assessed in this study. Furthermore, in order to assess the risk, only accidents that can be associated to deep geothermal procedures are collected. These are the accidents happened in storage, transportation sectors and in the well drilling phase (Table 1).

In the operational phase, we consider the ORC binary cycle only since it is commonly more suitable than Kalina binary cycle due to the high complexity of the latter (e.g., Köhler and Saadat, 2003). The most common substances used in ORC cycle are n-pentane, isobutane, isopentane, benzene, toluene, n-butane and R134a. These chemicals are highly toxic and inflammable, meaning dangerous for human health and the environment. Among all the substances listed above, the risk related to the use of benzene and toluene is taken into account in this study due to the lack of accident data for the other aforementioned chemicals. Considering only events associated to deep geothermal procedures, for benzene and toluene only accidents related to the storage, the transportation and such that can be associated to ORC binary cycle systems (e.g., pump failure) are collected (Table 1).

3.2 *Blowouts*

Blowout accidents for deep geothermal systems are not present in the examined databases due to the novelty of this technology. Therefore, in order to assess the risk for blowout accidents, onshore data from oil and gas industries are collected. In fact, although, the deep geothermal and oil/natural gas differ in temperature (higher in deep geothermal), production pressure (lower in deep geothermal), and production rates (higher for deep geothermal) in the drilling phase (e.g., Tester et al., 2006), the risk of onshore blowout as estimated for oil/natural gas can be generally considered a sufficiently accurate starting point. Furthermore, only accidents that happened in onshore well areas are considered, since wells for deep geothermal systems are drilled onshore only.

Due to limited historical data on onshore blowout accidents, this study analyzed two specific regions, the province of Alberta (Canada) and the entire onshore USA. The data collected for these two countries are shown in Table 2.

Table 1. Summary of accidents related to the use of hazardous substances with at least 1 consequence (e.g., 1 fatality) in the time range 1990–2012 for OECD countries.

Hazardous substance	Immediate fatalities	Immediate injuries	Evacuees
	Acc/Fat	Acc/Inj	Acc/Eva
Caustic soda	17/39	177/1386	38/15263
Benzene	14/45	54/1273	91/96513
Toluene	31/37	110/1291	61/7826

Table 2. Summary of blowout accidents with at least 1 consequence (e.g., 1 fatality) in the time range 1990–2012 happened in USA and Alberta (Canada).

Country	Industry	Fatalities	Injuries	Evacuees
		Acc/Fat	Acc/Inj	Acc/Eva
USA	Natural gas	4/4	8/16	21/3819
	Oil	1/1	5/8	3/3041
Alberta	Natural gas	9/9	22/33	4/7
	Oil	0/0	35/44	11/50

4 METHOD

4.1 *Overview*

Risk can be decomposed into the product of the frequency and severity (e.g., Haimes, 2009). The number of accidents per year gives the frequency, while severity measures the extent of the consequences of each accident. The frequency distribution is influenced by temporal trends, while the severity distribution is influenced by a number of parameters such as the material involved in the accident or the different products and the amount of material present, or the number of people in the vicinity of an accident. To assess the risk, the standard method of aggregated indicators is applied (e.g., Burgherr et al., 2013). The latter provides a direct comparison of accident consequences (e.g., fatalities) per unit of electricity produced (e.g., GWeyr) between, for example, hazardous substances.

4.2 *Normalization*

In order to derive a comparable measure of accident risk for both the use of hazardous substances and blowouts, the indicators are normalized by the energy production in terms of GWeyr. The Gigawatt-electric-year (GWeyr) is chosen because large individual plants have capacities in the neighborhood of 1 GW of electrical output (GWe). This makes the GWeyr a natural unit to use when presenting normalized indicators generated within technology assessment (e.g., Burgherr et al., 2013).

4.2.1 *Hazardous substances*

In order to assess the normalization factor in GWeyr for each hazardous substance analyzed in this study, the share of the total production of them used in deep geothermal energy systems has to be estimated. In order to do this, the OECD total production for each substance in the time period 1990–2012 is collected (Table 3). Afterwards, a base case 7MW power plant with a capacity factor of 95% and a lifetime of 30 years is considered, which

Table 3. Normalization Factor (NF) for risk indicators in the use of hazardous substances. NF is calculated as the ratio between the total amount of substance used at the power plan and the product of the OECD's total production in the time period 1990–2012 of the substance and the power plant total production in GWeyr over its entire lifetime (30 years).

Hazardous substance	OECD's total production (kg)	Total used over power plant lifetime (kg)	Normalization factor
			GWeyr
Caustic soda	1.03E+12	3E+4	6.78E+06
Benzene	3.74E+11	7.486E+3	9.89E+06
Toluene	2.24E+11	7.417E+3	5.99E+06

results in a total production of 1.98E-1 GWeyr for its entire lifetime.

The use of caustic soda as additive in drilling mud is not constant over the entire drilling phase. Caustic soda is added for short time mainly to stabilize the pH in the underground between 9.5 and 10.5 (e.g., Tester et al., 2006). However, due to the lack of information on the effective quantity of caustic soda handled per well drilled, as a first approximation the use of this substance is considered constant for the entire drilling phase. According to (e.g., Kaiser and Fäs, 2004), 1 kg of caustic soda is used for 1 meter of drilling. Therefore, in this study, where 6 wells of 5000 m are considered to be drilled in the 30 years lifetime for the 7MW power plant, the total amount of caustic soda used in the geothermal drilling phase would be 30000 kg (Table 3).

On the other hand, the use of working fluids is based on the sum of the initial input, that is fixed to 436 kg and 432 kg for benzene and toluene, respectively, and the quantity of substance that has to be used in order to fill up the initial value due to a loss per year set to 8% (e.g., Rogge, 2004).

Finally, by considering the aforementioned data and that the 7 MW power plant is modeled with 5.05 units, the Normalization Factor (NF) in terms of GWeyr, see Table 3, for each hazardous substance over the entire lifetime (30 years) is then estimated as following:

NF = (GWeyr*total kg production (1990–2012))
/kg used over the power plant lifetime

where, GWeyr = 1.98E-1.

4.2.2 *Blowouts*

To assess the blowout risk for geothermal energy systems, accidents from onshore blowouts in oil and natural gas industries in USA and Alberta (Canada) are merged in order to avoid possible issues related to the lack of data. This operation is valid on a first approximation since oil and natural gas extractions are similar in engineering, e.g., use of the same drilling equipment, and physical, e.g., similar pressures involved, terms (e.g., UNEP and E&PForum, 1997).

Table 4. Normalization factor for risk indicators in the onshore blowout case.

Country	Industry	Onshore production
		GWeyr
USA	Natural gas	5480
	Oil	18435
Alberta	Natural gas	1493
	Oil	686

In order to merge the natural gas and oil datasets the accident's frequency for blowout has to be comparable. Therefore, the risk indicators for each industry are normalized by the amount of total production in the time period 1990–2012 in GWeyr. The total amount of oil and natural gas onshore production are collected from the U.S. Energy Information Administration (e.g., EIA, 2014) and from the Canadian Association of Petroleum Producers (e.g., CAPP, 2014) for USA and Alberta, respectively (Table 4).

5 RESULTS

In this section, the risk assessment results for three hazardous materials possibly used in deep geothermal systems and onshore blowouts are presented. The substances are caustic soda used as additive in the drilling phase, benzene and toluene used as working fluids in ORC binary cycle. Results are shown in terms of aggregated indicators for fatalities, injuries, and evacuees. Furthermore, in case of hazardous substances, fatalities and injuries refer to immediate ones, since no exposure and toxicity in this assessment are taken into account.

5.1 *Fatalities*

Figure 1 shows the fatality rate for each hazardous substance and onshore blowouts analyzed in this study. The fatality rate is estimated using all the accidents causing at least 1 fatality. Results clearly show a higher relative risk of onshore blowouts compared to the use of hazardous substances in both drilling and operational phases. Among the latter, all the considered substances show similar results, with a slightly higher risk for caustic soda.

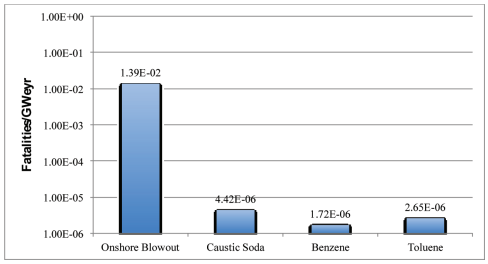


Figure 1. Fatality rate indicator for onshore blowouts and hazardous substances in deep geothermal systems.

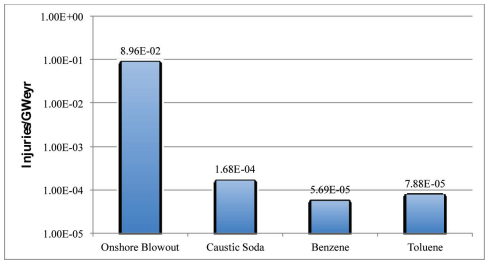


Figure 2. Injury rate indicator for onshore blowout and hazardous substances in deep geothermal systems.

Therefore, the drilling phase exhibits a higher fatality risk than the operational phase, mainly due to the high risk related to blowout accidents.

5.2 *Injuries*

Figure 2 shows the injury rate for the accident risks analyzed in this study. The injury rate is estimated using all the accidents causing at least 1 injury. Similar to fatalities, onshore blowouts show a substantially higher relative risk in comparison to the use of hazardous substances. Among the latter, caustic soda shows a higher risk than benzene and toluene. Therefore, as for fatalities, the drilling phase results to be more risk prone in terms of injuries compared to the operational phase.

5.3 *Evacuees*

Figure 3 shows the evacuee rate for the accident risks analyzed in this study. The evacuee rate is estimated using all the accidents causing at least 1 evacuee. The rate shows a distinctly higher relative risk for onshore blowouts compared to hazardous substances. Among them, benzene shows a higher risk than caustic soda, while toluene appears to be less risky. Therefore, as in the previous indicators, the drilling phase comprises a higher risk in terms of evacuees than the operational phase, mainly due to the high risk related to blowout accidents.

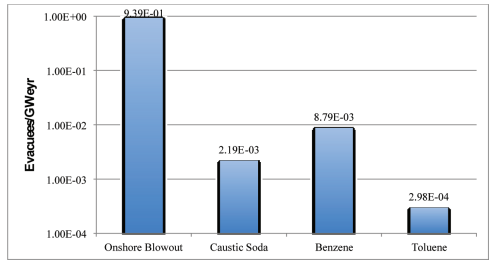


Figure 3. Evacuee rate indicator for onshore blowout and hazardous substances in deep geothermal systems.

6 CONCLUSION

In this study possible accident risks of deep geothermal systems are evaluated. Risks are quantified for blowout accidents and accidents related to the use of hazardous substances in both drilling and operational phases, which represent the main accident risks besides induced seismicity. The analysis showed that the accident risk of blowouts is significantly higher than the risk related to the use of hazardous substances. This is the case for all the considered risk indicators, i.e. fatality, injury and evacuee rates. Therefore, blowouts can be considered one of the main accident risks besides induced seismicity. In addition, based on these results, the drilling phase in deep geothermal systems exhibits higher risks compared to the operational phase.

This study provides a preliminary overview of possible accident risks for deep geothermal systems. Future research should analyze other sources of accident risks, e.g., the chemical composition of the geofluids in the operational phase. Furthermore, exposure and toxicity analyses need to be carried out for hazardous substances in order to correctly assess the risk of chemicals.

ACKNOWLEDGEMENTS

The presented work was supported by the project "Energie aus dem Innern der Erde: Tiefengeothermie als Energieträger der Zukunft?" of the Swiss Center for Technology Assessment (TA-Swiss), the GEOTHERM-2 project of the Swiss Competence Center Energy and Mobility and by the Swiss Competence Center for Energy Research—Supply of Electricity (SCCER-SoE).

REFERENCES

Aksoy, N., Şimsek, C. & Gunduz, O., 2009. Groundwater contamination mechanism in a geothermal field: A case study of Balcova, Turkey. *Journal of Contaminant Hydrology,* 103, 13–28.

Aqui, A.R. & Zarrouk, S., 2011. Permeability Enhancement of Conventional Geothermal Wells.

ATSDR, 2002. Managing Hazardous Materials Incidents. Volume III—Medical Management Guidelines for Acute Chemical Exposures: Sodium Hydroxide. U.S. Department of Health and Human Services Public Health Service.

Bachmann, C., Wiemer, S., Woessner, J. & Hainzl, S., 2011. Statistical analysis of the induced Basel 2006 earthquake sequence: introducing a probability-based monitoring approach for Enhanced Geothermal Systems. *Geophysical Journal International,* 186, 793–807.

Breede, K., Dzebisashvili, K., Liu, X. & Falcone, G., 2013. A systematic review of enhanced (or engineered) geothermal systems: past, present and future. *Geothermal Energy,* 1, 1–27.

Burgherr, P., Hirschberg, S. & Spada, M., 2013. Comparative Assessment of Accident Risks in the Energy Sector. *Handbook of risk management in energy production and trading.* Springer U.S.

CAPP, 2014. Statistical Handbook for Canada's Upstream Petroleum Industry. Calgary, Canada.

Chemwotei, S.C., 2011. Geothermal Drilling Fluids. United Nations University.

Clark, C. E., Harto, C.B., Schroeder, J.N., Martino, L.E. & Horner, R.M., 2013. Life Cycle Water Consumption and Water Resource Assessment for Utility-Scale Geothermal Systems: An In-Depth Analysis of Historical and Forthcoming EGS Projects.

Clark, C.E., Harto, C. B., Sullivan, J.L. & Wang, M.Q., 2011. Water Use in the Development and Operations of Geothermal Power Plants. Argonne National Laboratory.

Dipippo, R., 2012. Environmental Impact of Geothermal Power Plants. *Geothermal Power Plants.* Butterworth-Heinemann.

EIA, 2014. *Total Production of Oil and Natural Gas* [Online]. Available: http://www.eia.gov/cfapps/Ipdbproject/IEDIndex3.cfm.

EPA, 2013. *Geothermal Energy Production Wastes| Radiation Protection | US EPA* [Online]. Available: http://www.epa.gov/radiation/tenorm/geothermal.html.

Finger, J. & Blankenship, D., 2010. Handbook of Best Practices for Geothermal Drilling. Sandia National Laboratory.

Genter, A., Evans, K., Cuenot, N., Fritsch, D. & Sanjuan, B., 2010. Contribution of the exploration of deep crystalline fractured reservoir of Soultz to the knowledge of enhanced geothermal systems (EGS). *Comptes Rendus Geoscience,* 342, 502–516.

Gerber, L. & Marechal, F., 2012. Environomic optimal configurations of geothermal energy conversion systems: Application to the future construction of Enhanced Geothermal Systems in Switzerland. *Energy,* 45, 908–923.

Goldstein, B., Hiriart, G., Bertani, R., Bromley, C., Gutierrez-Negrin, L., Huenges, E., Muraoka, H., Ragnarsson, A., Tester, J. & Zui, V., 2011. Geothermal Energy. *IPCC Special Report on Renewable Energy Sources and Climate Change Mitigation.* Cambridge University Press.

Haimes, Y., 2009. On the complex definition of risk: a systems-based approach. *Risk Analysis,* 29, 1647–1654.

HSL, 2000. Drilling Fluids Composition and use within the UK Offshore Drilling Industry. Health & Safety Laboratory.

IEA, 2012. World Energy Outlook 2012. Paris, France.

INL, 2006. The Future of Geothermal Energy: Impact of Enhanced Geothermal Systems (EGS) on the United States in the 21st Century.

Kaiser, M. & Fas, M., 2004. Umweltverträglichkeitsbericht (Hauptuntersuchung) Deep Heat Mining, Basel, Switzerland.

Kohler, M. & Degering, D., 2010. Geothermal energy usage and dose assessments. EAN-NORM Workshop.

Kohler, S. & Saadat, A., 2003. Thermodynamic Modeling of Binary Cycles Looking for Best Case Scenarios. International Geothermal Conference, 2003 Reykjavik, Island.

Kutscher, C. & Costenaro, D., 2002. Assessment of evaporative cooling enhancement methods for air-cooled geothermal power plants.

Mendrinos, D., Kontoleontos, E. & Karytsas, C., 2006. Geothermal Binary Plants: Water or Air Cooled?

Mishra, G.S., Glassley, W.E. & Yeh, S., 2011. Realizing the geothermal electricity potential-water use and consequences. *Environ. Res. Lett.,* 6, 034023.

Parmaksiz, A., 2013. Measurement of naturally occurring radionuclides in geothermal samples and assessment of radiological risks and radiation doses. *Radiation Protection Dosimetry,* 157, 585–593.

Rogge, S., 2004. Geothermische Stromerzeugung in Deutschland Ökonomie, Ökologie und Potenziale. Technical University Berlin, Germany.

Roy, P.K., Bhatt, A., Kumar, B., Kaur, S. & Rajagopal, C., 2011. Consequence and risk assessment: Case study of an ammonia storage facility. *Arch. Environ. Sci.,* 5, 25–36.

Schulte, T., Zimmermann, G., Vuataz, F., Portier, S., Tischner, T., Junker, R., Jatho, R. & Huenges, E., 2010. Enhancing Geothermal Reservoirs. *Geothermal Energy Systems.* Wiley-VCH Verlag GmbH & Co. KGaA.

Sonderegger, M., 2014. *Geothermie-Projekt St.Gallen: Aktueller Stand / Erfahrungsbericht* [Online]. Available: http://www.geo-energie.ch/pdf/Geothermieprojekt_St_Gallen.pdf.

Tester, J.W., Anderson, B.J., Batchelor, A.S., Blackwell, D.D., Dipippo, R., Drake, E.M., Garnish, J., Livesay, B., More, M.C., Nichols, K., Petty, S., Toksoez, M.N. & Veatch, R.W., 2006. The Future of Geothermal Energy. *Impact of Enhanced Geothermal Systems (Egs) on the United States in the 21st Century: An Assessment.* MIT Press (MA).

UNEP & E&PFORUM, 1997. Environmental management in oil and gas exploration and production.

WEC, 2013. *World Energy Resources: 2013 Survey* [Online]. Available: http://www.worldenergy.org/publications/2013/world-energy-resources-2013-survey/.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Enhancement of IT Risk Assessments by UML

R. Mock, B. Truninger & P. Brunner
Institute of Applied Information Technology, Zurich University of Applied Sciences, Winterthur, Switzerland

T. Hruz
milliPay Systems AG, Zürich, Switzerland

ABSTRACT: Unified Modeling Language diagrams (UML) are considered as an underestimated knowledge source for Risk Assessment (RA) approaches. For this, a combination of Class and Sequence Diagrams is used to get relevant information for further risk analysis. In an IT enterprise, existing business processes source code can be used to automatically generate a full process Class Diagram. The paper suggests a way to significantly reduce the size of the Class Diagram. To do this, the most relevant business case of the audited enterprise is selected and used to generate a Sequence Diagram. Tools simplify this approach. The resulting Sequence Diagram only consists of classes and operations relevant to the chosen business case. They can then be matched to the initial full system Class Diagram. Elements in the Class Diagram that do not have a match in the Sequence Diagram can be removed, resulting in a reduced Class Diagram. The reduced Class Diagram is the base for RA heuristics, e.g., many incoming associations of a class suggest that other classes often depend on this class. Therefore, a failure of this class points to an increased impact value.

1 INTRODUCTION

The keyword "Industry 4.0" outlines the current shift of technical systems from well identifiable structures to indistinct infrastructural entities which depend on Information Technology (IT) to a large extent. This change also has impacts on how to do Risk Assessments (RA): It prompts questions about IT security, shifts assessment goals from hazard evaluation to vulnerability analysis and has to deal with highly dynamic and networked systems. The established tools of engineering RA have reached their methodological and practical limits to characterise this kind of technology (cf. (Mock et al. 2014)). The R&D project Micropayment at Zurich University of Applied Sciences ZHAW targets to merge the areas of engineering RA and IT security approaches in close cooperation with an industry partner in order to draw a profit in fault detection, IT system optimisation and methodological enhancements.

There are only a few methodologies combining both areas in a practice-oriented manner. They mainly base on check list-like procedures (audit, compliance check) or on a semi-formal notation. Some of the latter approaches base on close to business system graphs, e.g., Unified Modeling Language Diagrams (UML), Business Process Modelling (BPM) and Event-driven Process Chains (EPC). The paper substantiates the usage of specified UML diagrams for RA purposes as they are commonly known in enterprises as well as in Informatics. With this, the authors consider UML an unexploited resource for IT risk analyses. In doing so, the paper is structured as follows: Chapter 2 clarifies framework and terms in IT RA. Chapter 3 outlines UML diagrams as well as their current use in IT RA. It also positions them in the framework of engineering RA. In chapter 4, an approach is presented on how to utilise automatically generated UML of a business process in the framework of engineering RA. Open questions and further work are addressed. Conclusions in chapter 5 outline assets and drawbacks of the methodology.

2 IT RISK ASSESSMENT

The common procedures and tools offered for RA of IT depending infrastructural systems are unable to manage the fast modification rates. They have become laboured and too resource-intensive in order to meet the constraints of a fast moving and IT driven business community. Everyday measurements, as the installation of, e.g., a new router, may lever out existing reliability models (cf. (Milanovic et al. 2008)). Nevertheless, a methodology is needed to assess risks in practically relevant procedures. The proposed methodology will finally come to integrate engineering and IT RA approaches:

Definition 1. (Engineering Risk Assessment) *Established RA methodology and approaches as common in non-IT areas.*

The term engineering RA is mainly introduced to highlight differences to the IT RA concept. The framework is well defined in the (outdated) (ISO/IECGuide73 2002). The basic approaches and concepts as, e.g., FMEA, Fault Tree Analysis and Probabilistic Safety Analysis, are supposed to be known to the reader. Major goals are hazard identification and its impact on environment. Typical fields of application are chemical industry and nuclear power generation.

Definition 2. (IT Risk Assessment) *RA methodology and approaches to evaluate IT systems as common in computer sciences.*

The framework of IT RA is mainly influenced by IT security analyses dealing with Confidentiality, Integrity, and Availability (CIA) of data or assets. Major goals are the identification of external threats on and weak points of an IT infrastructure network. In fact, IT RA is a vulnerability analysis concordant with (ISO/IECGuide73b 2009) and (NIST 2012). It also comprises control analyses similarly to Bow Tie Diagrams. Following the definition of the NIST Guide, risk is:

Definition 3. (Risk) *A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*

Following the NIST Guide again, the IT RA process comprises four primary working steps:

1. *Prepare for risk assessment* (Derived from organisational risk frame)
2. *Conduct assessment*: identify threat sources and events; identify vulnerabilities and predisposing conditions; determine likelihood of occurrence; determine magnitude of impact; determine risk. (For the close connections of risk, vulnerability and resilience analysis see, e.g., (Pasman et al. 2013)).
3. *Communicate results*
4. *Maintain assessment*

MEHARI 2010 (Method for Harmonized Analysis of Risk) (MEHARI 2010) is a (rare) IT RA check list based approach following these steps, basing on (Stoneburner et al. 2002), and the Code of Practice in IT security (ISO/IEC-27002 2005).

3 UNIFIED MODELING LANGUAGE DIAGRAMS

3.1 *Framework and terms*

UML originally supports software development for business process modelling:

Definition 4. (UML) *The UML serves to "specify, visualize, and document models of software systems, including their structure and design …" (OMG 2013).*

In the meantime, "… just about any type of application, running on any type and combination of hardware, operating system, programming language, and network …" can be displayed in UML (OMG 2013). The UML is "… independent from […] subject and realisation area. It provides notation elements equally for static and dynamic models of analysis, design and architecture and especially supports object-oriented approaches" (Rupp and Queins 2012). This reference also states that UML notation and related diagrams are supported by various industrial branches which has made standardisation possible. The engineering RA community rarely uses UML. According to the authors' opinion, the UML proximity to business, IT and domain flexibility makes them an underestimated resource for RA of IT systems. However, UML does not provide risk assessment, meaning that extensions and adaptations to risk are necessary to develop as already be on hand for IT security analyses.

The OMG Website (OMG 2013) defines three major categories of UML 2.0 diagrams and overall thirteen different types:

1. **Structure Diagrams**: Class Diagram, Object Diagram, Component Diagram, Composite Structure Diagram, Package Diagram, Deployment Diagram
2. **Behaviour Diagrams**: Use Case Diagram, Activity Diagram, State Machine Diagram
3. **Interaction Diagrams** (all derived from the more general Behaviour Diagrams): Sequence Diagram, Communication Diagram, Timing Diagram, Interaction Overview Diagram

The methodical affinity between UML system diagrams and common system representations in engineering RA is obvious as both make extended use of graphs. However, the UML semantics are tailored to IT needs, but nevertheless there are already efforts to fit UML into the engineering RA framework e.g., (Viehmann 2012).

Two types of UMLs are most relevant for the paper. A *Class Diagram* pictures the *classes* and their relations (*associations*) in the system as well as how those classes are built and what *operations* they can execute. As Class Diagrams are Structure Diagrams, they cannot show any time-dependent behaviour. This can be done by *Sequence Diagrams*. They show the order and timing of processes and messages between parts of the system. A Sequence Diagram contains *classes* or *objects* that are connected by an *action* or *operation*.

3.2 *Actual use of UML in IT risk analysis*

Not all of the UML types listed in chapter 3.1 are common, practicable and convenient for IT RA purposes. (Petre 2013) analyses the propagation of UMLs for software engineering in industry. According to this study, UMLs in use are (decreasing number): Class Diagram, Sequence Diagram, Activity Diagram, State Machine, Use Case Diagrams. The same study notes, that professional practitioners consider UML as "primilarly an academic thing" whereby it "… has achieved penetration in software engineering education". For this, the named UMLs are known but neither widespread nor popular among software engineers.

(Neubauer and Heurix 2008) discuss approaches of IT system analysis with regard to IT security and IT risk following a non-frequentistic definition. They state a lack of IT security considerations within business processes because the basic Business Process Modelling (BPM) approaches do not support a semantic of security. UML and ARIS (Architecture of Integrated Information Systems) are named as most popular modelling languages for BPM whereas non of them include methods of "security-related entities". As a consequence, supplementary security (and risk) levels are needed.

With regard to IT security issues, UMLsec (Jürjens 2004) is most prominent in literature. Methodology and tool use a sophisticated UML notation, semantic and formalism to characterise IT security demands as well as to analyse the diagrams byan "automated first-order logic theorem prover."

CORAS is also a frequently named tool and "platform for risk analysis of security critical systems" (CORAS 2014). The CORAS procedure can be split into eight steps (CORAS 2013) following the common RA working steps as presented, e.g., in chapter 3. The methodology is designed around a graphical modelling language based on UML (Stølen 2013), i.e., on adapted Use Case Diagrams (c.f., (Lund et al. 2011)). These UMLs can be supplemented by a syntax for risk graphs(c.f., (Braber et al. 2006)). In four diagram types, the audit team can visualise the relations among assets, how actors threaten those assets, what risks have been discovered and how these specified risks can be treated. The diagrams are gradually built during brainstorming sessions or workshops between the audit team and representatives of the audited enterprise. The diagrams of the CORAS tool offer designated fields for *likelihood* and *consequence* value inputs. However, those fields do not enforce a formal input format. Therefore, the tool cannot be used to automatically calculate any risk values.

In the end, the UMLsec approach needs an extended training period at least. As a consequence, UMLsec is resource-intensive and a bit on the complex side for SME or everyday IT security checks. On the other hand, CORAS is mainly a tool to support brainstorming. Both approaches basically cover the area of IT security and therefore, they are no designated RA tools.

3.3 *Taxonomy for IT risk assessment purposes*

(Paintsil 2012) suggests a taxonomy for information system security RA approaches which clarifies the position and framework of UMLs as well as the proposed RA approach as presented in the following chapter. This taxonomy bisects RA approaches in bottom-up/IT-centric and top-down/information-centric. The (traditional) IT security RA approaches are bottom-up and asset oriented. "They assess risk by identifying an asset and its value, and the likelihood of an unwanted incident and its consequence for the asset". Checklist based or compliance audit approaches, UML-based CORAS approach, and Fault Tree Analysis belong to this category. "The top-down approach is requirement-oriented. It focuses on the security needs of a system or an organization. These security needs are based on requirements for CIA as well as risk to infrastructure, legal, and regulatory or statutory requirements". Non-traditional ("contemporary") approaches are, e.g., Colored Petri Nets (bottom-up) and UMLsec (top-down). According to this taxonomy, the proposed approach in chapter 4 is bottom-up/IT-centric.

4 METHODOLOGICAL ENHANCEMENTS

The proposed approach of this paper uses Class and Sequence Diagrams to analyse specific business processes for risks. For this, the UMLs are automatically generated based on the source code of the business process. However, a practical problem emerged as these diagrams show the complete business process which makes them quickly unclear for analysts. Moreover, these UMLs often encompass many details irrelevant for RA purposes. Therefore, the proposed RA approach includes a procedure to reduce the Class Diagrams which are then the base for further RA working steps. The RA approach is exemplified by a business process at milliPay Systems AG. The company develops and offers a micropayment system, which facilitates very small transactions (micro transactions) between users and vendors, ranging from 0.0001 to 3 Swiss Francs. The examples presented are greatly simplified for easier reading and understanding.

4.1 *Reducing the Class Diagram*

4.1.1 *Full System Diagram*

The starting point is the generation of UMLs from source code by a software tool. The authors use (Architexa 2013), because the tool offers Class and Sequence Diagram generation and is seamlessly integrable into *Eclipse*, milliPay's development environment. The tool does not modify the source code and Sequence Diagrams can be built step by step so that the user may leave out irrelevant information like library code or private methods. Further tools that offer similar support are, e.g., (Visual Paradigm 2014), Astah (Change Vision 2014), and eUML (Soyatec 2013). Figure 1 shows the automatically generated Class Diagram of milliPay's payment module.

In Figure 1 **`PaymentService`** *class* provides *operations* like `identifyUser(…)`, `transfer(…)` money and getting the product with `getProduct(…)`. Other *classes* are connected (*associated*) to **`PaymentService`** that symbolises the process structure. **`CryptoEngine`**, e.g., is used to secure the payment process.

4.1.2 *Sequence diagram of a specified process*

In the next step, the audit team decides which business process should be evaluated, e.g., **`PaymentService`** and `transfer(…)`. Then, a Sequence Diagram is generated showing each *operation* of the process. Again, *Architexa* supports the generation of this diagram. Figure 2 shows the resulting Sequence Diagram.

The Sequence Diagram shows the orders of *classes* and the execution of the *operations*. In Figure 2 **`PaymentService`** encompasses the main steps of the process by executing `transfer(…)`.

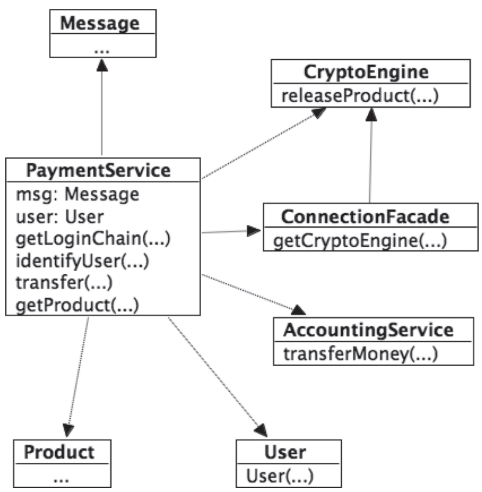


Figure 1. Full system Class Diagram (excerpt).

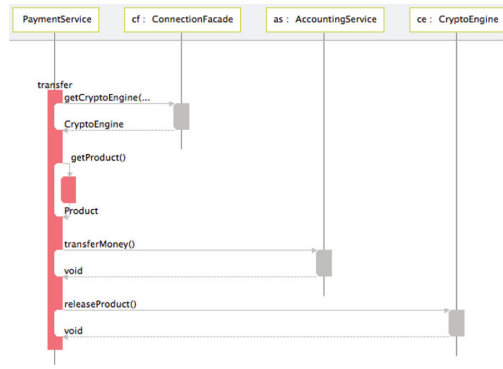


Figure 2. Sequence Diagram of specified business case.

4.1.3 *Reduced Class Diagram*

As mentioned before, the full Class Diagram also contains information that is not relevant to the chosen business process. For instance, there is no need to identify the user in the Class Diagram in Figure 1 for the specified process. (If she had not aready been identified, she would not be able to start a purchase). Thus, **`User`** and `identifyUser(…)` are removed from the Class Diagram. The easiest way to proceed is to go through the Sequence Diagram step by step, from left to right, as this diagram shows which *classes* and *operations* are needed for a process. Each step considers:

1. the starting *class*
2. the target *class*
3. the *operation* from the starting to target *class*.

Each of these three elements is labelled in the full scope Class Diagram. Labelling means that a specified *class* or *operation* is relevant and should not be removed. In this example, labelled classes are **`PaymentService`**, **`CryptoEngine`**, **`ConnectionFacade`**, **`AccountingService`** and **`Product`**, since these *classes* are used for *operations* in this Sequence Diagram. In the end, **`PaymentService`** contains two labelled *operations*, because **`transfer(…)`** also calls `getProduct(…)`. Other *operations* in other classes are labelled as well since they connect the marked objects.

Figure 3 depicts the resulting reduced Class Diagram.

4.2 *Utilisation of UML for RA purposes*

Figure 4 summarises the process by using automatically generated Class and Sequence Diagrams of a specified business process source code as raw material for IT RA purposes.

These UMLs do not contain any information about impacts, likelihoods and resulting risks.

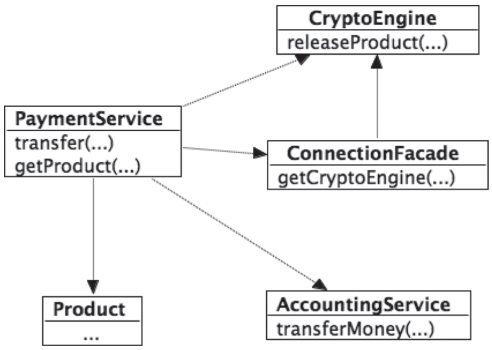


Figure 3. Reduced Class Diagram.

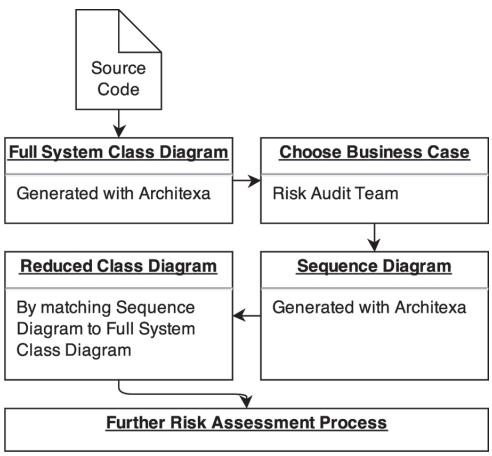


Figure 4. RA process.

However, they structure an FMEA-like RA approach and offer some heuristics to value the orders of magnitudes, e.g., on scales of 1 to 10 (1: rare/negligible to 10: frequent/disastrous). For this, the following working steps are suggested:

Step 0: Preparational Work: Selection of an *operation* to be analysed and generate Class and Sequence Diagrams.

Step 1: Analysis of Classes: The generated UMLs base on the same source code and as a result, the same business process is considered from different angles. In order to structure the IT RA process, *classes* and *operations* are disassociated.

– Many outgoing *associations* (edges) of a *class* in a Class Diagram indicate that it uses many other classes. The corresponding Sequence Diagram also shows many connected *classes*. This dependency exposes the *class* to an increased likelihood of malfunction and may also indicate a major impact. However, the latter needs business specific assessments (or depends on the analysis framework).
– Many incoming *associations* (edges) of a *class* indicate that it is used by many other *classes*. A malfunction points to an increased impact value.

Step 2: Analysis of Operations: Classes encompass *operations* showing further details of the specified business process. The malfunction of an *operation* is considered as a failure mode in the context of an FMEA approach. The Sequence Diagram shows its position within the business process chain. An initial position of an *operation* roughly indicates a more serious impact on the overall business process than a rear light one.

Following the milliPay example, `getProduct(…)` (e.g., an offered journal article) of `PaymentService` is in the beginning of the business process along `transfer(…)` as shown in the Sequence Diagram of Figure 2. A malfunction of this *operation* might result in the wrong amount of transferred money and to a wrongly released product, i.e., a serious impact on business. Note, this operation is indicated as a continuous red-shaded (dark grey in a black & white copy) area in the Sequence Diagram. Hence, any statements are associated with a closed sequence chain.

Step 3: Risk assessment: Following the common FMEA approach, the Risk Prioritisation Value (RPV) is used to identify most important risks, i.e., classes and operations as well as associated sub-business processes, underlying hardware and software, persons responsible to maintain the processes, etc.

The procedure of practical UML utilisation needs supplementary notes:

– *Comprehension*: As *classes* and *operations* in Class and Sequence Diagrams are extracted from the source code, they can easily be found in this code which gives the analyst detailed information about a process. For instance, the code shows the linkage of `getProduct(…)` with a vendor.
– *Impact assessment*: Impact evaluation within RA needs specifications of analysis goals: If the analysis considers, e.g., a single money transfer only, the malfunction of **`PaymentService`** is negligible according to the micropayment business model. If looking on money transfer in general, a malfunction fully touches the business model and consequences would be high.
– *Tools:* For the MICROPAYMENT project, Architexa is used to get UMLs from a Java source code because of practicability. The tool only generates low level (or simplistic) UMLs as shown in this paper, whereas the tool is also able to handle loops, iterations, and conditional statements.

4.3 *Further work*

Within the R&D project MICROPAYMENT, the utilisation process of UMLs for IT RA purposes is in its beginnings. Although the suggested RA procedure looks promising (and practical) for all project partners, the authors have already addressed further work and methodological enhancements. These evolutionary steps are outlined below, as they show the potential of the overall concept.

The original UMLs as provided by the Object Management Group (cf. (OMG 2013)) offer a multitude of notation elements enabling the analyst to depict nearly any system in detail. So, full scope of Class and Sequence Diagram semantics may indicate further information for RA purposes. Examples are (cf. OMG website):

- *associations* (edges) for linking *classes* in Class Diagrams: The basic notation is a non-directed and unlabelled edge between *classes*. Extended notation encompasses roles (indicating the purpose of the linked classes), multiplicity (various rules about the number of objects in each linked class, e.g., 1 to many (1… *)), navigability (unidirectional, bi-directional), aggregation (whole-part relation), composition (as aggregation but the whole-part relation means a physical unit), n-ary (more than two classes are linked), and generalisation (different levels of class abstraction).
- *messages* in Sequence Diagrams: conditional, repetitive, to self.
- The remaining eleven UML types as listened in chapter 3.1 offer further notations, semantics and types of *associations*.

The heuristic to value the risk parameters by Class and Sequence Diagrams is still straightforward. However, the Sequence Diagram makes patterns visible to the analyst. In Figure 5 the specified *operation* highlighted in red (dark grey in a black & white copy) calls-up sequences of *operations* and associated *classes*. Likelihood of malfunction of the specified *class* is expected to be high. The impacts depend on the *classes* involved and tends to be high (sum of impacts).

Figure 6 shows the reverse to Figure 5. The *operations* in red belong to a single *class* which needs the call-up of other *classes*. This may indicate a high likelihood of malfunction of the specified *class*. Impact is given by its malfunction (single class).

In Figure 7, the sequence of *operations* in red also belongs to a single *class*. However, its first *operation* needs a single other *class* and the second triggers the two *operations* of another class. This is an example of a combined sequence, which might be split up into the basic structures of Figures 5 and 6.

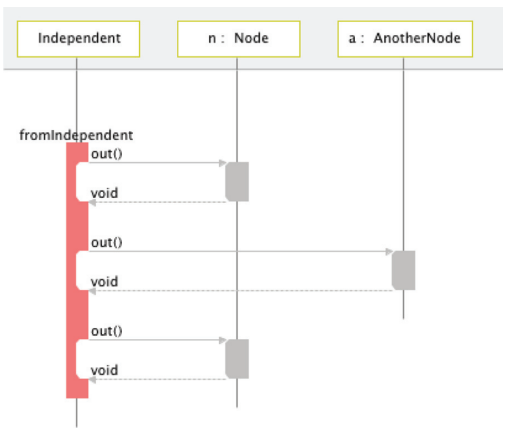


Figure 5. Sequence Diagram plain sequences.

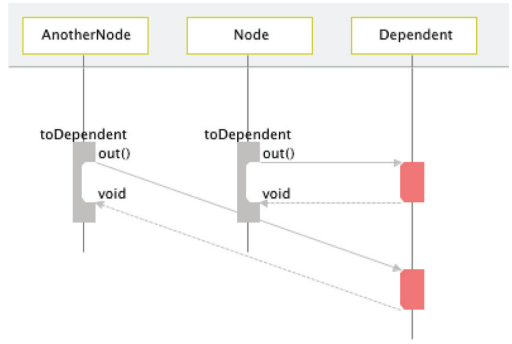


Figure 6. Sequence Diagram: Single class is needed by other classes.

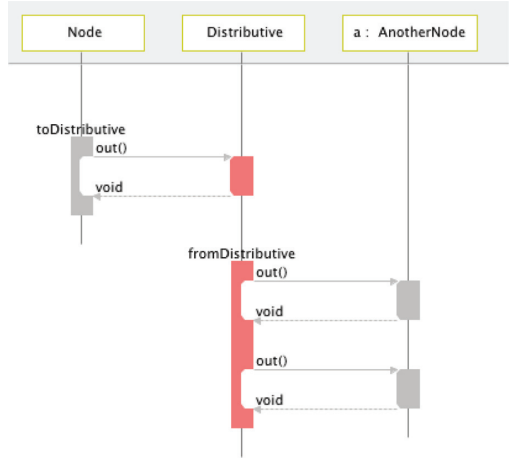


Figure 7. Sequence Diagram one incoming and two outgoing edges.

These basic configurations in Sequence Diagrams show similarities with State Flow Graphs (as, e.g., defined in (Rakowski 2012)). However, as MICROPAYMENT is a typical interdisciplinary R&D project, the possibility of an extended interpretation is still a matter of discussion among the participating engineering risk analysts and computer scientists. State Flow Graph would provide a different and formalised access to risks in the area of IT RA.

5 CONCLUSIONS

The usage of UML diagrams looks promising as it represents a rarely used access to a knowledge base for IT RA. For this, nearly every system or process can be modelled at least by hand. However, the automated generation of UML diagrams from source code highly increases the efficiency of RA. To make this work, a interdisciplinary team of risk analysts and computer scientists is a prerequisite.

The paper outlines basic principles of a UML-based methodology of IT RA. It offers heuristics in order to support the further development of a quick IT RA audit or risk prioritisation tool. As the detailed modelling or simulation of infrastructural IT systems is out of scope at most enterprises, this is considered as a practical approach.

REFERENCES

Architexa (2013). *Get Diagrams From Code*. Architexa. http: //www.architexa.com/; visited: Mar., 2014.

Braber, F.d., G. Brændeland, H.E.I. Dahl, I. Engan, I. Hogganvik, M.S. Lund, B. Solhaug, K. Stølen, & F. Vraalsen (2006, Sept.). The CORAS model-based method for security risk analysis. Technical report, SINTEF.

Change Vision (2014). *Astah*. Change Vision. http:// astah. net/; visited: Mar., 2014.

CORAS (2013, Nov. 28). The CORAS method. Website, CORAS. http://coras.sourceforge.net/.

CORAS (2014). CORAS risk assessment platform. http:// sourceforge.net/projects/coras/; visited: Mar., 2014. ISO/IEC-27002 (2005, June). Information technology—code of practice for information security management. Technical Report ISO/IEC 27002:2005(E), ISO/IEO.

ISO/IEC-Guide73 (2002). Risk management vocabulary guidelines for use in standards. Technical Report ISO/IEC GUIDE 73:2002(E/F), ISO/IEO.

ISO/IEC-Guide73b (2009). Risk management—vocabulary. Technical Report ISO/IEC GUIDE 73:2009(E/F), ISO/IEO.

Jürjens, J. (2004). *Secure Systems Development with UML*. Berlin, etc.: Springer.

Lund, M.S., B. Solhaug, & K. Stølen (2011). Risk analysis of changing and evolving systems using CORAS. In F. o. S.A. (FOSAD'11) and D. VI (Eds.), *Lecture Notes in Computer Science*, Volume 6858, pp. 231–274. Springer.

MEHARI (2010, August). Mehari 2010: Fundamental concepts and functional specifications. Methods, Club de la Securité de l'Information Français. http://www.clusif.fr/en/ clusif/present/; visited: Jan., 2014.

Milanovic, N., B. Milic, & M. Malek (2008). Modeling business process availability. *IEEE Congress on Services 2008*, 315–321.

Mock, R., H. Straumann, & A. Fischer (2014). A second chance for risk assessment in it system analysis? *Proc. of European Safety and Reliability Conference (ESREL 2013)*, 2237–2244.

Neubauer, T. & J. Heurix (2008, March 4–7, 2008). Defining secure business processes with respect to multiple objectives. In *Proc. of the Third International Conference on Availability, Security and Reliability Ares 2008*, pp. 187–194. IEEE Computer Society.

NIST (2012, Sept.). Guide for conducting risk assessments-information security (SP 800-30 Rev.1). Technical report, National Institute of Standards and Technology (NIST).

OMG (2013, Apr. 18). Introduction to OMG's Unified Modeling Language™ (UML®). Website, Object Management Group (OMG). http://www.omg.org/gettingstarted/ what_is_uml.htm/#12DiagramTypes.

Paintsil, E. (2012). Taxonomy of security risk assessment approaches for researchers. In *2012 Fourth International Conference on Computational Aspects of Social Networks (Cason)*, pp. 257–262.

Pasman, H.J., B. Knegtering, & W.J. Rogers (2013). A holistic approach to control process safety risks: Possible ways forward. *Reliability Engineering & System Safety 117*, 21–29.

Petre, M. (2013, May 18–26). UML in practice. In *35th International Conference on Software Engineering (ICSE 2013)*.

Rakowski, U. K. (2012, June). Zustandsflussgraphen (VDI 4008 Blatt 5). Technical report, Verein Deutscher Ingenieure. http: //www.beuth.de/de/technische-regel-entwurf/vdi-4008-blatt-5/143907370; visited: Mar., 2014.

Rupp, C. & S. Queins (2012). *UML 2 glasklar—Praxiswissen für die UML-Modellierung* (4. ed.). Munich: Carl Hanser Verlag.

Soyatec (2013). *eUML*. Soyatec. http://www.soyatec.com/euml2/; visited: Mar., 2014.

Stølen, L. (2013, Nov. 28). The CORAS language. Website, CORAS. http://coras.sourceforge.net/coras_language.html.

Stoneburner, G., A. Goguen, & A. Feringa (2002). Risk management guide for information technology systems. Technical report, National Institute of Standards and Technology (NIST).

Viehmann, J. (2012, Sept., 3–5). Reusing risk analysis results—an extension for the CORAS risk analysis method. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pp. 742–751.

Visual Paradigm (2014). *Visual Paradigm for UML 11*. Visual Paradigm. http://www.visual-paradigm.com/product/vpuml/; visited: Mar., 2014.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantitative risk assessment of new ship designs in damage conditions

M.K. Gerigk
Gdańsk University of Technology, Gdańsk, Poland

ABSTRACT: The paper is devoted to safety of ships in damage conditions. The novel contribution of the paper is connected with a new Multi-Task ship (MT-ship) design at the preliminary stage of design. There are a few problems at the preliminary stage that should be considered. One problem is connected with if the quantitative risk-based method is a reliable and formal method for safety assessment of such the new design (MT-ship) in damage conditions. The current method of safety assessment of commercial ships in damage conditions is based on the requirements included in the SOLAS 2009 regulations. The methods of safety assessment of navy ships in damage conditions belong to the different classification societies and navies. Further development of the SSADC method is connected with its application for safety assessment of a few novel designs.

1 INTRODUCTION

The novel contribution of the paper is connected with a new Multi-Task ship (MT-ship) design at the preliminary stage of design which does not belong to either the passenger, cargo or navy ships.

There are a few problems at the preliminary stage of such the design which have to be taken into account. One problem is connected with if the quantitative risk-based method is a reliable and formal method for safety assessment of such the new design (a new MT-ship) in damage conditions. Another issue is associated with an approach to safety assessment. It may still be considered to use a prescriptive or risk-based oriented approach included in the existing regulations depending on if the MT-ship is a special task ship for either a commercial or navy use. In such the situation the proposed method may still be treated as an alternative method for safety assessment of ships in damage conditions.

The current method of safety assessment of commercial ships in damage conditions is based on the requirements included in the SOLAS 2009 regulations. This method is of prescriptive character and based mainly on the experience in design and operation. It is reliable and harmonized. It is easy to apply for the commercial ships, passenger and cargo ships. It is more devoted to the design stage and is difficult to apply in operation. The measure of safety of a ship in damage conditions is the probability of surviving a collision known as the subdivision index A (IMO 2005, SOLAS 2005, Gerigk 2010, IMO 2014).

Those methods are prescriptive in their character and based on the probabilistic approach to safety. In some cases the semi-probabilistic components are incorporated in those regulations. The main disadvantage of those methods is that they do take into account the fixed set of scenarios of an accident. It means the safety assessment of ships in abnormal/damage conditions concerns considering the flooding of single compartments, groups consisting of two watertight compartments, groups consisting of three watertight compartments, etc. The next disadvantage associated with application of those methods regards the problem that using those methods in case of certain types of ships e.g. car-carriers, ro-ro vessels or passenger ships may lead to insufficient level of safety or provide unnecessary design or operational restrictions.

The basic criteria of the prescriptive method included in the SOLAS 2009 regulations is the condition as follows, (IMO 2005a, IMO 2005b, IMO 2008):

$$A > R \tag{1}$$

where A = attained subdivision index calculated for the draughts d_s, d_p and d_1 defined in regulation 2, according to the formula, IMO (2005):

$$A = \sum p_i s_i \tag{2}$$

where p_i = probability that only the compartment or group of compartments under consideration may be flooded, as defined in regulation 7-1; s_i = probability of survival after flooding the compartment or group of compartments under consideration, as defined in regulation 7-2; R = required subdivision index.

The probabilities p_i and s_i are calculated according to the well known formulae accepted by IMO,

(IMO 2005a, IMO 2005b, IMO 2007). The typical process of assessment of safety of ships in abnormal/damaged conditions at the design stage or when the survivability of existing ships is considered is directed to satisfy the criteria (1).

The methods of safety assessment of navy ships in damage conditions belong to the different classification societies and navies. For example the current quasi-static damage stability criteria method used by the UK MoD is largely based on the Sarchin and Goldberg work published in 1962 (Peters A.J. et al. 2009, Smith D. et al. 2009).

The method presented in the paper called as the SSADC (Ship Safety Assessment in Damage Conditions) method is a risk-based method. It is based on assessment of the ship performance and risk assessment. It enables to quantify the risk and use it a measure of a ship safety. The method is of non-prescriptive character. It may be treated as a prescriptive method form the formal point of view if the structure of requirements in the form of any known regulations are used.

Although some elements of the SSADC method have been published it is important to underline that further development of the SSADC method is connected with its application for safety assessment of novel ship designs and ocean engineering objects in damage conditions.

2 THE SSADC METHOD OF SAFETY ASSESSMENT OF SHIPS IN DAMAGE CONDITIONS

In the following chapter the basic information on the SSADC (Ship Safety Assessment in Damage Conditions) method is introduced. The methodology where the risk-based design and a formalized design methodology were integrated together the first time was introduced by Vassalos and the others, (Skjong et al. 2006, SSRC 2009, Vassalos 2006).

The SSADC method is a kind of performance-oriented risk-based method which enables to assess the safety of ships in damage conditions at the design stage, in operation and during the ship salvage using the same procedure, Gerigk (2010). Within the SSADC method the holistic approach to safety assessment is applied. The method is based on implementation of the system approach to safety. In general, the method takes into account the influence of design and operational factors on safety including the safety management related factors as well.

For the ship performance evaluation the statistics, investigations using the physical models and numerical simulation techniques may be applied. The ship performance estimation enables take into account the influence of the intermediate events, additional events (releases) and consequences on the ship behavior. This may be done for the data sequence of events for an accident under consideration.

The risk assessment is based on application of the matrix type risk model which is prepared in such a way that it enables to consider almost all the scenarios of events regarding the considered accident.

The criteria within the method is to achieve an adequate level of risk using the risk acceptance criteria, risk matrix or ALARP concept, Gerigk (2010).

Providing a sufficient level of safety based on the risk assessment is the main objective. It is either the design, operational or organizational objective. Safety is the design objective between the other objectives. The measure of safety of a ship in damaged conditions is the risk (level of risk).

The SSADC method may be used at any ship's life circle, including safety assessment of a ship during a catastrophe. Some elements of the method can be used for safety assessment of different means and systems of maritime transportation.

The SSADC is still being developed taking into account the latest developments regarding the safety of ships in damage conditions, (Vanem E. et al. 2009, Jasionowski A. 2011, Papanikolaou A. et al. 2013, Montewka J. et al. 2014).

The SSADC method is based on the following main steps:

- setting the requirements, criteria, limitations, safety objectives;
- defining the ship and environment;
- identifying the hazards and identifying the sequences of accident (scenarios development);
- assessing the ship performance in damage conditions;
- estimating the risk according to the event tree analysis ETA and matrix type risk model (risk is estimated separately for each scenario of the accident under consideration);
- assessing the risk according to the risk acceptance criteria (risk matrix and in some cases ALARP concept) and safety objectives;
- managing the risk according to the risk control options;
- selecting the design (or operational procedure) that meet the requirements, criteria, limitations, safety objectives;
- optimizing the design (or operational procedure);
- making the decisions on safety, (Abramowicz-Gerigk 2006, Abramowicz-Gerigk 2008b, Abramowicz-Gerigk & Burciu 2013, Arangio 2012, Burciu & Grabski 2011,

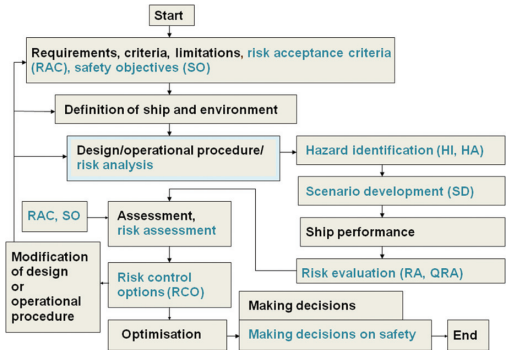


Figure 1. Structure of the method of risk and safety assessment of ships in damaged conditions.

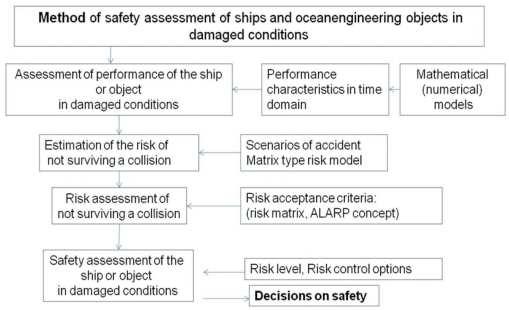


Figure 2. Structure of the SSADC sub-method for safety assessment of ships and oceanengineering objects in damaged conditions.

Gerigk 2004, Gerigk 2005, Gerigk 2006, Gerigk 2008, Gerigk 2010, Gerigk 2012, Nowakowski & Werbińka 2009).

The structure of the SSADC method is presented in Figure 1, Gerigk (2010).

The structure of the SSADC sub-method (see the module called as "Ship performance" in Fig. 1) for safety assessment of ships and oceanengineering objects in damaged conditions is presented in Figure 2, Gerigk et. al. (2012).

3 ASSESSMENT OF A SHIP (OBJECT) PERFORMANCE IN DAMAGED CONDITIONS

Flooding process and floodwater dynamics. The behaviour of a damaged ship is following from three major mechanisms:

– flooding process and dynamics of floodwater,
– interaction between floodwater and damaged ship,
– damaged ship motion in waves.

The flow through the damage (opening or openings) is estimated according to the equation which can be obtained from the Bernoulli's equation for the steady flow of water.

Interaction between floodwater and ship (object) dynamics. The effect of interaction between floodwater and damaged ship motion can be estimated using either the added weight or added force concept. According to the added weight concept, the floodwater should be treated as an added weight with a moving centre of gravity which changes the location of the ship's overall centre of gravity. It should be taken into account that as the total mass of the ship is changed during flooding so the inertia forces should be changed as well. The floodwater does not experience a negative vertical acceleration. In the case of the added force concept the forces due to the floodwater are treated as external forces. The forces due to floodwater should be calculated using the instantaneous acceleration rather than gravitational acceleration and by integrating water pressure at the compartment walls. There are three methods of modeling the floodwater—damaged ship motion interaction as presented in Table 1, ITTC (2011).

There are three methods of modeling the floodwater—damaged ship motion interaction as presented in Table 1, ITTC (2011).

As it is presented in Figure 1 the floodwater dynamics can be predicted using various models ranging from the second order ordinary differential equations through to numerical fluid mechanics (CFD).

Taking into account the modeling of floodwater-ship motion interactions it has been decided to use at this stage of research the quasi-static model first of all. Obtaining the promising results of assessment of performance using this model it has been decided to apply the quasi-dynamic model after that. It such the way it is possible to compare the behavior of the damaged ship applying both the models of the floodwater-ship motion interactions.

The excitation accumulated food water forces should be calculated according to the following assumptions:

– water in the flooded compartment moves in the quasi-static way;

Table 1. Models of the floodwater—damaged ship motion interaction.

	Floodwater treatment	Interaction concept
Quasi-static	Static	Added weight
Quasi-dynamic	Dynamic	Added weight
Dynamic	Dynamic	Added force

– free surface of water in the flooded compartment is flat and moves in different way depending on the model.

The schemes of the floodwater-ship interactions in the case of the quasi-static model with the horizontal free surface in the flooded compartment are graphically presented in Figure 3, ITTC (2011), bibliography (2012). In the case of the quasi-dynamic model the free surface in the flooded compartment is not horizontal. It is flat and changing according to the ship motions in each time step.

Damaged ship (object) motion in waves. Generally, the 2-D strip method or 3-D panel method may be used to calculate the radiation elements within the equations of damaged ship motions together with the direct integration used to calculate the non-linear restoring forces. Some studies calculate the damaged ship motion in 6DoF (six degrees of freedom) domain. At this stage of studies the 3DoF domain has been applied. The roll viscous dumping is added by the use of empirical formulae. The linear memory effect function (added mass and wave damping) is used even for the large amplitude motion and heeling condition, Bertram (2004), Dudziak (2008), Faltinsen (1990), Gerigk (2010), Krężelewski (1982). This issue has been recognized as a serious scientific and research problem to be solved in the future.

Assessing the damaged ship performance it has been anticipated that the ship may have six degrees of freedom in damaged conditions. Although at this stage it is assumed that the most important from the safety of damaged ship point of view are the following degrees of freedom: sway, heave and roll.

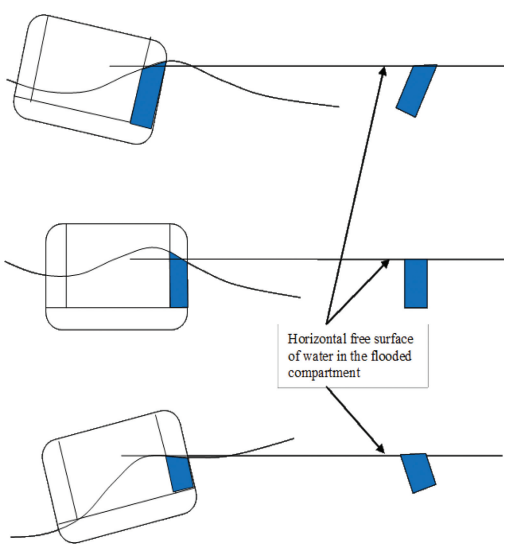


Figure 3. The graphical interpretation of the quasi-static model with the horizontal free surface in the flooded compartment.

4 THE MATRIX TYPE RISK MODEL

The safety case concerns the ships in abnormal/damage conditions when the ship skin is damaged due to the following hazards: collision, grounding, stranding or another reason, Gerigk (2010).

The risk assessment starts from the modeling of the risk contribution tree. For each hazard a separate event tree should be modeled using the Event Tree Analysis ETA, Gerigk (2010).

The holistic approach to ship safety has been applied. According to this approach two major assumptions have been done. First that the system failures can be either the hardware, software, organizational or human failures. The second assumption was that the risk model for assessment of safety of ships in abnormal/damage conditions should be the holistic risk model. The holistic risk model should enable to take into account almost all the possible scenarios development, Gerigk (2010).

From the mathematical point of view the relations between the events within an event tree (ETA) are represented by the conditional probabilities which are the components of the risk formula for each sequence of events (accident scenario), Gerigk (2010).

The basic formula for the risk evaluation associated with the different hazards and scenario development is according to the well known general formulae, Gerigk (2010):

$$R_i = P_i \times C_i \tag{3}$$

where P_i = probability of occurrence of a given hazard; C_i = consequences following the occurrence of the data hazard and scenario development, in terms of fatalities, injuries, property losses and damage to the environment.

The risk model (6) may have four different kinds of losses regarding the Human Fatalities (HF), Cargo and Ship Losses (CS), Environment pollution (E) and Financial losses ($) and for the ship in damaged conditions can be presented as follows:

$$R = P_c \, P_{c/f} \, PoC_{dam} \times C \tag{4}$$

where P_c = probability of collision (hazard); $P_{c/f}$ = probability of flooding having the ship hit from given direction at data position with given extent conditional on collision; PoC_{dam} = probability of capsizing in damaged conditions in given time conditional on having flooding when the ship is hit from given direction at data position with given

extent conditional on collision; C = consequences regarding the fatalities, property (cargo, ship), environment and finance ($C = C_{HF/C}, C_{CS/C}, C_{E/C}, C_{\$/C}$).

The PoC_{dam} probability of capsizing in damaged conditions in given time can be calculated according to the following formulae, Gerigk (2010):

$$PoC_{dam} = P_{c/f/ns} P_{c/f/ns/tts} \tag{5}$$

where $P_{c/f/ns}$ = probability of not surviving conditional on having flooding when the ship is hit from given direction at data position with given extent conditional on collision; $P_{c/f/ns/tts}$ = probability of given time to sink conditional on not surviving the conditional on having flooding when the ship is hit from given direction at data position with given extent conditional on collision.

The PoC_{dam} probability can be estimated during the accident at sea using the following methods, Gerigk (2010):

- binary method;
- method based on definition of the probability of surviving a collision;
- method based on definition of the damage stability;
- method based on definition of the ship performance during the accident.

In the case of the last method the roll function in time domain has been anticipated as a major characteristcs/function enabling the risk assessment, Gerigk (2010).

The risk analysis requires to calculate the conditional probabilities regarding the initial events ZI_i, major events (hazards) ZG_j, intermediate events ZP_k and final events ZK_l which can be treated as consequences. The basic mathematical formula are as follows, Gerigk (2010).

First of all the row matrix of initial events is evaluated:

$$P(ZI) = P(ZI_i) \text{ for } i = 1 \text{ to } n \tag{6}$$

Then the matrix of major events is calculated:

$$MP_{ZG} = P(ZG_j/ZI_i) \text{ for } j = 1 \text{ to } m \tag{7}$$

After that the matrix of intermediate events is calculated:

$$MP_{ZP} = P(ZP_k/ZG_j) \text{ for } k = 1 \text{ to m1} \tag{8}$$

Then the matrix of final events is calculated:

$$MP_{ZK} = P(ZK_l/ZP_k) \text{ dla l} = 1 \text{ do m2} \tag{9}$$

Finally, the row matrix of final events may be estimated as follows:

$$P(ZK) = P(ZI)\ MP_{ZG}\ MP_{ZP}\ MP_{ZK} \tag{10}$$

The above mathematical model is representing the entire risk model called as the matrix type risk model. This model enables to consider almost all the possible scenarios of an accident using an event tree. In the case when the additional events occur the $PoC(C_i)$ probability of occurring the C_i given consequences can be calculated according to the formula presented by Gerigk, Gerigk (2010). The typical additional events may concern the water on deck, air cushions, cargo leakage, additional heeling moments or passenger behavior.

5 APPLICATION OF THE SSADC METHOD

The ship accidents at sea may lead to the loss of life, loss of properties (ship and cargo) and pollution of environment. The modern approach to safety of maritime transportation requires to apply the so-called life-circle approach by integrating the design for safety, safe operation and safe salvage methods. The effective safety assessment methods requires to develop the methods, models and tools for the assessment of risk and safety of ships in damaged conditions.

The SSADC method of safety assessment of ships in damage conditions together with the matrix type risk model enables to assess a ship safety almost for all the possible accident scenarios including the ship survivability at each stage of flooding process including the preliminary, intermediate and final stages of flooding.

Such an approach to ship safety assessment in damage conditions is necessary to predict any further deterioration of the damage condition. If the ship survives flooding and is unable to return to port under own power it is necessary to solve the problems associated with the towing when waiting for an assistance. During the towing the risk and safety assessment of the ship should be permanently conducted (Perera & Soares Guedes 2011, Skjong & Vanem & Rusas & Olufsen 2006, Soares Guedes & Teixeira 2001).

The structure of the entire procedure for the assessment of safety of ships in abnormal/damage conditions during the accident at sea and for the salvage purposes was published by Gerigk, (Gerigk 2010, Gerigk 2012).

The example applications of the SSADC method has been done for two ships and one ocean engineering object.

An example of application concerning a new Multi-Task ship (MT-ship) is presented in the paper.

The MT-ship has the main data as follows:

- length: $L_{BP} = 60{,}0$ m
- breadth: $B = 8{,}0$ m
- heigth to the main deck: $H = 9{,}35$ m

The basic information on the hull form of the MT-ship is presented in Figure 4.

During the safety assessment of the MT-ship in damage conditions the following scenarios were considered to be flooded:

– scenario 1: combined compartment 1
– scenario 2: combined compartment 2
– scenario 3: combined compartment 3
– scenario 4: combined compartment 4
– scenario 5: combined compartment 5
– scenario 6: combined compartment 6
– scenario 7: combined compartment 7

The Mt-ship has no conventional arrangement of internal spaces therefore each combined compartment consists of a few sub-compartments.

The event tree analysis was done for the MT-ship. It is not published, yet,

Generally, thirteen safety functions have been used for each event tree from the MT-ship safety in damaged conditions point of view. Between them are as follows:

– function1 (avoiding the hazard),
– function 2 (hull skin damage (flooding)),
– function 3 (position and extension of damage),
– function 4 (equalization of the ship heel at the preliminary stage of flooding),
– function 5 (loss of the ship stability at the preliminary stage of flooding),
– function 6 (loss of the ship stability during the intermediate stages (and phases) of flooding),
– function 7 (loss of the ship stability at the final stage of flooding),
– function 8 (loss of the ship floatability at the final stage of flooding),

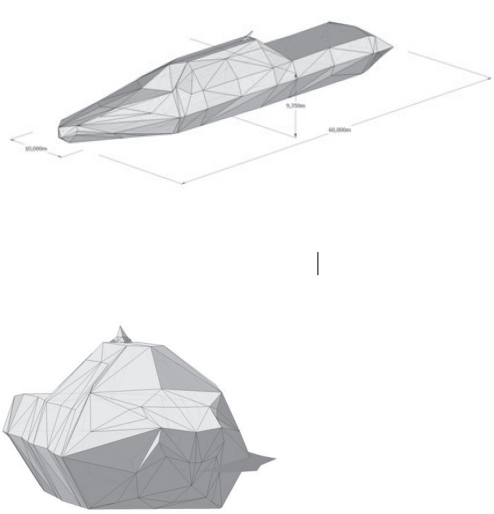


Figure 4. The hull form of the MT-ship.

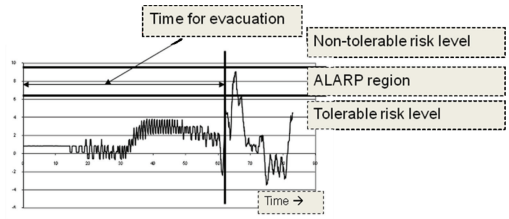


Figure 5. An example of the roll function in time domain and ALARP risk evaluation criteria applied for the assessment of safety of the MT-container ship in damaged conditions.

– function 9 (ship is waiting for assistance),
– function 10 (ship returns to port under own power),
– function 11 (ship returns to port by tow),
– function 12 (ship is continuing the mission),
– function 13 (fire and/or explosion).

Assessing the performance of the damaged MT-ship the following impacts were taken into account, (Abramowicz-Gerigk 2005, Abramowicz-Gerigk 2008a, Gerigk 2004, Gerigk 2005, Gerigk 2006, Gerigk 2008, Gerigk 2010, Gerigk 2012):

– gravitational forces,
– hydrostatic forces,
– excitation Froude-Krylov forces,
– excitation diffraction forces,
– accumulated flood water forces,
– cargo shift forces.

An example of the damaged MT-ship performance data as the roll function in time domain is presented in Figure 5. The vertical axis regards the angle of heel and the horizontal axis concerns the time in seconds. During the conference the latest results of investigations concerning the MT-ship performance data and risk assessment results will be presented.

6 CONCLUSIONS

A few elements of the method of assessment of safety of ships in damaged conditions are presented in the paper. The method is based on the assessment of ship performance and risk assessment.

The key issue to apply the method is to have the proper model for the performance assessment of ships in damaged conditions and risk model for the risk assessment. At this moment the model for the ship (object) performance assessment has been prepared to obtain the three major hydromechanics' characteristics of the damaged ships. These are as follows: sway, heave and roll. For estimating

the sway, heave and roll motions either the quasi-static or quasi-dynamic models presented in chapter 3 may be used. The crucial issue of the damaged ship (object) performance assessment is to decide which hydromechanics' characteristic in the form of the sway (heave or roll) process in time domain should be used to estimate the risk value. For the ships in damaged conditions it is the roll function. At this stage of research the risk assessment can be performed using the ALARP concept. This is to investigate how much time a captain has to evacuate the damaged ship (object).

The current research is associated with further development of the performance procedures of ships in damaged conditions.

The method has the following features:

1. no disadvantages which exist in SOLAS;
2. holistic approach to safety (design, operation, catastrophe, salvage);
3. holistic approach to safety: safety factors (sources of factors: design, operation, management, human factor);
4. holistic approach regarding the risk model;
5. assessment of safety for all the possible scenarios.

The key issue to apply the method is to have the proper matrix type holistic risk model. The proposed risk model enables to estimate the risk level for all the possible scenarios of an accident. The proposed risk model is much more complicated than the models published in literature.

The assessment of damaged ship performance using the CFD based method is the best way to obtain the damaged ship performance characteristics in time domain at the design stage. As an alternative the damaged ship performance may be performed using the model tests.

The current research is associated with further developing the risk models necessary for the ship performance-oriented and risk-based assessment. From the practical point of view the research should bring a model for the computer simulation of the ship salvage process.

The research has been carried out at the Gdansk University of Technology according to support obtained from the Ministry of Science and Higher Education in Warsaw. The author would like to express his sincere gratitude to the above organisations.

REFERENCES

Abramowicz-Gerigk T. 2005. Investigation on Standards for Ship Manoeuvring Performance at Slow Speed in Constrained Space. in C. Guedes Soares, Y. Garbatow & N. Fonesca (eds.), Maritime Transportation and Exploitation of Ocean and Coastal Resources. Vessels for Maritime Transportation. *Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean (IMAM'2005),* Lizbona, Portugalia 2005, Vol.1: 3–8. London, Balkema.

Abramowicz-Gerigk T. 2006. Determination of Safety Factors for Ship Berthing Operations. Proceedings and Monographs in Engineering, Water and Earth Sciences. *Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006), Volume 3,* Estoril, Portugal, 18–22 September 2006, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 2737–2742.

Abramowicz-Gerigk T. 2008a. Experimental study on the hydrodynamic forces induced by a twin-propeller ferry during berthing. *Ocean Engineering. Elsevier.* Vol. 35, Issues 3–4, March 2008: 323–332.

Abramowicz-Gerigk T. 2008b. The risk analysis of harbour operations. in S. Martorell, C. Guedes Soares & Julie Barnet (eds.) Safety Reliability and Risk Analysis: Theory, Methods and Applications. Proceedings of the ESREL 2008 and 17th SRA-Europe Conference, Valencia, Vol. 4: 3343–3350, London: Balkema.

Abramowicz-Gerigk T., Burciu Z. 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. in C. Guedes Soares, & F. Lopez Pena (eds.) *Developments in Maritime Transportation and Exploitation of Sea Resources. Proc. 15th Int. Congress of the International Maritime Association of the Mediterranean (IMAM'2013)*, A Coruna, Vol. 2: 699–704, London: Balkema.

Arangio, S., 2012. Reliability based approach for structural design and assessment: performance criteria and indicators in current European codes and guidelines. *International Journal of Lifecycle Performance Engineering*, 1(1), p. 64.

Burciu, Z. & Grabski, Fr. 2011. The experimental and theoretical study on the reliability of the life rafts. *Reliability Engineering and System Safety 96:* 1456–146.

Gerigk M. 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. *Polish Maritime Research*, No. 1 (39), Vol. 11, 8–13.

Gerigk M. 2005. Challenges of modern assessment of safety of ships in critical conditions. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean IMAM 2005*, Volume 2, Lisboa, Portugal, 26–30 September 2005, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 1529–1536.

Gerigk M. 2006. A method for assessing hazards, risks and safety of damaged ships at sea. Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006), Volume 3, Estoril, Portugal, 18–22 September 2006, Published by Taylor & Francis/Balkema, London/Leiden /New York/Philadelphia/Singapore, 2783–2790.

Gerigk M. 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference, ESREL 2008 and 17th SRA-Europe*, Volume 4, Valencia, Spain, 22–25 September 2008, Published by CRC Press, Taylor & Francis Group, Balkema, Boca Raton/London/New York/Leiden, 3303–3310.

Gerigk M. 2010. A complex method for safety assessment of ships in damaged conditions using the risk assessment (D.Sc. thesis), *Monography No. 101, Published by the Gdansk University of Technology (in Polish),* Gdansk 2010.

Gerigk M. 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. in *Sustainable Maritime Transportation and Exploitation of Sea Resources. Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM)*, Volume 2: 715–719, London: Balkema.

IMO, 2005. Report of the Maritime Safety Committee on Its Eightieth Session. *MSC 80/24/Add.1*, London, 2005.

IMO. 2008. http://www.imo.org.

IMO. 2009. Stability and Seakeeping Characteristics of Damaged Passenger Ships in a Seaway When Returning to Port by Own Power or Under Tow, A survey of residual stability margin, *Submitted by Germany, SLF 52/8/1*, London, 26 October 2009.

ITTC. 2011. The specialist Committee on Stability in Waves. Final Report and Recommendations to the 26th ITTC, *Proceedings of 26th ITTC—Volume II*, Rio de Janeiro, Brasil, 28 August–3 September, 2011.

ITTC. 2011. ITTC—Recommended Procedures and Guidelines. Numerical Simulation of Capsize Behaviour of Damaged Ships in Irregular Beam Seas, 7.5-02-07-04.4, *Proceedings of 26th ITTC—Volume II*, Rio de Janeiro, Brasil, 28 August–3 September, 2011.

Jasionowski, A. & Vassalos, D. 2006. Conceptualising Risk, *Proceedings of the 9th International Conference on Stability of Ships and Ocean Vehicles STAB 2006*, Rio de Janeiro, 25–29 September 2006.

Jasionowski A. 2011. Decision support for ship flooding crisis management, *Ocean Engineering*, Volume 38, Issues 14–15, October 2011, Pages 1568–1581.

Montewka J., Ehlers S., Goerlandt F., Hinz T., Tabri K., Kujala P. 2014. A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels, *Reliability Engineering & System Safety*, Volume 124, April 2014, Pages 142–157.

Nowakowski, T. & Werbińka, S., 2009. On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing*, 6(4), pp. 364–378.

Papanikolaou A., Hamann R., Lee B.S., Mains C., Olufsen O., Vassalos D., Zaraphonitis G., 2013. GOALDS—Goal Based Damage Ship Stability and safety standards, *Accident Analysis & Prevention,* Volume 60, November 2013, Pages 353–365.

Perera L.P. & Soares Guedes C. 2011. Detections of potential collision situations by relative motions of vessels under parameter uncertainties, *Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM),* Genova, Italy, 13–16 September 2011.

Peters A.J. & Wing D. 2009. Stability criteria evaluation and performance based criteria development for damaged naval vessels. *Proceedings of the 10th International Conference on Stability of Ships and Ocean Vehicles,* Sankt Petersburg, Russia, 22–26 June 2009.

Skjong, R. & Vanem, E. & Rusas, S. & Olufsen, O. 2006. Holistic and Risk Based Approach to Collision Damage Stability of Passenger Ships, *Proceedings of the 9th International Conference on Stability of Ships and Ocean Vehicles STAB 2006,* Rio de Janeiro, 25–29 September 2006.

Smith D. & Heywood M. 2009. Accidental Damage Templates (ADTS). A basis for the future of naval ship safety certification. *Proceedings of the 10th International Conference on Stability of Ships and Ocean Vehicles,* Sankt Petersburg, Russia, 22–26 June 2009.

Soares, C.G. & Teixeira, A.P., 2001. Risk assessment in maritime transportation. *Reliability engineering and System Safety*, 74, pp. 299–309.

SOLAS, 2005. International Convention for the Safety of Life at Sea. Lloyd's Register Rulefinder 2005—Version 9.4., pp. 1–910.

SSRC. 2009. http://www.ssrc.na-me.ac.uk.

Vanem E., Puisa R., Skjong R. 2009. Standardized risk models for formal safety assessment of maritime transportation. *In: ASME 28th international conference on ocean, offshore and arctic engineering (OMAE2009)*, 2009. p. 51–61.

Vassalos D. 2006. Passenger Ship Safety: Containing the Risk, *Marine Technology, Vol. 43, No. 4,* October 2006, pp. 203–213.

Vassalos D. 2007. Safe return to port, *Seminar for the 50th session of the IMO SLF Sub-Committee,* London, May 2007.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Review of risk concepts and perspectives in risk assessment of maritime transportation

F. Goerlandt & J. Montewka
Department of Applied Mechanics, Marine Technology, Research Group on Maritime Risk and Safety, Aalto University, Espoo, Finland

ABSTRACT: Shipping accidents can have severe consequences, causing concerns to various stakeholders. This has led to research into risk assessment methods for the maritime transportation system. This paper presents an analysis of risk concepts and perspectives adopted in 44 methods for risk assessment in maritime transportation. As a methodological framework for analysis, a historical classification of risk concepts and a novel categorization of risk perspectives along the realist-constructivist continuum are applied. Analyses reveal that in the maritime transportation, risk is strongly tied to probability and that a wide range of perspectives is found, from realism over scientific proceduralism to more constructivist views.

1 INTRODUCTION

Risk assessment methods for maritime transportation have received a growing interest in recent years and relevant organizations have provided recommendations to maritime authorities on the use of specific risk management tools (IALA 2009; IMO 2010). In the wider risk research literature, there is a relatively recent focus on foundational issues, with calls for increased discussion, reflection and analysis regarding applied terminology, principles and perspectives (Aven 2012a; Rosa 2010).

Answering to these calls, the aim of this paper is to provide a broad overview and analysis of how risk has been defined, and what risk perspective is taken in methods for risk assessment of maritime transportation. Our main interest is a number of "risk-theoretic" aspects, related to the underlying conceptualizations, perspectives and principles in the sense intended by Aven (2012a). Reflecting on foundational issues in the application area of risk assessment in maritime transportation requires a methodological framework. Two aspects of this framework are introduced in Sections 2 and 3, respectively addressing the risk concept (what risk "is"), and the risk perspective (how risk is "looked at"). While these aspects are closely linked in practical applications, making a clear distinction between these is important from a foundational viewpoint.

In the course of this research, 44 original methods for risk assessment for maritime transportation have been found and analyzed. The methods have been published in scientific journals over a time span of last 40 years, from 1974 to 2013, (Fujii et al. 1974; MacDuff 1974; Hara & Nakamura 1995; Pedersen 1995; Roeleven et al. 1995; Harrald et al. 1998; Fowler & Sørgård 2000; Merrick et al. 2000; van Dorp et al. 2001; Friis-Hansen & Simonsen 2002; Kaneko 2002; Merrick et al. 2002; Rosqvist et al. 2002; Kristiansen 2005; United States Coast Guard 2005; Merrick & Van Dorp 2006; COWI 2008; Przywarty 2008; Klemola et al. 2009; Ulusçu et al. 2009; Debnath & Chin 2010; Kaneko 2010; Klanac et al. 2010; Mermiris & Vassalos 2010; Montewka et al. 2010; van Dorp & Merrick 2011; Qu et al. 2011; Akhtar et al. 2012; Almaz 2012; Blokus-Roszkowska & Smolarek 2012; Montewka et al. 2012; Goerlandt et al. 2012; Jeong et al. 2012; Montewka et al. 2011; Montewka, Ståhlberg, et al. 2010; Sormunen et al. 2012; Rasmussen et al. 2012; Suman et al. 2012; Weng et al. 2012; Burmeister et al. 2013; Mulyadi et al. 2013; Talavera et al. 2013; Ståhlberg et al. 2012; Goerlandt & Kujala 2011).

2 A CLASSIFICATION OF DEFINITIONS FOR THE RISK CONCEPT

As a central part of our analysis concerns the applied risk concepts in risk assessments, a brief review of some basic categories of definitions of the risk concept is provided. The below classification is taken from a historic analysis of the risk concept by Aven (2012b), addressing the question what risk means in itself, i.e. what risk "is".

C1. Risk = Expected value (R = E)

a. The risk of losing any sum is the reverse of Expectation, and the true measure of it is, the product of the sum adventured multiplied by the probability of the loss.

b. Risk equals the expected loss
c. Risk equals the product of the probability and utility of some future event
d. Risk equals the expected disutility

C2. Risk = Probability of an (undesirable) event (R = P)
a. Risk is the chance of damage or loss
b. Risk equals the probability of an undesirable event
c. Risk means the likelihood of a specific effect originating from a certain hazard occurring within a specified period or in specified circumstances

C3. Risk = Objective Uncertainty (R = OU)
a. Risk is the objective correlative of the subjective uncertainty; uncertainty considered in the course of events in the external world
b. Risk is measurable uncertainty, i.e., uncertainty where the distribution of an outcome in a group of instances is known (either through calculation a priori or from statistics of past experience)

C4. Risk = Uncertainty (R = U)
a. In regard to cost, loss or damage
b. About a loss
c. About the happening of an unfavourable contingency
d. Of outcome, of actions and events

C5. Risk = Potential/possibility of a loss (R = PO)
a. Risk is the possibility of an unfortunate occurrence
b Risk is the possibility of an unfavourable deviation from expectations
c. Risk is the potential for realisation of unwanted, negative consequences of an event

C6. Risk = Probability and scenarios/(severity of) consequences (R = P&C)
a. Risk is a combination of hazards measured by probability; a state of the world rather than a state of mind
b. Risk is a measure of the probability and severity of adverse effects
c. Risk is equal to the triplet (s_i, p_i, c_i), where s_i is the ith scenario, p_i is the probability of that scenario, and c_i is the consequence of that scenario, $i = 1,2, \ldots, N$; i.e. risk captures: What can happen? How likely is that to happen? If it does happen, what are the consequences?

C7. Risk = Event or consequences (R = C)
a. Risk is a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain
b. Risk is an uncertain consequence of an event or an activity with respect to something that humans value

C8. Risk = Consequences/damage/severity of these + Uncertainty ($R = C\&U$)
a. Risk = uncertainty + damage
b. Risk is equal to the two-dimensional combination of events/consequences (of an activity) and associated uncertainties
c. Risk is uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value
d. Risk is the deviations from a reference level (ideal states, planned values, expected values, objectives) and associated uncertainties

C9. Risk = Effect of uncertainty on objectives (R = ISO)

3 FOUNDATIONS OF VARIOUS PERSPECTIVES TO RISK ASSESSMENT

In a risk assessment, risk is described or measured for the purpose of informing a decision, but there are different views regarding how to do this. The foundational view on risk assessment applied in the process of informing a decision is referred to as a risk perspective. It thus does not concern the question what risk "is", but how risk is "looked at" and which processes are applied in making statements concerning risk.

There are important and long-standing debates between opposing philosophical positions related to risk assessment, ranging from realism/positivism to constructivism/cultural relativism (Klinke & Renn 2002; Shrader-Frechette 1991; Rosa 1998).

The realist risk philosophy is rooted in a dualism between the mind and the external material world. Under such a view, knowledge relates to a discovery of the world as it really is and to discover the laws of causality in that world (Jore & Njå 2010). Realists are convinced that a true risk exists and that technical estimates of risk are representations of this true risk, affecting people as predicted by the calculated results regardless of the beliefs or convictions of the assessor (Klinke & Renn 2002).

Constructivism acknowledges that modeling is a cognitive process in which the complexity of the world is reduced to a mental construct, where the analysis does not aim to uncover the truth about risk but provides a reflection of somebody's mental construction conditional to a specific background knowledge, see (Jore & Njå 2010; Klinke & Renn 2002). Important characteristics of constructivism are that there is no reference to a true risk and that different assessors can have different mental constructions.

Extreme constructivists posit that any risk construct is equally valid, i.e. that no mental construction is superior to others, and adhere to a form of cultural relativism (Shrader-Frechette 1991).

Another major schism exists between positivists and cultural relativists in that the former see no role for values in risk assessment, whereas the latter conceive risk assessment as a combination of facts, values and public perceptions (Shrader-Frechette 1991). Rather than an absolute dichotomy between realists/positivists and constructivists/cultural relativists, there exists a continuum between these extremes (Shrader-Frechette 1991).

A schematic version of this continuum has been presented by Jore and Njå (Jore & Njå 2010), in the context of terrorism risk, focusing on the role and use of models and on the interpretation given to the outcome of an analysis.

In Table 1, a novel and extended version of this classification is presented. The description of the perspectives should be seen as an approximation of the general features of some common approaches to risk assessment. In the following subsections the brief overviews of the perspectives are given.

3.1 *Realism and true judgments*

The most realist views rely exclusively on data and engineering models. It is based on the conception that objectivity can only be achieved by application of data, mathematical calculations and engineering models.

Table 1. Risk perspectives in the realist/constructivist continuum.

	Foundational perspective	Risk expression	Risk interpretation
I	Realism Positivism	Model seen to describe true risk	Truth Risk is a property of the world. Based only on "hard" evidence.
II	True judgments	Model seen to describe true risk Expert judgment as truth-approaching Uncertainty sporadically mentioned	Judgment aiming at truth Risk is a property of the world. Based on "hard" evidence and judgment Uncertainty related to imprecision of underlying true risk
III	Probability of frequency Uncertainty quantification	Model seen to describe true risk Expert judgment is truth-approaching Uncertainty is quantified	Judgment aiming at truth Risk is a property of the world. Based on "hard" evidence and judgment Uncertainty related to imprecision of underlying true risk
IV	Precautionary perspective	Model is seen to describe a true underlying risk Direction of bias away from true risk is qualitatively evaluated.	Judgment aiming at truth Risk is a property of the world. Based on "hard" evidence and judgment. Uncertainty related to imprecision of underlying true risk
V	Scientific proceduralism	Model is seen to describe a true underlying risk Model is seen as compromise between stakeholder groups Quantitative and qualitative	Judgment and values Risk is a property of the world. No truth-claims are possible concerning risk judgments. Risk assessment is the result of judgments of both experts and lay people, balancing facts and values. Analytic-deliberative process.
VI	Argument view	Model is seen as an expression of argument Quantitative and qualitative	Judgment Risk results from an interpretation. Based on "hard" evidence and judgment. Adversarial approach.
VII	Uncertainty view	Model is seen as an expression of uncertainty Quantitative and qualitative Broad qualitative uncertainty evaluation	Judgment and uncertainty Risk is uncertainty of an assessor related to events/consequences. Based on "hard" evidence and judgment
VIII	Constructivism Cultural relativism	Qualitative descriptions	Judgment, values and perceptions Risk is a cultural or social phenomenon. Lay people oriented.

In a "true judgment" view, expert judgment is used, but it is applied to estimate a true underlying risk. In this view, expert judgment is seen as an alternative only when there is no data available. Assessments under this view typically rely on heavily on data, calculations and models and less on judgment.

3.2 *Probability of frequency and uncertainty quantification*

Kaplan (1997) proposes the so-called "probability of frequency" approach to risk assessment, based on a risk concept in line with risk definition C6 (R = P&C), where subjective probabilities are used to express uncertainty about true frequentist probabilities. The assessment thus focuses on quantifying uncertainty about an underlying true risk, which is estimated. Kaplan's view is strongly tied to realism, as the risk description focuses on a true risk as determined by experts. Closely related perspectives are those where uncertainty is quantified around a true risk, such as in the traditional Bayesian perspective where uncertainty is quantified in relation to model parameters (Aven & Heide 2009). Such uncertainty quantification can also be done using non-probabilistic representations of epistemic uncertainty (Helton & Johnson 2011). These methods typically consider a risk problem in a highly mathematized form.

3.3 *Precautionary perspective*

Rosqvist and Tuominen (2004) propose a precautionary approach to risk assessment, based on a risk concept in line with C6 (R = P&C). They propose a framework in which risk is quantified using probabilities, supplemented with a systematic analysis of model bias to account for model uncertainty. The bias analysis aims to assess whether the risk estimates are optimistic, realistic or conservative in relation to the true risk of the system (Rosqvist & Tuominen 2004). While starting from a realist conception because a true risk is in focus, uncertainty is assessed through biases in a qualitative way. This less quantity-focused approach is in our view a step towards constructivism in comparison with the perspective by Kaplan (1997). Through the bias analysis, it allows for a more reflective stance towards underlying assumptions and simplifications, which places the risk problem in a wider qualitative context.

3.4 *Scientific proceduralism*

Shrader-Frechette (1991) advocates a middle-way between realism and constructivism which she terms "scientific proceduralism". Its rationale is based on three premises: (i) explanatory power as tested by prediction, (ii) naturalistic approach to theory choice and (iii) testing the predictive and explanatory power of our risk theories and by subjecting risk evaluations to intelligent debate, criticism, and amendment by the scientific community and lay people. Concerning expert judgment, she notes that "[…] there is little reason to believe that experts are always able to calculate actual or *real* risk" (Shrader-Frechette 1991), and that "experts' trust in their probability estimates is typically a function of how much information they have gathered, rather than a function of its accuracy of its predictive success" (Shrader-Frechette 1991). Her views seem to be on the one hand rooted in the existence of a "true risk", because it can be tested by prediction and because the estimation of a probability implies the existence of a "correct" or "true" probability. Thus, scientific proceduralism has strong ties to realism. She also stresses the explanatory power and debate aspects of risk modeling, which are elements of a more constructivist view. The probabilities and risk models can in this sense be understood as tools for argumentation. This aspect of her scientific proceduralism has been influential to conceiving risk assessment as an analytic-deliberative process (Stern & Fineberg 1996).

3.5 *Argument view*

Watson argues for an understanding of risk assessment as "an expression of argument, rather than a revelation of truth" (Watson 1994). The strength of argument depends on the quality of the data, the adequacy of the model and the agreement in expert judgments, and is seen as input on a debate on the safety of a system. Watson thus sees a risk assessment as a translation of the available background knowledge into a tool to inform a decision, placing judgment and argumentation central in the risk description. Watson's view represents a significant step towards constructivism because, unlike the above risk perspectives, there is no reference to a true, mind-independent risk. Expert judgment and subjective probability is not seen as a means to estimate a true risk, but as a means to quantitatively put forward an argumentation. We shall refer to this perspective as "argument view".

3.6 *Uncertainty view*

Aven and Renn argue for an uncertainty-based view on risk and risk assessment, where risk is conceptualized in line with definition class C8 (R = C&U). In their view, risk assessment is an expression of an assessor's uncertainty about the occurrence of events and the consequences. Risk assessment can always be performed, as it is seen as a tool to describe uncertainties rather than a tool to uncover the truth. Their view has a strong constructivist basis: "[…] risk does not exist independent of the assessor, as the uncertainties need to be assessed by somebody […] Uncertainty is not real, it is a construct of human imagination to cope

with potential future outcomes that can become real" (Aven & Renn 2009). However, they stress that their risk perspective is not a relativist social construction, because the events/consequences refer to an objective world (they can become real) and because the assessment can be based on the best available scientific data, models and judgment (Aven & Renn 2009). This view is similar to Watson's in that no "true risk" is conceived to exist and its measurement is a reflection of somebody's mental construct in light of evidence available to him/her (Aven 2010). In this perspective, more stress is placed on the importance of uncertainty in the background knowledge (Aven 2013), both in terms of evidential and outcome uncertainty. In this sense, this perspective is a further step towards constructivism in comparison with the "argument view". We shall refer to this view as the "uncertainty view".

4 HISTORIC OVERVIEW OF RISK DEFINITION AND PERSPECTIVE

In Figure 1, a historic overview of the applied risk definitions is given. It is clear that a wide variety of definitions is applied in practical settings. Of the nine categories, risk definitions in the application area are clustered in the categories C1 (R = E), C2 (R = P), C5 (R = PO) and C6 (R = P&C). Over the years, risk has been strongly tied to probabilities and only weak historic trends can be identified. Risk is considered as the probability of an event in the earliest work in the field, after which such views have disappeared for more than two decades, re-emerging in recent work. From 1995 onwards, the predominant definitions involve both the probability of events and consequences. Both the definition through expected values of probabilities and consequences (C1) as well as the combination of probabilities and consequences (C6) are approximately equally often found. The definition of risk in line with a potential or possibility of a loss (C5) is very sporadically used throughout the history.

Reflecting on the findings by Aven, it is found that the traditional engineering definitions (C1 and C6) and the definitions of decision analysts (C1) are the predominant views on risk, (Aven 2012b). Aven in (2012b) claims that the risk definitions of category C8 (R = C&U), where uncertainty rather than probability is seen as a fundamental component of risk, have recently replaced probability-based conceptualizations in the engineering fields. From our analysis, it is seen that this is not the case for the maritime transportation application area. In fact, such a view on risk is not found.

A more policy-oriented issue is that many applications do not follow the suggested definitions by relevant authorities. In the Formal Safety Assessment (FSA), which is commonly seen as the official guide for risk assessment in the maritime field, risk is defined as "the combination of the frequency and the severity of the consequence" (IMO 2007), i.e. a categorization in line with class C6. While the definitions based on expected values (C1) are close to this view as it consists of the same elements, the definitions in line with C2 and especially C5 represent significantly different risk classes. The ISO-definition, seeing risk as "the effect of uncertainty on objectives", is not applied in the application area.

In Figure 2, a historic overview of the risk perspectives in the application area is shown. It is seen that strong realist conceptions are found from the early work in the application area to the present day. Risk perspectives in line with the "true judgment" view have been present since the mid-1990s and are approximately equally often found as the strong realist views since that time. Views in line with the "probability of frequency" approach to risk assessment, where uncertainty is quantified around a true risk are relatively rare in the application area, starting from the mid-2000s. Only two such methods are found: one applying a traditional

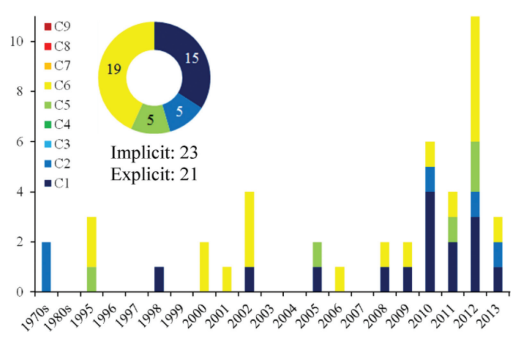


Figure 1. Historic overview of applied risk definition. Risk concept classes as introduced in Section 2.

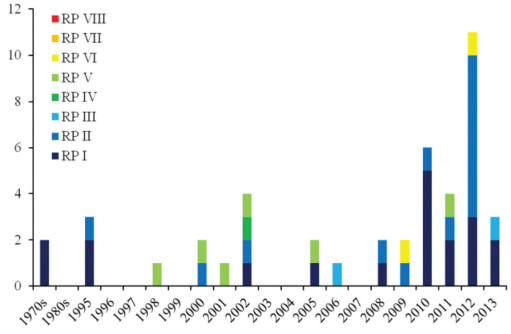


Figure 2. Historic overview of foundational Risk Perspective (RP). Classification on realist-constructivist continuum according to Table 1.

Bayesian approach and one applying Dempster-Shafer evidence theory to quantify uncertainty about model parameters. The precautionary view is only found once, in the early 2000s, and hence represents somewhat of an outlier view in the application area. There is relatively more work in line with the scientific proceduralism view on risk assessment, from the late 1990s onwards. The argument view, where expert judgment is taken as a core element of the risk description, represents a minority of the perspectives on risk assessment.

The historic overview clearly shows that a wide range of perspectives has been applied in risk assessments for maritime transportation. Most of the work is rooted in the idea that a true, mind-independent risk exists in line with realist perspectives on the continuum of Table 1. Using different modeling approaches, the majority of the methods aim to estimate this true risk. While the use of expert judgment has gained steady support, many of the applications rely heavily on accident and traffic data. Even when judgment is applied, it is considered to be truth-oriented. From the overview, it is also found that constructivist views, where the assessment is seen rather as a reflection of an assessor's interpretation of the system risk, are rare. The uncertainty view, where an assessor expresses his uncertainty about the occurrence of events and consequences, is not found in the application area.

5 RELATION BETWEEN RISK DEFINITION AND RISK PERSPECTIVE

In Figure 3, the applied risk definitions are grouped per risk perspective. It is observed that definitions of risk of classes C1 (R = E) and C6 (R = P&C) are found across the realist-constructivist continuum. Definitions in line with C2 (R = P) are mostly found in the realist part of the spectrum. Definitions C5 (R = PO) are also linked to more realist conceptions.

This implies that the adopted definition does not necessarily provide much information regarding the foundational perspective. E.g. risk definitions based on expected values (C1) can lead to very realist perspectives on risk if such a definition is taken to literally mean that risk as a concept is equal to an expected value, as e.g. in (Kaneko 2002; Mermiris & Vassalos 2010; Akhtar et al. 2012; Montewka, Ehlers, et al. 2010). However, the same definition can be used in a more stipulative sense, to define risk measures as in e.g. (Harrald et al. 1998; Ulusçu et al. 2009). The risk concept is then implicitly understood more widely, but the C1-definition is seen as useful in the specified context.

Nonetheless, if a risk definition is posited without reflection on the underlying risk concept or the applied risk perspective, misunderstandings can easily occur. The presence of a range of competing underlying views on risk assessment, all applying similar terminology, signals that possible disagreements on adopted approaches run deeper than a semantic discussion on applied terminology.

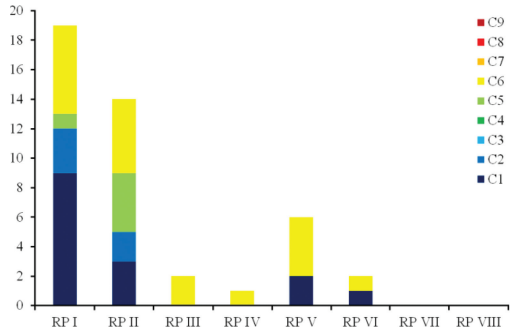


Figure 3. Overview of risk definition (C) in relation to Risk Perspective (RP).

6 DISCUSSION

Our analysis of the adopted perspectives in risk assessment of maritime transportation shows that many competing views on risk analysis exist, as argued by other risk researchers (Shrader-Frechette 1991; Klinke & Renn 2002; Rosa 1998; Jore & Njå 2010). While this has not received much attention in the application area, our analysis shows that this is also the case in risk assessment for maritime transportation. This this is not merely a matter of defining the word "risk", but a matter of more deep running philosophical positions.

In the field of maritime transportation, risk assessment is overall very strongly tied to probabilities, both in relation to the adopted definition as in the applied risk description. This may be at least in part due to the definition in the Formal Safety Assessment (FSA), as "the combination of the frequency and the severity of the consequence" (IMO 2007).

Much work is rooted in the realist-oriented perspectives on risk assessment, with much fewer applications in line with scientific proceduralism or more constructivist conceptions. However, adopting a constructivist-based view to risk assessment requires an adaptation of the expectations of risk assessment as a tool to inform a decision, which has repercussions also in judging the risk acceptability or the decision regarding the adopted risk management strategy.

In many applications, risk is not defined. In light of the existence of a plenitude of conceptual classes in the general risk research field and in the application area, an implicit assumption that the term is sufficiently self-explanatory is in our view unfortunate.

7 CONCLUSIONS

Our findings confirm earlier research claiming that somewhat of a terminological and conceptual chaos exists the risk research field. Four distinct classes of risk definitions are found in applications, mostly considering probability as a component of risk. While applications are based on a wide range of perspectives on the realist-constructivist continuum, most work is positioned on the realist part of the spectrum, focusing on a true, mind-independent risk.

It is hoped that some insights gained from the analysis can serve to illustrate the need for more focus on foundational issues concerning risk assessment in the application area. We are convinced that further conceptual refinements would benefit the practice of risk analysis in the maritime field.

ACKNOWLEDGMENT

This study was conducted as a part of EU funded project on Human Factors in Risk-based Ship Design Methodology—FAROS (2012–2015) (Grant no. 314817), the FP7 program. Merenkulun säätiö from Helsinki is appreciated for the travel grant.

REFERENCES

Akhtar, J., Bjornskau, T. & Jean-Hansen, V., 2012. Oil spill risk analysis of routeing heavy ship traffic in Norwegian waters. *WMU Journal of Maritime Affairs*, 11, pp. 233–247.

Almaz, O.A., 2012. *Risk and performance analysis of ports and waterways: the case of Delaware river and bay,* New Brunswick, New Jersey: Rutgers University.

Aven, T., 2012a. Foundational issues in risk assessment and risk management. *Risk analysis: an official publication of the Society for Risk Analysis*, 32(10), pp. 1647–56. Available at:

Aven, T., 2010. On how to define, understand and describe risk. *Reliability Engineering & System Safety*, 95(6), pp. 623–631.

Aven, T., 2013. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety*, null(null).

Aven, T., 2012b. The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, 99(0), pp. 33–44.

Aven, T. & Heide, B., 2009. Reliability and validity of risk analysis. *Reliability Engineering & System Safety*, 94(11), pp. 1862–1868.

Aven, T. & Renn, O., 2009. On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12(1), pp. 1–11.

Blokus-Roszkowska, A. & Smolarek, L., 2012. Collision risk estimation for motorways of the sea. *Reliability: Theory & Applications*, 7(2), pp. 58–68.

Burmeister, H.-C. et al., 2013. Maritime risk assessment: modeling collisions with vessels lying at an anchorage. In *Safety, Reliability and Risk Assessment. Advances in Marine Navigation—Marine Navigation and Safety of Sea Transportation*. London: Taylor & Francis Group, pp. 287–291.

COWI, 2008. Risk analysis of sea area traffic in the area around Bornholm.

Debnath, A.K. & Chin, H.C., 2010. Navigational traffic conflict technique: a proactive approach to quantitative measurement of collision risks in port waters. *Journal of Navigation*, 63(1), pp. 137–152.

Fowler, T.G. & Sørgård, E., 2000. Modeling Ship Transportation Risk. *Risk Analysis*, 20(2), pp. 225–244.

Friis-Hansen, P. & Simonsen, B.C., 2002. GRACAT: software for grounding and collision risk analysis. *Marine Structures*, 15(4–5), pp. 383–401.

Fujii, Y., Yamanouchi, H. & Mizuki, N., 1974. Some factors affecting the frequency of accidents in marine traffic. II—the probability of stranding and III—the effect of darkness on the probability of collision and stranding. *Journal of Navigation*, 27(2), pp. 239–247.

Goerlandt, F. & Kujala, P., 2011. Traffic simulation based ship collision probability modeling. *Reliability Engineering & System Safety*, 96(1), pp. 91–107.

Goerlandt, F., Ståhlberg, K. & Kujala, P., 2012. Influence of impact scenario models on collision risk analysis. *Ocean Engineering*, 47(-), pp. 74–87.

Hara, K. & Nakamura, S., 1995. A comprehensive assessment system for the maritime traffic environment. *Safety Science*, 19(2–3), pp. 203–215.

Harrald, J.. et al., 1998. Using system simulation to model the impact of human error in a maritime system. *Safety Science*, 30(1–2), pp. 235–247.

Helton, J.C. & Johnson, J.D., 2011. Quantification of margins and uncertainties: Alternative representations of epistemic uncertainty. *Reliability Engineering & System Safety*, 96(9), pp. 1034–1052.

IALA, 2009. IALA Recommendation O-134 on the IALA risk management tool for ports and restricted waterways.

IMO, 2010. Degree of risk evaluation. SN.1/Circ.296.

IMO, 2007. Formal safety assessment—Consolidated text of the guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (MSC/Circ.1023-MEPC/Circ.392).

Jeong, J.S., Park, G.-K. & Kim, K. Il, 2012. Risk assessment model of maritime traffic in time-variant CPA environments in waterway. *Journal of Advanced Computational Intelligence and Intelligent Informatics*, 16(7), pp. 866–872.

Jore, S.H. & Njå, O., 2010. Risk of terrorism: a scientifically valid phenomenon or a wild guess? The impact of different approaches to risk assessment. *Critical approaches to discourse analysis across disciplines*, 4(2), pp. 197–216.

Kaneko, F., 2010. A method for estimation of grounding frequency by using trajectories of ships and geometry of seabed. In *5th International Conference on Collision and Grounding of Ships*. Espoo, Finland: Aalto University, pp. 123–132.

Kaneko, F., 2002. Methods for probabilistic safety assessments of ships. *Journal of Marine Science and Technology*, 7(1), pp. 1–16.

Kaplan, S., 1997. The Words of Risk Analysis. *Risk Analysis*, 17(4), pp. 407–417.

Klanac, A. et al., 2010. Environmental risk of collisions in the enclosed European waters: Gulf of Finland, North-

ern Adriatic and the implications for tanker design. In *5th International Conference on Collision and Grounding of Ships*. Espoo, Finland: Aalto University, pp. 55–65.

Klemola, E. et al., 2009. A cross-disciplinary approach to minimising the risks of maritime transport in the Gulf of Finland. *World Review of Intermodal Transportation Research*, 2(4), pp. 343–363.

Klinke, A. & Renn, O., 2002. A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Analysis*, 22(6), pp. 1071–1094.

Kristiansen, S., 2005. *Maritme transportation: safety management and risk analysis* 1st ed., Routeledge.

MacDuff, T., 1974. The probability of vessel collisions. *Ocean Industry*, pp. 144–148.

Mermiris, G. & Vassalos, D., 2010. Collision risk revisited. In *Proceedings of the 4th Design for Safety Conference and 3rd Risk-based approaches in the Marine Industry Workship*. Trieste, Italy.

Merrick, J.R.. et al., 2000. A systems approach to managing oil transportation risk in Prince William Sound. *Systems Engineering*, 3(3), pp. 128–142.

Merrick, J.R.W. et al., 2002. The Prince William Sound Risk Assessment. *INTERFACES*, 32(6), pp. 25–40.

Merrick, J.R.W. & Van Dorp, R., 2006. Speaking the Truth in Maritime Risk Assessment. *Risk Analysis*, 26(1), pp. 223–237.

Montewka, J., Ståhlberg, K., et al., 2010. Elements of risk analysis for collision of oil tankers. In *Risk, Reliability and Safety*. London: Taylor & Francis Group, pp. 1005–1013.

Montewka, J. et al., 2011. Marine traffic risk modelling—an innovative approach and a case study. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 225(3), pp. 307–322.

Montewka, J., Hinz, T., et al., 2010. Probability modelling of vessel collisions. *Reliability Engineering & System Safety*, 95(5), pp. 573–589.

Montewka, J., Ehlers, S. & Tabri, K., 2010. Elements of risk analysis for LNG tanker maneuvering with tug assistance in a harbor. In *11th International Symposium on Practical Design of Ships and Other Floating Structures, PRADS 2010*. pp. 1563–1572.

Montewka, J., Goerlandt, F. & Kujala, P., 2012. Determination of collision criteria and causation factors appropriate to a model for estimating the probability of maritime accidents. *Ocean Engineering*, 40, pp. 50–61.

Montewka, J., Goerlandt, F. & Kujala, P., 2014. On a systematic perspective on risk for Formal Safety Assessment (FSA). *Reliability Engineering & System Safety*, 127 (July), pp. 77–85.

Mulyadi, Y. et al., 2013. Development of ship sinking frequency model over subsea pipeline for Madura Strait using AIS data. *WMU Journal of Maritime Affairs*.

Pedersen, P.T., 1995. Collision and grounding mechanics. In *Proceedings of the Danish Society of Naval Architects and Marine Engineers*. pp. 125–157.

Przywarty, M., 2008. Probabilistic model of ships navigational safety assessment on large sea areas. In *Proceedings of the 16th International Symposium on Electronics in Transport*. Ljubljana, Slovenia.

Psaraftis, H.N., 2012. Formal Safety Assessment: an updated review. *Journal of Marine Science and Technology*, 17(3), pp. 390–402.

Qu, X., Meng, Q. & Li, S., 2011. Ship collision risk assessment for the Singapore Strait. *Accident Analysis & Prevention*, 43(6), pp. 2030–2036.

Rasmussen, F.M. et al., 2012. Quantitative assessment of risk to ship traffic in the Fehmarnbelt Fixed Link project. *Journal of Polish Safety and Reliability Association*, 3(1–2), pp. 1–12.

Roeleven, D. et al., 1995. Inland waterway transport: Modelling the probability of accidents. *Safety Science*, 19(2–3), pp. 191–202.

Rosa, E.A., 1998. Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, 1(1), pp. 15–44.

Rosa, E.A., 2010. The logical status of risk—to burnish or to dull. *Journal of Risk Research*, 13(3), pp. 239–253.

Rosqvist, T. et al., 2002. The implementation of the VTMIS system for the gulf of Finland—a FSA study. In *Proceedings of the RINA International Conference on Formal Safety Assessment*. London.

Rosqvist, T. & Tuominen, R., 2004. Qualification of Formal Safety Assessment: an exploratory study. *Safety Science*, 42(2), pp. 99–120.

Shrader-Frechette, K.S., 1991. *Risk and rationality: philosophical foundations for populist reforms*, Berkeley: University of California Press.

Sormunen, O.-V.E., Ehlers, S. & Kujala, P., 2012. Collision consequence estimation model for chemical tankers. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*.

Ståhlberg, K. et al., 2012. Uncertainty in analytical collision dynamics model due to assumptions in dynamic parameters. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 6(1), pp. 47–54.

Stern, P.C. & Fineberg, H.V., 1996. *Understanding risk: informing decisions in a democratic society*, Washington, D.C.: National Academy Press.

Suman, S. et al., 2012. Ship collision risk assessment using AIS data. *International Journal of Innovative Research & Development*, 1(10), pp. 509–524.

Talavera, A. et al., 2013. Application of Dempster–Shafer theory for the quantification and propagation of the uncertainty caused by the use of AIS data. *Reliability Engineering & System Safety*, 111, pp. 95–105.

Ulusçu, Ö.S. et al., 2009. Risk analysis of the vessel traffic in the strait of Istanbul. *Risk Analysis*, 29(10), pp. 1454–1472.

United States Coast Guard, 2005. Ports And Waterways Safety Assessment (PAWSA).

Van Dorp, J.R. et al., 2001. A Risk Management Procedure for the Washington State Ferries. *Risk Analysis*, 21(1), pp. 127–142.

Van Dorp, J.R. & Merrick, J.R.W., 2011. On a risk management analysis of oil spill risk using maritime transportation system simulation. *Annals of Operations Research*, 187(1), pp. 249–277.

Watson, S.R., 1994. The meaning of probability in probabilistic safety analysis. *Reliability Engineering & System Safety*, 45(3), pp. 261–269.

Weng, J., Meng, Q. & Qu, X., 2012. Vessel collision frequency estimation in the Singapore Strait. *Journal of Navigation*, 65, pp. 207–221.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk based assessment on increased gas safe machinery spaces of liquefied natural gas fuelled ship

Xiao Jian Li & Rui Ping Zhou
School of Energy and Power Engineering, Wuhan University of Technology, Wuhan, Hubei, China

ABSTRACT: A new concept of machinery spaces called increased gas safe machinery spaces (hereafter Increased Type) of liquefied natural gas fuelled ship is introduced in this paper. This paper develops a practical methodology to assess that kind of machinery spaces based on risk based technology. According to the methodology, the sources of leaks of the gas supply system are firstly identified using Fault Tree Analysis (FTA). Then the frequencies of leakage, ignition and failure of ventilation and detection in risk assessment are estimated from generic historical statistics and with FTA and Event Tree Analysis (ETA). Based on that, frequency analysis of hazards, such as failures of pipes, valves, filters, fans and detectors, under different failure modes, is carried out. As for consequence evaluation, consequence areas of different types of outcome like flash fire, jet fire and vapor cloud explosion are logically preceded from the mechanism of each possible outcome. After all the steps above, risk of each identified hazard is determined and the risk of the machinery spaces ultimately is summarized. In addition, the tolerability of Risks is developed, which determines whether the risk is acceptable, unacceptable or needs risk management as low as reasonably practicable.

1 INTRODUCTION

The potential of LNG to be a 'fuel of the future' for the shipping industry is a hot spot almost daily. There is no doubt that LNG ticks the box in terms of emissions reductions compared to conventional fossil fuels (Michael D. Tusiani and Gordon Shearer 2007). But the expansion of LNG as a fuel into the mainstream shipping industry throws up a combination of technological and regulatory challenges that the industry must address.

It's well known that IACS have provided insight over the past year on the drivers for adopting LNG as a fuel, examining the Classification issues of technology, safety and the regulatory framework. Inherently gas safe machinery spaces and ESD protected machinery spaces have been accepted (IMO 2009; GL 2010; ABS 2011; DNV 2012), which can reach the existing levels of safety of conventional machinery spaces. In addition, recently, a new concept called increased gas safe machinery spaces (CCS 2013), whose safety level was not clear, was creatively put forward to meet the current demand of diesel-LNG dual fuel conversion for existing ships by China Classification Society. Based on that, to accelerate its extensive application, it's extremely necessary to develop a feasible assessment methodology.

2 ARRANGEMENT OF INCREASED TYPE

Figure 1 is the sketch of the arrangement of Increased Type according to *Rules for Natural Gas Fuelled Ships (2013)*, merely showing the portside, which is set as the object of risk assessment.

It's significant to know that pressure in gas supply lines within machinery spaces is less than 10 bar. Full penetration butt joint is one of the obvious features of Increased type. In addition, anywhere in machinery spaces including GVU is covered by two sets of gas detectors. As far as ventilation is concerning, the air space within the machinery spaces and GVU are equipped with mechanical extraction ventilation having a

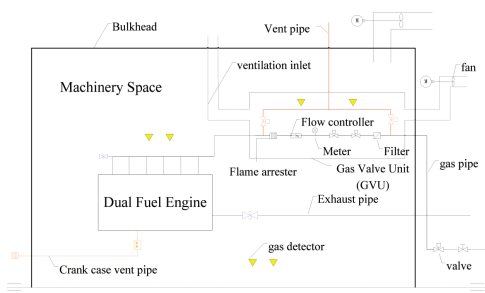


Figure 1. Increased safe machinery spaces arrangement.

capacity of at least 30 air changes per hour for Increased Type.

3 RISK ASSESSMENT METHODOLOGY

3.1 *Steps in risk assessment*

Risk based Assessment is a scientific methods or tools and processes used to manage the risk of a component or system, which normally carried out using a formal process. The main steps are hazard identification, frequency analysis, consequence assessment, risk summation, risk assessment, and risk management. Figure 2 summarizes those steps.

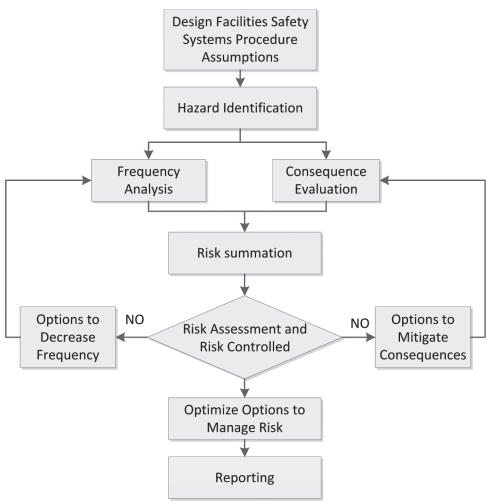
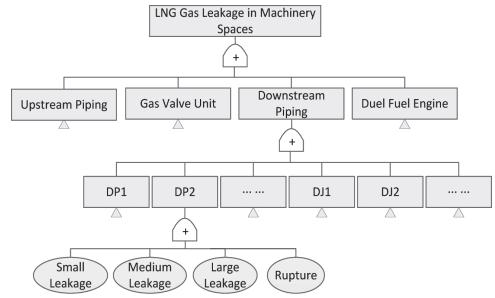


Figure 2. Basic steps in risk assessment.



DP1-Downstream Piping 1; DP2-Downstream Piping 2; DJ1-Downstream Joint 1; DJ2-Downstream Joint 2

Figure 3. FTA for hazard identification.

3.2 *Hazard identification*

A hazard is a source of harm that interacts with people or things in a negative manner. Hazards may be identified through accident history, judgment of knowledgeable individuals or some technical process such as FTA.

The determination of hazards for LNG begins with an understanding of the properties of the fuel. The following characteristics are important to identifying LNG hazards: storage parameters, tendency to form combustible mixture, ignition and explosion characteristics, means of controlling combustion and environmental effects.

Vaporized LNG fuel within the gas supply system in the machinery spaces presents non-toxic gas state, temperature and pressure of which should be recognized. It can be seen that flammability plays a major hazardous role during the LNG fuel's supplying. Thus, gas leak, the base of flammability, should be emphasized during hazard identification. A typical model of sources of leakages are showed in Figure 3. The gas supply system is divided into four units including Upstream Piping (UP), Gas Valve Unit (GVU), Downstream Piping (DP) and Duel Fuel Engine to identify hazards logically.

3.3 *Frequency analysis*

Frequency information is required to match the event specification and consequence calculation. In general, leak frequencies of hole sizes (small, medium, large, rupture), see Table 1, in risk assessments are estimated from generic historical leak statistics, which works well for common items (pipes, valves, pumps, etc.) that have been collected and provided by COVO (Rijnmond Public Authority 1982; Crossthwaite P.J., Fitzpatrick, R.D. and Hurst N.W. 1988), DNV (DNV consulting 2005) and API (API 2008).

The event tree approach (Fig. 4) is used to track outcomes from gas leakage and branch outward based on binomial choices on possible outcomes (e.g., ignition yes/no). Using the equation (1), (2), (3) can determine the final probabilities of every estimated outcomes.

$$pvce_{v,n} = pf_{v,n} \cdot pov \cdot pod \cdot poop \cdot poi(1 - poii) \cdot pvcedi \quad (1)$$

$$pff_{v,n} = pf_{v,n} \cdot pov \cdot pod \cdot poop \cdot poi(1 - poii) \cdot pffdi \quad (2)$$

$$pjet_{v,n} = pf_{v,n} \cdot pov \cdot pod \cdot poop \cdot poi \cdot poii \quad (3)$$

where $pvce_{v,n}$ = the probability of a vapor cloud explosion given a vapor release associated with the nth release hole size; $pf_{v,n}$ = the release frequency associated with the nth vapor release hole size; pod = the probability of abnormal

detection; poop = the probability of outer wall failure; $poi_{v,n}$ = the probability of ignition given a release; $poii_{v,n}$ = a vapor release associated with the nth release hole size; pvcedi = the probability of VCE given a delayed ignition of a release of a flammable vapor associated with the nth release hole size; pffdi = the probability of flash fire given a delayed ignition of a release of a flammable vapor associated with the nth release hole size; $pff_{v,n}$ = the probability of a flash fire given a vapor release associated with the nth release hole size; $pjet_{v,n}$ = the probability of a jet fire given a vapor release associated with the nth release hole size.

3.4 *Consequence evaluation*

Consequence assessment is the main part of risk based assessment and models for different outcome types-dispersion, flash fire, jet fire, vapor cloud explosion are presented in the later sections. As the Figure 5 shows, consequence areas, component damage areas and personal injury areas concluded, of each identified hazard with a range of hole size is determined based on LNG gas properties and ambient condition.

Table 1. Release hole sizes used in frequency analysis and consequence evaluation.

Release hole number (n)	Release mode	Range of hole size (mm)	Specific release hole diameter, d_n (mm)
1	Small	0–6.35	$d_1 = 6.35$
2	Medium	>6.35–50.8	$d_2 = 25.4$
3	Large	>50.8–152.4	$d_3 = 101.6$
4	Rupture	>152.4	d4 = min [D,406.4]

3.4.1 *Release rate*

There are two regimes for flow of gases or vapors through an orifice: sonic for higher internal pressures and subsonic flow for lower pressures. After analyzing, the release rate of LNG gas supply system is computed using Equation (4), which is based on discharge of gases and vapors at subsonic velocity through an orifices.

$$W_n = \frac{0.9}{1000} \cdot \frac{\pi \cdot d_n^2}{4} \cdot P_s \sqrt{\left(\frac{k \cdot MW}{R \cdot T_s}\right)\left(\frac{2}{k+1}\right)^{\frac{k+1}{K-1}}} \tag{4}$$

where W_n = the theoretical release rate associated with the nth release hole size[kg/s]; d_n = the diameter associated with the nth vapor release hole size[mm]; Ps = Is the storage or normal operating pressure[kPa]; K = Is the release fluid ideal gas specific heat capacity ratio; MW = the release fluid molecular weight[kg/mol]; R = the universal gas constant = 8314 [J/(mol·K)]; Ts = the storage or normal operating temperature[K].

3.4.2 *Vapor cloud explosion*

In the machinery spaces, a vapor cloud explosion can occur as a result of a delayed ignition of LNG gas that disperses. The TNT equivalency method can be used to estimate the overpressure VCE producing. This method determines the amount of available energy in the cloud and relates this to an equivalent amount of TNT using Equation (5):

$$W_{TNT} = \frac{\eta \cdot mass_{vce} \cdot HC_v}{HC_{TNT}} \tag{5}$$

where W_{TNT} = the energy released in an explosion expressed as equivalent mass of TNT[kg];

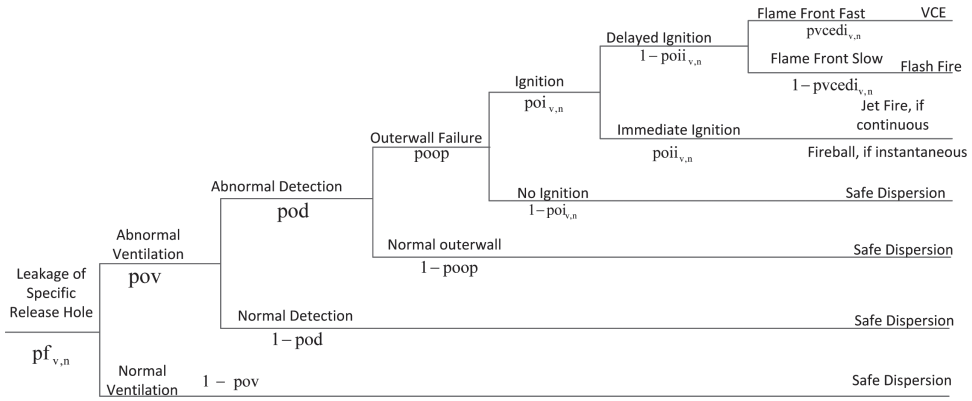


Figure 4. ETA used in machinery spaces.

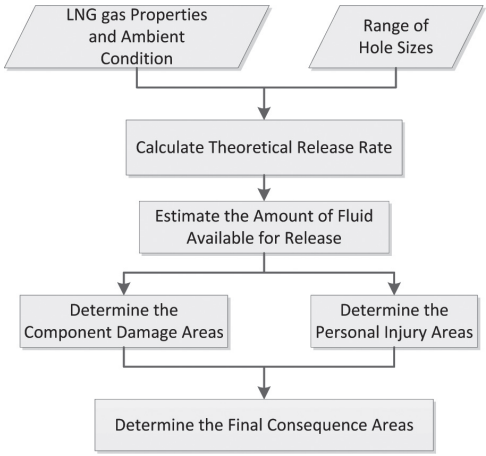


Figure 5. Consequence analysis procedures.

$mass_{vce}$ = the mass of flammable material in the vapor cloud used in the VCE calculation[kg]; η = the explosion yield factor; HC_{TNT} = the heat of combustion of TNT ≈ 4648 [kJ/kg].

$$P_{SO,n} = 100 \cdot \left(\begin{array}{l} -0.059965896 + \frac{1.1288697}{\ln[\bar{R}_{HS,n}]} - \frac{7.9625216}{\left(\ln[\bar{R}_{HS,n}]\right)^2} \\ + \frac{25.106738}{\left(\ln[\bar{R}_{HS,n}]\right)^3} - \frac{30.3967}{\left(\ln[\bar{R}_{HS,n}]\right)^4} + \frac{19.399862}{\left(\ln[\bar{R}_{HS,n}]\right)^5} \\ - \frac{6.8853477}{\left(\ln[\bar{R}_{HS,n}]\right)^6} + \frac{1.2825511}{\left(\ln[\bar{R}_{HS,n}]\right)^7} - \frac{0.097705789}{\left(\ln[\bar{R}_{HS,n}]\right)^8} \end{array} \right) \quad (6)$$

where $P_{SO,n}$ = the side-on overpressure associated with the nth release hole size[kPa], 34.5 kPa for component damage; $\bar{R}_{HS,n}$ = the Hopkinson's scaled distance used in the blast calculations associated with the nth release hole size.

Using the Equation (6), (7) can determine the safe distance (xs_n^{vce}) from the vapor cloud explosion for component damage, with the side-on overpressure ($P_{SO,n}$) of 34.5 kPa. For personal injury, the safe distance can calculated be based on the Equation (8) and the Pr value can be set at 0.5.

$$\bar{R}_{HS,n} = \frac{xs_n^{vce}}{W_{TNT}^{1/3}} \quad (7)$$

$$Pr = -23.8 + 2.92 \cdot \ln[1000 \cdot P_{SO,n}] \quad (8)$$

where xs_n^{vce} = the safe distance from the vapor cloud explosion for component damage associated with the nth release hole size[m]; Pr = the probability value, typically set at 0.5 (50% probability).

Once the safe distances, $xs_{cmd,n}^{vce}$ and $xs_{inj,n}^{vce}$, are determined, the following equations is carried out for personal injury area and component damage area for each of the release hole size.

$$CA_{cmd,n}^{vce} = \pi \cdot \left(xs_{cmd,n}^{vce}\right)^2 \quad (9)$$

$$CA_{inj,n}^{vce} = \pi \cdot \left(xs_{inj,n}^{vce}\right)^2 \quad (10)$$

where $xs_{cmd,n}^{vce}$ = the component damage consequence area for VCE associated with the nth release hole size[m^2]; $xs_{cmd,n}^{vce}$ = the safe distance from VCE for component damage associated with the nth release hole size[m]; $CA_{inj,n}^{vce}$ = the personal injury area for VCE associated with the nth release hole size[m^2]; $xs_{inj,n}^{vce}$ = he safe distance from VCE for personal injury associated with the nth release hole size[m].

3.4.3 *Flash fire*

Flash fire, like VCE, can occur as a result of a delayed ignition of a vapor cloud. However, unlike VCE, the flame speed is relatively slow and overpressures do not occur. The consequence are for personnel from a flash fire, $CA_{cmd,n}^{flash}$, is merely the flammable cloud boundary. As for the flammable cloud boundary, it can be determined using the Gaussian Models, with the LFL set 0.05 at and the UFL set at 0.15 for LNG gas. Equation (11) determines the component damage consequence area for flash fire.

$$CA_{cmd,n}^{flash} = 0.25 \cdot CA_{inj,n}^{flash} \quad (11)$$

where $CA_{cmd,n}^{flash}$ = the component damage consequence area for flash fire associated with the nth release hole size[m^2].$CA_{inj,n}^{flash}$ = the personal injury consequence area for flash fire associated with the nth release hole size[m^2].

3.4.4 *Jet fire*

Jet fires or fireball occurs as a result of immediate ignition of LNG gas from the gas supply system. As all the release type of the leakage in machinery space is continuous after analyzing, the consequence of fireball is not evaluated in this paper. For jet fire, the main deleterious effect is the heat flux produced by the jet fire.

The amount of energy radiated by the jet is a fraction of the total combustion power of the flame, as Equation (12) shows.

$$Qrad_n^{jet} = 0.35 \cdot W_n \cdot HC_v \quad (12)$$

where $Qrad_n^{jet}$ = the total energy radiated from a jet fire associated with the nth release hole

size[W]; HC_v = the heat of combustion of vapor fuel[J/kg].

The received thermal flux at some location away from the jet fire can be calculated with the Equation (13). The acceptable distance away from the jet fire is determined by the thermal radiation limit, 12.6 kW/m^2 for individual death and 37.8 kW/m^2 for component's damage.

Once the acceptable distance, $xs^{jet}_{cmd,n}$ and $xs^{jet}_{inj,n}$, are calculated, Equation (14) and Equation (15) are used to determine the jet fire consequence area.

$$Ith^{jet}_n = 0.5 \cdot Qrad^{jet}_n \cdot \frac{1}{4\pi \cdot xs^2_n} \tag{13}$$

$$CA^{jet}_{cmd,n} = \pi \cdot \left(xs^{jet}_{cmd,n}\right)^2 \tag{14}$$

$$CA^{jet}_{inj,n} = \pi \cdot \left(xs_{inj,n}\right)^2 \tag{15}$$

where Ith^{jet}_n = the radiant heat flux received at a distant receiver location from a jet fire associated with the nth release hole size[W/m^2], 12.6 kW/m^2 for individual death and 37.8 kW/m^2 for component's damage; $CA^{jet}_{cmd,n}$ = the component damage consequence area for a jet fire associated with the nth release hole size [m^2]; $xs^{jet}_{cmd,n}$ = the safe distance from the jet fire flame surface for component damage associated with the nth release hole size[m]; $CA^{jet}_{inj,n}$ = the personal injury consequence area for a jet fire associated with the nth release hole size [m^2]; $xs^{jet}_{inj,n}$ = the safe distance from the jet fire flame surface for personal injury associated with the nth release hole size[m].

3.5 *Risk summation*

The risk of some identified hazard which can be calculated using the Equation (16), (17), (18) that is the weighted average of jet fire, VCE and flash fire consequence area.

$$R^{flam}_{cmd} = \sum_{n=1}^{4}\left(\begin{array}{l} pjet_n \cdot CA^{jet}_{cmd,n} + pvce_n \\ \quad \cdot CA^{vce}_{cmd,n} + pflash_n \cdot CA^{flash}_{cmd,n} \end{array}\right) \tag{16}$$

$$R^{flam}_{inj} = \sum_{n=1}^{4}\left(\begin{array}{l} pjet_n \cdot CA^{jet}_{inj,n} + pvce_n \\ \quad \cdot CA^{vce}_{inj,n} + pflash_n \cdot CA^{flash}_{inj,n} \end{array}\right) \tag{17}$$

$$RS_i = \max\left[R^{flam}_{cmd}, R^{flam}_{inj}\right] \tag{18}$$

where R^{flam}_{cmd} = the risk concerning component damage[m^2/year]; R^{flam}_{inj} = the risk concerning personal injury[m^2/year]; RS_i = the final risk concerning hazardous area of an identified hazard [m^2/year];

As all the hazards of the in the machinery space are assumed as relatively independent events, the total risk of the machinery space can be determined using the Equation (19) (20).

$$R_i = RS_i \cdot (U_{cmd} + p_{inj}U_{inj}) \tag{19}$$

$$R = P_{all} \cdot U_{all} = \sum R_i \tag{20}$$

where R_i = the total risk of an identified hazard [\$M[①]/year]; U_{cmd} = the equipment economic value per square meter of the machinery spaces[\$M/m^2]; U_{inj} = 1\$M/m^2, conservatively assuming 1death for every hazardous square meter; p_{inj} = 1/S, conservatively assuming one crew stay in the engine spaces at any time, 'S' is the gross area of the engine spaces[m^2]; R = the total risk of the machinery spaces [\$M/year]; P_{all} = the gross probability of fire and explosion of machinery spaces, [1/year].

U_{all} = the total consequence of fire and explosion of machinery spaces, [\$M/year].

3.6 *Tolerability of risks*

Two graphic forms to convey risk result—individual risk contours and societal risk F-N curves are recommended by the Rijnmond Public Authority (1982). Compared with individual risk, Societal Risk expressed in an FN-diagram allows a more comprehensive picture of risk. Moreover, each type of accident (e.g. fire and explosion) can make use of Societal Risk expression (IMO 2007). Therefore, a kind of F-N curves (Fig. 6) is recommended, which is taken from a public environmental impact statement, published on the Hong Kong Environmental Protection Department Environmental Impact Assessment (EIA) website (DNV 2007). However, F-N curves merely focus on

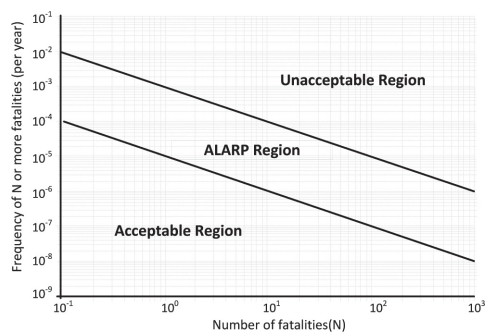


Figure 6. F-N curves.

①It refers to million dollars.

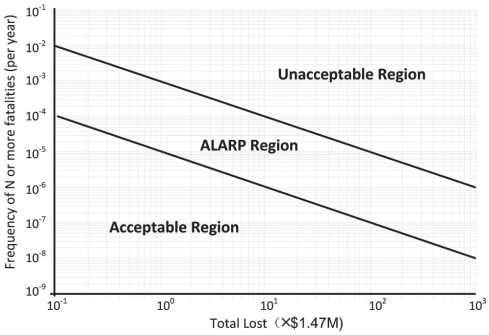


Figure 7. F-TL curves.

human fatalities without considering financial loss. It's worth combing human fatalities and financial loss together into a new type curves deriving from F-N curve assuming that a fatality correspond to 35 lost life-years, the median value correspond to $1.470.000 (DNV 2000). The new type of curves can be called F-T.L. curves. See Figure 7. As F-T.L. curves show, the ALARP zone refers to as low as reasonably practicable-a tolerated zone of risk, only if all reasonable measures have been taken to reduce or mitigate the risk.

As for engine spaces of LNG gas fuelled ship, it's critical to determine which zone the total risk of machinery spaces locate, equation (20). According to Figure 6(b), equation (21), (22) can be deduced.

$$\log10(P_{all}) + \log10(U_{all}/1.47) \le \log10(10^{-5}) \quad (21)$$

$$\log10(10^{-5}) \le \log10(P_{all}) + \log10(U_{all}/1.47) \le \log10(10^{-3}) \quad (22)$$

Thus, for acceptable zone, it should meet the equation (23) deriving from equation (21). In the similar way, for ALARP zone, it should meet the equation (24) deriving from equation (22).

$$R = P_{all} \cdot U_{all} \le 1.47 \times 10^{-5} = R_{lower\,\lim it} \quad (23)$$

$$R_{lower\,\lim it} = 1.47 \times 10^{-5} \le R = P_{all} \cdot U_{all} \le 1.47 \times 10^{-3} = R_{lower\,\lim it} \quad (24)$$

4 DISCUSSION

The introduction of alternative fuels for marine design presents a challenge for commercial ship industry. The novel designs and technologies of increased safe machinery spaces put forward by CCS is not covered by current standards needs to meet adequate levels of safety. This research develops a practical methodology to assess increased safe machinery spaces, which will contribute to the perfection of relevant specifications, rules or standards.

1. This methodology takes over the basic framework of risk based technology (Fig. 2) and some limitations or issues are noteworthy.
2. The risk of fire and explosion in increased gas safe engine spaces of LNG gas fuelled ship is merely discussed in this research. However, risks outside, like collision, tank explosion, freezing damage and stranding and so on, are exclusive, which deserve further study.
3. As leaking orifice is divided into four ranges, small, medium, large and rupture, and generic historic data may be not able to meet the requirement, interpolation method (Yu L. J., Duo Y. Q. and Shi Li Chen. 2007) could be applied to the frequency analysis of this methodology.
4. A factor influencing consequence is ignition. Different type of ignition would lead to different consequences. If the release is immediately ignited at the release point, then outcomes will be jet fire for gas leakage. If the ignition is remote or delayed in time, then flash fire and Vapour Cloud Explosion (VCE) are possible. Currently, several empirical formulae (Spencer H, Daycock JH and Rew PJ 1998; Bai YZ et al. 2010; Ronza A, Vilchez JA, Casal J 2007) have been developed to estimated ignition likelihood. John L. However, Woodward and Robin M. Pitblado (2010) point out that a flammable cloud has a probability of ignition that depends both on its flammable extend and the number, strength and duration of coverage of local ignition sources, which needs further research to define probability of ignition accurately.
5. As for flash fire and vapour cloud explosion, the hazardous areas are determined by flammable cloud boundary, which can be calculated by CFD codes, like CFX and Fluent. However, due to the large amount of calculation, Gaussian Models can be an alternative method to analyse flammable cloud boundary at the expense of the precision.

REFERENCES

American Bureau of Shipping (ABS). 2011. Guide for propulsion and Auxiliary Systems for Gas Fuelled Ships. Houston: American Bureau of Shipping (ABS).

American Petroleum Institute (API). 2008. Risk-Based Inspection Technology. 2nd ed. Washington, D.C.: American Petroleum Institute (API).

BAI Yong-zhong, YU An-feng, DANG Wen-yi, WU Zhi-feng and ZHAO Xiang-di. 2010. Determination of Ignition Source and Ignition Probability of Leaking Accidents in Petrochemical Processes. *China Safety Science Journal.* 20(1):61–66.

China Classification Society (CCS). 2013. Rules for Natural Gas Fuelled Ships. Beijing: China Communication Press.

Crosthwaite P.J., Fitzpatrick, R.D. and Hurst N.W. 1988. Risk Assessment for the Siting of Developments Near Liquefied Petroleum Gas Installations. IChemE Symposium Series, No 110.

DET NORSKE VERITAS (DNV). 2007. Liquefied Natural Gas (LNG) Receiving Terminal and Associated Facilities, part 2, Section 13. EIA Report by the Environmental Resources Management, Hong Kong, China.

DET NORSKE VERITAS (DNV). 2012. Gas Fuelled Ship Installations. Oslo: DET NORSKE VERITAS (DNV).

DNV consulting, New Generic Leak Frequencies for Process Equipment, Published online 13 October 2005 in Wiley InterScience.

Germanischer Lloyd (GL) AG. 2010. Guidelines for the Use of Gas as Fuel for Ships. Hamburg, German: Germanischer Lloyd (GL) AG.

International Maritime Organization (IMO). 2000. FORMAL SAFETY ASSESSMENT: Decision parameters including risk acceptance criteria (MSC72/16). London: International Maritime Organization (IMO).

International Maritime Organization (IMO). 2007. FORMAL SAFETY ASSESSMENT: Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (MSC/Circ.1023-MEPC/Circ.392). London: International Maritime Organization (IMO).

International Maritime Organization (IMO). 2009. INTERIM GUIDELIINES ON SAFETY FOR NATURAL GAS-FUELLED ENGINE INSTALLATIONS IN SHIPS (MSC.258(86)). London, England: International Maritime Organization (IMO).

John L. Woodward and Robin M. Pitblado. 2010. LNG Risk Based Safety: Modelling and Consequence Analysis. Hoboken, New Jersey: John Wiley & Sons, Inc.

Michael D. Tusiani and Gordon Shearer. 2007. LNG: A Nontechnical Guide. Tulsa, USA: PennWell Corporation.

Rijnmond Public Authority. 1982. A Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area. Dorderecht, Holland: D. Reidel Publishing Company, Dordrecht.

Ronza A, Vilchez JA and Casal J. 2007. Using transportation accident databases to investigate ignition and explosion probabilities of flammable spills. *Journal of Hazardous Materials*, 146:106–123.

Spencer H, Daycock JH and Rew PJ.1998. A model for the ignition probability of flammable gases. WS Atkins for HSE.

YU Li-jian, DUO Ying-quan, SHI Li-chen, WEI Li-jun and WU Zong-zhi. 2007. Method for Determining Probabilities of Leaks in Quantitative Risk Assessment. *Journal of Safety Science and Technology*. 3(6): 27–30.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Semi-qualitative method for ship collision risk assessment

W. Zhang, J. Montewka & F. Goerlandt
Department of Applied Mechanics, Marine Technology, Research Group on Maritime Risk and Safety, Aalto University, Espoo, Finland

ABSTRACT: In this paper we introduce a method for the assessment of the complexity of ship-ship encounters, linked with the risk level of such encounters. The method combines traffic data obtained from the Automatic Identification System and experts' judgment. The collected data describes maritime traffic over the Northern Baltic Sea, including the Gulf of Finland, which is potentially one of the most heavily trafficked sea areas in the world.

Based on the method, we develop a risk model, which differentiates between four types of ship-ship encounters, associating a risk level to each of them. The encounters are of the following types: normal encounter, collision avoidance, close-encounter and accident. The obtained results reveal that the areas of the highest risk are related to the waterways crossing between Helsinki and Tallinn, as well as approaches to harbours. The risk model developed here can be used for efficient data screening for encounters of various risk levels as well as for the comparison of traffic situations from various time epochs.

1 INTRODUCTION

Maritime transportation is the main transportation mode for both domestic and international trade. It is estimated that 90% of the world trade volume is carried by sea (IMO 2008). While major shipping accidents are relatively rare occurrences, their consequences can have devastating effects measured in human or economic losses and in terms of damage to the marine environment. Worldwide, groundings, collisions and fires are the most frequently occurring accident types (Soares & Teixeira 2001). However, in local sea areas with high traffic intensity such as the Gulf of Finland and the Singapore Strait, ship-ship collisions are one of the most frequently occurring accident types (Kujala et al. 2009; Weng et al. 2012).

In response to stakeholder concerns regarding the safety of maritime transportation, various approaches to ship collision risk have been proposed. Where the risk is seen as a measure of safety. Some studies concern probabilistic risk assessment and management. Such methods are aimed at probabilistically identifying areas of high ship collision risk e.g. using statistical methods (Friis-Hansen & Simonsen 2002), traffic simulation (Goerlandt & Kujala 2011) and combined accident statistics and ship domain analysis (Montewka et al. 2012). Another studies concern operational risk assessment, where ship collision risk is considered in real-time dynamic traffic situations onboard vessels or in Vessel Traffic Service (VTS) centers. Various methods for decision support in collision avoidance have been proposed, e.g. based on fuzzy ship domains (Kao et al. 2007; Pietrzykowski & Uriasz 2008; Gucma & Pietrzykowski 2006), or statistical models (Mou et al. 2010).

However most of these methods rely on scarce accident statistics, predictive traffic flow methods (Fowler & Sørgård 2000) or simulation techniques (Goerlandt & Kujala 2011), which necessitate assumptions on what constitutes a vessel encounter. This may lead to an unreliable identification of risk areas, as discussed in (Goerlandt & Kujala 2014). Therefore, the method presented in this paper utilizes non-collision information from actually observed traffic to assess system risk and avoid assumptions, which may question the reliability and validity of the method.

The model presented in this paper follows an approach determining a Risk Indicator reflecting the complexity of ship-ship encounters in a given sea area. The logic behind is that the more complex a meeting between two ships is the more difficult is to handle the situation as the number of simultaneous goals gets higher and tenser (planning, conducting and assessing the efficiency of the evasive action), navigators may begin to operate in a higher stress mode, which contributes to the higher probability of making an error, see for example (Hollnagel 1998; Yang et al. 2013). Therefore, we introduce the complexity of an encounter as a Risk Indicator.

The method presented in this paper applies experts judgment and micro-level ship traffic data

as obtained from the Automatic Identification System (AIS) as background information. From this, a set of traffic metrics is deduced, which are combined in a collision Risk Indicator.

The developed model behaves as expected, which has been proven in a series of tests, presented in the paper. The analysis of the collision risk for the maritime traffic over the Northern Baltic Sea shows very good agreement of the obtained results with the previous studies.

The remainder of the paper is organized as follows: Section 2 introduces conceptual basis for the Risk Indicator. In Section 3 the Risk Indicator is formulated and in subsequent section it is quantified and the behavior tests are carried out. Section 5 demonstrated the results of collision risk assessment with the use of the Risk Indicator for the Northern Baltic Sea. In Section 6 we discuss the developed model and the obtained results, whereas Section 7 concludes.

2 CONCEPTUAL BASIS

2.1 *Risk concept and perspective*

In risk research literature, there is increasing focus on the theoretical basis of risk assessment, particularly in terms of the adopted conceptual risk definition and the adopted perspective on how risk is described (Aven & Zio 2013). The work presented in this paper adopts the view that risk can conceptually be defined as "the possibility of an unfortunate occurrence", see e.g. (Aven 2012). This concept can be summarized as follows:

$$Risk = Po(A) \tag{1}$$

where $Po(A)$ signifies the potential of occurrence of A, where A stands for the event of interest, which in this context is a ship-ship collision.

The risk perspective, which aims at the description of risk, adopts a situation-dependent indicator (I). The indicator describes how possible the occurrence is in a particular context, which can be summarized as:

$$Risk \sim I(A) \tag{2}$$

$$I(A) = f(S) \tag{3}$$

where $I(A)$ signifies the indicator of the occurrence of event A, expressed either quantitatively or qualitatively. The indicator I depends on a set of system states S, in the context of this paper these are the traffic metrics—distance between two meeting ships, the relative speed and the difference in their headings—deduced from the micro-level ship traffic data.

2.2 *Traffic conflict technique*

The indicator-based risk perspective is compatible with the methodological framework of the Traffic Conflict Technique (TCT). This technique, originally proposed in road traffic safety analysis (El-Basyouny & Sayed 2013; Sacchi et al. 2013; Young et al. 2014), has recently been applied in navigational risk assessment, see for example (Debnath & Chin 2010). Relying on scarce accident statistics, predictive traffic flow methods (Fowler & Sørgård 2000) or simulation techniques (Goerlandt & Kujala 2011) which necessitate assumptions on what constitutes a vessel encounter may lead to an unreliable identification of risk areas (Goerlandt & Kujala 2014). Therefore, the method presented in this paper utilizes non-collision information from actually observed traffic to assess system risk.

The concept of the TCT is rooted in the idea that not only accidents, but also all conflict situations, i.e. situations in which traffic system users encounter one another such that accidents can occur, provide insight in the system risk level. The hierarchy of different levels of nearness to an accident encompasses undisturbed passages, conflicts of various severity, near misses and accidents. This hierarchy has been conceptually presented as a pyramid (Hyden 1987) or a diamond (Svensson 1998). The most significant advantage of the TCT is the fact that vessel conflicts of various severity levels occur more frequently than collision accidents, such that more information about the system risk level can be obtained in shorter time periods (Debnath & Chin 2010).

In this paper we introduce a method for detecting and classifying the ship-ship encounters, using AIS data, and experts judgments. Subsequently the method is adopted to develop a risk model, which quantifies the risk level over a sea area in tempo-spatial manner, associating the magnitude of Risk Indicator with the level of complexity of an encounter. The model attempts to convert available data into information first, and then information to understanding. Data serves here as the input to the risk assessment model, information contains the risk description, which is based on the data,

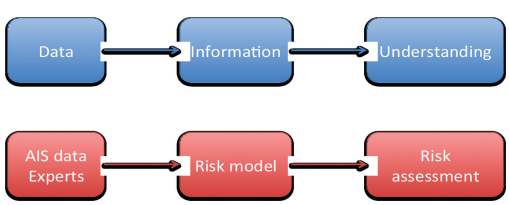


Figure 1. A systematic way of transforming available data into understanding of the analysed system.

and understanding relates to the process of risk assessment and obtained results, see for example (Aven 2013; Montewka et al. 2014) and Figure 1.

3 FORMULATION OF RISK INDICATOR

In this chapter, the methodological framework is provided for the developed model, which detects and ranks the complexity of ship-ship encounters. First, the available micro-level ship traffic data, as obtained from the Automatic Identification System (AIS), is outlined. Subsequently, the process and outcome of an expert elicitation related to the development of a quantitative Risk Indicator (I). The latter is a measure of risk in the sea area, based on detection of vessels encounters and their complexity. Then, the mathematical formulation of the indicator is presented, both in regards to the model structure and model parameters. Finally, the obtained results need to be clustered to arrive at qualitative Risk Indicator. Thus, the purpose and rationale of the applied clustering technique is outlined.

3.1 *Micro-level ship traffic data: Automatic Identification System (AIS)*

The AIS system identifies every vessel equipped with an AIS transmitter, individually, along with its specific position and movements, enabling a virtual picture to be created in real time. The data is transmitted at an interval of about 3–10's, and a number of key parameters are recorded. The data used in this paper was obtained from HELCOM (Baltic Marine Environment Protection Commission—Helsinki Commission), and it covers the Northern Baltis Sea, including the Gulf of Finland and a period of two months: May and July 2011. The raw data includes fundamental navigation information such as time, latitude, longitude, speed, course, heading, etc, see (US Department of Homeland Security 2013).

3.2 *Risk indicator*

Risk Indicator, developed in the course of this study, utilizes two types of data: first, judgement of experts (nautical officers and captains with the record of at least 5 years of sea service), second, AIS data. The former is used to define the structure of the mathematical model for Risk Indicator, whereas the latter quantifies the model parameters. Both are described in the following subsections.

3.2.1 *Determining the model structure*

Risk Indicator is intended to measure the risk through the complexity of an encounter between two ships at sea, both being under way. This type of encounter is regulated by the International Regulations for Preventing Collisions at Sea, (IMO 2003). In this paper we measure the encounter complexity through the available time that officers have to perform the evasive action and the magnitude of that action. The time available is directly determined through the distance between two meeting ships and their relative speed, whereas the magnitude of action is assessed based on the difference in ships headings. Beside, two ship encounter, there exist multiple-ship encounters, however they are out of the scope of this analysis.

Risk index takes its value from a range of [–n, n]. A positive value indicates that the encounter may require an action from an officer in charge to ensure safe passage of the ships. A negative value indicates a safe situation, where action is not required. The Risk Indicator presented here comprises three interrelated elements, as follows: 1) the distance between two ships; 2)the rate of change of the distance in the course of encounters, measured by the relative speed between two ships; 3) the relative orientation of two ships, described by the difference between their headings.

Such a triplet attempts to describe the complexity, thus the risk level, of an encounter between two ships.

Distance

As distance alone does not describe the complexity of an encounter, it must coexist with other parameters. However, for the purpose of this study, we assume that an increased distance between two ships corresponds to a decreased complexity of an encounter. Thus, distance and complexity are inversely proportional in the mathematical model describing I.

$$I \approx f(Distance)^{-1} \tag{4}$$

Relative Speed

The rate of change of distance between two ships is another relevant factor in the model. This can be described by relative speed, which is calculated based on true headings of two ships and their actual speeds, as depicted in Figure 2. The higher the relative speed, the less time an officer has to address and solve the situation. Therefore, the existence of a positive correlation between the two parameters is assumed. It is not yet clear, however, what kind of relation best describes the correlation.

$$I \approx f(Relative\ speed)^{2} \tag{5}$$

However, in certain encounters like overtaking, a high relative speed may be preferable, as this shortens the time of the manoeuver. In such situations the above relation does not hold, therefore it would

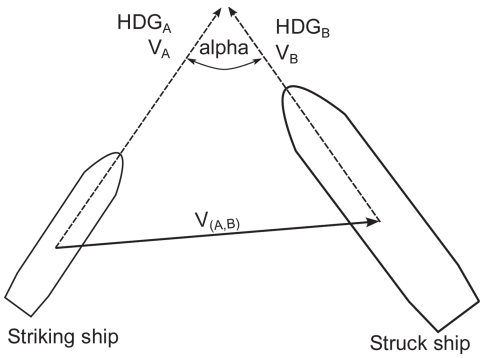


Figure 2. The relations between ships headings, their actual speed and the resulting relative speed.

be desirable to introduce alternative relations and measure their effect on the Risk Indicator. The anticipated effect of the changes in this parameter of the model outcome is elaborated in the discussion part of the paper.

Phase

Through phase we specify the relative location of two vessels and the magnitude of course alteration that is anticipated to perform collision evasive action. The range of phase is [–180,180], where a negative indicates that the encounter is not of interest to navigators, as the ships are receding from each other. Positive phase indicates that the ships are approaching one another. The interpretation of this parameter is given in Figure 3.

$$I \approx f(Phase) \tag{6}$$

Considering the range of phase, $f(Phase)$ is periodic function, and the period is 2π

$$f(x) = f(x + 2\pi) \tag{7}$$

A negative phase corresponds to a situation, where there is no risk of collision. For the positive phase, the collision risk exists and varies with the time, as two encountering ships approach each other. We can define $f(x)$ as an odd function, that is

$$f(-x) = -f(x) \tag{8}$$

The function describing I would contain three parameters, bound with the following relationships:

$$I \approx f(Distance)^{-1},\ (Relative\ Speed)^2,\ g(Phase) \tag{9}$$

where $g(Phase)$ is a periodic and odd function. The mathematical model quantifying the I is presented in the following section.

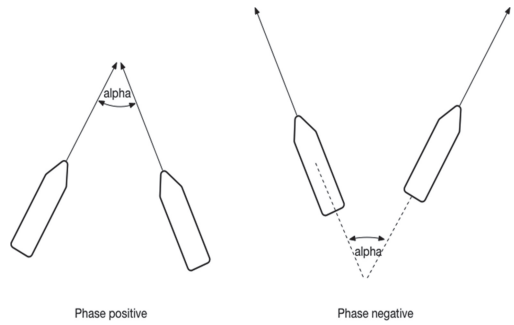


Figure 3. Interpretation of parameter "phase". On the left phase is positive, on the right it is negative.

3.2.2 *Formulation of the Risk Indicator*

It is known that every periodic function $x(t)$, with T denoting its period, can be expanded into a Fourier series:

$$x(t) = \sum_{k=-\infty}^{+\infty} a_k \cdot e^{jk\left(\frac{2\pi}{T}\right)t} \tag{10}$$

Here,

$$a_k = \frac{1}{T}\int_T x(t) \cdot e^{-jk\left(\frac{2\pi}{T}\right)t} \tag{11}$$

Since $f(x)$ is an odd function, considering

$$e^{j\theta} = sin\theta + j \cdot cos\theta \tag{12}$$

Thus $f(x)$ can be described as a sine series,

$$f_0(x) = \sum_{-\infty}^{+\infty} b_k \cdot \sin(kx) \tag{13}$$

In order to reduce the complexity of computation, we use the first two terms of the Fourier series only, that is,

$$f_o(x) = b_1 \cdot sinx + b_2 \cdot sin\,(2x) \tag{14}$$

In light of the previous discussion, the following expression can be stated for Risk Indicator (I):

$$I(x,\ y,\ z) = ((kx^{-1} + my^2)(b_1 \cdot \sin(z) + b_2 \cdot \sin(2z)) \tag{15}$$

where, x represents Distance, y represents Relative speed, z represents Phase.

3.2.3 *Parameter estimation*

To estimate the paramters of the equation quantifying the Risk Indicator, we selected data samples from some typical encounters. Then, we applied the least squares method to obtain the numeric values for the parameters.

For this purpose we predefined two distances. The first is 6 NM, which is the usual observation range of shipborne radar in high seas, the second is 1 NM. For these two ranges, we propose the values for the Risk Indicator, as follows:

1. The absolute value of I at 6 NM range should take some small value, let's take 5:

$$E(I(x,y,z))|_{x=6} = 5 \tag{16}$$

where E is mathematical expectation.

2. The absolute value of I at 1 NM range, is taken as 100:

$$E(I(x,y,z))|_{x=1} = 100 \tag{17}$$

In a short distance like 1 NM, some factors like phase have more influence than in a longer distance like 6 NM, and can not be ignored. Then, traffic scenarios containing phase in the range of [165, 180] are chosen in calculation.

There are four parameters that need be calculated to quantify the Risk Indicator (k, m, b_1, b_2). Since phase involves direction and course, b_1 and b_2 are supposed to be 1. Then, the other two parameters can be estimated by the method of least squares.

$$f = \min\left(\sum \Delta I_i\right) = \min\left(\sum_i^n a_i (k x_i^{-1} + m y_i^2)\right) \tag{18}$$

Let

$$\begin{cases} \dfrac{\partial f}{\partial x} = 0 \\ \dfrac{\partial y}{\partial x} = 0 \end{cases} \tag{19}$$

That is,

$$\left(\sum_i^n a_i^2 x_i^{-2}\right) k + \left(\sum_i^n a_i^2 x_i^{-1} y_i^2\right) m = \sum_i^n a_i x_i^{-1} I_i \tag{20}$$

and

$$\left(\sum_i^n a_i^2 x_i^{-1} y_i^2\right) k + \left(\sum_i^n a_i^2 y_i^4\right) m = \sum_i^n a_i y_i^2 I_i \tag{21}$$

Eventually,

$$k = \frac{\sum_i^n a_i x_i^{-1} I_i \sum_i^n a_i^2 y_i^4 - \sum_i^n a_i y_i^2 I_i \sum_i^n a_i^2 x_i^{-1} y_i^2}{\sum_i^n a_i^2 y_i^4 \sum_i^n a_i^2 x_i^{-2} - \left(\sum_i^n a_i^2 x_i^{-1} y_i^2\right)^2} \tag{22}$$

$$m = \frac{\sum_i^n a_i x_i^{-1} I_i \sum_i^n a_i^2 x_i^{-1} y_i^2 - \sum_i^n a_i y_i^2 I_i \sum_i^n a_i^2 x_i^{-2}}{\left(\sum_i^n a_i^2 x_i^{-1} y_i^2\right)^2 - \sum_i^n a_i^2 x_i^{-2} \sum_i^n a_i^2 y_i^4} \tag{23}$$

4 QUANTIFICATION OF RISK INDICATOR

In this section we present the results of the quantification of the parameters of Risk Indicator and then we demonstrate the results of the behaviour tests, performed for the proposed model for several, preselected encounters.

4.1 *Quantification of the parameters of Risk Indicator*

Risk Indicator's parameters are determined with the use of data sampled from over 1500 various encounters recorded duering May and June 2011, adopting the procedure descirbed in Section 3.2.3. The encounters were sampled in a way, that the whole range of distances between 1 NM and 6 NM has been covered, see Table 1 for some exemplary data sample.

The following parameters describing the Risk Indicator has been found by (22) and (23): k = 36.84 and m = 3.81E – 4. Considering $b_1, b_2 = 1$, the final equation describing the Risk Indicator is as follows:

$$I(x,y,z) = (36.84x^{-1} + (3.81e-04)y^2) \times (\sin z + \sin(2z)) \tag{24}$$

4.2 *Classification of Risk Indicator*

To classify the traffic scenarios of different value of Risk Indicator, into meaningful categories, attempting to reflect the risk level, cluster analysis

Table 1. Traffic data sample.

Scenario	Dist (km)	Relative speed (NM/hour)	Phase (deg)
36	5.6	13.6	56.8
	5.3	13.6	56.8
63	1.7	7.3	179.3
	0.9	3.0	178.8
89	5.5	26.1	83.9
	5.1	25.1	83.9
91	1.5	8.4	179.8
	0.9	12.2	179.8

is performed. In this study we anticipate four risk levels, follows:

1. regular encounter—distance between ships is less than 6 NM, but far more than 1 NM.
2. collision avoidance—Ship-ship distance is more than 1 NM but not large enough.
3. close-encounter—ship-ship distance is close to 1 NM, manoeuvre is necessary.
4. risk encounter—ship-ship distance is less than 1 NM, significant course alteration or speed change is deemed necessary.

Cluster analysis is a class of statistical techniques that can be applied to data that exhibit "natural" groupings. Cluster analysis sorts through the raw data and groups them into clusters. A cluster is a group of relatively homogeneous cases or observations. Objects in a cluster are similar to each other. They are also dissimilar to objects outside the cluster, particularly objects in other clusters.

For the purpose of this study we used *K*-means clustering, which is a method of vector quantization. *K*-means clustering aims to partition *n* observations into *k* clusters in which each observation belongs to the cluster with the nearest mean, serving as a prototype of the cluster. This results in a partitioning of the data space into Voronoi cells. *K*-means clustering algorithm can be described as follows:

Given a set of observations $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$, where each observation is a *d*-dimensional real vector, *k*-means clustering aims to partition the *n* observations into *k* sets $(k \le n)\ \mathbf{S} = \{S_1, S_2, \ldots, S_k\}$ so as to minimize the within-cluster sum of squares:

$$\arg\min \sum_{i=1}^{k} \sum_{x_j \in S_i} \left\| x_j - \mu_i \right\|^2 \tag{25}$$

where $\boldsymbol{\mu}_i$ is the mean of points in S_i.

In Table 2 the preliminary results of classification are show, where the corresponding ranges of Risk Indicator are found for each encounter type. However precise categories need lots of traffic scenarios as training data. This will be executed in further study.

Table 2. Risk range to safety level in ship-ship encounter.

Risk Indicator range	Encounter type
<50	Regular encounter
50–100	Collision avoidance
–500	Close-encounter
>500	Risk encounter

4.3 *Behavior tests of the Risk Indicator*

The behaviour tests attempt to check, if the developed Risk Indicator behaves as supposed, when input variables are changed accordingly. For this purpose we selected numerous traffic scenarios, representing the predefined four types of encounters. For each scenario we calculated Risk Indicator and compared it with the selected traffic situations. With this exercise we gained confidence in proper behavior of the Risk Indicator model and proper recognition of various encounters.

5 ASSESSMENT OF COLLISION RISK IN THE NORTHERN BALTIC SEA APPLYING THE RISK INDICATOR

Finally, we carried out the assessment of ship collision risk for the Northern Baltic Sea, with the use of the Risk Indicator introduced here. For this purpose we utilized the traffic data for May and July 2011 with the primary aim to assess the historic collision risk level in various locations of the Northern Baltic Sea in order to draw a spatial risk map for the analyzed sea area.

In Figure 4 all the encounters are plotted for the Northern Baltic Sea, and Figure 5 contains information for the Gulf of Finland. Four levels of risk, stemming from the four encounter types, are marked with different colors. Green means regular encounter, blue is collision avoidance, yellow stands for close-encounter, and red means risk encounter. The areas where the Risk Encounters occur are related to the waterways crossing between Helsinki and Tallinn, as well as approaches to major harbours. The former finding is expected, as there is a broad agreement among experts about riskiness of this area. Previous studies for this sea area support the findings, see for example (Kujala et al. 2009; Goerlandt & Kujala 2011; Montewka et al. 2012). The harbours approaches were recognized by the risk model presented here as locations of increased risk. This is mostly related to the close distance at which the ships are passing and the situations where a pilot boat approaches a ship to transfer a sea pilot. Despite the close distance between these two ships, such cases are considered safe, and the ship-ship collision risk is low. The model shall be further improved in order to detect such cases and classify them accordingly. As for now, the model classifies them as risk encounters, this unnecessarily increases the number of such encounters.

The locations of ship-sip meetings classified by the model as Close Encounters correlate with the locations where Risk Encounters were detected. This is an interesting finding, strengthening the arguments for the justification of the previous type of encounters. Most of meeting of this type occur

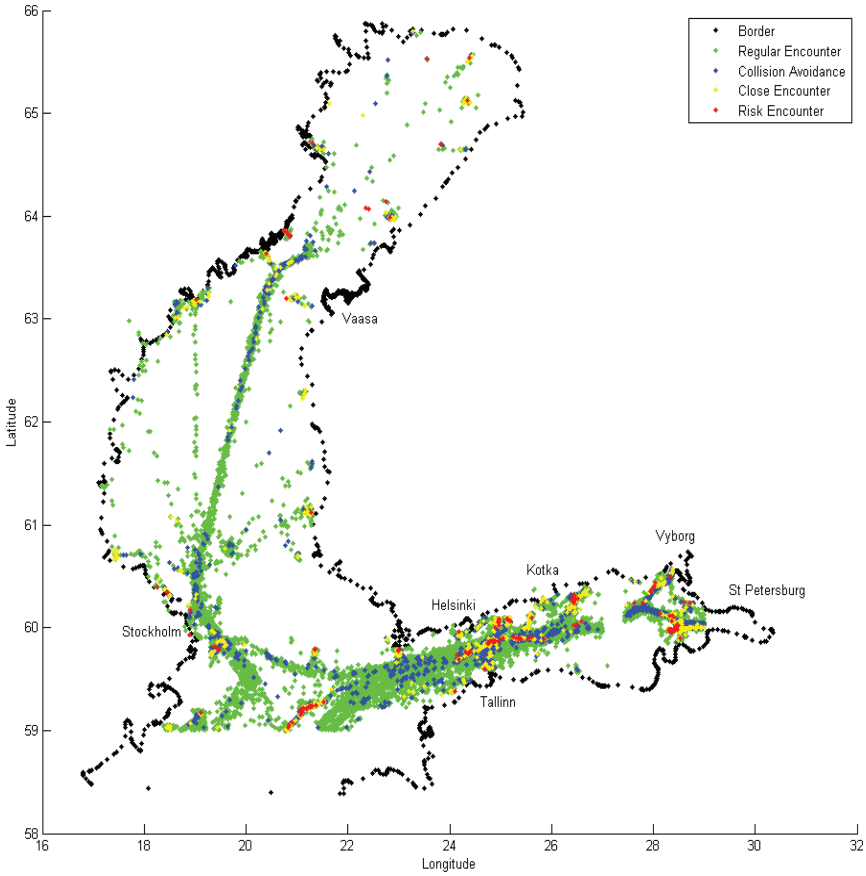


Figure 4. Preliminary risk assessment for ship-ship collision in the Northern Baltic Sea.

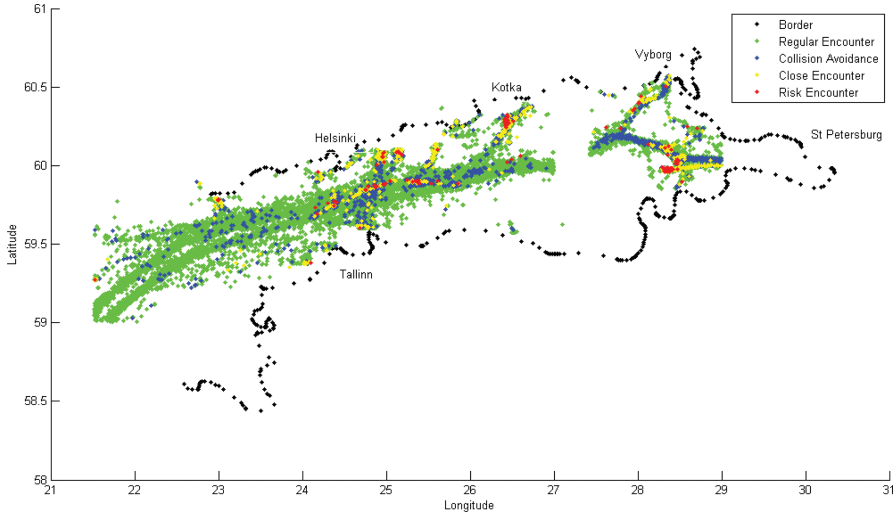


Figure 5. Preliminary risk assessment for ship-ship collision in the Gulf of Finland.

in the waterways leading to harbours. This seems sound, as the navigable space is usually limited in such locations, two types of meetings are predominant—overtaking and passing on reciprocal courses. This implies evasive actions at close range. Such an encounter may be of less risk than the same encounter in the open sea. In the former case the officers are aware of the situation and aware of the action of another ship. In the latter case, the situation may be more ambiguous, and officers more confused, which results in the increased probability of wrong performance. Nevertheless, the data presented in Figure 9 about this type of encounters correlates with the sound judgement and background knowledge about the potential places where the traffic is complex.

The encounters belonging to the type Collision Avoidance are distributed in a random fashion in the Gulf of Finland. However certain routes can be defined in the Sea of Bothnia, and the majority of encounters are happening along these routes. In the Gulf of Bothnia the number of encounters significantly drops, compared to the other sea areas, and they are concentrated along the waterways leading to main harbours of the Bay of Bothnia.

The spatial distribution of the last type of encounters, namely Regular Encounter, shows almost random nature of this encounter in the Gulf of Finland. However, for the Sea of Bothnia the location of detected encounters correlates with the major shipping lanes. Despite almost zero level of collision risk of this type of encounters; they are plotted to form a background picture. By determining the number of this type of encounter we get a reference point to calculate the share of other three types of encounters, as presented in Table 3. It is evident, that the type 4, which is of the highest risk, takes 0.84% of the total number of encounters. Actually, it is less, as the miss-classified cases increases it, as discussed earlier. Type 2 takes 4.3% and type 2 takes 7%. Such a distribution of encounters of various risk levels is in line with the pyramid hierarchy of an accident, as discussed in (Hyden 1987).

Table 3. Results of ship collision risk assessment for the Northern Baltic Sea.

Encounter type	Amount	Share [%]	Color code used in Figures 4, 5
1—Regular encounter	33,456	87.83%	Green
2—Collision avoidance	2,666	7.00%	Blue
3—Close-encounter	1,651	4.33%	Yellow
4—Risk encounter	319	0.84%	Red
Total	38,092	100%	–

Table 4. Results of ship collision risk assessment for the Gulf of Finland.

Encounter type	Amount	Share [%]	Color code used in Figure 4
1—Regular encounter	25,361	90.21%	Green
2—Collision avoidance	1,573	5.60%	Blue
3—Close-encounter	979	3.48%	Yellow
4—Risk encounter	199	0.71%	Red
Total	28,112	100%	–

Despite the problems of miss-classification, the hierarchy detected and the spatial distribution of encounters seem reasonable.

6 DISCUSSION

The model assessing the Risk Indicator introduced in this paper features novelty in how an encounter between two ships in the open sea is looked at. Unlike most of the existing approaches it combines three parameters, which are relevant to collision risk: distance between meeting ships, their relative speed and the difference in their headings. The latter indicates the magnitude of action required to solve the meeting situation. These parameters have been thoroughly described in Section 3, therefore in this section only the outstanding issues are addressed.

First is the form of relation between these three factors. The type of relation between Risk Indicator and distance or phase is relatively clear, as discussed earlier. However the function binding Risk Indicator and relative speed may raise concern. In the model we adopt the quadratic dependency, however there is no strong arguments for such a selection. Basically any other kind of relation is equally probable, this brings the uncertainty to the model, which in future can be addressed by alternative hypotheses testing, and studying the effect of the changes on the levels of Risk Indicators and their spatial distribution.

On the other hand, in the adopted form of Risk Indicator model the equation parameters for distance and relative speed are summed. The accompanying factors k and m take the values, which are 4 orders of magnitude apart. This leads to a situation, where the distance between two meeting ships is weighted more than their relative speed. Therefore, in the presented Risk Indicator model the effect of relative speed is not as important as the effect of distance.

Another issue is related to the size of encountering ships, which may affect the distance at which

the ships pass. In case of small vessels the safe passing distance is most probably shorter than in the situations where large ships are involved. Therefore, ship size shall be accounted for in the future studies.

Neither the effect of hydro meteorological conditions like the wave height and visibility has been included. However, the collected data refers to May and July, which are rather favourable months in the Baltic Sea. The time of the day has not been considered either. However over May and July the length of the day is on average 18 hours for the Gulf of Finland and even longer for the Sea of Bothnia and Bothnian Bay. This means, that our study focuses mainly on daytime conditions.

7 CONCLUSION

In this paper we propose a new method for ship-ship collision risk assessment in the large sea areas, applying the concept of Risk Indicator, which has been defined and developed for the purpose of this study.

The Risk Indicator considers the following factors influencing the complexity of an encounter thus collision risk: the distance between two ships, the relative speed of two ships and the difference in course of two encountering ships. The risk model developed here differentiates between four types of ship-ship encounters, associating a risk level to each of them. The encounters are of the following types: normal encounter, collision avoidance, close-encounter and accident.

The method applies experts' judgment together with micro-level ship traffic data obtained from the Automatic Identification System corresponding to the Northern Baltic Sea and summer season (Many, July 2011).

Finally, the risk model has been applied for the assessment of ship collision risk in the Baltic Sea and the obtained results have been benchmarked with other available risk models existing in the literature and the existing background knowledge on the phenomena analyzed. The benchmarking results show that the proposed model correctly classifies the various encounter types and the spatial map of risk levels for the maritime traffic in the Northern Baltic Sea corresponds to the actual traffic and the areas, which are known for featuring the increased collision risk.

The presented model can be used for efficient data screening for various types of encounters as well as for the comparison of traffic situations from various time epochs. The latter is especially relevant, as changes have been made, and the effect of these changes needs to be quantified in a post assessment strategy.

ACKNOWLEDGEMENTS

The financial assistance by Merenkulun Säätiö from Helsinki in the form of a travel grant is gratefully acknowledged.

REFERENCES

Aven, T., 2012. The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, 99(0), pp. 33–44.

Aven, T., 2013. A conceptual framework for linking risk and the elements of the Data–Information–Knowledge–Wisdom (DIKW) hierarchy. *Reliability Engineering & System Safety*, 111, pp. 30–36.

Aven, T. & Zio, E., 2013. Foundational issues in risk assessment and risk management. *Risk Analysis*.

Debnath, A.K. & Chin, H.C., 2010. Navigational traffic conflict technique: a proactive approach to quantitative measurement of collision risks in port waters. *Journal of Navigation*, 63(1), pp. 137–152.

El-Basyouny, K. & Sayed, T., 2013. Safety performance functions using traffic conflicts. *Safety Science*, 51(1), pp. 160–164.

Fowler, T.G. & Sørgård, E., 2000. Modeling ship transportation risk. *Risk Analysis*, 20(2), pp. 225–244.

Friis-Hansen, P. & Simonsen, B.C., 2002. GRACAT: software for grounding and collision risk analysis. *Marine Structures*, 15(4–5), pp. 383–401.

Goerlandt, F. & Kujala, P., 2014. On the reliability and validity of ship–ship collision risk analysis in light of different perspectives on risk. *Safety Science*, 62, pp. 348–365.

Goerlandt, F. & Kujala, P., 2011. Traffic simulation based ship collision probability modeling. *Reliability Engineering & System Safety*, 96(1), pp. 91–107.

Gucma, L. & Pietrzykowski, Z., 2006. Ship Manoeuvring in Restricted Areas: An Attempt to Quantify Dangerous Situations Using a Probabilistic-Fuzzy Method. *Journal of Navigation*, 59(02), p. 251.

Hollnagel, E., 1998. *Cognitive Reliability and Error Analysis Method (CREAM)*, Elsevier Science. Available at: http://www.amazon.com/Cognitive-Reliability-Error-Analysis-Method/dp/0080428487 [Accessed August 6, 2013].

Hyden, C., 1987. The development of a method for traffic safety evaluation: the Swedish traffic conflicts technique. *BULLETIN LUND INSTITUTE OF TECHNOLOGY, DEPARTMENT*, (70).

IMO, 2003. *COLREG: Convention on the International Regulations for Preventing Collisions at Sea, 1972,* International Maritime Organization.

Kao, S.-L. et al., 2007. A Fuzzy Logic Method for Collision Avoidance in Vessel Traffic Service. *Journal of Navigation*, 60(1), pp. 17–31.

Kujala, P. et al., 2009. Analysis of the marine traffic safety in the Gulf of Finland. *Reliability Engineering & System Safety*, 94(8), pp. 1349–1357.

Montewka, J., Goerlandt, F. & Kujala, P., 2012. Determination of collision criteria and causation factors appropriate to a model for estimating the probability of maritime accidents. *Ocean Engineering*, 40, pp. 50–61.

Montewka, J., Goerlandt, F. & Kujala, P., 2014. On a systematic perspective on risk for Formal Safety Assessment (FSA). *Reliability Engineering & System Safety*. http://dx.doi.org/10.1016/j.ress.2014.03.009.

Mou, J.M., Tak, C. van der & Ligteringen, H., 2010. Study on collision avoidance in busy waterways by using AIS data. *Ocean Engineering*, 37(5–6), pp.483–490.

Pietrzykowski, Z. & Uriasz, J., 2008. The Ship Domain—A Criterion of Navigational Safety Assessment in an Open Sea Area. *Journal of Navigation*, 62(01), p.93.

Sacchi, E., Sayed, T. & deLeur, P., 2013. A comparison of collision-based and conflict-based safety evaluations: the case of right-turn smart channels. *Accident; analysis and prevention*, 59, pp.260–6.

Soares, C.G. & Teixeira, A.P., 2001. Risk assessment in maritime transportation. *Reliability Engineering & System Safety*, 74(3), pp.299–309.

Svensson, A., 1998. *A method for analysing the traffic process in a safety perspective*. Lund: Lund University.

US Department of Homeland Security, 2013. Class A AIS position report.

Weng, J., Meng, Q. & Qu, X., 2012. Vessel collision frequency estimation in the Singapore Strait. *Journal of Navigation*, 65, pp.207–221.

Yang, Z.L. et al., 2013. A modified CREAM to human reliability quantification in marine engineering. *Ocean Engineering*, 58(null), pp.293–303.

Young, W. et al., 2014. Simulation of safety: A review of the state of the art in road safety simulation modelling. *Accident; analysis and prevention*, 66, pp.89–103.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

RAPP method: Failure analysis and risk determination in automobile fleets within the case study electric actuator

Stefan Bracke & Sebastian Sochacki
Chair of Safety Engineering and Risk Management, University of Wuppertal, Wuppertal, Germany

ABSTRACT: The increasing complexity of product functionality and manufacturing process parameters often leads to complex failure modes during the product life cycle. These field information are the basis for risk analysis and damage case prognosis with the goal of an early risk detection and leads to the possibility of nearby interactions, e.g. product and manufacturing optimisation or recall action. This paper outlines the essential procedure of the new developed method "Risk Analysis and Prognosis of complex Products (RAPP)". The main focus of the RAPP method is the detection, visualisation and prognosis of risks and damage cases depending on their life span variables regarding to a product fleet—based on a risky production batch—in field. The theory and application of the RAPP method is explained within an automotive case study electric actuator based on a synthetic data set, which includes real effects of typical field failure behaviour.

1 INTRODUCTION

The development and manufacturing of technically complex products as well as capital goods are confronted to central challenges: The increasing complexity of product functionality and manufacturing process parameters often leads to complex product damage symptoms and failure modes during the product life cycle. In case of this paper technically complex products are meant to be electronic goods, home appliances, consumer electronics or automobiles. These products are manufactured in series with an amount of middle up to a high production batches (statistical population), for example $N \geq 100$ products per day. After the sales of such production batches the products are passed into the use phase. The term product fleet denotes each production batch with the same construction stage (same grade of upgrade/innovation stage) of a component.

During the usage phase a huge amount of operational data (operating time, operating temperature, load characteristics etc.) regarding each product is generated. A special type of operational data collection can be found in case of failure occurrence during the usage phase of such components. For instance the time of damage appearance, the failure mode as well as the life span at the failure occurrence is recorded. These field informations are the basis for risk analysis and damage case prognosis with the goal of an early risk detection, visualisation and prognosis. Finally, it leads to the possibility of nearby interactions e.g. product and manufacturing optimisations or recall actions.

As part of the research work the RAPP approach (Risk Analysis and Prognosis of technical complex Products) has been already developed (Bracke 2013): In this paper, the RAPP method is now developed in a comprehensive extended procedure. The overarching goal of the RAPP method is the analysis of product fleet risks in the use phase depending on their life span variables regarding to certain failure modes.

2 GOALS OF THE RAPP APPROACH

The challenges and requirements of a risk analysis and risk prognosis based on the RAPP approach with regard to product fleets in the use phase are as follows:

a. Detection of specific risks regarding to a product fleet in field, which is based on a risky production batch.
b. Prognosis of the future amount of units at risk depending on their life span variables (e.g.: operating, switching cycles, operating time or operation parameters).
c. Visualisation of the determined risk as a basis for further decisions (e.g.: recall actions, garage actions).

This paper demonstrates on the one hand the developed theoretical background of the RAPP method and on the other hand an application of the shown RAPP steps due to the automotive engineering case study electric actuator. The case

study is based on a synthetic field data set. The creation of these data and information was based on characteristics with respect to real damage case data sets. The result of the RAPP method application is the estimation of the risk regarding the product fleet during the usage phase based on a detected failure mode. The data set includes e.g. field operating times, kilometrage and observation time based on the car-level.

3 RAPP APPROACH AND CASE STUDY: BASE OF OPERATIONS

The basis of every risk analysis constitutes two parts (Bracke & Haller 2011): On the one hand the knowledge of the damage case at a certain observation period and on the other hand the empirical product use phase behaviour. The observation of both data base is independent from each other.

The knowledge of the damage case includes data and information regarding the amount of damaged components as well as data of the life span variables regarding the point of observation, when the damage of each component appeared in the use phase (e.g.: operating hours, operation cycles, start and shut down activities). In addition, external conditions (e.g.: temperature, air humidity) have to be analysed and documented (Persin et al. 2013).

The knowledge of the empirical product usage phase behaviour includes data and information regarding the determination and mapping of the products' life span variables. This data is based on independent observations regarding the damage cases: The data base is collected from the whole—not damaged—product fleet in the field during the usage phase. This means that the data are not censored.

The precondition with regard to the RAPP approach is the correlation between the progression of the analysed failure mode variable and the chosen life span variable. This can be verified with the help of the Spearman's rank correlation coefficient (Sachs 2002).

An excerpt of the data and information of the case study electric actuator regarding the damage case and the empirical product use phase behaviour is shown in Table 1.

Table 1. Excerpt of data and information of the automotive case study electric actuator regarding damage cases and product fleet (synthetic field data set).

Nr.	Data array	Format/content
Information regarding the product fleet		
1.1	Production batch (automobile fleet)	$N_{PF} = 15.833$
1.2	Production period	03.2011–06.2011
1.3	Kilometrage profile of the product fleet regarding the life span of the product	Log-Normal distribution (parameters: μ; σ)
Field damage case information		
2.1	Observation time of concerned automobile fleet in field	12 months
2.2	Failed electric actuators up to observation time	$n = 211$

4 RAPP METHOD: OVERVIEW, PRINCIPALS AND STATISTICAL TOOLS

The essential procedure of the RAPP method (Risk Analysis and Prognosis of complex Products) includes five steps A–E, which are shown in Figure 1 (Bracke 2013). The single steps of the method and the used statistical tools are summarised in an overview in this chapter and explained in Table 2.

A detailed application of the RAPP method based on the theoretical steps is explained within the automotive case study electric actuator in chapter 5. The main goal of step A is the detection of the failure mode related to the product life span variables and the statistical mapping and prognosis of the Failure Mode (FM). Base of operations is data out of the technical analysis of damaged components and field data (e.g. guarantee/goodwill database).

The focus on step B is the empirical mapping of the product fleet (PF) behaviour based on the failure mode related life span variables (step A). The goal of step C is the estimation of the critical area regarding the failure mode related life span variables by definition of a range using the borderlines of important quantiles of the failure mode and the product fleet distribution models. The step D of the RAPP method focuses on the determination of the risk in product fleets in terms of a detected failure mode. Furthermore, step D considers the



Figure 1. Overview of the RAPP method (Bracke 2013).

Table 2. Essential procedure of the RAPP method.

	Step	Data Bases, statistical tools, procedure
Step A: Mapping and prognosis of the failure behavior		
No.	Action	Statistical tools and data bases
A1	Analysis of failure mode related life span variables	Technical analysis of damaged components
A2	Determination of life span variable's correlation	Spearmans ς; Kendalls τ
A3	Analysis of the behaviour development of the failure mode	Distribution models; e.g. Weibull distribution (two parameter model: b, T)
A4	Prognosis of the parameters of the statistical model of the Failure Mode (FM)	Regression analysis; coefficient of determination r^2
A5	Analysis and mapping of clearing effects: e.g. replacement part operations	Consideration of market charging via distribution models
Step B: Mapping field load profile		
No.	Action	Statistical tools
B1	Analysis of the life span variables of the Product Fleet (PF)	Correlation analysis between technical analysis and product fleet
B2	Empirical mapping of the life span variable development	Distribution models; e.g. log-normal (parameters μ, σ)
B3	Analysis and mapping of clearing effects: e.g. product fleet reduction	Consideration of market scrap influences via distribution models
Step C: Estimation of the critical area		
No.	Action	Statistical tools
C1	Determination of critical areas (quantiles)	E.g.: 50%, 95% 99%-quantile of FM and PF models
C2	Mapping of life span variable quantiles regarding failure mode and product fleet	E.g.: $l_{CLL\text{-}CUL} = \lvert Q_{PF\text{-}LL;0.05} - Q_{FM\text{-}UL;0.95} \rvert$
Step D: Risk analysis and risk prognosis		
No.	Action	Statistical tools
	Risk analysis	
D1	Risk probability in product fleets regarding actual point of time, based on critical areas	Overlap of FM and PF distribution models results in risk probability P_{FM}
D2	Determination of function "Damage Appearance (DA)"	Overlap of FM and PF distribution models results in density function f_{DA}
D3	Analysis of risk probability and damage appearance peaks development [retrospective]	Regression analysis at different points of time t_x leads to damage appearance function
D4	Analysis of significant changes: risk in-/decrease	Significance tests (e.g.: Mann-Whitney U-Test; Siegel-Tukey-Test, Fisher-Test) and confidence intervals
	Risk Prognosis	
D5	Risk probability regarding future points of time [future]	$P_{Prog\text{-}PF}$
D6	Prognosis of risk probability and Damage Appearance (DA) peaks development [future]	f_{DA}
D7	Determination of clearing effects: e.g. product fleet reduction/replacement part operations	Consideration of market charging distribution models
Step E: verification of risk analysis and—prognosis		
No.	Action	Statistical tools
E1	Field observation regarding to the risk point of time	Determination of failure rate λ and products at risk n
E2	Simulation of the failure and the product fleet behavior	Monte Carlo simulation

estimation of the retrospective and the expected risk development within the product fleet. The last step E of the RAPP method is the verification of the risk analysis and prognosis (step D) based on field observation and Monte Carlo simulation methods. The application of step E regarding the case study electric actuator is part of future research works.

5 RAPP RISK-ANALYSIS AND—PROGNOSIS WITHIN THE CASE STUDY

5.1 *Step A: mapping and prognosis of the failure mode*

Out of the field data base a density function is generated to represent the statistical area of the empirical Failure Mode (FM). A common

distribution model to approximate such failure modes is the three parameter Weibull distribution (density function (1)). An advantage to approximate such failure modes using a three parameter Weibull distribution is the interpretation of the utilised parameters (t_0 = failure-free time; T = characteristic lifetime; b = shape parameter; (Bertsche 2008)). The estimation of the parameters is done by state of the art methods such as Trust-Region method (Celis et al. 1985) or Maximum-Likelihood-Estimator (Meyna & Pauli 2010).

$$f(x)_{FM} = \frac{b}{T-t_0}\left(\frac{x-t_0}{T-t_0}\right)^{b-1} \cdot \exp\left(-\left(\frac{x-t_0}{T-t_0}\right)\right)^{b} \quad (1)$$

Regarding the case study, the point of time of field data analysis is early (12 Month in Service (MIS); Table 1), when the failure behaviour is not comprehensive known. Based on this special case, the use of an approach, which considers an additional prognosis of changing failure behaviour, is useful: The given damage cases within a limited observation period can be splitted into a certain number of classes (e.g. quarter division: 3, 6, 9, …, 24 months in service). With the use of each location parameter T, the mean value as well as the shape parameter b, the prospective parameters of the failure behaviour regarding the second year (24 month in service) can be calculated by using non-linear regression methods (Fig. 2).

A paradigmatic example is shown in Figure 2. The abscissa represents the Month in Service (MIS) regarding to different field observation times, whereas the ordinate reflects the estimated values of the parameters regarding the Weibull distribution models. If the gradient of the regression functions converges to zero, the parameters are not changing and therefore it is assumed, that the failure behaviour is constant. According to the risk prognosis point of time (MIS point, RAPP method step D), it is possible to choose the predicted parameters based on Figure 2.

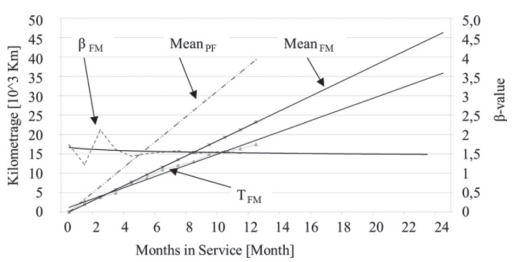


Figure 2. Estimation of Weibull parameters T, b, $t_0 = 0$ and arithmetic mean value x, using non-linear regression methods for prognosis of the comprehensive failure mode, product fleet field observation time 24 months in service; exemplified by the case study electric actuator.

5.2 *Step B: mapping field load profile*

A kilometrage profile can be generated (Table 1) out of the empirically known field data of the Product Fleet (*PF*). An important criterion is the timeframe between the product approval (e.g.: car registration) and the failure occurrence, the latter describes the risks observation point inside the RAPP method.

In many cases distribution functions for mapping a product fleet kilometrage profile can be described with the help of a log-normal distribution (2) (Sachs 2002), normal distribution as well as the Weibull distribution model (1).

$$f(x)_{PF} = \frac{1}{x \cdot \sigma \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{(\lg(x)-\mu)^2}{2\sigma^2}\right) \quad (2)$$

5.3 *Step C: estimation of the critical area*

The estimation of the critical area has to be evaluated by limiting the two density functions within the given one-sided quantile (Q) of each function. A typical one-sided quantile in case of the automotive industry (Lower Limit LL = 0.05/Upper Limit UL = 0.95) is used in the constituted case study. Therefore, the left-sided failure mode distribution was limited by using a 0.05 quantile (Q_{LL}) and the kilometrage distribution by applying a right-sided 0.95 quantile (Q_{UL}). In case of a right-sided failure mode, the quantile borders have to be switched. The schematic visualisation of the critical area within the case study electric actuator is shown in Figure 3, (Bracke 2013).

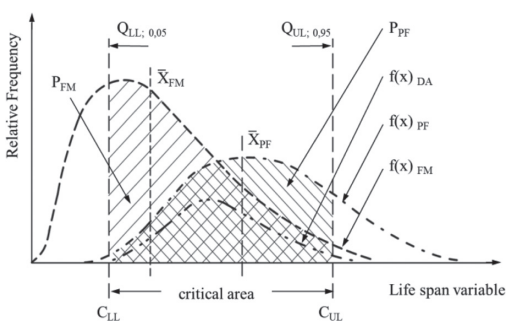


Figure 3. Visualisation to determine the critical area [$c_{LL} = Q_{LL;0.05}$; $c_{UL} = Q_{UL;0.95}$] as well as the overlapping of $f(x)_{PF}$ and $f(x)_{FM}$ to determine the risk parameters P_{RPF} and $f(x)_{DA}$ (Bracke 2013).

5.4 *Step D: risk analysis and risk prognosis*

The RAPP approach provides the calculation of three characteristics:

- P_{RPF}: Risk probability regarding the product fleet (Index: *RPF*),
- $f(x)_{DA}$: Probability function of damage appearance (Index: *DA*) and
- $P_{RPF\text{-}Prog}$: Prognosis of the future risk probability (Index: *RPF-Prog*).

Besides the kilometrage function $f(x)_{PF}$ and the failure mode function $f(x)_{FM}$, the introduced characteristics are visualised in Figure 3.

The calculation of the RAPP characteristics is as follows: The risk probability of the critical product fleet P_{PF} can be estimated using the failure occurrence probability P_{FM} (Integral of $f(x)_{FM}$ (1) regarding to the critical area, step C) and the product fleet kilometrage probability P_{PF} (Integral of $f(x)_{PF}$ (2) regarding to the critical area, step C).

$$P_{RPF} = \mathrm{P_{FM}} \cdot \mathrm{P_{PF}} = \int_{C_{LL}}^{C_{UL}} \frac{b}{T-t_0}\left(\frac{x-t_0}{T-t_0}\right)^{b-1} \cdot \exp\left[-\left(\frac{x-t_0}{T-t_0}\right)^{b}\right] \cdot \int_{C_{LL}}^{C_{UL}} \frac{1}{x \cdot \sigma \cdot \sqrt{2\cdot\pi}} \cdot \exp\left(\frac{(\lg(x)-\mu)^2}{2\sigma^2}\right) \tag{3}$$

The function $f(x)_{DA}$ describes the failure occurrence probability of the product fleet in dependence on a life span variable (e.g.: kilometrage). With this specific characteristic the failure occurrence probability can be determined (4) at any point of observation time with respect to an appropriate life span variable. Furthermore, the probability to find one unit at the point of observation can be easily calculated by finding the maximum of the failure occurrence function (5).

$$f(x)_{DA} = \frac{\mathrm{b}}{\mathrm{T}-\mathrm{t_0}}\left(\frac{x-t_0}{T-t_0}\right)^{b-1} \cdot \exp\left[-\left(\frac{x-t_0}{T-t_0}\right)^{b}\right] \cdot \int_{C_{LL}}^{C_{UL}} \frac{1}{x \cdot \sigma \cdot \sqrt{2\cdot\pi}} \cdot \exp\left(\frac{(\lg(x)-\mu)^2}{2\sigma^2}\right) \tag{4}$$

$$f'(x)_{DA} = 0 \tag{5}$$

The probability $P_{RPF\text{-}Prog}$ maps the prognosis in the field of expected damage cases in the future at a specific point of observation time t_{RP}. The general procedure is identical to the determination of the first risk characteristic P_{RPF}. The difference is the adjustment of the product fleet's kilometrage function $f(x)_{PF}$ in relation to the prognosis point of time and thus the renewed determination of the left-sided lower quantile $Q_{LL(Prog);0.01}$. In case of additional changing failure behaviour, the adjusted failure mode function and its appropriate quantile have to be considered.

Referring to equation (3) the probability $P_{RPF\text{-}Prog}$ can be calculated as follows:

$$P_{RPF\text{-}Prog} = P_{FM\text{-}Prog} \cdot P_{PF\text{-}Prog} \tag{6}$$

In the presented electric actuator case study the risk analysis and prognosis based on the RAPP method is using the field data set regarding the first twelve MIS. Afterwards, the results of the risk prognosis are compared to the real failure behavior at the point of time 21 MIS. The results of the RAPP risk analysis and the respective risk prognosis (step D; Fig. 6) are shown in Table 4.

Regarding to Figure 3 the following Figure 4 and Figure 5 shows the overlapping of the den-

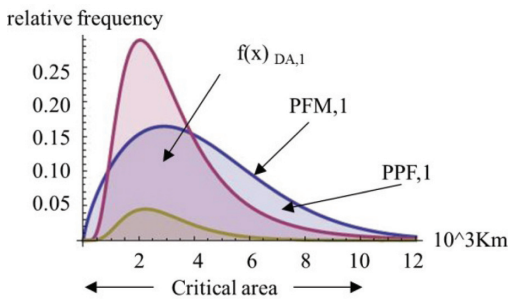


Figure 4. Visualisation of the overlapping $f(x)_{PF}$ and, $f(x)_{FM}$ and the product of both to determine the risk parameters $f(x)_{DA}$ after one MIS.

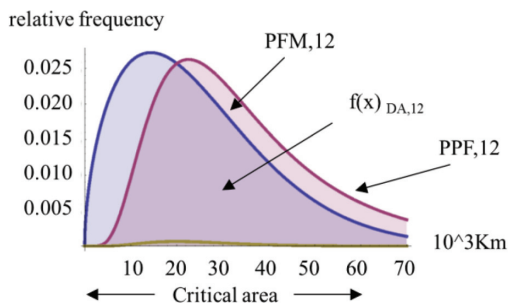


Figure 5. Visualisation of the overlapping $f(x)_{PF}$ and, $f(x)_{FM}$ and the product of both to determine the risk parameters $f(x)_{DA}$ after twelve MIS.

sity functions of cars based on the electric actuator failure mode (Weibull distributed, (1)) and the associated product fleet (Lognormal distributed, (2)) after one and twelve MIS.

After the first MIS the major section of the product fleet is moved in the range of cars with electric actuator failure mode (82.03%). The peak $f'(x)_{DA,1}$ is at 2,239 kilometres. At the beginning of 12 MIS regarding the product batch the fleet moved to a mean kilometrage of 23,179 kilometers. The risk analysis in product fleet (P_{RPF}) dropped from 82.03% to 31.58% by simultaneous increasing the range of the critical area (4,780 to 83,880 kilometres). Comparison of $f'(x)_{DA,1}$, $f(x)_{PF,1}$ and $f(x)_{FM,1}$ with $f'(x)_{DA,12}$, $f(x)_{PF,12}$ and $f(x)_{FM,12}$ shows a proportional process, therefore it can be assumed, that the failure behaviour is not completely developed. Additionaly the dispersion of $f(x)_{FM,i}$ and $f(x)_{PF,i}$ have a similar development which is an indicator (in conjunction with a linear arithmetic mean development) for a random failure behaviour. But it can be received that a short quantity of cars is in the critical area (max 71.04%) of the electric actuator and could breakdown in higher kilometrage. The following Table 3 summerises the results regarding the risk analysis at 1 MIS and 12 MIS.

The extrapolation of the Weibull distribution parameters of $f(x)_{FM,1\text{-}12}$ show a prognosis of the electric actuator failure behaviour after 21 MIS based on the prognosis of the shape and location parameters (Fig. 1).

Table 3. Results of the RAPP risk analysis after one and twelve MIS; case study electric actuator.

Risk characteristics	Result
Results after one month in service	
$P_{PF,1}$	82.03%
Note: Risk analysis in product fleet; observation point of time: 1 MIS	
$P_{PF,1}$: c_{LL}/c_{UL}	0.00/12.26 [10^3 km]
Note: Critical area regarding to the life span variable within 1 MIS observation time	
$f'(x)_{DA,1}=0$	2.239 10^3 km
Note: Damage appearance, 1 MIS	
Results after twelve months in service	
$P_{PF,12}$	71.04%
Note: Risk analysis in product fleet; observation point of time: 12 MIS	
$P_{PF,11}$: c_{LL}/c_{UL}	4.78/83.88 [10^3 km]
Note: Critical area regarding to the life span variable within 12 MIS observation time	
$f'(x)_{DA,12}=0$	23.179 10^3 km
Note: Damage appearance, 12 MIS	

Table 4. Results of prognosis from focus of failure mode and proportion of cars at risk compared with the fair values after 21 MIS.

Risk characteristics	Result
Prognosis of the damage appearance	
$f'(x)_{DA,Prog,21}$	32,338 km
Note: Damage appearance prognosis: 21 MIS	
Real values of Damage appearance	
$f'(x)_{DA\,21}$	24,765 km
Note: Damage appearance 21 MIS	
Risk probability prognosis	
$P_{RPF,\,Prog,21}$	17.81%
Note: Risk probability prognosis: 21 MIS	
Real values proportion of the risk probability	
$P_{RPF,21}$	12,57%
Note: Risk probability 21 MIS	

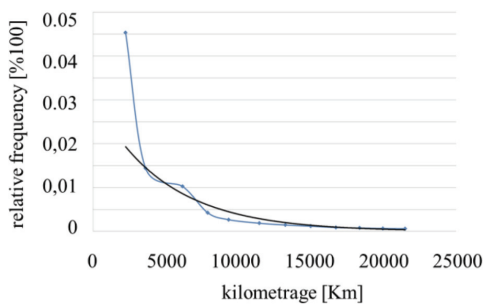


Figure 6. Visualisation of the maxima of damage appearance density function $f'(x)_{DA,1\text{-}12}$.

The determination of the function "damage appearance" (4) for each month in service $f(x)_{DA,1\text{-}12}$ shows the centered area of the $P_{RPF,1-12.}$ After finding the maximum with (5) the x-value of $f'(x)_{DA,1\text{-}12}=0$ expose the focus of kilometrage from the electric actuator for each month. Figure 6 presents $f(x)_{DA,1}$ till $f(x)_{DA,12}$.

Primarily, it can be observed that the y-value of the $f'(x)_{DA,1\text{-}12}$ are very small, therefore it is difficult to show $f(x)_{FM,1\text{-}12.}$ $f(x)_{PF,1\text{-}12}$ and $f(x)_{DA,1\text{-}12.}$ in one plot. In the first month the focus of the failure mode ($f'(x)_{DA,1}=0$) can be located at 2,239 kilometres. In the following months the focus increases proportionately while the dispersion of $f(x)_{DA,2\text{-}12}$ gets disproportionately higher. With the increase of the range of $f'(x)_{DA,1\text{-}12}$ the validity of focus of the failure mode gets lower. The black line describes a possible model fit by using an exponential function. The following Figure 7 compares the failure mode focus (damage appearance, (5)) with the proportion of cars from P_{PF} in the critical area of P_{FM} ((6)) for each month.

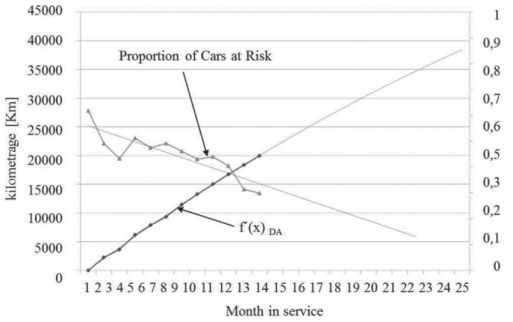


Figure 7. Prognosis of the damage appearance focus ($f''(x)_{DA} = 0$) and the proportion of cars from P_{PF} in the critical area P_{FM} based on 12 MIS.

According to Figure 7 it can be observed, that the damage appearance is changing to linearly a higher kilometrage. The prognosis shows the increase trend of failure mode focus regarding the kilometrage for the next 13 MIS (Total: 25 MIS). Comparison of the prognosis with the real values of 21st MIS based on field data shows a related behaviour, but overrates the real occurrence. The reason is the increase of the dispersion after twelve months in service and the following MIS.

The critical area of the risk probability regarding the product fleet has a linear course. Comparing the prognosis with real values 21 months in service the risk probability will be overrated after the period of observation. While the damage appearance gets higher simultaneously the proportion of cars at risk gets lower which is an indicator that the overlapping of P_{FM} and P_{PF} gets smaller. The following table summarises the important results and values of the Figure 7.

The results of the 21 MIS prognosis regarding to the real behaviour of the failure mode after 21 MIS leads to significant deviations. In this case the damage appearance prognosis as well as the risk probability prognosis overrates the failure behavior. Taking into account of the difficultness of random failure behavior the RAPP method gives well oriented results to forecast of the failure behaviour.

6 CONCLUSION

This paper outlines the RAPP method and its application within the electric actuator case study for determination of risks in product fleets within the usage phase. The focus is the analysis and prognosis of the field failure behaviour of a defect electric actuator unit based on product field data. The results lead to a visualised risk analysis and prognosis on the basis of the existing failure mode and the product fleets life span variables at a certain point of observation. Furthermore, the estimation of the risk prognosis with respect to the expected damage cases within the product fleet is feasible. The comparison of the RAPP method versus industrial state-of-the-art methods (Eckel 1977) has not been verified yet and is an inherent part of future research work.

The advantages of the present procedure are: The RAPP method, in comparison to the industrial standards of risk prognosis methods, considers a direct link of different dimensions (e.g. operating time, switching cycles) causing a specific damage case and the product's life span variables without a mathematical conversion. Thus, the method generates the possibility of direct visualisation of damage cases (failure behaviour) and life span areas at a specific point of observation time to estimate the existing risk potential. The visualisation includes the critical area between a product's life span variable and a present failure mode, which can be calculated by using p-quantiles of the failure behaviour probability function and the empirical life span variables. Furthermore, the adjusting empirical life span variable as related to the failure behaviour can be visualised properly and analysed subsequently. Finally the developing of the damage appearance regarding the predicted behaviour of the failure mode and the product fleet is calculable.

The disadvantages of the shown procedure are: The fitted density functions of the empirical failure modes and the product fleet's life span variables are fundamental for the presented method. Thus the deviation due to different probability functions and the fitted model itself can lead to different results of the risk analysis. The current research results due to different probability functions show a marginal influence in the result. However, some case studies led to adverse risk prognosis based on small critical areas, which is also a part of the future research work.

REFERENCES

Bracke S. 2013. RAPP. A new approach for risk prognosis on technical complex products in automotive engineering. In: R.D.J.M. Steenbergen et al.: *Safety, Reliability and Risk Analysis: Beyond the Horizon. Proceedings: ESREL, 2013*.

Bertsche, B. 2008. Reliability in Automotive and Mechanical Engineering. Determination of Component and System Reliability. Berlin: Springer.

Bracke, S. & Haller, S. 2011a: Field damage analysis (FDA) concept: Contribution to the comprehensive reliability analysis of complex field damage causes. *Proceedings: RAMS 2011, Annual Reliability and Maintainability Symposium*, Florida, USA.

Bracke, S. & Haller, S. 2011b. The RAW concept: Early identification and analysis of product failure behaviour in the use phase. *Proceedings: ESREL 2011, European Safety and Reliability Conference*, Troyes, France.

Celis, M., Dennis, J.E. & Tapia, R.A. 1985. A trust region strategy for nonlinear equality constrained optimization. *Numerical Optimization* (Boggs, P., Byrd, R., Schnabel, R. eds), Philadelphia: SIAM.

Eckel, G. 1977. Determination of the initial course of the reliability function of automotive components. *In Qualität und Zuverlässigkeit 22* (9): 206–208.

Meyna A. & Pauli B. 2010. *Zuverlässigkeitstechnik—Quantitative Bewertungsverfahren.* Hanser, München, 2010.

Persin, S., Haller, S. & Bracke, S. 2013. IDREMA-Process: Identification of Reference Market for Defect Parts Routing. *Proceedings: RAMS (2013)—Annual Reliability and Maintainability Symposium*, *Orlando, Florida, USA IEEE Reliability Society*; ISSN 014a-144X.

Sachs, L. 2002. Applied Statistics. Berlin: Springer Verlag.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Composite methodology for tsunami vulnerability assessment based on the numerical simulation of 1755 Lisbon tsunami—application on two Portuguese coastal areas

J.L. Barros
Centre for Social Studies, University of Coimbra, Portugal

A. Emídio & A. Santos
Centre for Geographical Studies, Institute of Geography and Spatial Planning, University of Lisbon, Portugal

A.O. Tavares
Centre for Social Studies and Department of Earth Sciences, University of Coimbra, Portugal

ABSTRACT: Different methodologies for tsunami risk assessment have been developed, namely for reconstitution of previous hazardous events and for planning awareness and alert systems and civil protection resources. The vulnerability analysis is frequently based on simulations using precursor impact damages and on modeling hydrodynamic floods. Our innovative approach is applied on two distinctive coastal Atlantic areas, with urban and rural/natural context from Setúbal and Figueira da Foz counties. We presented a deepened methodology for assessing vulnerability to tsunamis in its social, structural and morphological component that results of new inputs that distinguish this from previous studies. The tsunami inundated areas were obtained from tsunami numerical modeling. The morphological and structural analysis is based on field work element collection using a matrix with 18 parameters. For the social impacts evaluation, a multi-components analysis is performed, using 47 socio-economics variables, expressing the expected impacts. A composite territorial index of vulnerability is presented and mapped.

1 INTRODUCTION

The evaluation of the degree of exposure and vulnerability to natural disasters in the last decade has seen a notable increase (Wisner et al., 2004; Douglas, 2007). Even after the 2004 India Ocean Tsunami, and more recently the 2011 Japan Tsunami there has been a focus on the hazard process assessment and mapping through physical models (Liu et al., 2007; Santos et al., 2007; Santos, 2011; Satake et al., 2011; Singh et al., 2012). Other approaches have been focusing on the analysis of territorial vulnerability resulting from past impact in predicting future events (Dominey-Howes and Papathoma, 2007; Dall'Osso et al., 2009; Dominey-Howes et al., 2009; Hart and Knight, 2009; Dominey-Howes et al., 2010). On the other hand, several studies have been pointing the importance of conceptual requirements and technical problems for territorial vulnerability assessment, like the scale analysis (Fekete et al., 2010; Kienberger et al., 2013), the perception of natural and technological risks (Tavares et al., 2011), the supporting data (Papathoma et al., 2003; Silva and Pereira, 2014) and the comparativeness of models (Smit and Wandel, 2006), to develop detailed territorial approach and strong risk analysis. Furtermore, different authors underlined the vulnerability assessment and territorial coping capacity on tsunami affected areas based on natural scope (Taubenböck et al., 2008; Kaplan et al., 2009; Hart and Knight, 2009), according the building fragilities (Papathoma and Dominey-Howes, 2003; Ghobarah et al., 2006; Dominey-Howes et al., 2010; Omira et al., 2010; Leone et al., 2011; Reese et al., 2011) or empathizing the support capability (Post et al., 2009; Freire et al., 2013). In addition, an enlarged understanding of vulnerability related with natural hazards has been enhanced (Turner et al., 2003; Cutter et al., 2003; Cardona, 2004; Adger, 2006; Douglas, 2007; Mendes, 2009) emphasize not only in the impacts and coping post events, but also the long term recovery capacity and the adaptation to the reframed conditions.

In this study two coastal areas of Portugal were selected (Fig. 1): Figueira da Foz, located in the central region of Portugal and Setubal located nearby Lisbon. Therefore, the objective of this study is to propose a multidimensional vulnerability analysis for coastal areas with a potential

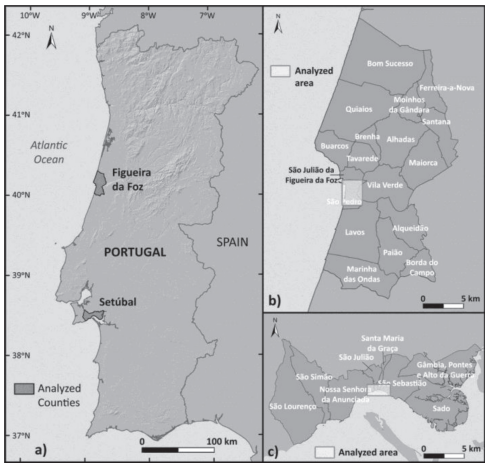


Figure 1. Location of the two studied areas: a) Portugal framework; b) Figueira da Foz; c) Setubal.

tsunami hazardous impact. First is calculated the morphological index of vulnerability (Mv) that combines the different physical and occupation characteristics of the analyzed area. Secondly, is calculated the structural vulnerability index (Bv) that estimates the vulnerability of the different potentially affected buildings. Thirdly, the social vulnerability (Sv) that analyzes the socioeconomic characteristic of the study area is calculated.

Finally, is calculated the Composite Index of Vulnerability (CVI) that aggregates the three indices previously calculated.

The main goal is to assess a potential tsunami impact by considering the coastal natural scope, the existing building characteristics and the societal capability, in the sense of (Deneulin and McGregor, 2010).

2 METHODOLOGY

The tsunami inundated areas used in this study are based on the worst case scenario which is the 1755 Lisbon Tsunami. This is an innovative approach because these results were obtained from the tsunami numerical modeling carried out by Santos et al. (2012) and Santos & Koshimura (2013).

Then, a multidimensional vulnerability analysis for the two coastal areas is proposed. Furthermore, this study presents a new methodological approach to evaluating the structural, morphological and social vulnerability to tsunamis. This methodology was supported on the collection and assessment of large data from fieldwork and databases. The data processing and analysis were supported by statistical tools for a composite vulnerability index characterizing the potential inundated areas. For the process associated with the morphological component analysis a total of 5 parameters (Table 1) were taken into consideration, in particular by adapting the coastal vulnerability index (Pendleton et al., 2010) and the physical vulnerability index presented in Ismail et al. (2012).

A matrix was built for the data acquisition and evaluation of the parameters. In this matrix, to each parameter was assigned a value ranging from −1 to +1, with positive values representing an increase in vulnerability, and negative values a decrease in vulnerability.

After assigning values to each of the different parameters, the morphological vulnerability index was calculated, ranging from "very low" to "very high". Regarding the structural component, the potential affected buildings by the tsunami inundation were analyzed. A total of 13 parameters were included in the matrix, which characterize the buildings in its structural, architectural and occupational tools (Table 2). On the other hand, the data acquisition was based on fieldwork in order to collect several intrinsic characteristics of the building and the surrounding areas.

Furthermore, in the structural component new parameters were introduced related to the

Table 1. Morphological assessment parameters (Mv).

Morphological assessment parameters
Morphology of the flooded area
Consolidation of geologic materials
Average slope (°)
Distance to coastline
Use and land cover

Table 2. Structural assessment parameters (Bv).

Structural assessment parameters
Number of floors
Construction material
Date of built
Preservations conditions
Hydrodynamics of r/c
Existence of underground floors
Foundations type
Occupation form
Number of utilization units
Average number of daily visitors or residents per unit of use
Occupation floating
Built form plan
Emerged building height in relation to the wave

occupation of the buildings that are not included in the previous methodologies presented by Dall'Osso et al. (2009) and Ismail et al. (2012). The introduction of parameters "form of occupation", "number of units for use"; "average daily number of persons present or visitors per unit of use" and "floating occupation" allow complementary analysis of buildings including through its functional distinction seasonal and occupational, thereby enhancing the analysis. For each attribute is assigned a value that vary from –1 to +1, whereas positive values represent an increase of vulnerability and negative values a decrease of vulnerability. The parameters included in the structural component do not influence the building's vulnerability in the same way. For this reason it was necessary to assign weight for the different parameters. Weights have been calculated via pair-wise matches between each of the factors, using M-Macbeth3 software, that is a platform for multi criteria analysis and decision making processes (Bana e Costa et al., 2004; Bana e Costa & Chagas, 2004). After assigning values to each of the different parameters, the index of structural vulnerability was calculated, ranging from "very low" to "very high". The methodology for assessing social vulnerability was based on the methodology performed by Cutter et al. (2003), Mendes (2009), atribuir Schmidtlein et al. (2008) and Chen et al. (2013) using factor analysis performed in SPSS. Initially were collected a total of 172 variables of social, economic, demographic and the ones related with buildings in the studied areas. Social vulnerability was analyzed by using factor analysis, which allows the elimination of redundant data, their standardization and their grouping factors. The analysis was performed for a total of 15 municipalities and 88 parishes. As a result, the correlation matrix of data was evaluated, where all the data with a correlation higher than 0.7 were removed. A factor analysis was performed until a set of parameters was obtained to validate the sample. These parameters are: KMO of 0.717, more than 0.6 communalities and a variance rate of 78% (Comrey & Lee, 2009).

From this analysis, the initial 172 variables were reduced to 47, which are grouped in Table 3.

Table 3. Social vulnerability variables (Sv).

Group of variables	Number of variables
Agriculture	3
Buildings/sccommodation	19
Economy	6
Population	13
Services	3
Social support	3

After the factor analysis was calculated the social vulnerability for each parish based on SoVI® classification of Cutter et. al. (2003), ranging the vulnerability from "very low" to "very high". After calculating the morphological, structural and social vulnerability a Composite Vulnerability Index (CVI) was calculated, which integrates the three components with the following formula:

$$\mathrm{CVI} = Mv + Bv + Sv \quad (1)$$

where Mv = weighted sum of the morphological parameters; Bv = weighted sum of the structural parameters; and Sv = factorial analysis scores of the social vulnerability.

The final composite vulnerability index, was obtained by the simple mean of three parameters. The index ranging from "very low" to "very high", based on standard deviation, according to the categories: "very low": <–1 SD; "low": [–1, –0.5 [SD; "moderate": [–0.5, +0.5 [SD; "high": [0.5, 1 [SD; "very high": ≥1 SD.

3 STUDY AREAS' CHARACTERIZATION

The municipality of Figueira da Foz is located in the central coastal area of Continental Portugal and has an area of 379 km^2 (Fig. 1a). According to the 2011 Census (INE, 2011) the county records a population of 62,125 inhabitants, divided unequally by 18 parishes with a population density of 163.3 (hab/km^2). In this study the area of Cabedelo, the industrial zone of the port of Figueira and Cova-Gala were analyzed (Fig. 1b). These areas are located on the left bank of the Mondego river, belonging to the parish of S. Pedro. The choice of Figueira da Foz was justified by the fact that of the existence of historical accounts related to the 1755 Lisbon Tsunami (Santos et al., 2009; Santos et al., 2012), the high seasonal population dynamics and the existence of a major harbor and industrial zone along the coast. The analyzed area in Figueira da Foz is characterized by low altitudes between 0 and 8 m with gentle slopes and the existence of dunes. In terms of the sediment consolidation, the area is characterized by the existence of unconsolidated sediments, beaches and mudslides. With regard to land use and occupation the area presents natural/agricultural areas and salines, and an industrial area that includes Cabedelo, industrial harbor. This study area also included artificialized spaces with residential urban fabric, health and social equipments in Cova Gala, on the left bank of the river Mondego.

The second study area has an urban occupation that belongs to the Setúbal city, which is located in the Sado estuarine region (Fig. 1c). According to

the 2011 Census (INE, 2011) the municipality of Setúbal has a population of 121 185 inhabitants distributed by 8 parishes with a population density of 520.1 (hab/km^2) and has an area of 172 km^2. The choice of Setúbal is justified by the fact of the existence of historical accounts related to the 1755 Lisbon Tsunami (Santos & Koshimura, 2013), reporting the existence of many fatalities and severe damage, the urban area is located on low altitudes of about 4 m, and the existence of marinas and an important harbor. The area is mostly represented by alluvial deposits and landfills, observing generally low altitudes (between 3 to 4 m) and very low slopes. The land use and occupation area is characterized by urban fabric and close to the shoreline by harbor and leisure facilities

4 RESULTS AND DISCUSSION

4.1 *Morphological vulnerability*

The morphological differentiation of vulnerability's mainly result in the distance to the coast, verifying in general, a decrease of vulnerability with increasing their distance (Fig. 2). The Figueira da Foz area also presents "moderate" to "high" levels of vulnerability in the estuarine area related with flat zones and narrow channels (Fig. 2a). For the Setúbal area, namely artificialized, the differentiation of morphological vulnerability results from the distance to the shoreline and the low slope, showing a general decrease of vulnerability with increasing their distance (Fig. 2b).

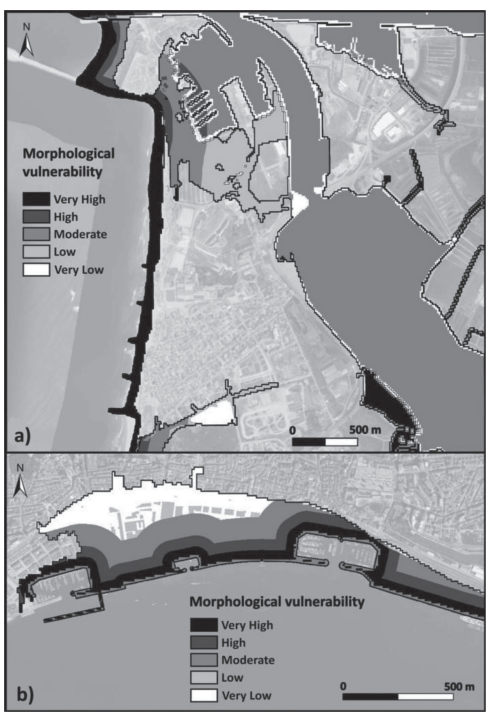


Figure 2. Morphological vulnerability: a) Figueira da Foz; b) Setúbal.

4.2 *Structural vulnerability*

In the analyzed area in the municipality of Figueira da Foz there were identified a total of 47 buildings potentially affected by the occurrence of a tsunami similar to the 1755. Making an analysis of all the buildings evaluated is concluded that 42% present the following categories: warehouses, shipyards, workshops and outhouses, 30% have take an exclusively residential typology, 13% are industrial buildings, 11% are commercial buildings and 4% represent fabric allocated to services. However, it could be identified two distinct zones within the study area: the Cabedelo zone and the industrial harbor are clearly dominated by industrial buildings, warehouses and buildings belonging to shipyards. Further southern in the Cova-Gala the residential buildings dominate. The different land occupation shows two zones for the structural vulnerability. Also noted was the camping, that was not affected by the tsunami inundation. However, it could be isolated because the only access to it could be completely inundated. The structural vulnerability varies from "high" vulnerability to "low" vulnerability, but where most of buildings (85%) are classified with "moderate" vulnerability. (Fig. 3a).

The analyzed area in the municipality of Setúbal presents an urban riverfront downtown, where are located the recreational and fishermen docks, and also the equipments of Setúbal harbor. The area is bounded on the north by the historic city center and to the south by the Sado estuary. A total of 468 potentially affected buildings were identified, mostly with commercial use or assigned to administrative services (60%). A number of 135 buildings (29%) has mixed function, (ie, residential and commercial use), and only 54 (11%) have an exclusively residential typology. This area also presents two distinctive structural vulnerabilities based on the buildings characteristics, separated by the main city Avenue. One to the north, where the buildings has residential function, among which are some properties degraded in narrow streets located in the historic city center; and another area to the south, where stands out the buildings connected to the two main economic activities characteristic of this riverside area—the shops and restaurants connected to the fishing industry, and the port of Setúbal. As presented on

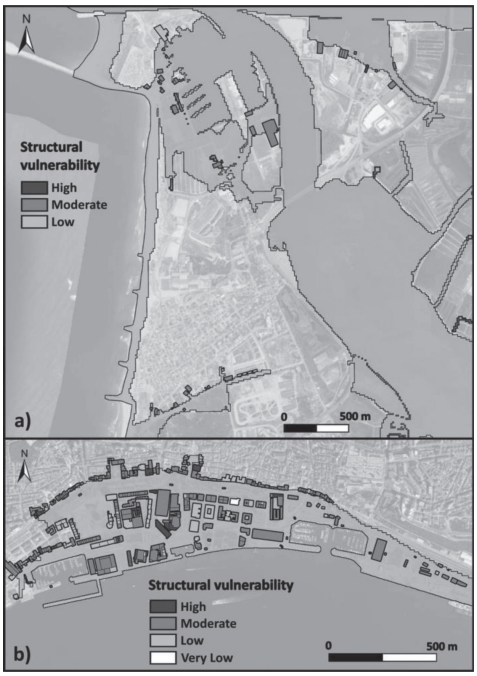


Figure 3. Structural vulnerability: a) Figueira da Foz; b) Setúbal.

the Figure 3b the structural vulnerability of the buildings range from the "very low" vulnerability to the "high" structural vulnerability.

4.3 *Social vulnerability*

For the social vulnerability analysis it was considered the entire county areas (Figueira da Foz and Setubal). Then, the obtained results were projected for the two studied areas. In the Figueira da Foz the social vulnerability for each parishes varies between "low" vulnerability and "very high" vulnerability (Fig. 4a). In the municipality of Setúbal the social vulnerability varies between "very low" and "high" vulnerability (Fig. 4b). In general, the municipality of Figueira da Foz has a social vulnerability higher than the municipality of Setúbal. Regarding to the specific analyzed area part of the municipality of Figueira da Foz, the Cabedelo zone and Cova Gala (located in the parish of S. Pedro) present a "very high" social vulnerability. In the municipality of Setúbal the analyzed area is divided in 4 parishes, which present different social vulnerability rates. The parishes of Nossa Senhora da Anunciada and São Sebastião have a "high" social vulnerability, the São Julião parish presents a "low" vulnerability and the Santa Maria da Graça parish presents a "very low" social vulnerability rate. The studies

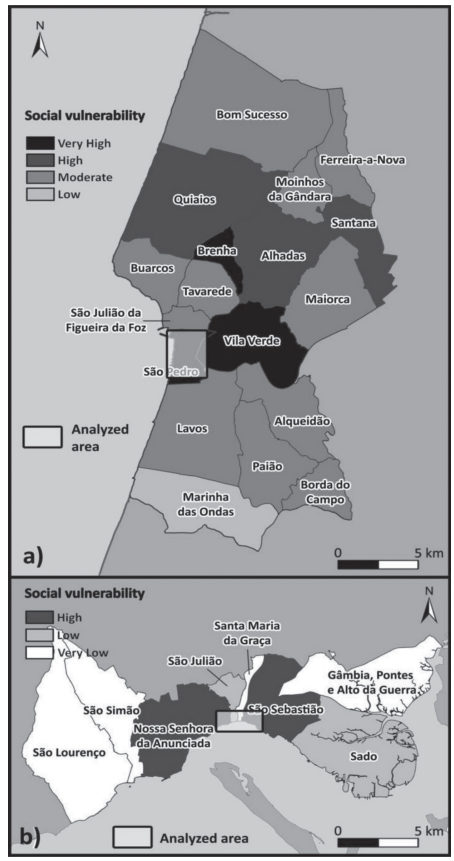


Figure 4. Social vulnerability: a) Figueira da Foz; b) Setúbal.

areas show that social vulnerability rates are very marked by administrative boundaries, as a result of demographic, social and economic variables.

4.4 *Composite vulnerability index*

After calculating the morphological, structural and social vulnerabilities, the Composite Vulnerability Index (CVI) was calculated. This new index combines all the previously calculated indexes. The results in Figueira da Foz study area are: mean = 0.465, and the standard deviation is 0.026. The results also show that the CVI present the highest values in front impact zone (Fig. 5a), with a decrease in vulnerability, with rare exceptions, to the inland of the study area, attending to an indirect relationship between vulnerability and distance to the shoreline. In the analyzed area the CVI varies from "very low" to "very high" (Table 4). 8% of the area is classified as "very high" vulnerability, corresponding almost exclusively to the coastal

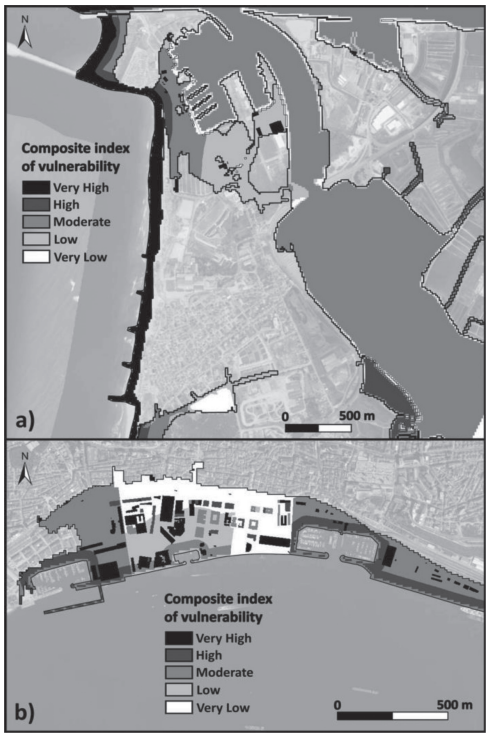


Figure 5. Composite Vulnerability Index (CVI): a) Figueira da Foz; b) Setúbal.

Table 4. Classification of Composite Vulnerability Index (CVI) to Figueira da Foz.

Standard deviation classes	Classification interval	Nominal classification
<–1 SD	0.394–0.439	Very low
[–1, –0.5 [SD	0.439–0.452	Low
[–0.5, +0.5 [SD	0.452–0.478	Moderate
[+0.5, +1 [SD	0.478–0.491	High
≥+1 SD	0.491–0.696	Very high

area and some buildings. With "high" vulnerability rate is classified 4% of the area, which corresponds to the stretch near the coastline and saline areas. 73% of the area presents "moderate" vulnerability that corresponds to the zones near de Mondego river and the harbor zone. With "low" vulnerability (10%) and "very low" vulnerability (5%) are identified the inland areas mostly in the south of Cova Gala and in the fishery and industrial zones.

The results in Setubal study area are: mean is 0.439, and the standard deviation is 0.084.The results of the CVI in Setúbal study area (Fig. 5b)

Table 5. Classification of Composite Vulnerability Index (CVI) to Setubal.

Standard deviation classes	Classification interval	Nominal classification
<–1 SD	0.287–0.356	Very low
[–1, –0.5 [SD	0.356–0.398	Low
[–0.5, +0.5 [SD	0.398–0.481	Moderate
[+0.5, +1 [SD	0.481–0.523	High
<+1 SD	0.5228–0.7028	Very high

show an increase of the vulnerability of the buildings, mainly in western and eastern zones, where the majority of buildings present a rating of "very high" vulnerability. Also noted is a large area in the central zone classified as "low" and "very low" CVI, which is a result of the positive social and economic characteristics of the population, expressed by the social vulnerability index. In this area de importance of the morphological component is still present, namely by the parameter that refers to the distance to the shoreline parameter, standing out essentially on the western and eastern zones with a stretch of high vulnerability around the shoreline.

Analyzing the cartographic output (Table 5), 13% is classified as "very high" composite vulnerability index, corresponding exclusively to buildings. With "high" CVI is classified 15% of the area, which corresponds to the band around the coastline, as well as some buildings. Most of the area (37%) has "moderate" composite index. The "low" (11%) and "very low" vulnerability (24%) CVI rates are presented on the central zone, but representing very few buildings.

5 CONCLUSIONS

The multidimensional approach presented in this article allowed the introduction of new parameters that differentiate it from previous methodologies. The analysis and evaluation of morphological, structural and social vulnerability components allows a comprehensive assessment of the studied areas, which is complemented by calculating the CVI that aggregates all the three vulnerability components. The CVI expresses differences between the two studied areas. In both areas the vulnerability varies from "very low" to "very high". However, there are differences between both. In the Figueira da Foz studied area the CVI is fundamentally influenced by the physical characteristics, namely the distance to the shoreline and the slope. Other parameter that emerge on the vulnerability analysis are the land use occupation characteristics, namely associated with

industrial and harbor activities. In Setúbal the CVI is influenced mainly by the socioeconomic characteristics and the urban fabric, namely by the existence of different types of buildings.

The deepen methodology used for vulnerability analysis made possible a better understanding of local characteristics, highlighting specific parameters or the combination of parameters. The Composite Vulnerability Index (CVI), resulting from structural, morphological and social variables allows to the decision makers a more adequate response. Some specific preparation, reduction and mitigation action or measures related with tsunami impact can be supported by this vulnerability composite analysis.

ACKNOWLEDGEMENT

This research was supported by the TsuRiMa Project—TSUnami RIsk MAnagement for spatial planning and civil protection (PTDC/CSGEO/118992/2010), funded by the Foundation of Science and Technology (FCT), Portugal.

REFERENCES

Adger, W.N. 2006. Vulnerability. Global Environmental Change 16, 268–281.

Bana e Costa, C.A. 2004. Multicriteria Evaluation of Flood Control Measures: The case of Ribeira do Livramento. Water Resour. Manag., 18, 263–283.

Cardona O.D. 2004. The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. In: Frerks, G. and Hilhorst, D. (eds) Mapping Vulnerability: Disasters, Development and People. London: Earthscan Publishers.

Chen, W., Susan, S.L., Emrich, C.T., Shi, P. 2013. Measuring social vulnerability to natural hazards in the Yangtze river delta region, China. Int. J. Disaster Risk Sci. 4 (4): 169–181.

Comrey, A. & Lee, H. 2009. A first course in factor analysis. New York: Physiology Press.

Cutter, S., Boruff, B.J., Shirley, W.L. 2003. Social Vulnerability to Environmental Hazards. Social Science Quarterly, 84 (2): 242–261.

Dall'Osso F., Maramai, A., Graziani, L., Brizuela, B., Cavalletti, A., Gonella, M., Tinti S. 2009. Applying and validating the PTVA-3 Model at the Aeolian Islands, Italy: assessment of the vulnerability of buildings to tsunamis. Nat. Hazards Earth Syst. Sci., 10, 1547–1562.

Dominey-Howes, D. & Papathoma, M. 2007. Validating a tsunami vulnerability assessment model (the PTVA model) using field data from the 2004 Indian Ocean tsunami. Natural Hazards, 40, 113–136.

Dominey-Howes, D., Dunbar, P., Varnes, J., Papathoma M. 2010. Estimating probable maximum loss from a Cascadia tsunami Natural Hazards, 53, 43–61.

Douglas, J. 2007. Physical vulnerability modelling in natural hazard risk assessment. Nat. Hazards Earth Syst. Sci., 7, 283–288.

Fekete A., Damm, M., Birkmann J. 2010. Scales as a challenge for vulnerability assessment. Nat Hazards 55, 729–747.

Freire, S., Aubrecht, C., Wesgscheider, S. 2013. Ad vancing tsunami risk assessment by improving spatiotemporal population exposure and evacuation modeling, Natural Hazards, 68, 1311–1324.

Fuji, Y., Satake, K., Sakai, S., Shinohara, M., Kanazawa, T. 2011. Tsunami source of the 2011 off the Pacific coast of Tohoku Earthquake, Earth Planets Space, 63, 815–820.

Ghobarah A., Saatcioglub, M., Nistorb, I. 2006. The impact of the 26 December 2004 earthquake and tsunami on structures and infrastructure. Engineering Structures 28, 312–326.

Hart, D.E. & Knight G.A. 2009. Geographic Information System assessment of tsunami vulnerability on a dune coast. Journal of Coastal Research, 25, 131–141.

Ine. 2011. Recenseamento Geral da População e da Habitação. Instituto Nacional de Estatística, IP—Lisboa, Portugal.

Ismail, H., Abd Wahab, A.K., Mohd Amin, M.F., Mohud Yunus, M.Z., Jaffar Sidek, F., Esfandier, B. 2012). A 3-tier tsunami vulnerability assessment technique for the nort-west coast of Peninsular Malaysia. Natural Hazards, 63, 549–573.

Kaplan, M., Renaud, F., Lüchters, G. 2009. Vulnerability assessment and protective effects of coastal vegetation during the 2004 Tsunami in Sri Lanka. Natural Hazards Earth System Science. vol. 9, no. 4, 1479–1494.

Leone, F., Lavigneb, F., Parisc, R., Denaina, J.C., Vineta, F. 2011. A spatial analysis of the December 26th, 2004 tsunami-induced damages: lessons learned for a better risk assessment integrating buildings vulnerability. Appl Geogr 31 (1): 363–375.

Mendes, J.M. 2009. Social Vulnerability Indexes as Planning Tools: Beyond the preparedness paradigm. Journal of Risk Research, 12 (1): 43–58.

Omira, R., Baptista, M.A., Miranda, J.M., Toto, E., Catita, C., Catalão, J. 2010. Tsunami vulnerability assessment of Casablanca-Morocco using numerical modelling and GIS tools. Natural Hazards, 54, 75–95.

Papathoma, M. & Dominey-Howes D. 2003. Tsunami vulnerability assessment and its implications for coastal hazard analysis and disaster management planning, Gulf of Corinth, Greece. Nat. Hazards Earth Syst. Sci., 3, 733–747.

Pendleton E.A., Barras J.A., Williams S.J., Twichell D.C. 2010. Coastal vulnerability assessment of the northern gulf of Mexico to Sea-Level rise and coastal change. US Geological Survey Open-File Report 2010–1146 [Accessed January 15, 2014] http://pubs.usgs.gov/of/2010/1146/.

Post, J., Wegscheider, S., Mück, M., Zosseder, K., Kiefl, R., Steinmetz, T., Strunz, G. 2009. Assessment of human immediate response capability related to tsunami threats in Indonesia at a sub-national scale. Nat. Hazards Earth Syst. Sci., 9, 1075–1086.

Reese, S., Bradley, B.A., Binda, J., Smarta, G., Powerc, W., Sturmana. 2011. Empirical building fragilities from observed damage in the 2009 South Pacific tsunami. Earth-Science Reviews 107, 156–173.

Santos, A., Koshimura, S., Imamura, F. 2007. Lessons from the 2004 Indian Ocean Tsunami. Proceedings of the Tohoku Branch of the Japan Society of Civil Engineering, 2 pp.

Santos, A., Koshimura, S., Imamura, F. 2009. The 1755 Lisbon Tsunami: Tsunami source determination and its validation. Jour. Dis. Res., 4 (1): 41–52.

Santos, A., Análise preliminar do tsunami de Tohoku de 2011. VIII Congresso da Geografia Portuguesa, Repensar a Geografia para Novos Desafios, Comunicações, APG, Lisboa, 6 p, [Accessed January 15, 2014] http://riskam.ul.pt/images/pdf/Risco_69-428-1.pdf.

Santos, A., Fonseca, N., Pereira, S., Zezere, J.L., Koshimura, S. 2012. Tsunami risk assessment at Figueira da Foz, Portugal. 15 World Conference of Earthquake Engineering, Lisbon, Portugal [Accessed January 15, 2014] http://riskam.ul.pt/images/pdf/paper_1931.pdf.

Santos, A. & Koshimura, S. 2013. Tsunami hazards at Setubal urban area considering the 1755 Lisbon Tsunami. In Pinto Correia, T.; Henriques, V.; Julião, R.P. (ed), IX Congresso da Geografia Portuguesa—Geografia: Espaço, Natureza, Sociedade e Ciência, Évora, 28–30 Novembro 2013. Portugal [Accessed January 15, 2014] http://riskam.ul.pt/images/pdf/ix_cgp_santos_koshimura_2013_hazard.pdf.

Schmidtlein, M.C., Deutsch, R.C., Piegorsch, W.W., Cutter, S.L. 2008. A Sensitivity Analysis of the Social Vulnerability Index. Risk Analysis 28(4): 1099-1114.

Singh A.P., Murty, T.S., Rastogi B.K., Yadav R.B.S. 2012. Earthquake Generated Tsunami in the Indian Ocean and Probable Vulnerability Assessment for the East Coast of India. Marine Geodesy, 35:1, 49–65.

Smit B. & Wandel J. 2006. Adaptation, adaptive capacity and vulnerability. Global Environmental Change, vol. 16 282–292.

Taubenböck H., Prost J., Kiefl, R., Roth, A., Ismail, F.A., Strunz, G., Dech S. 2009. Risk and vulnerability assessment to tsunami hazard using very high resolution satellite data: The case study of Padang, Indonesia. EARSeL eProceedings, 8(1): 53–63.

Tavares, A.O., Mendes, J.M., Basto, E. 2011. Percepção dos riscos naturais e tecnológicos, confiança institucional e preparação para situações de emergência: O caso de Portugal continental. Revista Crítica de Ciências Sociais, 93. 167–193.

Turner, B.L., Kasperson, R.E., Matson, P.A., McCarthy, J.J., Corell, R.W., Christensen, L., Eckley, N., Kasperson, J.X., Luers, A., Martello, M.L., Polsky, C., Pulsipher, A., Schiller, A. 2003. A framework for vulnerability analysis in sustainability science. *Proceedings of the National Academy of Sciences US*, 100, 8074–8079.

Wisner, B., Blaikie, P., Cannon, T., Davis I. 2004. At Risk: Natural Hazards, People's Vulnerability and Disasters. London: Routledge.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Monte Carlo simulation and Bayesian Evidence Synthesis

U. Sahlin & Y. Jiang
Lund University Centre of Environmental and Climate Research, Lund, Sweden

ABSTRACT: We can all agree that Monte Carlo simulation is a useful technique to propagate uncertainty through a quantitative model. Besides used for sensitivity analysis, the resulting uncertainty in the output of a Monte Carlo simulation can be used to inform decision making. If so, it must be acknowledged that this is a technique for simulation which needs to be complemented by a conceptual framework that assign a meaningful interpretation of uncertainty in output. Now, the interpretation differs with the chosen perspective of risk. Also, the chosen perspective of risk influences the way uncertainty ought to be treated and assigned to input variables in a Monte Carlo simulation. Bayesian Evidence Synthesis is a framework for model calibration, statistical inference of multiple sources of evidence and quantitative modelling to support decision making. In addition, Bayesian Evidence Synthesis provides means to take qualitative aspects of knowledge into account. Therefore, this framework can be used to conceptually frame a Monte Carlo simulation under, not only the Bayesian, but also a general perspective of risk.

1 INTRODUCTION

Monte Carlo simulation is a technique to propagate uncertainty in quantitative models, but that is all. It does not in itself provide any principles to integrate information or to treat uncertainty. Also, it does not adhere to a certain perspective on risk.

If used for sensitivity analysis, where the effects on outputs by varying inputs are in focus, the interpretation of the results of a Monte Carlo simulation does not depend on the interpretation assigned to its inputs and outputs. Sensitivity analysis is in this sense unproblematic.

The situation of concern is when Monte Carlo simulation is used to quantify uncertainty in quantities in order to inform decisions. It is important to keep in mind that a Monte Carlo simulation should not be associated to a particular framework. Introductory text books and common computer programs for Monte Carlo simulation describe methods to quantify uncertainty in input parameters and provide tools to describe the uncertainty in output. Vose (2008) present different statistical principles and argue for uncertainty being subjective, at the same time as the impression is that principles from classical statistical statistics are seen as the first choice. The tutorial for @RISK (Palisade Corporation, 2013) rightly present the quantification and interpretation of uncertainty in a neutral way e.g. by talking about Monte Carlo simulation as a technique "*to combine all the uncertainties you identify in your modeling situation*" leading to "*results presented in the form of probability distributions*". However, statements like "*you can explicitly include the uncertainty present in your estimates to generate results that show all possible outcomes*" gives the impression of an objective known value that is to be accurately described, and thereby a classical statistical view on uncertainty. A Monte Carlo simulation can be made in a simplistic way, e.g. when input parameters are assigned distributions either as the ones that describe data best or that best describes our belief in the possible range of values of that parameter. There is of course more advanced Monte Carlo simulation which more or less takes into account the issues considered here.

We repeat the point made by previous work (e.g. Aven and Kvaløy, 2002, Rettedal et al., 2000) that the use of a Monte Carlo simulation requires a conceptual framework which assigns an interpretation of the uncertainty in the output. An additional purpose of the conceptual framework is to carry the principles to integrate background knowledge into the assessment of risk. It is therefore important that the conceptual framework also is valid under the chosen perspective on risk. Different perspectives on risk can be divided into classical Bayesian, classical statistical and general (Aven, 2013). In an ideal case, a risk assessor decides which perspective of risk that is valid in a particular situation and supports the integration of knowledge into the assessment by principles consistent with that perspective on risk. The purpose of this paper is not to argue that Monte Carlo simulations often are done or framed in a faulty way, but to test the usefulness of a conceptual framework to guide quantification and interpretation of uncertainty. Instead of asking how to interpret uncertainty in a Monte Carlo simulation, it is more relevant to ask

whose interpretation to consider. Most would say it is the interpretation by the decision makers. In the manual for @RISK we read "*the decision-maker must interpret these probability distributions, and make a decision based on the interpretation*" (Palisade Corporation, 2013). It is then up to the assessor to quantify uncertainty in a way that adhere to the interpretation asked for by the decision maker. More emphasis on, and guidelines that adhere to, scientific principles to assess risk are important to strengthen the value of future quantitative assessments.

Some issues arise. Risk assessment should consider all available information. Thus, a desirable characteristic of a conceptual framework would be to handle multiple sources of evidence. A nice feature offered by Monte Carlo simulation is that it is possible to account for correlations between input parameters. In its simplest form, these correlations are assigned assuming a pair-wise linear association between parameters. However, there are other ways to capture the correlation between parameters based on the same sources of evidence. Some sources of uncertainty are missed when parameters are predictions from other models. For example the link to the source of evidence is lost when not considering uncertainty in parameters that have been predicted by statistical regression models.

Two possibly desirable characteristics of a conceptual framework to embrace a Monte Carlo simulation are to

I) give an interpretation of the output for the MC, and
II) provide principles to quantify uncertainty in input that combines with I.

Bayesian Evidence Synthesis (BES) is a possible framework which provides both an interpretation and principles for treating uncertainty in association to a quantitative assessment model applied with the purpose of inform decision making. The aims of this paper are i) to demonstrate how BES incorporates MC simulations and ii) to reflect how BES works under different perspectives on risk.

The paper is organized as follows. First, the different perspectives on risk are illustrated on a simplified risk assessment is used to illustrate the discussion. Then, we will describe Bayesian Evidence Synthesis and show how it can complement a Monte Carlo simulation. Then, we discuss the suitability of BES to give the conceptual framework for MC-simulation under different perspectives on risk. We end with some conclusions.

2 DIFFERENT PERSPECTIVES ON RISK

Risk is perceived in different ways. Aven (2013) distinguish three perspectives: the classical Bayesian, the classical statistical and the general risk perspectives. These perspectives differs in what the risk assessment is set out to measure, such as actual not yet observed states of a system (classical) or risk assessors subjective uncertainty in not yet observed states of a system (Bayesian and general). The perspectives of risk use different measures to quantify uncertainty, Bayesian probabilities in the Bayesian, relative frequencies in the classical, and any measure (probabilistic and non-probabilistic) in the general. Which perspective is appropriate depends on the context in which it is applied and the strength of the prevailing epistemic situation in the background knowledge. This strength can be judged on to what extent the background knowledge provide the bases to assign probabilities to quantify uncertainty (Aven, 2013).

2.1 *An example*

Below we discuss how a Monte Carlo simulation is used under these perspectives. The discussion is illustrated by a Population Viability Analysis (PVA) which is used in ecological risk assessment of species extinction. Risk is quantified as the probability of a population of a bird, mammal or fish to go extinct within 100 years. The system is defined by the state of the population, N_t, through the variable population size at time t. A population is extinct when N_t is zero, but it may very well be doomed to go extinct given enough small population size. Therefore it is customary to instead look at quasi-extinction, which occurs when the population size falls below an assigned critical threshold N_{qe}.

A PVA is conducted by simulating the population during 100 years and calculate the proportion of simulation runs in which N_t falls below N_{qe} at some point in time. In this example, population dynamics is assumed to follow the Ricker growth function with negative density dependence given by the following model

$$N_{t+1} = N_t \exp\left(\alpha\left[1 - \frac{N_t}{K}\right] + \varepsilon_t \right)$$

This means that population growth is negative when population size exceeds its carrying capacity K. The temporal variability in growth rate at carrying capacity is expressed by Gaussian noise with α and σ^2 as mean and variance, respectively. Given this model structure the knowledge about the population is provided by the parameters $\theta = \{\alpha, K, \sigma\}$ and system's initial state N_0.

The purpose with the PVA is to evaluate current risk of extinction and alternatives to manage this risk. Three management alternatives are compared:

A) do nothing, B) increase carrying capacity by 10%, and C) increase the current number of individuals by 10%.

A Monte Carlo simulation quantifies uncertainty in output given a state of the world according to the parameters in θ. Carrying capacity and population average intrinsic growth are assumed to be constant over time. A two dimensional Monte Carlo simulation is therefore appropriate. The inner loop considers the uncertainty arising from variability in growth rate given by the parameter σ and uncertainty in initial population size N_0. The output is the proportion of population going quasi-extinct, $p_{ext}|\theta$ (Fig. 1a). Thus, the final outcome of the assessment is a proportion or a relative frequency indicating to what extent the population is threatened to go extinct (Fig. 1b). Uncertainties in the parameters of the assessment are considered in the outer loop of the Monte Carlo simulation. The output is a sample of proportions taken over a sample of θ, showing the epistemic uncertainty in the assessed proportion of populations going extinct (Fig. 1c). Note that the output of the MC—simulation is a probability (relative frequency) and that this probability is uncertain, since it is a function of uncertain parameters. A common sensitivity analysis is to explore the role a change in a parameter have on the output (Fig. 2).

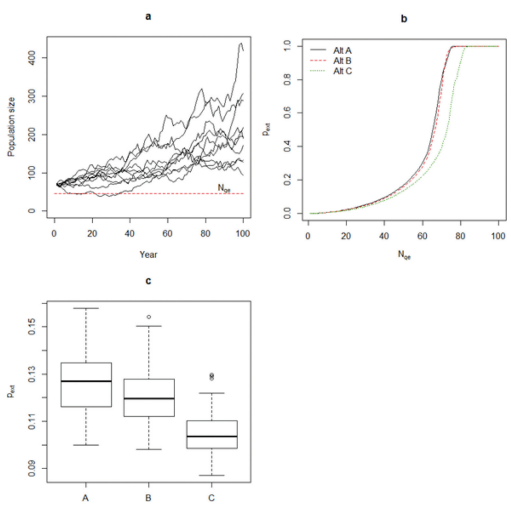


Figure 1. a) Monte Carlo simulations of population size for alternative A. The dash line indicates a suggested threshold of 45 individuals. b) Probability of quasi-extinction (p_{ext}) under different threshold (N_q) for alternative A, B and C with median parameters of MCMC, and c) Probability of quasi-extinction (p_{ext}) for alternative A, B and C for a given threshold ($N_q = 45$) with uncertainty in parameters shown as boxplots.

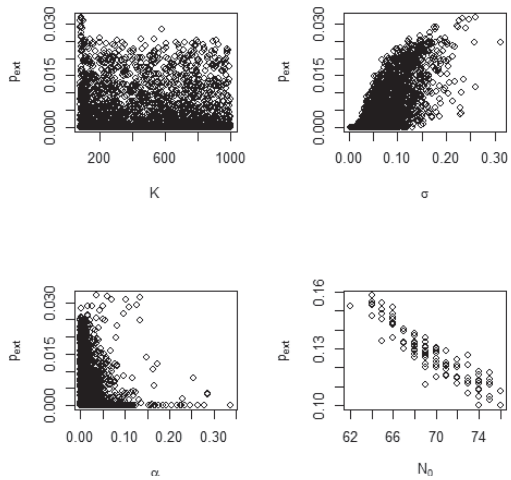


Figure 2. Sensitivity analysis plotting each input parameter to the estimate of risk based on that parameter. The reason p_{ext} differs for N_0 is that the sensitivity analysis is made on the outer instead of the inner two dimensional Monte Carlo loop.

2.2 *The interpretation of uncertainty in output*

Let us first describe some possible interpretations of the output uncertainty from a MC-simulation. A *classical statistical interpretation* of uncertainty in output is found by imagining the assessment as a simulation experiment mimicking a large number of repetitions of the system process that the assessment model is describing (Vose, 2008). An output variable takes different values/states according to a relative frequency. Increasing the number of repetitions will asymptotically approach the probability distribution of the outcome of the system process. This is a possible interpretation of the quasi-extinction probability p_{ext} of the inner loop in the PVA example (Fig. 1b). Those skeptical to this approach argue that that it is not meaningful to talk about a relative frequency when the system process is extremely hard to repeat in the real world, which makes it difficult to talk about true asymptotic probabilities.

Another interpretation of MC output is found when the seeing the simulation experiment as performed under a design corresponding to the assessor's degree of believes in input parameters of the assessment model. Under this *classical Bayesian interpretation*, uncertainty in output is described using knowledge-based probability conditioned on the background knowledge (Aven, 2013).

A separation of variability and knowledge-based uncertainty is important to properly propagate uncertainty in an assessment. There are different ways to reach the knowledge-based probabilities

describing the output of the assessment. One is to, as in the PVA example, use a Monte Carlo simulation that separate variability and knowledge-based uncertainty. If so, the uncertainty in the outcome is subjective probabilities on relative frequencies. The result is a mixture of Bayesian and classical probabilities and is referred to as uncertainty analysis on the classical approach or the *probability of frequency interpretation* (Nilsen and Aven, 2003). This is a possible interpretation of the uncertainty in the quasi-extinction probability resulting from the outer loop of the Monte Carlo simulation in the PVA example (Fig. 1c).

However, the resulting uncertainty consists of a mixture of probabilities (knowledge-based and relative frequencies). Emphasis on one kind of uncertainty in the assessment outcome can be easier in a decision-making context (Aven and Kvaløy, 2002, Rettedal et al., 2000). Variability is relevant for understanding, but of less interest to debate decision alternatives. To "get rid of" variability one can implement it in as process models and parameters expressing stochastic uncertainty at different levels in the assessment. The variability that left unexplained can be treated as a source of knowledge-based uncertainty. Uncertainty in output under this *fully Bayesian interpretation* is simply the assessor's subjective degree of belief. This idea behind this is to adopt a predictive Bayesian approach with focus on inference of observable future system states.

To reach a fully Bayesian interpretation, it may be necessary to reformulate what is the output from the assessment. Returning to the PVA-example there are two options. One option is to show the knowledge-based uncertainty in the system states, here population size, over time. This brings a lot of information that needs to be evaluated further to be of value to the decision maker. Another option is to view the Monte Carlo simulation as a simulation experiment with the purpose to test statements that are important for the decision maker. The statement could for example be if the probability of quasi-extinction is unacceptably high. Let us refer to this as the event A. Regarding 5% as the limit for what is acceptable, our uncertainty about A is $P(A) = P(p_{ext} > 0.05)$. This probability summarizes all knowledge-based uncertainty into a single probability which can easily be communicated to the decision maker.

Some problems with adding the quantification of uncertainty in A as the last step of the assessment are that no consideration is taken to the decision maker's aversion to knowledge-based uncertainty and it can be sensitive to the chosen thresholds in the assessment. Further, the simulation experiment is made within the simplification and assumptions upon which the assessment model is built.

We note that the uncertainty in output from a MC-simulation of an assessment model heavily relies on the assessment model being viewed as appropriate for the application. Model averaging techniques or ensemble modelling can be used to address uncertainty associated to the assessment model. The assessment is then made under a sample of possible assessment models weighted according to our confidence in them being a true representation of the system process.

Even if uncertainty in output is interpreted as subjective degree of belief, it may still be meaningful to talk about uncertainty in this probability. Inaccuracies of the assessment fall back on the limitations of the assessor's knowledge and deliberately made simplifications (Nilsen and Aven, 2003). The former type can be seen as uncertainty in the substance of knowledge. The latter is an example of a wider view on uncertainty associated to the procedures of problem framing and knowledge production, and the sources dependent on the context in which the assessment is made (Maxim and van der Sluijs, 2011). When inaccuracies in the underlying models are high, the bases to assign Bayesian knowledge-based probabilities may be weakened. The added uncertainty that follow from a varying strength of knowledge can refer to different things (Aven 2013), can be seen as qualitative and may or may not be mixed up with probabilities in the Bayesian framework. The general perspective of risk allows different kinds of uncertainties to enter the assessment and allows any kind of quantification.

A classical statistical interpretation of the output from a MC-simulation is suitable when there is enough data to support the assessment (Rettedal et al., 2000). It is not settled to what extent "enough data" implies the existence of empirical data associated to the Monte Carlo simulations inputs and outputs, for which a statistical model can be fitted. If this holds, the assessment model coincides with a statistical model, and the Monte Carlo simulation makes predictions from this model. If no observations for the output have been made, the Monte Carlo simulation can be seen as a simulation experiment. The purpose of such simulation experiment can be to derive relative frequencies on future states varying the input parameters expressing control variables.

The Bayesian and general perspectives on risk ask for interpretations of output uncertainty as knowledge-bases subjective degree of belief, without and with additional assessment of the strength of knowledge, respectively.

2.3 *The input parameters*

Now, we turn to the quantification of uncertainty in input parameters. First, we realize that

the input parameters for which a Monte Carlo simulation draw samples consists of actual parameters (expressing knowledge of the real world) and state variables, describing the system that is under assessment. In some way or another, a MC involves some kind of control measures, which can be implemented as explicit control variables or by changing the levels on parameters or state variables. In the PVA example, control was implemented by changing the parameter K or the initial state of the system. The mixture of parameters, state- and control variables, makes it difficult to generally talk about the quantification of uncertainty in input parameters in a conceptual framework.

The parameters in the PVA example consist of actual parameters $\theta = \{\alpha, K, \sigma\}$ and a state variable N_0. The assessor is uncertain of the actual size of the current population, and describes this uncertainty as a probability distribution over possible values on N_0. To get informed the assessor can request observations from the current population and use a probability model to arrive at the uncertainty in the size of the population. The probability model of the observation process also has associated parameters, let us call them π. The parameters in θ and π can be fitted from time-series on population sizes using a suitable probability model for the system process.

The parameterizations of π and θ can be made based on both classical statistical and Bayesian principles of inference. The major difference between these two is that the Bayesian framework treat parameters as random variables, while the classical statistical regard them as fixed. Probabilities under the Bayesian framework are subjective and express the assessor's degree of belief. Bayesian inference follows by assigning prior distribution to π and θ expressing one's state of knowledge before observing the data. Bayes rule is then applied to update the beliefs into posterior distribution.

In the classical statistical framework uncertainty in parameters (which are perceived as having a true value) is expressed as relative frequencies resulting from drawing random samples from an underlying population. Some argue for a classical statistical approach since it is seen as objective, and objectivity is a valued characteristic for something based on science. However, risk assessment is seldom objective. It can for example be difficult to motivate a mixture of parameters with uncertainty derived by a classical statistical approach and parameters with uncertainty based on expert judgment.

There are situations where the classical and Bayesian inference result in similar probability distributions. It can be argued that classical statistical methods are easier to use, but that can be dealt with by statistical training focusing on the most widely applicable principles of inference, namely the Bayesian. In his widely used book introducing Monte Carlo simulations Vose (2008) mention both classical and Bayesian principles for inference. It is interesting to note that the presentation of the Bayesian methods discuss the consideration of how data has been observed and state of knowledge: "The amount of information contained in data is dependent on two things: (1) the manner in which the data were collected (observation process) and (2) the state of our knowledge prior to observing the data and the degree to which it compare with the likelihood function" (Vose, 2008). This is not the case in the classical statistics. In fact, the classical statistical framework to quantify uncertainty in input parameters is only valid when there is lot of data on everything. Someone faithful to the classical framework would regard everything not derived from data as assumptions.

In a risk assessment situation, the Bayesian framework is the most suitable to quantify uncertainty in input parameters. It allows for a gradual change between situations with a lot of data, in which Bayesian inference could (if the models are the same) show similar results as the classical statistical, to situations based on expert judgment. Bayesian principles for inference play an important role under a general perspective risk, where a decreasing strength in background knowledge asks for an increased use of alternative probabilistic and non-probabilistic measures.

3 BAYESIAN EVIDENCE SYNTHESIS

3.1 *Description*

Evidence synthesis is a term used for synthesis of results from diverse sources and covers a wide range of analysis approaches (Sutton and Abrams, 2001). Bayesian Evidence Synthesis (here denoted as BES) is a statistical framework for explicitly modeling several related and connected sources of data, in which uncertainty in model parameters are incorporated (Jackson et al., 2013). BES can be seen as a complex meta-analysis (Sutton and Abrams, 2001), where complex means to consider multiple effects from an intervention. Classical meta-analyses are usually based on studies that directly have observed the effect of an intervention. A broader view on meta-analyses allows for studies on effects on a lower level which are combined with quantitative modelling to assess the effect of an intervention on a higher level. In this view, a risk assessment can be seen as a meta-analysis (Linkov et al., 2009). Opening up for a quantitative assessment (or complex computer) model to "measure" effects, makes it possible to synthesize evidence for effects which are difficult, if at all, to empirically observe. In the PVA example, there is for example no possibility of

making a randomized controlled experiment testing which management interventions that best would reduce the risk of that population going extinct. It would be unethical to perform an experiment where populations deliberately are kept at high risk, the results from such experiment would take 100 years before being known, and most importantly, there is only one population to study.

A BES is formulated as a cost-efficiency problem that uses a quantitative system model to evaluate chosen measures of cost-efficiency. Based on the state of knowledge on parameters, the quantitative system model is simulated to produce a distribution for model outputs. The system model depends on one or several parameters, which relate to phenomenon in the real world (Fig. 3). In order to avoid confusion with other types of models in the framework, we refer to the quantitative system model (or complex computer model) as a simulator. The parameters of the real world may or may not be observed directly. However, their influence on what have been, or can be, observed are modelled. In this way empirical observations contribute to evidence. A strong link between the quantitative system model and the models for informing parameters makes BES a methodological framework that in a transparent and defendable way enables conclusions to be made based on available evidence to support decision-making.

Jackson et al. (2013) summarize the steps of BES as follows:

1. Build a Directed Acyclic Graph (DAG) according to the underlying causal relationships,
2. Compute posterior probability distributions,
3. Propagate parameter uncertainty through the model to generate uncertainty distribution for the results required for policy making.

In this way "the distributions of the results give appropriate weights to each parameter value, according to how much evidence there is in the data, thus providing a natural way to calibrate the model against the data".

In our view, the advantage with BES is that it provides a generic conceptual framework for statistical inference with the purpose to inform quantitative model and provide a transparent link to empirical data. This statistical framework applies hierarchical (or latent variable) modelling and distinguish between observation and system processes (Fig. 3). System processes are needed to understand where empirical observations come from. The assessment model (simulator) consists of similar or different system processes as those needed to generate the evidence.

It is acknowledged that observations are associated with errors and show patterns that depend on the way they have been observed. Observation processes are described to formulate the appropriate probability models to allow inference from data. In the PVA example, it may not be possible to completely observe the population since individuals move around and can be difficult to find in their environment. The observation process can be modelled as a Binomial-Count process (Kéry and Schaub, 2012). An observation of Y individuals is the result of a draw from a Binomial distribution of in total N possible individuals in the population and a detection probability p (Fig. 4). The detection

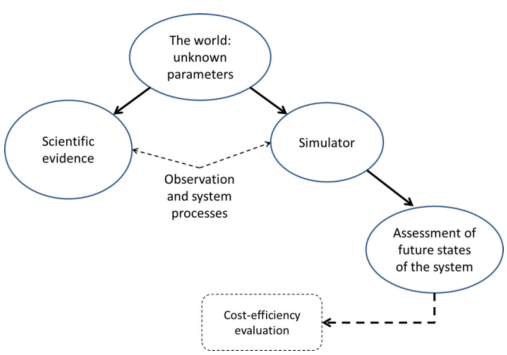


Figure 3. A conceptual graph of Bayesian Evidence Synthesis (modified from Spiegelhalter and Best 2003).

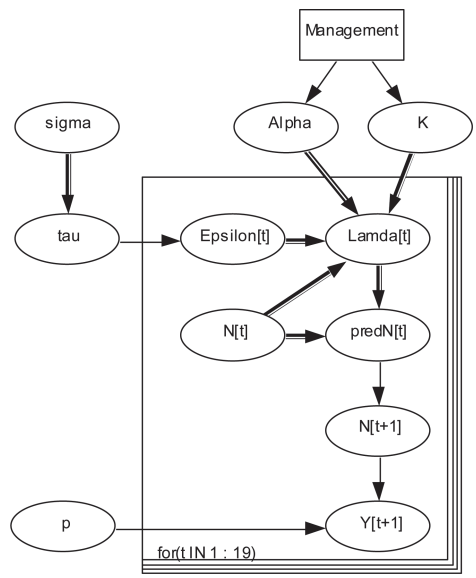


Figure 4. The left hand side of the Bayesian Evidence Synthesis for the PVA example implemented in OpenBUGS showing the links between parameters $\theta = \{\alpha, K, \sigma\}$ and system state variable N_t and between the detection probability p and the observation variable Y_t.

probability can be updated by the Bayesian model or assigned from expert's judgment of the quality of the observation process. In this way, relevant sources of variability and uncertainty are taken into account in a structured way.

Parameterization is seen as calibration of the simulator. Sampling from the posterior of parameters is made using Markov Chain Monte Carlo simulation. The sample can be used directly in the Monte Carlo simulation. Here we ran OpenBUGS (Lunn et al., 2009) from R (R Development Core Team, 2008), which makes it possible to parameterize the model and run the simulator in the R environment.

3.2 *Its use in risk assessment*

Bayesian Evidence Synthesis brings together several methodologies, which more or less are used by risk assessors today. It has its roots in decision analysis within health assessments (Jackson et al., 2013). It is similar to evidence-informed causal modelling and Bayesian Belief Networks (Cox, 2012), and is, in that sense, not a new method. A search on Web-of-Science Core Collection April 4 2014 using the search terms "Bayesian evidence synthesis" generated 237 hits, the first starting from 1995. Adding AND (risk OR safety) reduced the number of hits to 182. The number of publications has grown with time, but not so much for those using the words "risk OR safety" (Fig. 5). The journal of Medical Decision Making had a special issue on Evidence Synthesis 2013. We looked into the papers in three common risk and safety journals. The only paper in the Journal of Risk Analysis using the word "Bayesian Evidence Synthesis" was published 2013. No publication so far in Journal of Risk Research or Safety Science. The search results from this very simple overview indicate that Bayesian Evidence Synthesis is receiving an increasing attention in quantitative risk assessment. The results are limited to peer-reviewed literature only, and perhaps a different picture had been found if searching through actual reports of risk assessments in the gray literature.

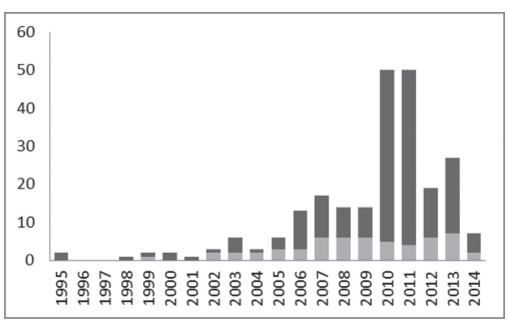


Figure 5. Number of publications related to Bayesian Evidence Synthesis. The bars represent total number of publications with the topic of Bayesian Evidence Synthesis. The light part of the bars represents the number of publications in which the word risk or safety was used as well.

3.3 *Bayesian Evidence Synthesis as a framework for Monte Carlo simulation*

BES has been designed to provide principles for treating uncertainty in association to a quantitative assessment model applied with the purpose of inform decision making. Therefore BES can be a conceptual framework to incorporate MC-simulation, which is the procedure on the right hand side in Figure 3.

A difference between BES and text book type of MC-simulation is how the sample for the MC-simulation is generated. A BES samples from a joint posterior distribution. Thus, there is no shared step where probability distributions of the input parameters of the assessment models must be explicitly specified. Instead, specification occurs at different levels between the actual input parameter and data. Complexity and errors in data is acknowledged by using hierarchical and latent variable modelling to distinguish between actual states and the observations of them. When no data is available, uncertainty of an input parameter is given as priors. Instead of assigning a parameter for an assumed linear correlation, this structure open up for sampling correlative relationships between input parameters informed by the same source of evidence. The text book type of MC-simulation to specify uncertainty in input parameters is easier compared to that of BES, but this procedure is more prone to break the link between underlying data and the assessment output.

A possible critique against BES is that it is a framework to analyze decisions, but not risk. Risk paradigms differ in to what extent risk management is allowed to be part of risk assessment. In some fields management is complex involving management strategies that adapt to the development of the system. If so, decisions and risk is intertwined. An assessment of risk to support decision making come as explicit assessments of risk or are involved in assessments of the impact of risk management interventions on consequences of importance (Cox, 2012). In the former the output of the assessment is quantified observables referring to events and consequences or both (Aven and Eidesen, 2007). The output in the later is quantified efficiency of management interventions. Focus on the efficiency of interventions is common in applications where

consideration of multiple management objectives and conflicting values needs to be taken into account. This is being made without diminishing the importance of cautious management, which is implemented by evaluating efficiency under constraints given by thresholds of acceptance and safety margins on risk. Thus, framing risk assessment in a framework for decision analysis ought not to be a problem.

4 RESULTS

4.1 *Under a Bayesian perspective on risk*

The uncertainty brought by BES is described as weights which have a direct link to underlying sources of evidence. BES presents these weights as the strength of evidence for having a certain output. These weights are interpreted as Bayesian subjective probabilities.

The final outcome of interest is cost-efficiency which summarizes the performances and open up for a comparison of alternative decision alternatives. Thus, focus is more predictive (lower node in Fig. 3) than parametric (upper node in Fig. 3). This does not mean that the final output is a single probability $P(A)$ (see section 2.2). The propagated predictive posteriors of cost-efficiency show the precision, and a narrow distribution can be seen as a qualitatively stronger weight. Our conclusion is that BES supports a Bayesian perspective on risk.

4.2 *Under a classical statistical perspective on risk*

A classical statistical perspective is supported by BES when (i) one can motivate the existence of a statistical model of the processes captured by the simulator and (ii) there is a lot of data to support all parameters in the Monte Carlo simulation. The first condition happens when observations have been, or can (within reasonable time) be made, on similar events that are to be assessed. This would mean that the right hand side in Figure 3 is included in the left hand side. If the second condition is met, classical statistical frequentistic and Bayesian principles of inference result in precise and similar parameters values. Therefore the difference in quantified uncertainty in output, under these two principles, can be small and the BES could be seen as supporting a classical statistical approach.

However, the last condition is difficult to achieve, and most often expert judgments are needed to inform a MC-simulation. Therefore, it is only in exceptional cases when a classical statistical perspective on risk is motivated over a Bayesian treatment of uncertainty. We conclude that BES can support a classical statistical perspective on risk in those rare situations when this is warranted.

4.3 *Under a general perspective on risk*

A risk assessment is subjective, not only in the knowledge put in, but also in the decision taken by the assessor on what and how to make the assessment. The epistemic situation in background knowledge plays a role for what is possible to do. Quality can be considered by evaluating the influence on risk on deviations from the original assessment (Aven, 2013).

We find that BES can be a conceptual framework under a general perspective of risk in which the Bayesian perspective is seen as the base-line. A general perspective, based on Bayesian principles, can be made by allowing for judgment of quality into the quantification of uncertainty. The outcome of a MC-simulation is in fact several outcomes representing different aspects of quality that is taken into account.

The possibility to include judgments of quality is a great advantage with the principles of BES. This is possible since a BES is designed as a framework to combine multiple source of evidence for meta-analysis. Also, new kind of sensitivity analysis can be made. Spiegelhalter and Best (2003) consider the influence of expert judged qualities in three data sources through the observation process models.

Going back to the PVA example, we demonstrate a sensitivity analysis towards the sources of evidence. Consider there are two time-series with observations of the population. One time series is long and one is short. Inference based on the longer is, everything else equal, evidence of higher quality. A BES can be formulated to incorporate both time series by allowing for data-set specific observation processes, here determined by the detection probabilities (Fig. 6). The longer time-series will have a stronger influence on final weights, since it contribute to more data points to the likelihood. This influence can be controlled by assigning strong priors on the detection rates, p_1 and p_2. It can also be made by assuming that one is better than the other. Bayesian MCMC sampling from the posterior will depend on the assumptions made on quality, and the kind of probabilities that come out may be different than the ones where quality is not imposed to the model. Uncertainty is not only presented by probability but also as a sensitivity analysis to aspects of quality. What if the decision makers are sensitive to the choice of time-series in the PVA? The sensitivity of this decision on the cost-efficiency can be evaluated by running the MCMC on a BES based on both data sets, and by removing one data set at

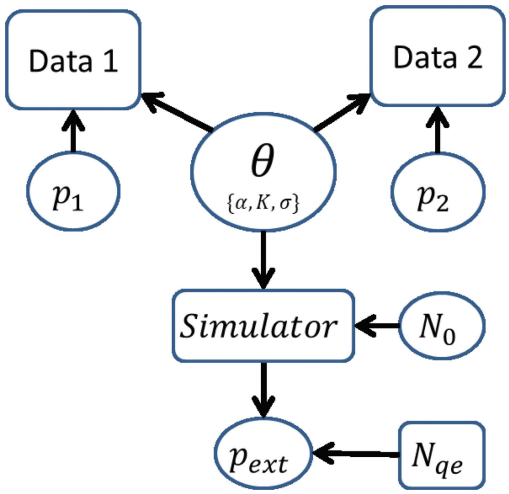


Figure 6. The Bayesian Evidence Synthesis based on two sources of evidence to inform the parameters θ.

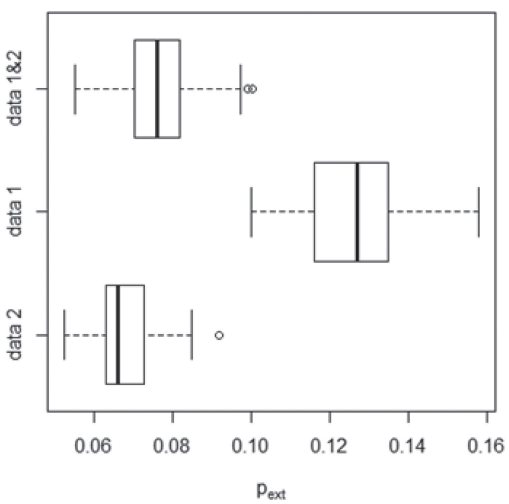


Figure 7. Posterior distributions of quasi-extinction risk informed by two data sets, showing the influence of removing one data set at a time.

a time (Fig. 7). In this example, the risk of extinction was sensitivity to the data set that informed the MC-simulation.

5 DISCUSSION

Here we discuss principles of parametric and predictive inference and views on probability in risk and decision analysis perspectives, with respect to the use of simulations from quantitative model to inform decision making. A difficulty with this discussion is that the term *parameter* and *probability* have different meanings throughout the steps or levels of the assessment process. For example, let X be an input to an assessment model. A probability model is set up to quantify uncertainty in X. This probability model has associated parameters. Under Bayesian inference these parameters are uncertain. In parametric inference the focus is on the uncertainty in these parameters. In predictive inference the focus is on the resulting uncertainty in predictions of X. Here the focus is on uncertainty in the output of an assessment model in which X is an input parameter, thus adding an additional step of prediction. Bayesian probabilities can be used in the inference step and decision analysis, while relative frequencies can exist in the probability models supporting inference or assessment models.

A cause of confusion is the ambiguity of what actually constitute output in a specific Monte Carlo simulation. Again referring to the PVA example, what we use as output could be the states of the system, N_t, the relative frequencies of undesired events, p_{ext}, or the probability that this frequency is unacceptable high $P(A)$. The interpretation of uncertainty may depend on at which of these levels the uncertainty to be interpreted lie.

This discussion uses a typical MC-simulation to illustrate the need of emphasizing foundational issues how to perceive risk and assure quality of the assessment procedure. Students in fields relying on the use of quantitative assessments, such as risk, reliability or system analysis, learn about MC-simulation and different ways to quantitatively describe uncertainty. It is important not to end there, but give the students, and future quantitative assessors, the ability to fully understand what this uncertainty represents and on what scientific principles it can be assessed. We would like to point at Bayesian Evidence Synthesis as a suitable framework to teach predictive statistical principles involving simulations from a computer model. BES is useful both in scientific research and risk assessment and can therefore close the gap between these two highly important processes of knowledge production.

ACKNOWLEDGEMENTS

This work is part of Sahlin's project Quality in evidence-based methods 219-2013-1217 funded by the Swedish Research Council FORMAS. Additional financial support from the strong research environment Biodiversity and Ecosystem services in a Changing Climate at Lund University and the PLANFISH project are appreciated.

REFERENCES

Aven, T. 2013. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety,* 115, 136–145.

Aven, T. & Eidesen, K. 2007. A predictive Bayesian approach to risk analysis in health care. *Bmc Medical Research Methodology,* 7.

Aven, T. & Kvaløy, J.T. 2002. Implementing the Bayesian paradigm in risk analysis. *Reliability Engineering & System Safety,* 78, 195–201.

Cox, L.A. 2012. *Improving risk analysis,* New York, Springer.

Jackson, C.H., Jit, M., Sharples, L.D. & De Angelis, D. 2013. Calibration of Complex Models through Bayesian Evidence Synthesis: A Demonstration and Tutorial. *Medical Decision Making*.

KéRy, M. & Schaub, M. 2012. *Bayesian population analysis using WinBUGS: a hierarchical perspective*, Boston, Academic Press.

Linkov, I., Loney, D., Cormier, S., Satterstrom, F.K. & Bridges, T. 2009. Weight-of-evidence evaluation in environmental assessment: Review of qualitative and quantitative approaches. *Science of the Total Environment,* 407, 5199–5205.

Lunn, D., Spiegelhalter, D., Thomas, A. & Best, N. 2009. The BUGS project: Evolution, critique and future directions. *Statistics in Medicine,* 28, 3049–3067.

Maxim, L. & Van Der Sluijs, J.P. 2011. Quality in environmental science for policy: Assessing uncertainty as a component of policy analysis. *Environmental Science & Policy,* 14, 482–492.

Nilsen, T. & Aven, T. 2003. Models and model uncertainty in the context of risk analysis. *Reliability Engineering & System Safety,* 79, 309–317.

Palisade Corporation 2013. @RISK Risk Analysis and Simulation Add-In for Microsoft®Excel *Version 6 September, 2013* Palisade Corporation.

R Development Core Team 2008. R: A language and Environment for Statistical Computing. *R Foundation for Statistical Computing*.

Rettedal, W.K., Aven, T. & Gudmestad, O.T. 2000. Integrating QRA and SRA methods within a Bayesian framework when calculating risk in marine operations: Two examples. *Journal of Offshore Mechanics and Arctic Engineering-Transactions of the Asme,* 122, 181–187.

Spiegelhalter, D.J. & Best, N.G. 2003. Bayesian approaches to multiple sources of evidence and uncertainty in complex cost-effectiveness modelling. *Statistics in Medicine,* 22, 3687–3709.

Sutton, A.J. & Abrams, K.R. 2001. Bayesian methods in meta-analysis and evidence synthesis. *Statistical Methods in Medical Research,* 10, 277–303.

Vose, D. 2008. *Risk analysis: a quantitative guide,* Chichester, England; Hoboken, NJ, Wiley.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Amendments of the existing guidance on PSA application to nuclear power plants in Germany

H.P. Berg & M. Krauß
Bundesamt für Strahlenschutz, Salzgitter, Germany

M. Röwekamp
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Cologne, Germany

ABSTRACT: The German nuclear regulation has been significantly enhanced by the "Safety Requirements for Nuclear Power Plants" issued in January 2013 and the corresponding "Interpretation of the Safety Requirements for Nuclear Power Plants" issued in December 2013. These enhancements also concern probabilistic safety analyses as supplementary tool for assessing nuclear power plants´ safety. The most recent PSA activities in the frame of Periodic Safety Reviews (PSR) focus on extending Level 1 PSA scope more explicitly to fuel damage states and further improvements with respect to Low Power and Shutdown (LPSD) plant operational states including internal hazards, in particular fire. Moreover, a more complete and systematic consideration of external hazards is intended for full power states. These improvements are in line with recent international activities.

The material for the update of PSA methods and data in the frame of PSR has already been provided in order to issue the intended supplement to the existing documents in 2014.

While probabilistic assessment was mainly used in Germany in the frame of PSR in the past, PSA applications shall be further extended to regulatory oversight activities in the future. The above mentioned Safety Requirements define relative probabilistic criteria to be applied for plant or organizational modifications applied by the licensee or for evaluating events or phenomena which may have a non-negligible effect on PSA results. For these applications a short document is in preparation as well.

1 INTRODUCTION

In general, the nuclear regulatory framework in Germany is a deterministic one with very detailed and comprehensive nuclear requirements, guidelines and recommendations, safety standards and rules incorporated in a corresponding legal hierarchical structure.

In the past, the safety concept of Nuclear Power Plants (NPPs) as well as licensing decisions by the competent authorities and their experts in Germany were mainly based on deterministic principles such as prevention or control of abnormal plant operational conditions and incidents by technical means to ensure high reliability. In the meantime, Probabilistic Safety Analyses (PSA) are mainly applied in the frame of periodic safety reviews and shall supplement deterministic safety demonstrations to verify the balance of the plant design related to safety.

The German nuclear regulatory framework has recently been significantly enhanced promulgating state-of-the-art "Safety Requirements for Nuclear Power Plants" issued by the Federal Ministry of the Environment, Nature Conservation and Reactor Safety (BMU 2013a and 2013b). These enhancements also concern safety demonstrations by deterministic as well as probabilistic safety assessment in more detail.

In this context, PSA shall also supplement deterministic safety demonstrations to assess the safety significance of modifications of Structures, Systems and Components (SSC), measures or procedures as well as of findings that have become known from safety-relevant events or phenomena that have occurred and which can be applied to the nuclear power plants in Germany that are referred to in the scope of application of (BMU 2013a), for which a significant influence on the results of PSA can be expected.

Compared with the unchanged conditions of the plant, modifications of measures, equipment or the operating mode of the plant shall neither result in an increase of the average Core Damage Frequency (CDF) and/or the average frequency of large and early releases (LRF/LERF), for power operation nor for low power and shutdown states, considering all plant internal events as well as all

internal and external hazards including extremely rare man made ones.

Hence, the new German safety requirements contain an implicit definition of quantitative safety criteria: Mean CDF and LERF of full scope PSA Level 1 and 2, respectively, must not increase due to a planned plant modification. However, no absolute value is given, by which the current risk of the plant can be assessed to be acceptable.

The CDF values have been calculated in the frame of the comprehensive (periodic) safety reviews. The results of the latest safety review for the respective NPP are the basis for the comparison in case of modifications.

The fundamental boundary conditions for performing PSA including requirements with respect to their documentation are provided in (BMU 2005). The safety requirements for NPPs in (BMU 2013a) further require that state-of-the-art methods, models and data have to be applied in the frame of PSA.

As far as possible plant specific data have to be applied. If no suitable plant specific data are available from the operating experience, generic data may be used if justified. Such data are provided for common cause failures and fire protection features in (FAK 2005b).

2 UPDATE OF TECHNICAL DOCUMENTS FOR APPLYING PSA IN THE FRAME OF SAFETY REVIEWS

A first set of guidelines and supplementary technical documents providing guidance on the contents and performance of a Periodic Safety Review (PSR), have been issued in 1997.

The PSR, since 2002 called Safety Reviews (SR) for NPPs in Germany, have to be performed at least every ten years. The obligation to submit the results of a SR and evaluation shall not apply if the licensee gives a binding declaration to the regulatory body at the Federal State level stating that operation of the installation will be permanently discontinued latest three years after the dates specified in the German Atomic Energy Act (2013).

For PSA, a revised guideline (BMU 2005) and its corresponding technical documents on PSA methods (FAK 2005a) and data (FAK 2005b) have been developed extending the application area to external hazards for Level 1 PSA for full power operation, to low power and shutdown Level 1 PSA for plant internal initiating events and to Level 2 PSA for plant internal initiating events during power operation.

As a result of the German decision to phase out of nuclear energy until 2022, only two or three SRs remain obligatory to be performed for German NPPs. Therefore, updating the PSA Guideline is no longer be continued and the originally planned comprehensive update of (FAK 2005a) and (FAK 2005b) will not be elaborated anymore.

However, various activities for updating specific topics regarding probabilistic safety analyses have been performed since 2008, in particular with respect to methods with respect to human reliability, external hazards, Level 1 low power and shutdown PSA and some aspects of Level 2 PSA as well as with respect to data on human reliability, common cause failures and reliability of active fire protection features.

It is intended to issue the updated material on methods and data for PSA applications in the frame of SR as a supplementary document in 2014.

In the following, the amendments with respect to Level 1 PSA are presented in more detail.

2.1 *Aspects regarding Level 1 PSA*

2.1.1 *Human reliability*

For performing Human Reliability Analysis (HRA) a specific methodology is required. Different methods are available that can be used depending on the purpose of the analysis and the scope of the methodological approach.

The update of the section on HRA in particular considers issues such as:

- Consistent integration of findings and results on HRA from operational experience,
- Identification of potential vulnerabilities by more detailed modeling,
- Consideration of component failures or system functions representing external contextual factors in the development of a dynamic event flow path with effects on decision making,
- Identification of fundamentally different types of errors such as faulty human actions due to incorrect diagnoses and decisions,
- Errors of commission leading to damage increasing actions.

Moreover, the description of the task, the qualitative analysis and the evaluation of human reliability has been extended.

It is recommended that a detailed human reliability analysis should be applied using advanced methodological approaches reflecting why people act in a certain manner and what action triggers the human error.

In several cases, methods such as THERP (Swain & Guttmann 1983) are applicable, in other cases they are not. Therefore, in the last decade a number of advanced methods and techniques has been developed and according to the objective of the HRA applied to some extent.

In the revised section on HRA "profiles" for several HRA methods are provided, because there are more than one method available being applicable for all kind of questions. These profiles contain a brief description of the underlying procedures of these methods and address the areas of their application to date, their capabilities and limitations as well as cost-benefit aspects.

2.1.2 *External hazards*

Originally, a more comprehensive update of the section on external hazards was planned. To date, the supplementary document, however, will focus on seismic events and external flooding.

Relating to robustness investigations resulting from the stress tests in Germany performed after the Fukushima Dai-ichi reactor accidents, the main emphasis will be on earthquakes and external flooding including a graded approach with respect to flooding events (scope of analysis), possible "cliff-edge effects", checking the parameters currently assumed as well as their superposition and to improve the determination of failure probabilities of permanent or temporary flood protection measures. Moreover, extreme weather conditions are to be addressed. One major activity is the introduction of a procedure to identify the relevant SSSs in case of an earthquake and the benefits of plant walk-downs in this context.

2.1.3 *Level 1 low power and shutdown PSA*

The overall goals of the planned update of the section on low power and shutdown Level 1 PSA in (FAK 2005a) are to provide more precise terms and definitions with particular reference to the different phases of low power and shutdown states in German nuclear power plants (with Boiling Water Reactor (BWR) or Pressurized Water Reactor (PWR)) as well as an adaptation and clarification of the examples for the analyses provided in the document.

Clarification has been given on the specification of operating conditions for Low Power and Shutdown (LPSD) states. A precise definition and identification of initiating events with special consideration of erroneous human actions before such an event occurred has been provided. In addition, a clear definition of the end states of event sequences during low power and shutdown is available. Last not least, Fire PSA methods have been adapted to these Plant Operational States (POS).

Low power and shutdown plant operational states are characterized by several phases, during which either different initiating events can occur or the same initiating events have to be controlled under highly different conditions. The specification of the phases results from the plant specific conditions for processes to take place, together with the current status of the physical parameters during these phases. For LPSD phases, the physical and technical conditions as well as the planned maintenance related and organizational measures may still vary so that a further subdivision with respect to plant operating conditions may be required.

The following definition of an uncontrolled end states has been provided: "Fuel damage states during low power and shutdown operation are characterized by a significant release of radionuclides that may occur due to a loss of fuel cooling and the subsequent heating of the fuel rods or by mechanical damage to the fuel rod cladding. Uncontrolled end states may also result from a loss of reactivity control." Thus, for low power and shutdown states fuel damage states have to be considered instead of core damage states.

Moreover, guidance for performing Fire PSA for LPSD plant operational states is provided and described below.

For each phase during low power and shutdown those compartments or plant areas have to be identified, where fire events may inadmissibly impair items important to safety. In particular, the following changes and enhancements with respect to the input data have to be considered:

- The total compartment inventory of Systems, Structures and Components (SSC) including cables has to be associated to POS in accordance with their safety functions to one of the following three classes (1—no safety relevance, 2—basic event in the PSA plant model, 3—failure may contribute to an initiating event).
- Depending on the POS, changes of the status with regard to fire protection in certain compartments are possible (e.g. BWR containment no longer filled with inert gas). These changes as well as well as changes with respect to fire barriers, amount and distribution of fire loads, effects of maintenance and repair work, changes in the number of persons present and the duration of their presence in certain fire compartments have to be considered for Fire PSA.
- In case of a fire induced loss of the entire compartment inventory, the list of potential initiating events should be adapted and, if necessary, further completed depending on the respective POS.
- For those compartments and/or plant areas identified to be significant within the screening, detailed analyses have to be carried covering the following three analytical steps:
  - Fire occurrence frequency determination:
    For that purpose, the methods in place for full power operational states can be applied, taking into account the changes in fire safety according to the conditions during LPSD.

– Fire damage frequency calculation:
  The methods for full power operation (fire specific event tree analysis) can be applied.
– Fuel damage frequency estimation:
  For this calculation the event tree analysis of the respective initiating event from LPSD PSA can be used. It has to be checked, if those human actions needed for control of initiating events still can be performed in case of fire.

2.2 *Update of data for PSA using German operational experience*

2.2.1 *Data for HRA*

In addition to the activities for facilitating enhanced methods and approaches for PSA, investigations are needed for providing additional or updating data in the areas of human reliability and reliability of fire protection features.

The first activity is aiming to provide additional data for Human Reliability Analysis (HRA) when applying the THERP method. Currently, the data used for HRA in the context of PSA studies mainly stems from the THERP database (Swain & Guttmann 1983), which consists of tables with more than 100 Human Error Probabilities (HEP) for a variety of tasks important to nuclear power plant operation. A persistent problem is the question of whether this generic data is compatible with the operational practice of the power plant in question. Moreover, the amount of data available is insufficient to cover all needs. Therefore, in order to both validate and extend the THERP database, the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety sponsored two research projects to gather human reliability data from the operational experience of German nuclear power plants. For this purpose, a method utilizing the German licensee event reporting system has been developed, which allows, for certain tasks with specific attributes, to determine the number of times a specified task was performed in the past, as well as the number of errors that occurred. Thus, a statistical procedure allows obtaining HEP estimates from these data.

The first project, which ended in 2010, contributed altogether 37 HEP estimates. In all except three cases an agreement within the uncertainty bounds with the THERP database was found; moreover, 21 HEP estimates for which THERP provides no data was contributed.

The methods and results of this project are reported in (Preischl & Hellmich 2013). The second project, which ended in early 2013, continued the activities started in the first one, and moreover contributed human reliability data obtained from tasks which have remained below the reporting threshold of the event reporting system, i.e. they have not yet produced a reportable event, but unambiguously would result in a reportable one in case of an error.

2.2.2 *Data regarding common cause failures*

In (FAK 2005a) methods for quantification of Common Cause Failures (CCF) according to the state-of-the-art at that time are described and generic CCF probabilities for 21 different component types (such as different types of valves, batteries, diesel generators, heat exchangers) are listed (FAK 2005b) based on the operating experience available at this time. This list included all types of components for the time from the start of operation of the German plants until June 15, 1985. For some types of components data of other operating times were available, the most recent ones up to 1998.

However, there was not sufficient operating experience from German plants available for all types of components. Therefore, data from the international operating experience had to be included. These data were mainly based on reports of the IAEA/NEA Incident Reporting System.

In the meantime, the operational experience could be significantly expanded. The operational experience of the operating 17 nuclear power plants in Germany for the period up to the end of December 2010 has been completely evaluated. Since the amount of data has increased the use of foreign operating experience in the determination of CCF probabilities is no longer necessary.

During plant operation components were frequently modified, based on operating experience, new knowledge and new technical developments.

In addition, operational procedures were changed and additional monitoring methods implemented. Therefore, for most component types it is possible to focus only on the operating experience beyond 1990.

2.2.3 *Data regarding reliability of fire protection features*

In the context of modeling plant specific fire event and fault trees, reliability data with regard to fire protections means are required. In (FAK 2005b) technical reliability data for various active fire protection features have been provided resulting from plant specific analyses of the operating experience from different NPPs.

In order to update the already existing reliability data (in particular, failure rates per hours of plant operation) as well as to extend the database covering an additional plant unit the following components and systems installed in six nuclear power plant units at five plant sites:

– Fire detection systems with the corresponding main fire alarm panels, subsidiary fire alarm

boards, detection drawers, detection lines/groups as well as automatic and manual fire detectors,
- Fire dampers and smoke extraction dampers in ventilation ducts with different actuation mechanisms (thermally by fusible link or remote controlled by typically electro-mechanical or pneumatic actuation),
- Fire doors between rooms, partly equipped with electrically hold-open devices, and
- Stationary fire extinguishing systems and equipment including the corresponding extinguishing media supplies, fire water pumps, hydrants, etc.

The data has been evaluated by analyzing the documentation of periodic in-service inspections as well as additional information and reports which resulted from the inspection findings. For more complex systems such as the fire detection systems, in addition to the components' reliability data, fault trees are presented to calculate the system's reliability.

These data are then used in a second step to provide generic data, only based on German operational experience.

The updated and extended generic database covers 104 plant operational years of in total six German NPP units of different type (PWR as well as BWR) and age. These enhancements have increased the level of confidence significantly.

More details regarding the derivation of the new data set are provided in (Forell et al. 2012) and (Forell et al. 2014).

This set of data may also be applied as a-priori information for estimating the reliability of components of a similar design and an equivalent inspection and maintenance practice in the frame of Fire PSA for nuclear power plants in other countries.

3 PSA APPLICATION IN THE FRAME OF PERMANENT REGULATORY OVERSIGHT ACTIVITIES

3.1 *PSA application for the assessment of modifications*

While PSA was mainly used in Germany in the frame of (P)SR in the past as explained earlier, according to (BMU 2013) PSA applications as a supplementary analytical tool to be used in the nuclear regulatory framework shall be further extended.

As already explained in Section 1, due to these new regulations relative probabilistic criteria should be applied for assessing modifications of measures, equipment or the operating mode of the plant.

This results in the extended use of PSA to regulatory issues beyond PSR, such as a regulatory oversight on modifications applied by the licensee or an evaluation of those safety relevant events or phenomena which may have significant effects on the PSA results.

Including probabilistic considerations in the assessment is particularly useful in the evaluation of decision alternatives and strategies. A typical application in the past was the assessment of modifications with respect to in-service inspection intervals.

A recent example is described in (Babst et al. 2014). The licensee has recently requested the regulatory body for approving technical plant modification concerning the spent fuel pool cooling. Major differences of the intended plant modifications compared to the original situation are the number of emergency power supply systems available and the systems used for cooling the spent fuel.

In order to facilitate practical support allowing interpretations and explicit applications of these new requirements, an expert group on PSA in the frame supervisory activities, chaired by the Federal Office for Radiation Protection (BfS), has been established in fall 2012. One topic of discussions is the definition of a significant impact on the PSA results. Moreover, practical examples shall be collected to illustrate a possible risk informed approach.

The intention is to develop a document providing, among others, guidance if e.g. probabilistic considerations within the analyses of plant specific modifications have to be made, but analyses of the current state of the system are not available (e.g. regarding large and early releases of radionuclides, assessment of external hazards in the frame of LPSD PSA or Level 2 PSA).

If possible, the transferability of results for external hazards from full power operational states to low power and shutdown states including plant states representing neither commercial operation nor a formal decommissioning process should be discussed for Level 1 and Level 2 PSA.

3.2 *PSA application for the assessment of operating experience*

Furthermore, guidance shall be developed and examples be provided for the assessment of operating experience in line with (BMU 2013a), because this is generally not covered in the supplementary document on methods and data for PSA discussed in Section 2.

Only in case of human reliability, this aspect has been addressed. For such a retrospective event analysis, a comprehensive root cause analysis has to be performed for determining the causal relationships, e.g. the error mechanisms occurred with the aim of identifying causes that have contributed

to the action errors. This requires, in addition to the identification of the immediate causes, an investigation of the whole process.

Moreover, an example of an enhanced HRA analysis method has been added, which is intended to complement the existing THERP example in (FAK 2005a). As example of an analysis from past operating experience the fire event at the Forsmark NPP has been chosen.

4 CONCLUDING REMARKS AND OUTLOOK

The German Guide on Probabilistic Safety Analysis (BMU 2005) provides fundamental methods and boundary conditions for performing PSA including requirements with respect to their documentation. The recently issued Safety Requirements for Nuclear Power Plants (BMU 2013a) further require that state-of-the-art methods, models and data have to be applied in the frame of PSA.

While in Germany PSA was used in the past mainly in the frame of the ten years (Periodic) Safety Reviews, PSA as a supplementary analytical tool to be applied in the daily nuclear regulatory oversight in case of modifications by the licensee or for an assessment of those events or phenomena for which a significant influence on the results of the PSA results can be expected shall be further extended in the future.

As a result of the German decision to phase out of nuclear energy until 2022, only two or three Safety Reviews remain to be obligatory performed for nuclear power plants in Germany. Therefore, it is intended to provide the updated material on methods and data for PSA applications in the frame of PSR as a supplement to the existing technical documents on PSA (FAK PSA 2005a und 2005b). This supplement will reflect experiences from the German safety review processes and the resulting improvements in line with international developments. It is intended to issue this supplementary document in 2014.

To facilitate practical support allowing interpretations and explicit applications of the new requirements, it is planned to develop a document providing, among others, the definition of a significant impact on PSA results, collecting practical examples to illustrate a possible procedure.

Moreover, guidance should be given for those cases, where more or less detailed probabilistic analyses of plant specific modifications have to be performed, but probabilistic analyses of the current plant state or results of the comparison between unchanged and modified situation are not available (e.g. regarding large and early releases of radionuclides, assessment of external hazards in the frame of LPSD PSA or Level 2 PSA). This document is intended to be issued in 2015.

REFERENCES

Atomic Energy Act *(Act on the peaceful utilisation of nuclear energy and the protection against its hazard*). December, 23, 1959, as amended and promulgated on July, 15, 1985, last amendment of August 28, 2013.

Babst, S., Röwekamp, M., Schwarz, M. & Türschmann, M. 2014. Conducting Fire PSA for the post-commercial shutdown phase. In *Proceedings of the International Workshop on Fire PRA*, Garching, Germany, 28–30 April 2014.

Facharbeitskreis (FAK) PSA. 2005a. *Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke. Stand: August 2005*. BfS-SCHR-37/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany (in German).

Facharbeitskreis (FAK) PSA. 2005b. *Daten zur probabilistischen Sicherheitsanalysen für Kernkraftwerke. Stand: August 2005*, BfS-SCHR-38/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany (in German).

Federal Ministry of the Environment, Nature Conservation and Reactor Safety (BMU). 2005. *Guideline for conducting the safety review according to § 19a of the Atomic Energy Act—Guideline on PSA—30 August 2005*. Federal Gazette Nr. 207a.

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU). 2013a. *Safety requirements for nuclear power plants*. Federal Gazette, 24 January 2013 (in German).

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU). 2013b. *Interpretation of the safety requirements for nuclear power plants of 22 November 2012*. 19 November 2013 (in German).

Forell, B., Einarsson, S., Röwekamp, M. & Berg, H.-P. 2012. Updated technical reliability data for fire protection systems and components at a German nuclear power plant. In *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11/ESREL 2012), Curran Associates, Inc., Red Hook, NY, USA*.

Forell, B., Einarsson, S. & Röwekamp, M. 2014. Extension of the plant specific database of fire protection systems and components failure rates. In *Proceedings 12th International Probabilistic Safety Assessment and Management Conference, Honolulu, USA*, in preparation.

Preischl, W. & Hellmich, M. 2013. Human error probabilities from operational experience of German nuclear power plants. *Reliability Engineering and System Safety* 109: 150–195.

Swain, A.D. & Guttmann, H.E.D. 1983. *Handbook of human reliability analysis with emphasis on nuclear power plant applications, final report*. NUREG/CR-1278F, U.S. Nuclear Regulatory Commission, Washington, D.C., USA.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Focus areas for a Level 2 PSA that supports a site NPP risk analysis

D.M. Helton
United States Nuclear Regulatory Commission, Rockville, MD, USA

M. Zavisca & M. Khatib-Rahbar
Energy Research Incorporated, Rockville, MD, USA

ABSTRACT: The US Nuclear Regulatory Commission is developing a site Level 3 Probabilistic Safety Analysis (PSA) for the two operating nuclear power plants, and associated spent nuclear fuel storage facilities at the Vogtle site. The development of this integrated PSA, along with its intended end-uses, shifts the focus in the Level 2 (accident progression and radiological source term) portion of the analysis toward greater realism. This paper describes ways in which this focus affects the analytical approach. Presently in the US, Level 2 PSAs for operating reactors are most frequently performed in either a simplified manner (to support environmental impact studies), or for comparison with a (safety case-related) figure-of-merit. These applications often rely on simplifying assumptions. The present Vogtle analysis is novel in its scope, encompassing all major radiological sources on the site in concert, while assessing a range of hazards and plant operating configurations. As risk assessment technology advances, as computational capabilities increase, and in light of the multi-unit event at Fukushima Daiichi, this type of PSA activity is expected to proliferate. Interactions between the nuclear safety and risk communities at this stage will facilitate the development of more efficient methods. This paper will describe the approach being taken in several areas of the reactor and the spent fuel pool Level 2 PSA to promote realism in the treatment of the overall site risk. These areas include structural failure characterization, modeling of severe accident phenomena, survivability of equipment and instrumentation, and modeling of accident management actions. Whereas a systems-level view of the subject site design and operation would suggest very little dependency between the two reactors and the SFPs, this paper will make the case that after one or more radiological sources have proceeded to a severe accident (i.e., fuel melting) the detailed overall site accident progression becomes very inter-dependent.

1 INTRODUCTION

The United States Nuclear Regulatory Commission (US NRC) is developing a site Level 3 Probabilistic Safety Analysis (PSA) for the two operating nuclear power plants, and associated spent nuclear fuel storage facilities at the Vogtle site in Georgia, USA. In nuclear power plant risk assessment terminology, Level 3 refers to the modeling of accidents from their initiation to the offsite consequences caused by the accidents (public health effects and property damage). The scope of the Vogtle Level 3 PSA is events caused by both internal and external hazards, excluding acts of sabotage. The development of this integrated (a.k.a., extended) PSA, along with its intended end-uses, shifts the focus in the Level 2 (accident progression and radiological source term) portion of the analysis toward greater realism.

This paper describes ways in which this focus affects the analytical approach. Presently in the US, Level 2 PSAs for operating reactors are most frequently performed in either a simplified manner (to support environmental impact studies), or for comparison with a safety case-related figure-of-merit such as large early release frequency. These applications often rely on simplifying assumptions. The present Vogtle analysis is novel in its scope, encompassing all major radiological sources on the site in concert, while assessing a range of hazards and plant operating configurations.

This paper will describe the approach being taken in several areas of the reactor and the spent fuel pool Level 2 PSA to promote realism in the treatment of the overall site risk. Specifically, the following sections describe the modeling approach in the areas of structural failure characterization, severe accident phenomena, survivability of equipment and instrumentation, and severe accident management. In each section, examples are given where realistic treatment leads to better estimation of site-wide accident interactions. In addition to the interplays between radiological sources within a given modeling area, the paper will also point out

the way in which these different modeling results inherently affect the other modeling areas. Whereas a systems-level view of the subject site design and operation would suggest very little dependency between the two reactors and the SFPs, this paper will make the case that after one or more radiological sources have proceeded to a severe accident (i.e., fuel melting) the detailed overall site accident progression becomes very inter-dependent.

2 STRUCTURAL FAILURE CHARACTERIZATION

In the structural failure characterizations for the reactor and spent fuel pool Level 2 PSA modeling, NRC is relying on a combination of (i) past assessments, (ii) new calculations using three-dimensional finite element analysis in conjunction with statistical data for the failure strain of the liner materials, as well as models for tearing of the liner, and (iii) assessments using engineering criteria. Of particular interest here are the characterizations of containment severe-accident-induced failure and spent fuel pool seismic failure.

Vogtle's physical layout is typical of dual-unit US pressurized water reactors. The two containments are each surrounded by other structures for large portions of the azimuth (the extent varies by elevation), namely the equipment building and the main steam valve rooms. The spent fuel pools are located in-line, between the two reactor containments, with a distinct pool for each reactor. The two pools are normally hydraulically connected to one another through a common cask loading pool, via fuel transfer gates that extend to an elevation just above the spent fuel storage racks. The containment design is typical of pre-stressed concrete containments, having a tendon gallery (square cross-section tunnel) that extends the full 360-degrees of the azimuth, oriented just below the containment's external wall. The tendon gallery is accessed through three vertical shafts: one accessed in the yard (i.e., open to the environment), one accessed through the control building roof, and the other accessed through the equipment building. Numerous electrical and piping containment penetrations exist in both the portions of the containment surrounded by other structures and those leading to the yard. The containment has three access points: the main equipment hatch opens to the yard, the personnel airlock leads to the equipment building, and the emergency airlock leads to one of the tendon gallery access shafts.

The results of the new containment calculations have been compared back to the structural assessments performed by the licensee during the Individual Plant Examination study (1990s), and are also leveraging the failure characterization work stemming from extensive experimental and analytical investigation performed at Sandia National Laboratories (e.g., Petti et al., 2013).

The updated containment analyses estimate that the internal static pressure at which enhanced leakage initiation would occur is roughly the same as estimated in the IPE study (e.g., 7% variation relative to the failure pressure) for the wall-basemat junction, the equipment hatch, the emergency airlock, and the personnel airlock. For the wall-basemat junction failure, the assessments indicate that cracks would develop at the base of the wall and basemat slab and that the likely leakage path would be through cracks in the concrete extending to the tendon gallery under the containment wall (this was not addressed by the IPE analysis). This in turn would pressurize the tendon gallery, potentially failing the doors connecting to the access shaft. The resulting failure area for all of the aforementioned failure locations is expected to be only large enough to prevent further pressure escalation. Based on site-specific MELCOR analyses focusing on long-term molten core concrete interaction, and separately on the results of the structural analysis, this leakage area could range from $2 \cdot 10^{-3}$ m^2 to 0.1 m^2.

From a site Level 3 PSA perspective, the range of potential static over-pressure failures presents an interesting spectrum of possibiilities between environmental radiological releases and habitability/survivability concerns. First, wall-basemat junction failure in to the tendon gallery may cause habitability concerns (temperature, combustible gas, and radiological) in areas near the equipment building tendon gallery access shaft. This in turn has implications for both instrument and equipment survivability and local operator accident management actions, some aspects of which are discussed later. The surrounding structures are relatively compartmentalized, but clearly not designed to accommodate combustion events. Thus, the zone of influence of these habitability and survivability concerns becomes greater if a combustion occurs.

Similarly, other potential failure locations include a mix of release pathways, ranging from those that are preferentially directly to the environment (the equipment hatch), those that are preferentially in to surrounding structures (the personnel airlock), and those that have components of both (the emergency airlock). It's also important to note that the non-catastrophic nature of the rupture will limit the rate of change of containment and ex-containment conditions following failure, which may affect the likelihood of combustion and its effects. While a particular failure location must be assumed for deterministic reactor analysis,

the range of failure locations may be an important modeling uncertainty for the integrated risk analysis.

The spent fuel pool assessments are ongoing as of this writing, but preliminarily indicate that spent fuel pool failure caused by very large seismic accelerations (e.g., accelerations that are an order of magnitude higher than the plant's design basis), were it to occur, would preferentially occur at the bottom of the pool wall. The failure would be oriented such that the associated tear in the spent fuel pool liner would potentially occur at an elevation above the rack baseplate. In terms of propagating effects, the immediate implication is the flooding of areas that surround the backside of the pool wall. Much of this flooded area does not contain instrumentation or other equipment, and does have floor drains. If the drains are not able to keep up with the water flow, the potential exists for the failure of doors leading to internal flooding in areas that contain instrumentation and accident mitigation equipment. This also has the potential to affect both reactor and spent fuel pool accident management actions. In this case, a simplified SFP MELCOR model has been developed to aid in the tracking of conditions within and around the SFP, prior to significant fuel uncovery (at which point a more detailed MELCOR model is employed). These inter-dependencies from a structural failure and physical layout perspective represent important considerations for the integrated site risk analysis.

3 SEVERE ACCIDENT PHENOMENA

MELCOR 2.1 is being used to support the deterministic accident progression modeling in the Vogtle project. MELCOR is a fully integrated, system-level computer code that models the progression of severe accidents in light-water reactor nuclear power plants. MELCOR development is led by Sandia National Laboratories under NRC sponsorship, and is the successor to the Source Term Code package. A broad spectrum of severe accident phenomena in both boiling and pressurized water reactors is treated in MELCOR in a unified framework. These include thermal-hydraulic response in the reactor coolant system, reactor cavity, containment, and confinement buildings; core heatup, degradation, and relocation; core-concrete attack; hydrogen and other combustible gas production, transport, and combustion; and fission product release and transport behavior. In some cases, MELCOR results are used as boundary conditions to standalone tools to investigate specific phenomena (e.g., detonation).

In the Vogtle project, MELCOR is being used for confirmatory reactor Level 1 success criteria and accident sequence development activities (leveraging the licensee's existing Level 1 PSA), reactor severe accident progression (Level 2 PSA) activities, and all aspects of the spent fuel pool deterministic accident progression modeling. When convolving the physical characteristics of the Vogtle plant with the strengths and limitations of MELCOR, it was decided to construct and exercise three MELCOR models. The first represents one unit's reactor and containment in detail, along with a simplified treatment of the surrounding structures. The second represents both spent fuel pools and the fuel handling building, in a detailed fashion. The third model represents one containment, both spent fuel pools, and the fuel handling building in a simplified manner that is conducive to fast-running sequence timing calculations prior to fuel melting. As of this writing, the first and third models have been developed and extensively tested. The second model is currently under development.

Beyond the general need for more models and additional modeling flexibilities, the site risk characterization being developed leads to specific situations where the project scope influences accident modeling decisions. The first example is one that was highlighted by both the Fukushima Daiichi accident, as well as the concurrent NRC State-of-the-Art Reactor Consequence Analysis project (Chang et al., 2012), and involves the modeling of hydrogen (and other combustible gas) generation and transport. Customarily, combustible gasses are tracked within the containment as a potential cause of containment failure. However, when they leak out of containment, they pose a challenge to reactor accident management, site accident management, and as a potential means of instigating or exacerbating an accident at another onsite radiological source (e.g., the spent fuel pool). Given the proximity and inter-connectedness of the auxiliary building, fuel handling building, equipment building, and control building, a combustion event in one of these structures has the potential to cause problems in any of the other. That said, these buildings at Vogtle are generally very compartmentalized, which may limit the zone of influence of a combustion event. However, this compartmentalization makes realistic modeling of such events difficult with the current state-of-practice. Here the project is taking a balanced approach. Pathways between the containment and these structures are modeled and the various elevations of the structures are modeled. However, details about compartmentalization within an elevation (e.g., the breakdown in air space volumes, the failure characteristics of intervening doors, etc.) are not modeled. This allows for statements about the

potential for spatial interactions, without investing the significant resources needed to model the issue in a more sophisticated fashion (which might belie the uncertainties in leakage pathways and combustible gas transport modeling).

As another example of where the project is striving for greater realism, MELCOR results are being used directly in the assessment of accident management actions. This will be discussed in more detail later in the paper; here the focus is on the MELCOR modeling. Since the occurrence of a significant event onsite could impact the effectiveness of diagnosis or implementation activities associated with accident management, it is important to account for such events in the context of the human reliability modeling. Specifically, the onset of core damage, the rupture of the vessel, a combustion event, and the failure of containment are each being tracked closely from both the traditional accident release perspective and as a discrete event that could affect the reliability of the ongoing diagnosis and implementation activities. This situation was seen most clearly in the Fukushima accident, in which combustion events interrupted efforts to restore power, damaged hardware (e.g., a vent valve, fire hoses), injured personnel, scattered radiological material which in turn affected access, and caused evacuation of non-essential personnel (INPO, 2011), (Government of Japan, 2011), and (The National Diet of Japan, 2012).

4 SURVIVABILITY OF EQUIPMENT AND INSTRUMENTATION

The purpose of equipment and instrumentation survivability assessment is to ensure that hardware is not being credited when it would in fact be expected to fail due to the environmental conditions to which it is exposed. Instrumentation survivability is critical to the navigation through severe accident management guidelines because plant conditions (as measured through instrumentation) is the means of establishing accident management priorities and weighing the pros and cons of taking a specific action.

The two main tools for establishing the loads on instrumentation and equipment are the scenario characterization (e.g., stuck-open relief valves, interfacing system pipe ruptures) and the deterministic analyses (in this case the aforementioned three-dimensional finite element analysis and MELCOR analysis). The conditions of interest are humidity, static and dynamic pressure, temperature, and radiation. All of these except radiation are readily calculated by MELCOR, though dynamic temperature and pressure estimation requires additional investigation using separate tools for specific phenomena (e.g., detonation). Near-field radiation can also be estimated based on MELCOR outputs (e.g., see Section 4.3.5 of LaChance et al., 2012), however the Vogtle project handles this more qualitatively. Tentatively, ex-containment equipment not exposed to high radiation fields during design-basis accidents (and thus not subjected to high radiation fields during environmental qualification) is assumed to fail if exposed to such conditions during a given scenario (e.g., equipment near an interfacing system pipe rupture unsubmerged break following core damage). The same general treatment is given for humidity.

Temperature and pressure loads are extracted for various plant locations using the MELCOR results of representative scenarios, in order to develop trends. These loads are compared for various phases of the accident (post core-damage) against the environmental qualifications of the plant equipment and instrumentation within the same location, to estimate whether the equipment/instrument's survival is: (i) likely; (ii) not likely; or (iii) indeterminate. In some cases significant interpretation is required (e.g., the environmental qualifications do not explicitly account for dynamic loads caused by combustion events), which increases the likelihood of reaching an indeterminate finding in those circumstances. A list is made of those that are indeterminate for future investigation, depending on their overall contribution to the release category results. As discussed in the previous section, the MELCOR model is capable of calculating environmental conditions in the containment with high resolution (relative to the spatial resolution of equipment qualification information), and low resolution in the surrounding structures.

As an example of where site integration presents new challenges, consider the case of a hydrogen deflagration in the equipment building (the portion of the auxiliary and fuel handling buildings directly adjoining containment), caused by containment penetration leakage. Such an event has the potential to cause high pressures (and temperatures) in this area of the plant. As is typical of PWR designs, the cabling for ac power and dc control for the spent fuel pool cooling pumps is also located in this general area. Thus, hydrogen (or carbon monoxide) emanating from a reactor accident, migrating in to the equipment building from a containment penetration leak, has the potential to damage equipment and instrumentation used for normal, abnormal, and accident SFP cooling. This type of interaction can only be assessed by investigating the containment leakage paths and environmental loads caused by the reactor accidents, and comparing them on a spatial basis, to the equipment and instrument

environmental capacities of potentially-affected equipment.

A second example posits a similar situation, but in reverse. In the unlikely event that an SFP drainage accident goes unterminated (e.g., due to a large seismic event tearing the SFP liner), the resulting oxidation of SFP fuel in a steam environment can produce hydrogen (the same as a reactor accident), resulting in a hydrogen combustion event. Due to the proximity of the SFP to the auxiliary and control buildings, that has the potential to damage instrumentation used in reactor accident management (e.g., containment purge instrumentation used in controlled venting, hydrogen sampling equipment used in assessing the likelihood of in-containment hydrogen combustion events). This has the potential to adversely affect concurrent accident management activities associated with preventing core damage or mitigating fission product release from the reactor.

5 ACCIDENT MANAGEMENT

The final area of focus in this paper is accident management, which is affected by each of the previous areas. Here, the central focus is the plant's Severe Accident Management Guidelines (SAMGs), with other procedures and guidance (e.g., the Extensive Damage Mitigation Guidelines (EDMGs)) playing a supporting role. Again, the MELCOR results are used to characterize the accident. Specifically, output streams have been built in to the MELCOR model to provide all parameters used by the SAMG diagnostic flow chart and severe challenge status tree, as well as the computational aids that accompany the 12 specific guidelines documents. The exceptions are two guideline entry conditions that are based on projected or measured site doses, which for this project are assessed using trial runs of the US NRC's incident response computer code RASCAL (Radiological Assessment System for Consequence AnaLysis). The plant is being studied as it existed in 2012, so the changes presently being made to the US SAMGs (e.g., see LaBarge et al., 2013) do not apply. Similarly, the changes that will be made in response to ongoing NRC rulemaking related to SAMGs (e.g., US NRC, 2013) also do not apply.

The three basic steps of the human reliability analysis being performed to characterize accident management are identification of those actions to be modeled deterministically (based on a finite number of accident progression analyses), the assignment of screening (or simplified) probabilities that the action is not performed, and the development of more detailed probability bases for a subset of these actions. Identification is based on three aspects of the potential action: priority (relying on the hierarchical nature of the Vogtle SAMGs); duration of time that the entrance criteria for that action are met; and habitability. The screening probabilities are based on a combination of considerations related to: (i) instrumentation availability, (ii) priority, (iii) dependency, (iv) duration of entrance conditions being met, (v) the occurrence of significant accident progression events (vessel failure, containment failure, and combustion events), (vi) familiarity relative to emergency operating procedure and EDMG training, and (vii) survivability considerations. The goal is to then extract the trends and insights from these detailed analyses to inform an otherwise experience-based probabilistic modeling of accident management. The approach for the more detailed probability bases for a subset of the actions is under development.

Again, two examples are given where site integration adds complexity to the assessment of this focus area. The first example simply deals with the fact that the current (circa 2012) site accident management infrastructure is predominantly focused on dealing with a single-unit accident. Most notably, there is a single technical support center, a single operations support center, and (in some instances) a single set of supporting accident management equipment. Having multiple TSCs or OSCs is not inherently necessary, and limitations on staffing and equipment are being addressed through ongoing NRC activities. Nevertheless, it is the case that the accident management response involving more than one radiological source on-site will be coupled. To the extent that there may not be sufficient capacity to deal with multiple events completely in parallel, actions for a given source (be it diagnosis or implementation-oriented) will have to be prioritized within the overall site response. In cases where insufficient equipment exists, a decision will be needed to prioritize the deployment of that equipment (e.g., an ac-independent pump) to one radiological source over another. At best, the timing of the accident is such that it can be used in a serial fashion to try and mitigate the concurrent accidents. Given the potential number of instances where competing demands may exist in the site PSA, it may be necessary to take a retrospective approach (i.e., identify important instances of conflicts once results have been obtained without consideration of conflicts).

The second example is one where an accident at one radiological source creates a habitability challenge in an area needed to take a local action to mitigate an accident at another radiological source. For instance, if all cooling is lost to the SFP and the decay heat in the SFP is high, it will eventually begin to boil. This creates a high-humidity,

high-temperature condition within the fuel handling building. Portions of the fuel handling building are connected to the auxiliary and equipment buildings through normal doors. This potentially inhibits access to these areas, and poses operational challenges for preparing individuals to go in to these areas (fire-fighting turnout gear is typically designed for dry, rather than wet, heat). As such, an action that relies on connecting temporary hoses to a fire-header standpipe in order to refill a tank that will be used as part of a reactor mitigation strategy, could be greatly complicated if that stand-pipe is in the affected area of the auxiliary building. In related existing human reliability analysis guidance (Cooper, 2012) this plays in to the assessment of both feasibility and reliability.

6 CONCLUSION

This paper has described the approach being taken in several areas of the reactor and the spent fuel Level 2 PSA portions of the US NRC's Vogtle site PSA project to promote realism in the treatment of the overall site risk. While there are a number of complex challenges associated with analyzing and preparing for multi-unit nuclear power plant accidents, this paper shows the values of applying the existing tool set, in order to anticipate challenges that may arise, so that they can be contemplated and addressed prior to an accident occurring. As risk assessment technology advances, as computational capabilities increase, and in light of the multi-unit event at Fukushima Daiichi, this type of PSA activity is expected to proliferate within the US and elsewhere. Interactions between technical disciplines within the nuclear safety and risk communities at this stage will facilitate the development of more efficient methods. Interactions will also aid in identifying the potential site complexities that are more likely to manifest themselves for given design types, versus those that are simply theoretical.

REFERENCES

Chang et al., *State-of-the-Art Reactor Consequence Analyses (SOARCA) Report*, NUREG-1935, US Nuclear Regulatory Commission, 2012.

Cooper et al., *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines,* NUREG-1921 and EPRI TR-1023001, 2012.

Government of Japan, *Investigation Committee on the Accident at the Fukushima Nuclear Power Stations of Tokyo Electric Power Company,* Interim Report, December 26, 2011.

Institute of Nuclear Power Operations (INPO), *Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station,* INPO 11-005, November 2011.

LaBarge et al., Insights from Development of the Combined PWR SAMG, ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Columbia, SC, September 22–26, 2013.

LaChance et al., *Discrete Dynamic Probabilistic Risk Assessment Model Development and Application,* SAND2012-9346, Sandia National Laboratories, 2012.

Petti et al., *Effects of Degradation on the Severe Accident Consequences for a PWR Plant with a Reinforced Concrete Containment Vessel,* NUREG/CR-7149, US Nuclear Regulatory Commisison, 2013.

The National Diet of Japan, *The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission,* July 2012.

US NRC, Onsite Emergency Response Capabilities, Proposed Rule, in *Federal Register* Vol. 78, No. 221, 68774–68775, November 15, 2013.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A PSA Level-1 method with repairable components: An application to ASTRID Decay Heat Removal systems

R. Kumar, S. Bechta & P. Kudinov
Nuclear Power Safety, Royal Institute of Technology (KTH), Stockholm, Sweden

F. Curnier, M. Marquès & F. Bertrand
CEA, DEN, DER, Saint-Paul-lez-Durance, France

ABSTRACT: Technological advancements in area of sensor-based online maintenance systems have made the possibility of repairing some failed safety support systems of Nuclear Power Plants (NPP) such as electrical supply, I&C systems, ventilation systems. However, the possibility of repair during accident situation is yet to be included into PSA level-1. Therefore, this paper presents a scheme of PSA level-1 by implementing an integrated method of Repairable Event Tree (RET) and Repairable Fault Tree (RFT) analysis. The Core Damage Frequency (CDF) is calculated from consequence probabilities of the RET. An initiating event of Decay Heat Removal (DHR) systems of ASTRID reactor is analyzed. The proportionate CDFs estimated with repair and without repair have been compared and found that the recoveries can reduce CDF. In sum, this paper attempts to deal with the possibility of repair of some safety systems in PSA and its impacts on CDF of the NPP.

1 INTRODUCTION

Sodium cooled Fast Reactors (SFRs) present the characteristic of the large thermal inertia of its coolant systems and high coolant temperature (Saez 2013, Lee & McCormick 2011). This characteristic promotes usage of passive cooling systems and also allows for relatively long times for cooling recovery (Nayak & Sinha 2007) during reactor accidents. Particularly, the large thermal inertia allows a sufficient grace period or tolerance time for the possibility to recover failed components in a DHR system. This possibility of repair within a tolerable downtime or grace period has been further boosted by recent developments in the area of sensor-based online maintenance. For instance, the tools of online integrated risk monitoring system can detect the problem rapidly and possible repair can be realized within the time window given by the thermal inertia of DHR systems (Hashemian 2011, IAEA: TECDOC 1999). Robotic repair system in highly automated plants can restore the fault that was not possible by human interventions (Thomas 2012). Efforts are going on in the area of maintenance to repair a component without hampering the normal operation of a complex engineering system.

In addition, the possibility of repairing exists for some failed systems supporting safety of nuclear power plants such as electrical supply, I&C systems, ventilation systems. According to lessons learnt from events related to ventilation systems in the French civil nuclear facilities between 2005 and 2010, 80% of the incidents were the combination of unexpected ventilation shutdown and non-compliance of safety requirement related to dynamic confinement (Berne & Brunisso 2012). These incidents can be prevented by proper design and automated repairation systems. Similarly, some faults in electric supply system can be repaired within a short span of time once diagnosed. The faulty equipment can be plugged out and new one can be plugged in without hampering the normal supply after the detection (IAEA: NG-T-3.8 2012). This can be achieved by using state-of-the-art instrumentation and control systems. Recent technologies in supervisory and control systems provide client-server based digital supervision for efficient plant monitoring & operation functions and high performance controller for preservation of system reliability (Yamamori 2000). Additionally, the use of mobile electrical and cooling equipment available at site or nearby regional centers can make possible the real-time repair of failed safety support systems within a grace period.

The reliability problem of decay heat removal system falls into the category of a tolerable downtime reliability problem in which failure of safety barriers are hazardous if the duration of failure exceeds its tolerable grace period determined by

physical time constraint of the system. The safety of such system can be ensured if repair is performed within that grace period. The reliability characteristics of systems with repairable components have already been dealt in several literatures (Kiureghian et al. 2007 & Barlow 1975). An inhomogeneous state graph model based on semi-Markov process has been used to build component model systems with tolerable down times (Becker et al. 1995). To remove the restriction of constant failure and repair rate in the Markov process, a generalized equations have been derived for calculating the time-dependent unavailability, the failure intensity and the distribution of the time to the first undesired event for components with tolerable down time (Vaurio 1997).

The possibility of repair during accident situation is yet to be included into Probabilistic Safety Assessment (PSA). A PSA method Includes Event tree (ET) to generate accident scenario and Fault Tree (FT) used to quantify the probability of failure of the Safety Barrier (SB). In literature, there are some examples in which FT analysis has been done for systems with repair components. A FT analysis of phased mission systems has been performed with repairable and non-repairable components (Vaurio 2001). The other FT models with repairable basic events have been proposed based on renewal intensity principle and inclusion-exclusion methods (Yuge et al. 2012 & Yuge et al. 2013). However, ET analysis of Initiating Events (IE) with repairable SB has not been dealt before. Therefore this paper proposes a scheme of PSA level-1 for systems with repairable components using a simplified combination of Repairable Event Tree (RET) and Repairable Fault Tree (RFT).

The paper has the following structure. Section 2 describes the proposed scheme of PSA level-1 for systems with repairable components. In Section 3, proposed PSA level-1 method is used to calculate CDF for a system with some repairable components. In Section 3, the results of numerical examples are discussed. Finally, Section 4 concludes the work.

2 A SCHEME OF PSA LEVEL-1 WITH REPAIRABLE COMPONENTS

Probabilistic safety assessment level-1 is a systematic method for investigating the transformation of an undesired Initiating Event (IE) into a set of possible outcomes leading to core damage or not and their core damage consequences in the form of Core Damage Frequencies (CDF). In this proposed scheme of PSA, Repairable Event Tree (RET) is constructed for each IE to follow progression of event sequence through several Safety Barrier (SB) systems protecting the core. To evaluate the success or failure of each SB, a Repairable Fault Tree (RFT) is constructed with failures and recoveries of basic events that could result in the steady-state failure of SB systems. The top event probability of RFT is the probability of a branch path. This process is replicated for other branch path until the consequences. Finally, the sum of probabilities of all consequences provides the core damage frequencies.

2.1 *Repairable event tree analysis*

The proposed RET allows the construction of accident sequences after an initiating event with the possibility of repair of failed SB. The failure of repairable SB can be rectified within a grace period and the failed branch in ET may potentially be converted into success branch. The grace period is determined by physical behavior of the SB. The accident progression beyond repairable failed branch is virtually ceased if the restoration time is less than the grace period. Otherwise, it continues by following binary path sequentially through remaining SBs of the safety system. For non-repairable SB, the accident progression follows the binary tree of success and failure branch. Finally, we get the branch consequences defined by de-coupling criteria of the each branch. Figure 1 represents the proposed scheme of a typical RET.

2.1.1 *Notations and assumptions*

The basic assumptions are:

- Multiple SBs respond to the occurrence of IE in sequential manner.
- Grace period depends on impacts of failure sequences of SB systems on the physical behavior of system.
- Repair of failed items begins without any delay and brings failed SB as good as new without hampering the normal operation of other safety systems.
- SBs may be repairable or non-repairable during accident progression.

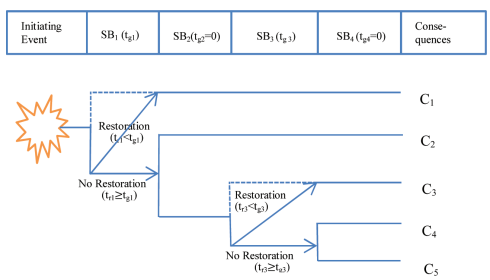


Figure 1. A proposed scheme of repairable event tree.

- Repair time of certain failed SB may be less than or more than its grace period depending on the repair management.

For RET analysis, as shown in Figure 1, the following notations can be taken:

IE = an initiating event harmful to the system
S_i = ith Safety Barrier (SB) along the accident progression
t_{gi} = grace/tolerable time of ith SB to avoid decoupling criteria due to IE and determined based on the deterministic behaviour
t_{ri} = repair time of ith failed SB if repairable
P_{C_k} = Probability of kth consequence C.

2.1.2 *Generation of partially dynamic RET*

Step 1: After occurrence of an IE, check the status of SB, $S_i(i=1, \ldots, l)$;
Step 1.1: If S_i succeeds, create success branch and skip to Step 3.
Step 1.2: If S_i fails, check its reparability. If not repairable, skip to Step 2 otherwise go to Step 1.2.1.
Step 1.2.1: If $t_{ri} < t_{gi}$, turn failed branch into success branch and skip to Step 3.
Step 1.2.2: If $t_{ri} \geq t_{gi}$, create failure branch and skip to Step 2.
Step 2: Move to S_{i+1} and repeat Step 1.
Step 3: Obtain consequence probability P_{C_k} $(k = 1, \ldots, m)$ using RFT analysis.

2.2 *Repairable fault tree analysis*

In general, the fault tree that considers failure and repair of its basic events is termed as Repairable Fault Tree (RFT). In some cases, basic events of RFT may or may not allow repair after failure. In RFT analysis, the outputs of basic events are feed into the immediate upper level through logical gate up to the top level. The failure output of gate can be changed to success output by repair of failed basic event within the tolerable mean down time. Thus the state transition of a gate can be termed renewal process which includes failure rate of gate output and corresponding repair rate (Yuge et al. 2012). The renewal intensities of logical gates are calculated using the mean up time and the mean down time by applying renewal theorem (Barlow 1975, Schneeweiss 1989 & Sherwin 2000).

2.2.1 *Notations and assumptions*

The basic assumptions are:

- The failure and repair of each component are statistically independent and follow exponential distributions.
- Repair is carried out immediately after the occurrence of failure and independent of the repair of other failed components.
- The gates, AND & OR, describe the interactions of state change of components. These two gates are building blocks used to build either a static or a dynamic RFT.
- Steady-State Availability (SSA) of a gate is the ratio of "mean up time" to "mean up time" plus "mean down time" over a long, theoretically infinite, period of all basic events.

For RFT analysis, the following notations can be taken:

λ_i = failure rate of ith component of a gate
μ_i = repair rate of ith component of a gate
P_i = Steady sate failure probability of a SB
A_i = Steady sate availability of a SB
A_{AND}, A_{OR} = SSA of AND & OR gate
v_{AND}, v_{OR} = mean uptime of AND & OR gates
u_{AND}, u_{OR} = mean downtime of AND & OR gates
$\lambda_{AND}, \lambda_{OR}$ = failure rate of AND & OR gates
μ_{AND}, μ_{OR} = repair rate of AND & OR gates

2.2.2 *Steady state probability of logical gates*

Two logical gates, AND & OR, are considered as the building blocks of RFT analysis. The combination of these two gates can be used to model static and dynamic RFT analysis. For example, the Functional Dependency Gate (FDEP), a dynamic gate that includes a trigger event on which other events depends, can be transformed into a static representation of AND & OR gates in RFT analysis.

This paper considers a repairable system's behavior as an alternating renewal process of an up state and down state in which the system failure and the system repair alternate. As the system reaches steady state, the mean time to failure and repair in a cycle also approaches a constant value which does not depend on the system's initial state.

2.2.2.1 AND gate

Steady state availability of an AND gate, as shown in Figure 2a, having n components with failure

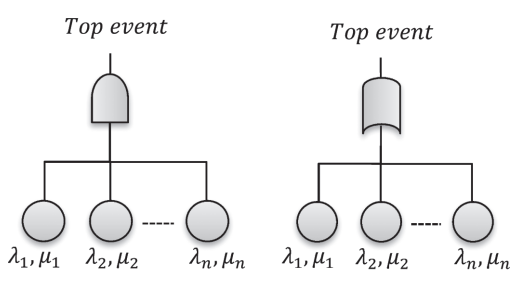


Figure 2. Two basic logical gates for FT analysis.

rate, $\lambda_{i=1,\ldots,n}$ and repair rate, $\mu_{i=1,\ldots,n}$ can be given by following mathematical expressions:

$$A_{AND} = 1 - \Pi_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \mu_i} \quad (1)$$

$$u_{AND} = 1 \Big/ \sum_{i=1}^{n} \mu_i \quad (2)$$

$$v_{AND} = \frac{u_{AND*} A_{AND}}{1 - A_{AND}} \quad (3)$$

2.2.2.2 OR gate

Steady state availability of an OR gate, as shown in Figure 2b, having n components with failure rate, ($\lambda_{i=1,\ldots,n}$ and repair rate, $\mu_{i=1,\ldots,n}$) can be given by following mathematical expressions:

$$A_{OR} = \Pi_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \mu_i} \quad (4)$$

$$v_{OR} = 1 \Big/ \sum_{i=1}^{n} \lambda_i \quad (5)$$

$$u_{OR} = \frac{v_{OR}(1 - A_{OR})}{A_{OR}} \quad (6)$$

2.2.3 *Procedure for analysis of RFT*

Step 1: Construct a RFT based on system configuration and functional logic.

Step 2: Transform dynamic gates, if any, of RFT into a static combination of AND & OR gates.

Step 3: Calculate the equivalent steady state reliability parameters of logical gates such as availability, mean up time, and mean down time using from Eq. (1) to Eq. (6).

Step 4: Determine the equivalent failure rate and repair rate of gates considering the transition of the gate output to be an alternating process as calculated by Step 3.

$$\lambda_{AND/OR} = \frac{1}{u_{AND/OR}} \quad (7)$$

$$\mu_{AND/OR} = \frac{1}{v_{AND/OR}} \quad (8)$$

$$A_{AND/OR} = \frac{v_{AND/OR}}{v_{AND/OR} + u_{AND/OR}} \quad (9)$$

Step 5: Repeat Step 3 and Step 4 for next immediate upper level and up to top level.

Step 6: Estimate the top event probability Pi as a probability of failure by $P_i = 1 - e^{-(\lambda_{AND/OR})t}$ where $\lambda_{AND/OR}$ is the equivalent steady state failure rate of top level gates calculated from Step 4 & 5.

2.3 *Core damage frequency*

The Core Damage Frequency (CDF) can be calculated from the combination of event tree and fault tree analysis. The calculation involves the following mathematical expressions for the proposed scheme of RET shown in Figure 1:

$$P_{C_k} = P(IE) \times (\Pi_{i=1}^{k} P_{i-1})(1 - P_k) \quad (10)$$

$$CDF = \sum_{k=1}^{l+1} P_{C_k} \quad (11)$$

Given, $P_0 = 1$ C_k = the kth consequence ($1 < k < l + 1$), and l is the total number of SB.

3 AN APPLICATION TO PSA STUDIES OF ASTRID DHR SYSTEMS WITH THE POSSIBILITY OF RECOVERY

This paper considered ASTRID DHR systems with an initiating event of primary pump trips to test the proposed scheme of PSA with RET and RFT.

3.1 *ASTRID DHR systems*

The ASTRID consists of four DHR systems namely BCS, RRA, RRB, and RRC, as shown in Figure 3, to deal with decay heat generated in the core and transferred through the hot pool (Saez 2013 & Curnier 2014). In normal conditions, the secondary systems (BCS) transfer the heat from the Intermediate Heat Exchangers (IHX) to the power conversion system. After reactor shutdown, the residual heat can be removed through the secondary loops (BCS) bypassing turbine generator. The use of BCS for residual heat removal is limited to 3 days due to design and operational constraints.

When BCS are not available, the decay heat removal relies on dedicated safety system known

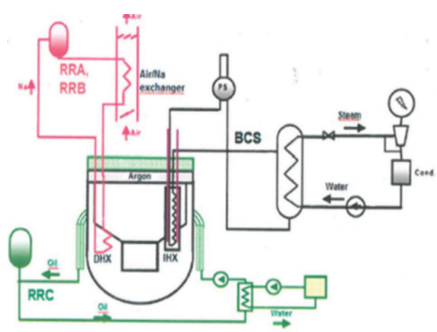


Figure 3. A schematic diagram of DHRS (Curnier et al. 2014).

as RRA, RRB, and RRC (each composed of two redundant trains). Each train of RRA and RRB systems is a Na/Na Decay Heat eXchanger (DHX) and an air/Na exchanger. The two trains of RRB operate in natural convection on both sodium and air sides while RRA trains operate in forced convection with electro-magnetic pumps. Another DHR system, RRC, is also investigated to complement the four DHX circuits. RRC is a diversified system operating through the reactor vault by means of an oil circuit. Figure 3 shows the schematic representation of ASTRID DHR system.

The grace period for repair of failed DHR system depends on the sequences of failure and their effects on the primary sodium temperature rise. A simplified numerical tool has been developed to estimate which transients lead the sodium temperature rise to critical temperature level of 650°C. Figure 4 shows the long term sodium temperature calculations (Gauthe et al. 2013) taking into account of the DHR system operation. In this figure, RVACS is equivalent to RRC of ASTRID DHRSs.

3.2 *An initiating event of primary pump trip*

In the example, an initiating event of ASTRID, trip of a primary pump, is analyzed for the demonstration of introduced scheme of PSA. Figure 5 and Figure 6 show the event tree scheme without repair and with repair of safety barriers. Sodium temperature curve has been calculated for the two sequences of ET and approximate grace periods for each determined for the purpose of performing repair. For the case in which there is no loss of electricity and BCS is working with strength, the grace periods to reach critical temperature and the point of structural damage are found to be 56 hours and 86 hours. For the second case in which there is a loss of electricity and BCS is not working, the grace periods to reach critical temperature and the point of structural damage are found to be 20 hours and 46 hours. If the failure of RRA and

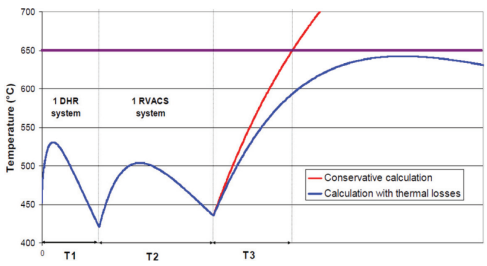


Figure 4. Sodium temperature curve for DHR systems operations (Gauthe et al. 2013).

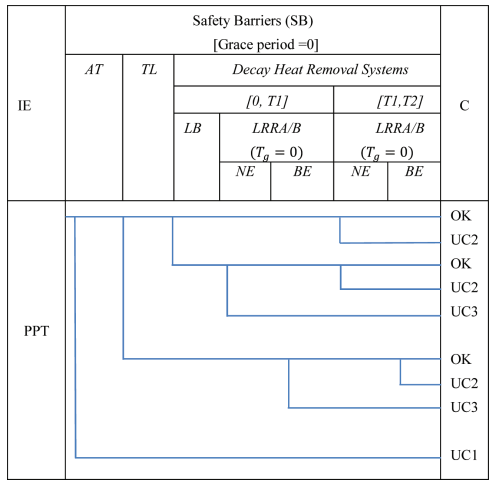


Figure 5. An ET of primary pump failure without repair.

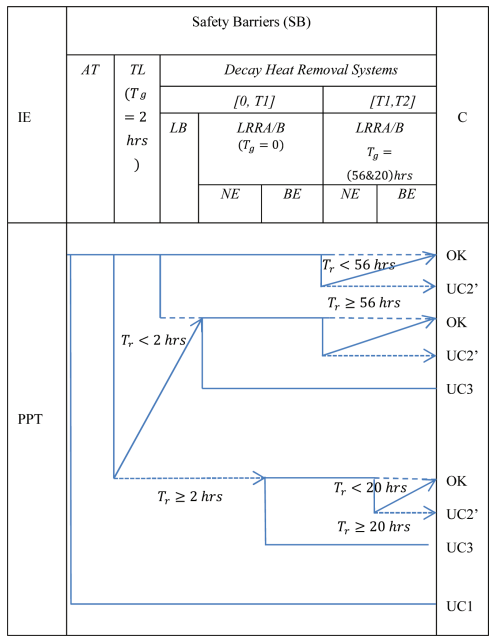


Figure 6. An RET of primary pump failure with some repair.

RRB can be rectified within these grace periods, the number of accidents sequences can lead to the progression towards OK conditions and thus CDF may be reduced significantly.

3.2.1 *Repairable event tree*

Figure 5 & 6 show the event tree of primary pump trip without and with repair possibilities. In Figure 6,

if the repair of failed Electricity loss or RRA/RRB can be done within estimated grace periods, the failure branch can be turned into success branch and failure consequences can be eliminated practically. In Figure 5 & 6, the abbreviations used IE, PPT, AT, TL, LB, LRRA/B, NE, BE, and C, are for initiating event, primary pump trip, automatic shutdown, total loss of electricity, loss of 4 BCS, loss of RRA/B, normal electricity, back-up electricity, and consequences. In Figure 6, grace periods during [T1, T2] for LLR/B are 56 hours for normal electricity and 20 hours for back up electricity.

Table 1 shows the occurrence ratio of UC1, UC2, and UC3 contribution in total CDF due to pump trip event. In case of repair possibility, the probability of consequence, UC2, can be reduced to a lower value after real-time repair, as shown by UC2' in Figure 6. Thus, the CDF can be minimized to a significant value practically. The probability value of UC2' can be calculated by taking into account of modified top event probabilities using RFT analysis. An example of RFT quantification is given in next Section 3.2.2.

The actual value of UC2' is not provided due to the unavailability of repair data of the components of ASTRID DHR. However, the next Section presents a case of RFT analysis of a FT with some recoverable components to estimate the reduction of top event probability.

3.2.2 *Repairable fault tree*

Figure 7 shows the example of a fault tree in which the top event probability or failure probability is calculated as per the procedure of repairable fault tree described in Section 2. In this FT, a dynamic gate, FDEP has been converted into a static tree with a combination of AND gate and OR gate.

Table 2 shows the calculation of top event probability for the FT given in Figure 7. The failure rates and repair rates have been generated randomly for exponential distribution of failure and repair activities. The data set used for [(λ_1,μ_1), (λ_2), (λ_3,μ_3), (λ_4), (λ_5,μ_5), (λ_6,μ_6)] is [(0.16, 0.69), (0.11), (0.22, 0.51), (0.11), (0.05, 0.51), (0.22, 0.11)] per 10^6 hours. For simplification, the time period taken is 10^6 hours. The top event probability for RFT and FT obtained as 0.06 and 0.11, respectively.

Table 1. Contribution of consequences on CDF.

Consequences	Occurrence ratio without repair	Occurrence ratio with repair
UC1	0.14	0.14
UC2	79,89	UC2' (<UC2)
UC3	19.97	19.97
Total CDF	100	UC2' +20.11

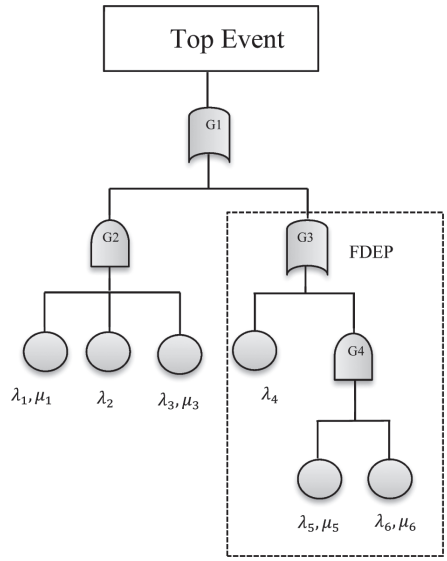


Figure 7. An example of FT with some repairable and non-repairable basic events.

Table 2. RFT results with and without the repair possibility.

	RFT (λ, μ)	FT (λ, $\mu = 0$)
Event probability at G1	$A_{G1} = A_{G2} * A_{G3}$ $v_{G1} = \frac{1}{1/u_{G2} + 1/u_{G3}}$ $u_{G1} = \frac{u_{G1} * (1 - A_{G1})}{A_{G1}}$ $P_{G1} = 1 - e^{-\left\{\frac{1}{u_{G1}}\right\}t}$	$R_{G1} = R_{G2} * R_{G3}$ $P_{G1} = 1 - R_{G1}$
Top event probability (P_{G1})	0.06	0.11

3.3 *Discussion*

The RET & RFT results signify the advantages of repairing failed item within the grace period estimated from the physical response of the item of the DHR system. The conservative grace period can help repair management to accommodate the repair process within the critical time by modifying the design or through introducing innovative design.

From the Table 1, the CDF value, in case of successful recovery of RRA/RRB within the grace period, can be reduced proportionately up to a significant value of the total CDF. In absence of actual calculation of CDF for an initiating event of PPT in Figure 6, the example calculation in

Figure 7 indicates that the top event probability with recovery possibility can be reduced up to 45% with respect to the probability of failure without any repair possibility. Though the reduction in probability failure can vary with the input data of failure rate and repair rate.

However, the future PSA studies of DHR system with repair possibility should consider the common cause failure in RET and RFT analysis to get clearer outline of the benefits. Moreover, the assumptions on exponential failure and repair distribution should be relaxed in RFT quantification as the failure and repair distribution in reality are non-exponential for mechanical and reactive systems.

4 CONCLUSIONS

This paper deals with the PSA level-1studies of a nuclear system with the possibility of recovery of some failed units during accident progressions. A scheme of PSA level-1studies with the combination of partially dynamic repairable event tree and repairable fault tree is introduced. The quantification of repairable fault tree is performed based on the concept of up-time and down-time ratio for steady state system. A case study on the PSA of ASTRID DHR system with an initiating event is performed and found that repair of some units within the grace period during accident progression can reduce the CDF considerably. In future works, the proposed scheme would be implemented using dynamic reliability methods with the considerations of common cause failures and non-linear failure behaviors.

REFERENCES

Barlow, R. & Proschan, F. 1975. *Statistical theory of reliability and life testing probability models*. New York: Rinehart and Winston Inc.

Becker, G. Camarinopoulos,L., & Zioutas, G. 1995. An inhomogeneous state graph model and application for a phased mission and tolerable downtime problem. *Reliability Engineering and System Safety* 49: 51–57.

Berne, M. & Brunisso, A. 2012. Lessons learnt from events relating to ventilation systems occurring between 2005 and 2010 in the French civil nuclear facilities "LUDD". *The 10th International Conference on Industrial Ventilation, Paris, 17–19 September, 2012*. INRS.

Curnier, F. et al. 2014. Preliminary results from PSA studies to support the ASTRID design process. *Proceeding of ICAPP, Charlotte, April 6–9, 2014.* Paper-14205.

Gauthe, P. et al. 2013. Use of simplified PSA studies in support of the ASTRID design process. *Proceedings of FR13, Paris, 4–7 March 2013*. Paper CN-199–221.

Hashemian, H.M. 2011. Online monitoring applications in nuclear power plants. *Progress in nuclear energy* 53: 167–181.

IAEA-TECDOC-1106. 1999. *Living probabilistic safety assessment (LPSA)*. Vienna: International Atomic Energy Agency.

IAEA-NG-T-3.8. Nuclear Energy Series No. 2012. *Electric Grid Reliability and Interface with Nuclear Power Plants*. Vienna: International Atomic Energy Agency.

Kiureghian, A.D., Ditlevsen, O.D., & Song, J. 2007. Availability, reliability, and downtime of systems with repairable components. *Reliability Engineering and System Safety* 92: 231–242.

Lee, J. C. & McCormick, N. J. 2011. *Risk and safety analysis of nuclear systems*. New Jersey: John Wiley & Sons.

Nayak, A.K. & Sinha, R.K. 2007. Role of passive systems in advanced reactors. *Progress in Nuclear Energy* 49: 486–498.

Schneeweiss, W. 1989. *Boolean Functions with Engineering Applications and Computer Programs.* Berlin: Springer.

Sherwin, D.J. 2000. Steady-state series availability. *IEEE Transaction on Reliability* 49(2): 131–132.

Saez, M., et al. 2013. Status of ASTRID nuclear island pre-conceptual design, *Proceedings of FR13, Paris France 4–7 March 2013*. Paper CN-199–127.

Thomas, K.D. 2012. Future Vision for Instrumentation, Information, and Control Modernization. *Third Intern. conf. on nuclear power plant life management (PliM). Salt Lake City, 14–18 May 2012*. IAEA.

Vaurio, J.K. 1997. Reliability characteristics of components and systems with tolerable repair times. *Reliability Engineering and System Safety* 56: 43–52.

Vaurio, J.K. 2001. Fault tree analysis of phased mission systems with repairable and non-repairable components. *Reliability Engineering and System Safety* 74: 169–180.

Yamamori, T., Ichikawa, T., Kawaguchi, S., & Honma, H. 2000. Recent Technologies in Nuclear Power Plant Supervisory and Control Systems. *Hitachi Review* 49 (2): 61–65.

Yuge, T., Tamura, N., & Yanagi, S. 2012. Repairable fault tree analysis using renewal intensities. *Quality Technology & Quantitative Management* 9(3): 231–241.

Yuge, T., Ozeki, S., & Yanagi, S. 2013. Fault tree analysis considering sequence dependence and repairable input events. *Journal of quality in Maintenance Engineering* 19(2): 199–214.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Effect of human factor in the analysis of changes to Limiting Conditions for Operation (LCO) applied to Residual Heat Removal System

S. Martorell, I. Martón, P. Martorell & M. Saiz
Department of Chemical and Nuclear Engineering, Universitat Politècnica de València, València, Spain

ABSTRACT: The objective of this paper is focused on studying the effect of epistemic uncertainty associated to human reliability in the context of the LCO changes. The methodology proposed in RG 1.174 is used in order to assessment and analysis of risk impact of proposed change. An example of application is provided that is centered on the Residual Heat Removal System (RHRS).

1 INTRODUCTION

RG 1.174 (USNRC, 2011) establishes a regulatory framework for the evaluation of risk impact of changes to license basis, RG 1.177 (USNRC, 2011) particularize to change to Technical Specification (TS), in particular Surveillance Requirements (SR) and Limiting Conditions for Operation (LCO). Probabilistic methods have developed to study changes in the TS using Probabilistic Risk Assessment (PRA) results. These regulatory guides establish the need of considering epistemic uncertainties in risk informed decision making, which have addressed in detail in NUREG-1855 (USNRC, 2009).

In addition, NUREG-1764 (USNRC, 2004) provides guidance in order to address human performance aspects of changes to operator actions that are credited for safety, especially those involving changes in the licensing basis of the plant, in the context of the framework depicted in RG 1.174.

The objective of this paper is focused on studying the effect of epistemic uncertainty associated to human reliability in the context of the LCO changes. An example of application is provided that is centered on the Residual Heat Removal system (RHRS).

2 HUMAN RELIABILITY

2.1 *Types of errors*

As part of the PRA for a NPP, a Human Reliability Analysis (HRA) is conducted to determine how human performance affects the safety of the plant. Human Reliability Analysis focuses on estimating Human Error Probability (HEP). With the aim of achieving this, it is necessary to classify the different types of Human Failure Events (HFE) which need to be included in the PRA. According to the ASME PRA-S-2000 (ASME, 2000) one can distinguish between two groups:

- Pre-initiator HFE—human errors committed during actions performed prior to the initiation of an accident, for example, during maintenance or calibration procedures.
- Post-initiator HFE—human errors committed during actions performed in response to an accident initiator

The latter are related to procedural or recovery actions, which contain cognitive tasks (detection, diagnosis), followed by execution tasks (recollection, action).

When an initiator event occurs, the operator performance consists of different phases (Rasmussen, 1986). Human errors in each phase are divided between Errors of Omission (EOO) and Errors of Commission (EOC). Omission errors are related to any human action that should have been performed, but which were not actually carried out. Commission errors are related to human actions that should not be performed, but which in fact are performed (Alvarenga et al. 2011).

The extended Operator Action Tree (OAT) (Kumamoto, 2007) in Figure 1, outlines different human errors for the Post-initiator group

- Slip: The necessary action is recollected correctly, but the action is not performed in time (omission), or is performed incorrectly (commission).
- Lapse: The necessary action is determined by the diagnosis correctly, but the action is not recalled at all (omission), or recalled incorrectly (commission).

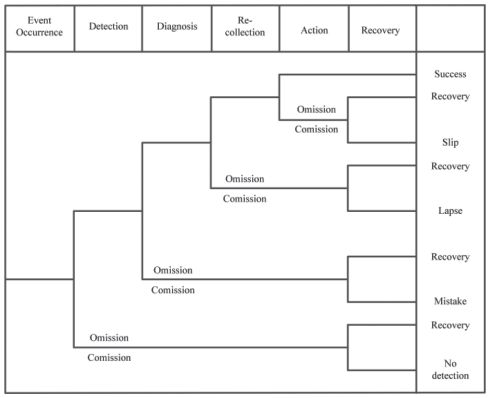


Figure 1. Operator action tree. Extended model (Kumamoto, 2007).

- Mistake: as a result of misdiagnoses, the action is not done (omission), or is done the incorrect action (commission). When the diagnosis does not finish in time, this can be regarded as omission if nothing is done.
- No detection: No action is taken because of a lack of detection (omission), or irrelevant things are performed because of a false detection (commission).

2.2 *HRA techniques*

The birth of the HRA techniques dates back to year 1960. Since mid-80 s several methodologies have been developed, which can be divided into two categories: first and second generation methods (Di Pasquale et al. 2013). Focused on the Post-initiator group, the following review of HR is presented.

First generation methods are strongly influenced by the viewpoint of PRA. These tend to be atomistic in nature, namely, breaking a task into component parts, incorporating the impact of factors such as time pressure, equipment design and stress, known usually as Performance Shaping Factors (PSF). These tools employ the dichotomy omission-commission for human error, and this cognitive model is based on the classification of human behaviour divided into skill-based, rule-based, and knowledge-based (Rasmussen, 1984). Among first generation models, the most remarkable one is Technique for Human Error Rate Prediction (THERP), Swain & Guttmann (1983), which represents the main aspects of these methods generation. Other techniques are Success Likelihood Index Method (SLIM), Embrey et al. (1984); Accident Sequence Evaluation Program (ASEP), Swain (1987); Human Cognitive Reliability model (HCR), Parry et al. (1992). Moreover, The Electric Power Research Institute (EPRI), issued a guidance document for performing HRA known as Systematic Human Action Reliability Procedure (SHARP), Hannaman & Spurgin et al. (1984).

Second generation methods which were first applied in 1990, are based on a cognitive model that is more appropriate to explain human behavior. The focus shifted to the cognitive aspects of humans, the causes of errors rather than their frequency, the study of the interaction of the factors that increase the probability of error, and the interdependencies of the PSF (Felice & Petrillo, 2011). The most representative tools are: Standardized Plant Analysis Risk-Human reliability analysis method (SPAR-H), German et al. (2005); A Technique for Human Error ANAlysis (ATHEANA), NUREG-1624 (2000); as well as Cognitive Reliability and Error Analysis Method (CREAM), Hollnagel (1998).

Finally, the third generation of human reliability methods, started in 2005 and continues today (Di Pasquale et al., 2013), focusing on human performance shaping factors, relations, and dependencies. The only method now defined as third generation is Nuclear Action Reliability Assessment (NARA), Kirwan et al. (2005).

Nowadays, according to NUREG-1792 (USNRC, 2005) and NUREG-1842 (USNRC, 2006), HRA to support PRA uses a mix of techniques from different generations.

3 HEP MODELING

Spanish nuclear power plants have historically used the SHARP methodology to perform HRA. SHARP is not a specific quantification method itself. SHARP is a methodological framework for incorporating human interactions into PRA using a systematic approach. SHARP does not offer explicitly a quantification method, but it gives references to carry out quantification tasks.

Based on the original OAT (Hall et al., 1982), a new structure of the tree is presented in Figure 2, considering the NUREG-1842 (USNRC, 2006).

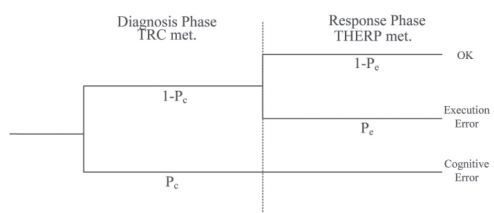


Figure 2. HEP quantification for a post-initiator HFE.

This simplified model decompose the post-initiator HFE in only two phases: diagnosis and response execution phase. As explained in Section 2.1 (Fig. 1), on the one hand the diagnosis phase comprise detection and diagnosis. On the other hand, recollection and action belong to the response execution phase.

HEP quantification can be expressed as:

$$\text{HEP} = P_c + (1 - P_c) P_e \quad (1)$$

where P_c = diagnosis or cognitive error probability, which includes errors due to no detection and mistakes; and P_e = response execution error probability, which includes slips and lapses.

Assuming EOO and EOC on the diagnosis phase as well as response, the most commonly used HRA methods in Spanish plants for post-initiators are:

– Time Reliability Correlation, (TRC), Hall et al. (1983), for the diagnosis phase. The TRC method uses a multivariate lognormal distribution to calculate the probability of an operator successfully responding to a situation within a given time.

This quantification system depends on primarily three factors: available time, whether it is a rule-based action (procedural actions) or a knowledge-based action (non-procedural), and whether the possibility of hesitating exists (Fig. 3).

Furthermore, the TRC method uses the Success Likelihood Indicator (SLI) of the SLIM method (Embrey et al., 1984) to account for the effect of other PSF (i.e. training/experience, workload, stress, procedures, etc.), identified by the experts who are performing the HRA. The influence of the PSF it is reflected as a multiplier which modifies the HEP base value obtained from the curves

– Technique for Human Error Rate Prediction, (THERP), for the response phase. The aim of this methodology is to calculate the probability of the successful performance of the necessary activities for the completion of a task.

THERP involves performing a task analysis to provide a description of performance characteristics of human tasks being analyzed. Results are represented graphically in an HRA event tree, which is a formal representation of the required actions sequence. THERP relies on a large human reliability database containing HEPs, which is based upon both plant data and expert judgments.

As in the diagnosis phase, also THERP applies some PSFs (mainly, experience/training and stress) as a multiplier of the base value.

Among others, these methods are recommended by NUREG-1842 (USNRC, 2006). For this reasons, it will be used both to evaluate the HEP.

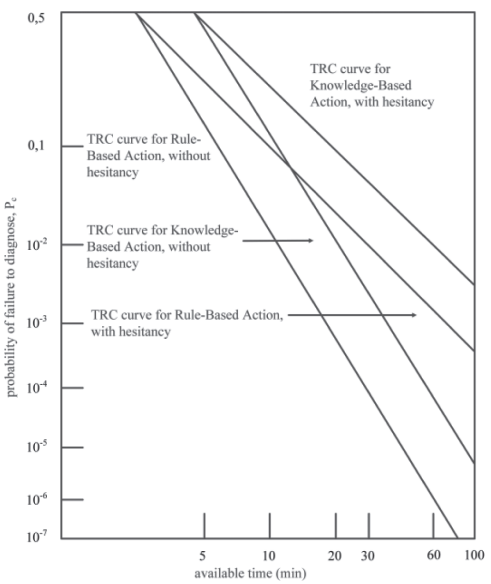


Figure 3. TRC curves for determining P_c.

4 EVALUATION OF RISK IMPACT OF CHANGES TO LIMITING CONDITION OPERATION (LCO)

4.1 *Modeling risk impact*

The PRA model is adopted for risk modeling. RG 1.174 establishes that PRA used should be performed in a manner that is consistent with accepted practices. RG 1.174 states that the quality of a PRA analysis can be measured in terms of its appropriateness with respect to scope, level of detail and technical acceptability. In addition, RG 1.177 requires that the quality of the PRA must be compatible with the safety implications of the TS change being requested and the role the PRA plays in justifying the change.

Thus, the original PRA modeling available should be refined if needed on the basis of the revision of the Capability of the PRA for the particular application to the analysis of changes to Completion Times (CT) and the way in which sources of uncertainty have to be addressed. This should include the identification of not only the usual sources of uncertainty linked to PRA models and data but also the sources of model and parameter uncertainties associated with the assumptions made in CT change evaluation.

RG 1200 (USNRC, 2009) describes one acceptable approach for determining whether the technical adequacy of the PRA used is sufficient to support an application. Specifically, RG 1.200 provides

guidance on the scope of the PRA and the level of detail, among other features.

There are several sources of uncertainty linked to both the inherent capability of the PRA available to quantify the required risk metrics and the additional assumptions made within the PRA application to evaluate the risk impact of the particular CT change.

Random and parametric uncertainties are built into the structure of the PRA model itself. It is this aspect of uncertainty that gives PRA the probabilistic part of its name. They are typically characterized by establishing probability distributions on the parameter values. However, there may be different options or alternatives on how the models should be formulated. Examples include approach to modeling human performance, common-cause failures, ageing of equipment, maintenance effectiveness, etc. This leads to modeling human performance. Human failure events are one of the inputs of the integrated decision-making described in RG 1.174.

4.2 *Revised HRA affected by the change*

In addition, NUREG 1764 provides guidance for use in determining the appropriate level of human factors engineering review of human actions based upon their risk-importance. This guidance uses a graded, risk informed approach that is consistent with Regulatory Guide (RG) 1.174, Rev.1 (USNRC, 2002)

Human actions that are considered more risk-significant receive a detailed review, while those deemed less significant receive a less detailed review. NUREG 1764 uses a two-phased approach to reviewing human actions. Phase 1 is a risk screening and analysis of the affected human actions identified by the licensee to determine their risk-importance and the level of HFE review that is appropriate in Phase 2. The second phase is an HFE review of those human actions that are found to be risk-important.

4.3 *Assessment risk impact*

Risk assessment is proposed by quantifying the usual risk metrics adopted in analyzing CT changes in the literature. It is proposed as a treatment of model and parameter uncertainties based on traditional sensitivity studies and uncertainty assessment respectively, the latter being based on the probabilistic approach for uncertainty formulation and propagation as set by the standard Monte Carlo Sampling technique.

The quantification of the risk impact involves obtaining numerical results from the PRA application, which are then used to calculate the required risk metrics including appropriate treatment of their associated uncertainty.

Basic risk measures applicable in evaluating the risk impact of CT changes are (RG 1.174, USNRC, 2011): 1) Conditional risk given the limiting condition of operation, 2) Incremental conditional risk and 3) Yearly CT risk, which can be formulated, adopting the CDF as a baseline risk measure that can be derived by using a Level 1 PRA, respectively as follows:

$$\Delta CDF_M = CDF_1 - CDF_0 \quad (2)$$

$$ICCDP_M = d_M \cdot \Delta CDF_M \quad (3)$$

$$CDF_M = f_M \cdot ICCDP_M = u_M \cdot \Delta CDF_M \quad (4)$$

Equation 2 represents the condition-specific risk, which represents the increased risk when the equipment is down for maintenance, CDF_1 [year^{-1}], as compared with the reduced risk when the component is known not to be down, CDF_0 [year^{-1}], as compared both with the baseline risk, CDF [year^{-1}]. Equation 3 represents the Incremental Conditional Core Damage Probability ($ICCDP_M$) [dimensionless], also known as single-event CT risk for the downtime, d_M [years], associated with one occurrence of the CT. Equation 4 represents the yearly CT risk associated with the average yearly frequency, f_M [year^{-1}], of occurrences of the CT.

Specifically concerning Technical Specifications, RG 1.177 establishes one more risk metric specific to CT changes for evaluating the risk impact associated with the revised CT, which corresponds to the single-event CT risk after the change, i.e. $ICCDP_M$, which can be derived directly using Equation 3 with the revised downtime, d_M.

The quantification of risk impact of the CT change, adopting the previous risk metrics, has to be performed in such a way that uncertainties are treated in the most appropriate way, which depends on the type of uncertainty. In this paper, special attention is paid to model and parameter uncertainties associated with human performance affected by the LCO change.

4.4 *Analysis of risk impact*

Once the risk impact of the CT change has been assessed as proposed in the previous Section 4.3, it must be compared against the numeric guidelines given in RG 1.174 (see Section 2.4 in RG 1.174). In addition, for CT changes, the risk impact should be compared also against the numerical guidelines presented in Section 2.4 in RG 1.177.

In particular, RG 1.177 proposes adopting two acceptance guidelines for the evaluation of CT changes when using a level 1 PRA. The first one, which is the same acceptance guideline proposed

by RG 1.174 for evaluating whatever change to the LB, uses the baseline CDF and ΔCDF. Thus, the numerical acceptance guidelines are given in RG 1.174 in terms of regions defined in the space of values {CDF, ΔCDF} where the results of the impact on risk of a CT change are placed (see RG 1.174 for a more detailed description of such regions).

RG 1.177 establishes a second acceptance guideline specific for evaluating the risk associated with changes to CT. It corresponds to the single-event CT risk metric assessed after the CT change. It establishes that the licensee has to demonstrate that the CT change only has a small quantitative impact on plant conditional risk. For example, an ICCDP of fewer than 5.0E-07 is considered small for a single CT change using a level 1 PRA. Linked to this second guideline, RG 1.177 establishes the ICCDP contribution should be distributed in time so that any increase in the associated conditional risk is small and within the normal operating background (risk fluctuations) of the plant. Clear indication is provided that ICCDP acceptance guideline of 5.0E-07 is based upon the hypothetical situation in which the subject equipment at a representative plant is out for five hours, causing the CDF of the plant, with an assumed baseline CDF of 1.0E-04 per reactor year, to conditionally increase to 1.0E-03 per reactor year during the five-hour period. Based on the previous paragraph, it seems that a conditional increase to 1.0E-03 per reactor year can be used as a reasonable acceptance guideline for the third risk metric. Based on this second acceptance guideline in RG 1.177, one can outline two regions in the space of values {CDF_1, ICCDP} where the results of the impact on risk of a CT change are placed. The region of acceptable changes is located below the boundary point {1.0E-03, 5.0E-07}.

5 APPLICATION CASE

5.1 *Problem description*

This application case is focused on studying the effect of human factor in the analysis of changes to LCO applied to manual starting of RHRS. The methodology proposed in RG 1.174 is used in order to assess and analyze the risk impact of the proposed change.

As mentioned in the RG 1.174, to quantify the risk impact and compare the results extracted with the acceptance criteria it is necessary to address all the sources of uncertainty. On the one hand, the model uncertainties due to the methodologies chosen for modeling the human performance. On the other hand, the parameter uncertainty in terms of HEP log-normally distributed, which is determined through Thermal-Hydraulic Analysis (THA). Finally, following the results, it is propose a change to LCO, specifically in the Completion Time (CT) change of the RHRS.

The accident sequence corresponding to the loss of the Residual Heat Removal System in Operating Mode 4 (OM 4) during cool down operations has been studied (Table 1). The analysis of this sequence is framed within the Low Power & Shutdown PRA (LPRA) of a typical Pressurized Water Reactor (PWR).

In shutdown conditions, one train of the RHRS removes the residual heat from the core. When the loss of one train of the RHRS is produced, the emergency procedures require checking the availability of the redundant RHR train. If the remaining train is not recovered, an alternative way of cooling the core is using the initial water inventory of the Steam Generators (SG), on the secondary. The Auxiliary Feedwater System (AFWS) prevents the SG from drying out. Next, if it is not possible to remove the heat by means of Steam Generators and pressure and temperature limits to restart the RHRS are exceeded, the "Feed and Bleed" function is required. Charge pumps injecting water can recover the lost inventory and maintain the cooling down as the residual heat is evacuated through a pressurizer relief valve or a RHR safety valve. Finally, in all cases it is necessary to restore the RWST to maintain the plant in a stable conditions in the long run.

5.2 *Modeling scenarios*

The LPRA of a typical PWR describes the event tree showed in Figure 4 for the loss of RHRS at OM 4. To evaluate the effect of parameter uncertainty by means of THA, the analysis is focused on the safety functions, the headers of the event tree, W2 and E1.

Safety function W2 consists of ensuring that the redundant RHR train is operational so as to continue removing the residual heat. This task consists of starting the pump of the RHR remaining train and the support systems required. Recently, in the last LPRA carried out, the possibility of recovery the RHR train in service was not taken into

Table 1. Characteristics of operating mode 4.

Description	Hot shutdown
Reactivity	<0.99
Ptherm	0
Tavg (K)	448 > Tavg > 366
PRCS (Kg/cm^2)	27

*RCS (Reactor coolant system).

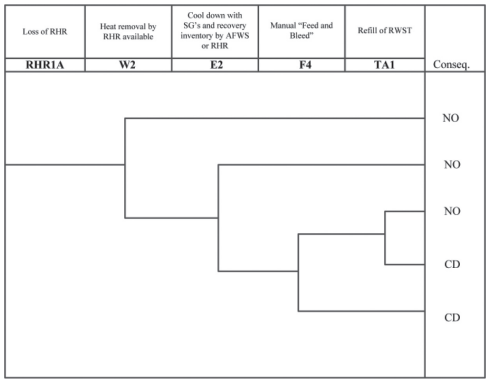


Figure 4. Event tree: loss of RHR at operating mode 4.

account. As a consequence, in OM 4 decreasing power, the pressure and temperature limits to start the standby RHR train exceeded quickly, not leaving any time available for the operator.

The other safety function, E1, states that the SG is an alternative way to evacuate the residual heat. Conservatively, it refers to only two SG whose inventory must be recovered through AFWS motor pumps. This header includes the possibility to restart the RHRS later, provided that the temperature and pressure conditions in the primary allow it.

In spite of what has been explained beforehand, in this application case the possibility of restarting the remaining RHR train is considered. The operator is provided with a specific time window which depends on the moment when the initiator occurs. Moreover, the HEP associated to start the pump is strongly influenced by the available time.

In the first place, the time windows have been extracted, which come from modelling taking into account the time between the start and the end of OM 4. By simulating the accident sequence described, three different time intervals can be considered (Table 2):

- TH1: time to start up the remaining RHR train, between the beginning of OM 4 until the pressure and temperature thresholds of the primary are exceeded to prevent commissioning it.
- TH2: interval to start up the heat removal by means of SG and the AFWS motor pumps to recover the inventory, with the aim of leading the plant to stable conditions.
- TH3: this time window is overlaps with TH2, and appears when the cool down from the SG result in the pressure and temperature conditions which allow to start up again the remaining RHR train.

Therefore, along with TH1 and TH2, the third time window which indicates the available time to evacuate the heat from the RCS through the SG relief valves together with the water injection comes from the AFWS, which is the sum of TH2 + TH3

Table 2. Time windows description.

Time window	Description	Header	System
TH1	Failure of the operator in the RHR restart	W2	RHR
TH2	Failure of the operator in the RHR restart	E1	RHR
TH2 + TH3	Failure of the operator in the start of AFWS motorpumps	E1	AFW

Table 3. HEP obtained for each time window.

Time window	Mean	Standard desviation	95th percentile	5th percentile
TH1	6.170E-01	3.389	1.350E-01	5.228E-03
TH2	3.884E-05	0.233	1.045E-04	6.630E-12
TH2 + TH3	6.642E-04	0.484	3.570E-04	2.322E-09

5.3 *Results of human error probability*

Once the different time windows have been determined by using thermal-hydraulic simulations, these should be evaluated in terms of HEP.

According to the HR modelling explained above, two techniques have been employed to lead the HRA, including it in the LPSA. On the one hand, for the diagnosis phase, the TRC method has been used. The direct influence of the different time windows extracted from thermal hydraulics simulations is directly reflected in the HEP quantification achieved by this technique. On the other hand, the manual or response phase has been carried out by using the THERP method.

The results obtained through HRA showed a HEP log-normally distributed, with the following proper-ties for each time window (Table 3).

5.4 *Assessment of risk impact*

Upon obtaining the HEP distribution for each time window considered, three different cases have been discussed. These are:

- Base case: According to the last LPRA event trees for the accident sequence studied, it is not possible to start the remaining RHR train due to the quick increasing in the RCS temperature and pressure, which surpasses the limits to

Table 4. Impact of the CT change in {CDF_1, ICCDP}.

	CDF_1 (year^{-1})			ICCPD (–)		
Study	Mean	5% perc.	95% perc.	Mean	5% perc.	95% perc.
Base case (CT = 1h)	1.500E-03	3.300E-04	3.730E-03	1.703E-07	3.741E-08	4.238E-07
Sensitivity HEP (CT = 1h)	3.430E-04	1.210E-04	7.930E-04	3.826E-08	1.355E-08	8.849E-08
Sensitivity HEP (CT = 24h)	3.430E-04	1.210E-04	7.930E-04	9.183E-07	3.252E-07	2.124E-06
Sensitivity HEP (CT = 5h)	3.430E-04	1.210E-04	7.930E-04	1.913E-07	6.775E-08	4.425E-07

Table 5. Impact of the CT change in {CDF, ΔCDF}.

	CDF_1 (year^{-1})			ICCPD (–)		
Study	Mean	5% perc.	95% perc.	Mean	5% perc.	95% perc.
Base case (CT = 1h)	7,830E-06	2,300E-06	1,780E-05	2,334E-10	5,125E-11	5,806E-10
Sensitivity HEP (CT = 1h)	7,830E-06	2,300E-06	1,780E-05	5,242E-11	1,856E-11	1,212E-10
Sensitivity HEP (CT = 24h)	7,830E-06	2,300E-06	1,780E-05	1,048E-10	3,712E-11	2,424E-10
Sensitivity HEP (CT = 5h)	7,830E-06	2,300E-06	1,780E-05	1,092E-10	3,867E-11	2,525E-10

recover the system. As a result, the HEP resulting from time windows TH1 and TH2 equals the unit, namely, the failure of the operator is bound to take place. The CT for the base case is 1 hour. This case represents the most conservative estimation.

- Sensitivity HEP case (CT = 1h): it is possible to start the remaining RHR train with a HEP modeling as explained in Section 4.3, using the available times of thermal hydraulics simulations. CT is the same as the base case (CT = 1 hour).
- Sensitivity HEP (CT = 24h): it is the last case, with a CT change consisting of extending it from1 to 24 hours.

The PRA is used to calculate the CDF_1 and CDF_0 basic risk measures, adopting 10^{-13} as the truncation limit. By using Equation 2 it is possible to quantify the conditional risk metric, ΔCDF_M.

Moreover, the maximum allowed downtime has been adopted. 1 or 24 hours for the CT, to measure the second risk metric, $ICCDP_M$ (Eq. 3).

The frequency of entering LCO has been estimated from plant data, i.e. $f_M = 0.00137$ years^{-1}, which is necessary to quantify the yearly CT risk, CDF_M (Eq. 4).

Tables 4 and 5 present the results as a summary of the study for the three different case.

5.5 *Analysis of risk impact*

This section presents the comparison of the results showed in the previous section with acceptance guidelines, reflected on Table 6.

Table 6. Acceptance guidelines.

Risk measure	Risk unit	Treshold	Reference
ΔCDF_M	(1/year^{-1})	1.000E-06	RG 1.174
CDF_M	(1/year^{-1})	1.000E-03	RG 1.174
$ICCDP_M$	(–)	5.000E-07	RG 1.177
CDF_1	(1/year^{-1})	1.000E-03	RG 1.174

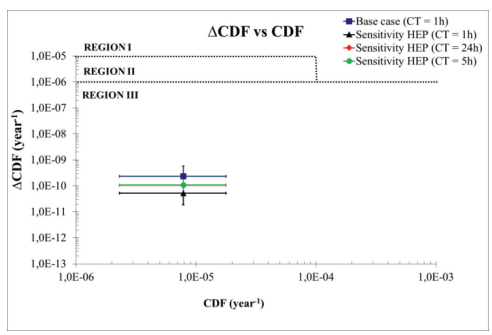


Figure 5. Impact of the CT change in {CDF, ΔCDF}.

In first place, couples {CDF, ΔCDF} have to be placed in the corresponding decision region linked to the first acceptance criterion established in RG 1.174 (USNRC). The mean values for the base case, as well as the sensitivity studies, confirms that the changes remain in the appropriate region, including percentiles (Fig. 5).

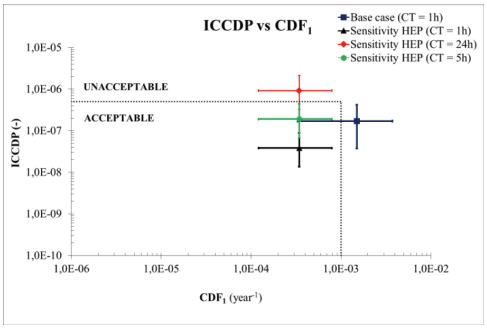


Figure 6. Impact of the CT change in {CDF_1, ICCDP}.

Furthermore, couples {CDF_1, ICCDP} are compared to the second acceptance criterion established in RG 1.177 in a similar way. For the base case, the CDF_1 mean value is out of the appropriate region (Fig. 6). Through modeling human reliability, the sensitivity HEP case satisfies these thresholds, for the mean values, but also for the percentiles. Due to this change, it is possible to extend the CT change, but not up to 24 hours. Using percentile 95%, the most restrictive measure, the maximum CT change which remains the mean value and the percentiles in the appropriate region, as determined by Equation 2:

$$d_M = 5.66h \approx 5h \quad (5)$$

6 CONCLUDING REMARKS

The purpose of this paper is show the effect of uncertainty associated to human reliability in the context of the LCO changes.

An example of application is provided that is centered in a manual starting of Residual Heat Removal System of a typical PWR Nuclear Power Plant. The assumption of more realistic approaches to define the human performance, by means of HRA techniques, allows changes into LCO, which are in the framework of the evaluation of Risk Impact addressed by RG 1.174 and RG 1.177.

The results of the study case shows the improvements following this methodology. Firstly, introducing the HEP distribution, improvements have been achieved in every risk measures. In the case of couples {CDF_1, ICCDP}, including the mean values and the percentiles in the appropriate region which assign the guidelines. Subsequently, is possible to make a change in the LCO of the RHRS, extending the CT from 1 to 5 hours.

Consequently, the paper shows the benefits of the HRA used in the PRA in order to improve and make changes in the LCO of systems, which acquires more importance in critical systems as RHRS.

ACKNOWLEDGMENTS

Authors are grateful to the Spanish Ministry of Science and Innovation for the financial support of this work (Research Project ENE2010/-17449).

REFERENCES

Alvarenga, M.A.B., Frutuoso e Melo, P.F., Fonseca, R.A. 2011. The treatment of commission errors in first generation human reliability analysis methods. *Proc. 2011 International Nuclear Atlantic Conference—INAC 2011 Belo Horizonte, Brazil, 24–28 October 2011*.

American Society of Mechanical Engineers. 2000. *ASME PRA-S–2000. Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, NY.

De Felice, F. , A. Petrillo et al. 2012. Human Reliability Analysis: A review of the state of the art. *IRACST-International Journal of Research in Management & Technology (IJRMT), Vol. 2, No. 1, 2012.*

Di Pasquale V., Iannone R., Miranda S. Riemma S. 2013. An Overview of Human Reliability Analysis Techniques in Manufacturing Operations. In Prof. Massimiliano Schiraldi (ed.), *Operations Management.*

Embrey, D.E., Humphreys, P., Rosa, E.A., Kirwan, B., and Rea. K. 1984. *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*, NUREG/CR-3518, Vols. I & II. Brookhaven National Laboratory. Washington, DC.

Gertman, D.I., Blackman, H.S., Byers, J., Haney, L., Smith, C., and Marble J. *The SPAR-H Method,* NUREG/CR-6883, Idaho National Laboratory. Washington, DC, August 2005.

Hall, R.E, Fragola, J.R. & Wreathall, J. 1982. *Post Event Human Decision Errors: Operator Action Tree/Time reliability Correlation,* NUREG/CR-3010, Brookhaven National Laboratory.

Hannaman, G.W. and Spurgin A.J. 1984. *Systematic Human Action Reliability Procedure*, EPRI NP-3583. Electric Power Research Institute. Monterey, CA.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method—CREAM*. Oxford: Elsevier Science.

Kirwan B., Gibson, H., Kennedy, R., Edmunds, J., Cooksley, G., Umbers. I. 2005. Nuclear action reliability assessment (NARA): a data-based HRA tool. *Safety & Reliability, Vol. 25. No. 2 pp 38–45.*

Kumamoto, H. 2007. *Satisfying Safety Goals by Probabilistic Risk Assessment*. London: Springer.

Parry, G. et al. 1992. *An Approach to the Analysis of Operator Actions in PRA*, EPRI TR-100259, Electric Power Research Institute, Palo Alto, CA.

Rasmussen, J. 1984. Skills, rules, and knowledge: signals, signs and symbols and other distinctions in human performance models. *IEEE Transactions: Systems, Man & Cybernetics SMC* 13:257–267.

Rasmussen, J. 1986. *Information Processing and Human-Machine Interaction: an Approach to Cognitive Engineering* New York: North-Holland.

Swain, A.D. & Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278. Sandia National Laboratories. Washington, DC.

Swain, A.D. 1987. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772. Sandia National Laboratories. Washington, DC.

U.S. Nuclear Regulatory Commission. 2000. *Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA)*. NUREG-1624. Washington, DC.

U.S. Nuclear Regulatory Commission. 2004. *Guidance for the Review of Changes to Human Actions,* NUREG-1764. Washington DC.

U.S. Nuclear Regulatory Commission. 2005. *Good Practices for Implementing Human Reliability Analysis (HRA)*, NUREG-1792. Washington DC.

U.S. Nuclear Regulatory Commission. 2006. *Evaluation of Human Reliability Analysis Methods against Good Practices*. NUREG-1842. Washington, DC.

U.S. Nuclear Regulatory Commission. 2009. *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making*. NUREG 1855, Vol 1. Washington D.C.

U.S. Nuclear Regulatory Commission. 2009. *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, RG 1.200, Revision 2. Washington DC.

U.S. Nuclear Regulatory Commission. 2011. *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, RG 1.174, Revision 2. Washington DC.

U.S. Nuclear Regulatory Commission. 2011. *An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications*, RG 1.177, Revision 1. Washington D.C.

U.S. Nuclear Regulatory Commission. 2011. *An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis*, RG 1.174, Revision 2. Washington DC.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Application of PSA for design optimization of VVER 440/213

P. Picca, F. Pierro & M. Giovannini
Enel Ingegneria and Ricerca S.p.a., Italy

J. Cech & P. Baumeister
Slovenské elektrárne a.s., Slovakia

J. Prochaska
Vuje a.s., Slovakia

ABSTRACT: The work presents the application of PSA as a design tool for VVER 440/213 type plant. The reference PSA model based on the state-of-the-art methodology is presented, with a focus on dependency modeling, human reliability, interface between PSA L1/L2, digital I&C modeling. Its application for risk informed decision making is detailed and the main achievements are outlined.

1 INTRODUCTION

Probabilistic Safety Assessment (PSA) represents an important tool in both design and operation of NPPs (e.g., IAEA-TECDOC-1200 and SSR 2/1). In fact, the probabilistic tools extend traditional deterministic analyses providing a better understanding of accidental sequences characterized by combined failures. Additionally, in parallel to deterministic safety assessment, PSA helps identifying plant vulnerabilities and dependencies between systems, examining different design options and prioritizing improvement areas.

The present work describes the application of PSA as a design tool for VVER 440/213 type plant. The reference power plant is Mochovce 3-4 NPPs, currently under completion in Slovak Republic. The corresponding PSA model is based on the state-of-the-art methodology, which includes both national (BNS I.4.2) and international standards (SSG-3 and SSG-4). In Sect. 3, a review of the methodology is provided with a focus on dependency modeling, human reliability, interface between PSA L1/L2, digital I&C modeling. The application of PSA for risk informed decision making is detailed (Sect. 4) and a selection of results is reported in Sect. 5.

2 SCOPE OF PROBABILISTIC SAFETY ASSESSMENT

The section defines the scope of PSA analysis with reference to national legislation and international standards.

2.1 *Initiating event coverage*

In accordance with the requirement of Slovak Nuclear Regulatory Body in BNS I.4.2, the scope of the probabilistic assessment shall cover a complete set of Postulated Initiating Events (PIE), including internal and external hazards. The definition of internal initiating events is based on the IAEA-TECDOC-749 which defines the list of PIEs to be considered for a VVER type reactor. The list is extended to account for the operational experience in other VVERs in general and mores specifically from the operating fleet in Slovak Republic. The analysis of risky manipulation that can cause a man-induced initiating event is also part of the initiating event definition and is based on operational experience on this VVER type.

2.2 *Plant operational states*

The probabilistic safety assessment is developed as an integral PSA model covering all Plant Operational States (POS) of the plant, covering full power, low power and shutdown states. The reference model considers 15 POSs to include the 6 operational modes combined with the typical configurations of the units during maintenance in shutdown states. The determination of these POSs was carried out on the basis of operational experience on other Slovak NPPs and includes plant-specific peculiarities deriving from detail design development.

2.3 *Core damage and large early releases*

Both level 1 and level 2 PSA are developed in compliance with IAEA SSG-3 and SSG-4 in order to

evaluate the scenarios of fuel damage (PSA L1) and radiological releases (PSA L2). The targets for Core Damage Frequency (CDF) and Large Early Releases (LERF) set in BNS I.4.2 for new reactors are respectively 10^{-5} and 10^{-6} per reactor per year (including internal/external hazards), i.e. one order of magnitude below existing and operating NPPs.

2.4 *System coverage and success criteria*

In accordance with the requirement of Slovak Nuclear Regulatory Body in BNS I.4.2 and general international requirements (SSG-3 and SSG-4), the PSA model shall be a comprehensive description of the NPP. In order to have useful information from PSA, a realistic model of the plant is necessary. To account for all relevant dependencies, all necessary support systems are included in the model such as HVAC, electrical supply and heat sink are included in the PSA model. The success criteria for front-end safety systems are derived based on detailed thermal hydraulic analysis specific for the plant and the fuel under analysis, both for core damage and for radiological releases.

2.5 *Input data*

In accordance with BNS I.4.2 and general international requirement, the PSA model implements as far as possible plant specific data for component/system reliability and frequencies. More specifically, for those components similar to those in operation in Slovak NPPs, the corresponding reliability data are used. For completely new technology components, detailed assessment is carried out (see for instance digital I&C in Sect. 3).

3 METHODOLOGY

The section details various aspects of the methodology chosen for the probabilistic assessment.

3.1 *Fault trees and event trees*

The general approach chosen for the PSA model is the large Fault Tree (FT)/small Event Tree (ET). Using this approach, the ET size is kept in manageable size and it is easier to understand the temporal evolution of the progression of accident. On the other hand, FTs form complex structure to include dependencies between various systems. FTs are composed in a modular form that are then suitably used to model functionality of systems considered in ETs to mitigate consequence of initiating events. Specific POSs conditions influencing operability of systems are implemented by using configuration FTs, which are then incorporated in system/sub-system fault threes. This approach enables the use of a limited number of functional events (top FTs linked to the ETs) to model any specific conditions (with reasonable extent) which facilitates development and maintenance of the model.

3.2 *Dependencies*

The functional link between systems is evaluated via a dependency matrix providing comprehensive overview of system relationships including all relevant support systems, such as: HVAC, electrical supply, heat sink, I&C, etc. The modular form of FT as defined in 3.1 enables easy linking of support system modules to catch particular dependencies.

The dependency between a class of components and/or various redundancies is modeled via classical common cause factors, using international best practices (alpha model) and data implementing operational feedback.

3.3 *PSA L1 and L2 interface*

Interface between PSA L1 and L2 is based on bridge tree approach in order to maintain consistency and integrity of the model. The chosen approach groups all core damage sequence from PSA L1 into characteristic typology, generally known as Core Damage End States (CDES) that reflects specific conditions of particular initiating event as well as possible progression of severe accident. The set of PSA L1 consequences in each CDES belong to the same POS and leads to similar initiating events in PSA L2 (e.g. large LOCA, medium LOCA, SGTR, IFSL or transient) with similar boundary conditions (e.g. availability of safety systems).

The bridge trees for PSA L2 reflects specific conditions inherited from PSA L1. Additionally hardware dedicated for severe accident mitigation and plant specific SAMGs are incorporated. Ad hoc FTs

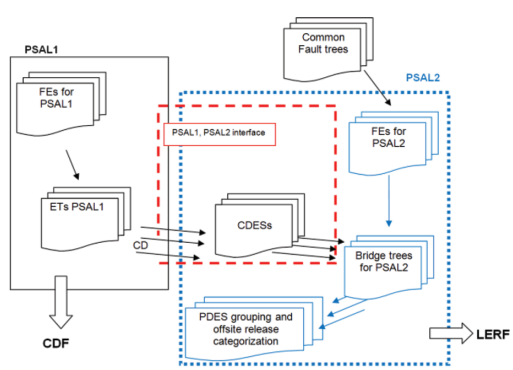


Figure 1. General overview of PSAL1—PSAL2 interface.

are used to model standard PSA L2 activities such as depressurization and cooling of reactor, containment isolation; their modeling is based on the same principles as for FTs of PSA L1.

3.4 *Human reliability*

The list of human action modeled in PSA is defined in accordance with valid EOPs/SAMGs and thermal hydraulic calculation in support for PSA. The evaluation of the human reliability is based on broadly accepted THERP/ASEP methodology (NUREG/CR-1278 and NUREG/CR-4722). The chosen approach is based on critical action concept. Any manual action, evaluated as Compound Human Error Probability (CHEP), can be composed from arbitrary number of tasks that are evaluated as Joint Human Error Probability (JHEP). JHEP is split between diagnosis and manipulation steps that are evaluated as basic human error probabilities. Self-recovery and independent recovery are considered where appropriate and with conservative approach. Recovery actions usually considers at least medium dependency between activities. The uncertainty propagation can be managed analytically as defined in NUREG/CR-1278. As a final verification, CHEPs having high importance are verified by using SPARH methodology as an independent verification.

After evaluation of human reliability, the actions performed by operators in control room are implemented at ET level in PSA L1, enabling a direct evaluation of dependencies between various actions. Activities performed within PSA L2 and by in-situ operators/technicians are implemented at FT level.

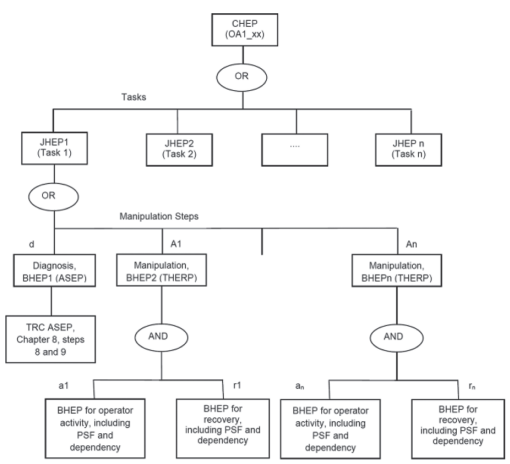


Figure 2. Example of HRA evaluation based on ASEP/THERP.

3.5 *Digital I&C*

The digital I&C considered for the project is new with respect to what is used in previous NPPs in Slovakia. For this reason there is no relevant operational experience from operating Slovak NPPs and the assessment of its reliability is based on the detailed reliability data from relevant suppliers. The reliability of the I&C is assessed based on standard FMEA analysis, followed by a fault tree analysis for reliability estimation. The potential common failure modes are accounted for with suitable common cause factors substantiated with detailed analysis. Input data used for its evaluation are taken from the operational experience of the digital systems operating in other NPPs. Several conservative assumptions (e.g., input reliability data) are considered to ensure that the final result is a bounding estimation.

Due to the complexity of I&C systems its reliability is evaluated by using separate model. Results of this model is then generalized and used as inputs for specific I&C basic events in main model.

3.6 *Symmetric model*

Particular POSs as well specific initiating events can often create asymmetries in the PSA model. The impact of this fact is important mainly for PSA application where for instance it is important to know the impact of the specific unavailability of a component on CDF/LERF. For this reason, the PSA model was adjusted to be symmetric, modeling relevant initiating events as loop-by-loop or system-by-system events.

3.7 *Internal hazard modeling*

The internal hazard modeling in PSA is carried out in accordance with IAEA SSG-3. Following this approach, the evaluation of any considered hazards is divided into various steps:

1. Qualitative screening: based on qualitative criteria, it can be shown that the initiating event cannot impair the safety.
2. Quantitative screening: in case the event has an impact on nuclear safety (either direct or indirect, e.g. through some support system). In such case there can be screened out all initiating events that cumulative contribution to the CDF, which is based on conservative assumptions, does not exceed reasonable threshold. The threshold considered in the framework of this project is set to 10% from safety target for PSA L1.
3. Detailed evaluation: events which cannot screened out based on qualitative and quantitative criteria are consequently included into

detail modeling to estimate their contribution to the CDF.

3.8 *External hazard modeling*

The external hazard modeling in PSA follows indications in IAEA SSG-3. In general, evaluation of external hazards uses similar approach as internal hazards.

In the framework of post-Fukushima stress test activity a thorough design review of the external hazard was carried out, re-assessing the reference level and their corresponding frequency.

4 APPLICATION OF PSA

The application of PSA in various phases of the design of Mochovce 3 and 4 completion project are detailed in the following sections.

4.1 *PSA in the early stage of the project*

The general PSA model was developed in various stages of the project. In preliminary safety analysis report, the model was based on basic design requirement and was used to evaluate the most relevant contributors to CDF and LERF.

PSA was used in this stage mainly as tool for the identification of the risk reduction measures. There were identified several important topic during this stage, such as:

- Hardware modifications (e.g., introduction of new automatic signals to cope with some scenarios in shutdown state where ESFAS actuation can be in maintenance or is disconnected)
- Operational procedure improvement (e.g. operation of water make-up system during cold shutdown to avoid penetration of nitrogen into primary circuit)
- Optimization of technical specifications (e.g. new requirement on availability of safety systems in shutdown states).

4.2 *PSA in detail design development*

During detail design development, the PSA model was regularly updated to reflect the technical modifications implemented in the plant completion. There were several iterations of this process due to successive improvements in several technical areas (e.g., power supply, seismic qualification).

In this phase, PSA was used for:

- Evaluation of design improvements: verification of the impact of a technical solution on the probabilistic figures, including the impact of post-Fukushima stress test measures.
- Definition of selected severe accident scenarios: in accordance with Slovak Decree 430/2011 and relevant international standards (e.g., IAEA SSR 2/1, WENRA Reference Levels), the definition of selected severe accidents shall be carried out also based on probabilistic evaluation.

4.3 *PSA during operation*

During operation, as prescribed in BNS I.4.2 and in relevant international guidelines (e.g., SSG-3 and SSG-4), PSA shall be used for risk-informed decision making purposes, such as safety monitor, in-service inspection optimization and analysis of near-misses. The use of PSA in the evaluation of needs of additional training for critical human action is also envisaged in accordance with BNS I.4.2 and IAEA-TECDOC-1200.

5 MAIN OUTCOMES OF PSA ANALYSIS

The PSA model for MO34 is implemented in Risk Spectrum software. Considering all combinations of POSs and PIEs, the model includes more than one thousand ETs and around two thousands of FTs.

5.1 *Selected results*

The assessment of core damage and large early release frequencies for MO34 NPP demonstrates that safety targets defined in BNS I.4.2 are fulfilled. Additionally, in accordance to general international guidelines (IAEA SSR 2/1, SSG-3, SSG-4), the PSA results show that:

- There is no Minimal Cut Set (MCS) that represents a significant share of the global risk for which additional risk reduction measures would be necessary; for PSA L1, most relevant MCSs are below 3% of the global CDF and for PSA L2 relevant contribution of dominating sequence is below 1%
- Considering the duration of each plant operational states, the risk is well-balanced between power state and shutdown conditions; as it is clear from Figure 3, the improvements due to risk reduction measures makes the hourly risk similar in power and shutdown states
- The risk is reasonably shared between IEs as there is not an initiating event that predominates over the others. As sketched in Figure 4 for power states, the contribution of PIE to CDF is well-balanced. In Figure 5, the rebalancing of the risk before and after design improvements is reported showing their effectiveness to deal with LOCA in shutdown states.

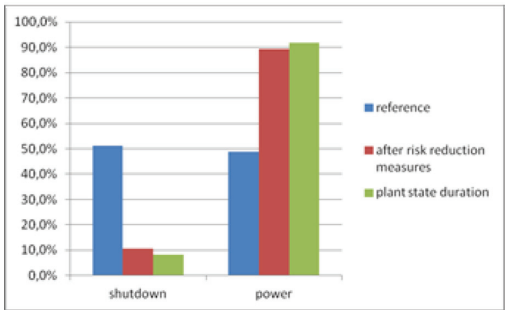


Figure 3. Example of PSA L1 risk repartition between plant operational states.

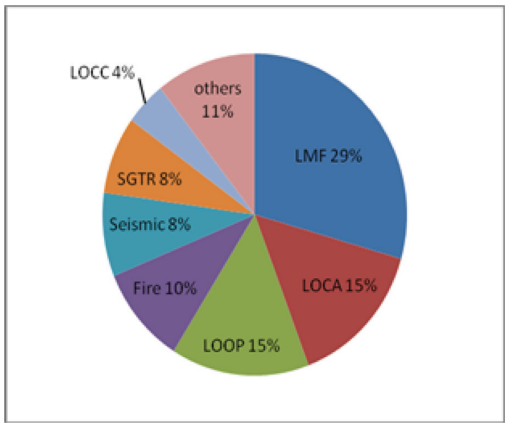
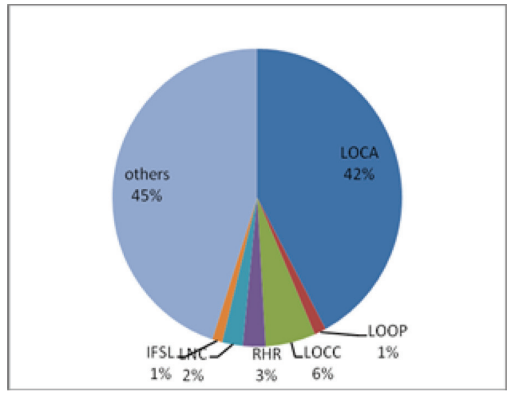
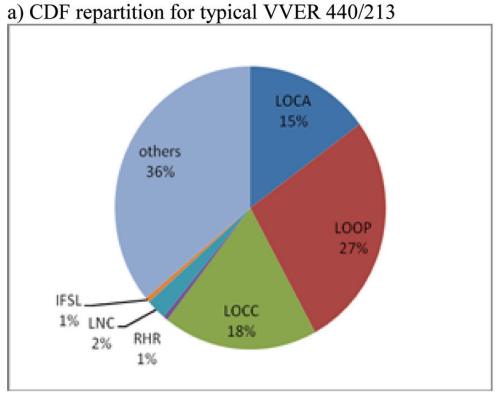


Figure 4. Example of contribution of various IEs to CDF in power state for a typical VVER 440/213 after design improvements and implementation of risk reduction measures.



a) CDF repartition for typical VVER 440/213



b) CDF repartition for after design improvements

Figure 5. Example of contribution of various IEs to CDF in shutdown state (excluding internal and external hazards). The lable "other" refers to the cumulative risk associated to postulated initiating events not directly included in the graphs.

It has to be mentioned that besides the redistribution of the risk, the risk reduction measures (including outcomes of stress test analysis) also helped reducing the global risks and meeting the very challenging targets for new reactors set in BNS I.4.2 (one order of magnitude below existing NPPs). Table 1 provides an estimation of the impact of design improvements (both hardware and operational) on CDF.

Table 1. Estimation of the variation of CDF after design modifications.

State	Δ_{CDF}
Full power	–11%
Shudown	–91%

5.2 *Uncertainty evaluation*

Two types of uncertainties are generally distinguished in PSA analysis, namely epistemic and aleatory uncertainty. Epistemic uncertainty evaluation is assessed during the review of the model and is suitably substantiated in the development and commenting of ETs/FTs. The main assumption of the model are reviewed in the PSA documentation and, where appropriate, a detailed reasoning and/or a sensitivity analysis is provided, with an evaluation of the impact on PSA figures. Aleatory uncertainty is treated by standard means, i.e. associating a probability density function to basic event and propagating uncertainties through the model by means of Monte Carlo simulations. Average error factor ranges between 4 and 5 for power or shutdown state respectively. The main contribution to aleatory uncertainty is due to human-induced events or human actions where the associated

error factor is generally larger due to the inherent variability of the basic events.

6 CONCLUDING REMARKS

In conclusion, general insights from PSA L1 and L2 results show how the implementation of risk reduction measures can be successfully used to meet the stringent probabilistic requirements for new reactors and to reach a well-balanced risk between plant operational states and between initiating events.

REFERENCES

BNS I.4.2-2006, *Requirements for the study of PSA*, 2006.

IAEA-TECDOC-1200, *Applications of Probabilistic Safety Assessment (PSA) for nuclear power plants*, (2001).

IAEA, SSR 2/1, *Safety of Nuclear Power Plants: Design*, 2009.

IAEA, SSG-3, *Development and Application of Level 1—Probabilistic Safety Assessment for Nuclear Power Plants*, April (2010).

IAEA, SSG-4, *Development and Application of Level 2—Probabilistic Safety Assessment for Nuclear Power Plants*, May (2010).

IAEA-TECDOC-749: Generic initiating events for PSA for WWER reactors, (1994).

NUREG/CR-4722, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, (1987).

NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, (1983).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Deriving a distribution for accident severity from an F-N curve

J. Braband
Siemens AG, Braunschweig, Germany

H. Schäbe
TÜV Rheinland, Cologne, Germany

ABSTRACT: In an earlier paper, we studied several approaches for modeling the accumulated severity of railway accidents in a certain time interval with the help of a compound Poisson process. The number of accidents can be modeled with a Homogeneous Poisson Process. The distribution of accident severity, however, has not been studied in detail until now.

F-N curves are frequently used to create a relation between accidents having a severity of a certain level or higher on the one side and an admissible number of accidents on the other side. Often F-N curves are used to create safety targets for collective risks.

In this paper, we show that, when an F-N curve is assumed, a Pareto distribution for the accident severity, i.e. for the jump height of the compound Poisson process, is obtained. Using standard statistical methods, we derive a procedure for statistical estimation of the parameters of the jump height. We give one and two-sample tests for testing equality with a given distribution of accident severities or testing equality of two distributions of severity. Moreover, we provide a test for checking whether the hypothesis of the distribution of accident severities holds.

Another application of this approach is the derivation of typical accident categories for use in semi-quantitative risk analyses. We use accident data collected by the European railways over the last decade as a basis for illustrative examples.

1 INTRODUCTION

In an earlier paper, we modeled the accident statistics of railways with the help of a Compound Poisson Process (CPP), see Braband & Schäbe (2011), Braband & Schäbe (2013b).

We first give a generic definition of the problem. We assume a CPP with N_t depicting the number of accidents until time t and $S_1, S_2, \ldots$ an independent, identically distributed (i.i.d.) sequence of random variables describing the severity of the accidents. The sum of all accident severities until time t, $X(t)$ is then distributed as

$$X(t) = \sum_{i=1}^{N_t} S_i. \tag{1}$$

From Birolini (2007), we also know the exact distribution if the jumps are independent and identically distributed (i.i.d.)

$$P\big(X(t) \le x\big) = 1 - F_1(t) + \sum_{n=1}^{\infty} G_n(x)\big(F_n(t) - F_{n+1}(t)\big), \tag{2}$$

where F_i and G_i denote the i-fold convolution of the distribution functions of the time between events and the severity, respectively. The distribution F_n can be motivated to be an Erlang distribution, which is motivated by the homogenous Poisson process describing the number of accidents.

In this paper, we motivate the choice of a distribution G for the jump height of the CPP, i.e. the accident severity. In section 2, we derive this distribution from the F-N curve. It turns out to be a Pareto distribution. In section 3, we give basic statistical information on parameter estimation and testing. This is straightforward, since the Pareto distribution is well known. In section 4, we provide an illustrative example.

2 DERIVATION OF THE DISTRIBUTION

Individual risk is simply the predicted frequency of the undesired outcome. Societal risk takes account of both the severity of the range of possible outcomes and the frequency at which they each are predicted to occur. It is usually presented as a two-dimensional relationship between frequency and cumulative severity of outcome, called an F-N curve. The F-N curve is frequently used for giving target values for maximal numbers of accidents (say F) with N or more accidents. The F-N

curve is used to provide group risks, see e.g. Proske (2008). F-N curves have also been computed from statistics, see e.g. Braband & Schäbe (2011) or used for the definition of risk targets, as e.g. in Rijswaterstaat (2002).

The F-N curve is a curve defined by

$$F = A*Na, \tag{3}$$

where A and a are parameters. F is the "frequency", i.e. the maximal tolerable number for accidents with N or more fatalities. The number of fatalities, N, is mainly measured in FWSI. This stands for Fatalities and Weighted Serious Injuries and has been defined by the European Union, see EC (2009). FWSI values are a sum of fatalities and the number of serious injuries multiplied by 0.1. In this manner, serious injuries are also taken into account. The factor 0.1 arises from experience that normally in accidents about 10 serious injuries occur as frequently as one fatality. Sometimes also equivalent fatalities are used, which take also into account slight injuries with a factor of 0.01. However, the definition of slight injuries is too different at least in the railway sector to allow it to be used in comparisons. Therefore, the smallest severity of an accident in terms of FWSI is 0.1.

Now, from (1) one can derive the probability that an accident occurs with more than s fatalities. It is just

$$Pr(S > s) = A*sa/A*0.1a = B*sa, \text{ with } s \geq 0.1 \tag{4}$$

where B is a new constant. Equation (2) presents the survival function of the distribution function of accident severities with severities of at least 0.1. Therefore, (2) is a conditional distribution function.

Obviously, the probability density of this survival function reads

$$f(s) = a*B*sa - 1 = a*sa - 1/0.1° \text{ for } s \geq 0.1 \tag{5}$$

and zero otherwise.

This is the Pareto distribution, which can be found in standard textbooks, such as in Johnson, Kotz & Balakrishnan (1994). This distribution is typical for the distribution of income.

3 ESTIMATION AND TESTING

When considering the distribution function (3), it is obvious that only one parameter needs to be estimated. The second parameter B is fixed by the requirement that only accidents with at least 0.1 FWSI will be regarded. The estimator of a is given in Johnson & et (1994) as

$$\hat{a} = \log(G/0.1) - 1, \tag{6}$$

where G is the geometric mean of the sample,

$$G = (\Pi\, S_i)^{1/n}, \tag{7}$$

where $\{S_i,\ i = 1, .. n\}$ is a sample of observed accident severity values. The product Π runs over I from 1 to n.

Johnson et al. (1994) mention that $2na/\hat{a}$ has a chi-squared distribution with $2(n - 1)$ degrees of freedom. This property can be used to test whether the sample comes from a certain population with given value a of the shape parameter. As soon as the inequalities

$$\chi^2(2(n-1); 1-\alpha/2) < 2na/\hat{a} < \chi^2(2(n-1); \alpha/2) \tag{8}$$

are fulfilled, one would accept the hypothesis that the sample comes from a population with shape parameter a. Here $\chi^2(2(n - 1);1 - \alpha/2)$ denotes a standard chi-square quantile from the table of the chi-square distribution. With α we denote an error of the first kind of the test.

The result (6) can also be used to provide confidence intervals on a. So the parameter a would lie with probability $1 - \alpha$ within a two-sided confidence interval given by

$$[\hat{a}\chi^2(2(n-1);1-\alpha/2)/(2n);\ \hat{a}\chi^2(2(n-1);1-\alpha/2)/(2n)] \tag{9}$$

Based on this property, it is also possible to construct a two sample test. Assume that $\hat{a}_1$ and $\hat{a}_2$ are estimators from two samples of size n_1 and n_2, respectively. Then,

$$T = (n1\hat{a}2)/(n2\hat{a}1) \tag{10}$$

has an F-distribution with $(2n_1;\ 2n_2)$ degrees of freedom. So, the test would accept the hypothesis of equality of the parameters a if

$$F(2n_1;\ 2n_2;\ \alpha/2) < T < F(2n_1;\ 2n_2;\ 1 - \alpha/2). \tag{11}$$

Another question is, whether the hypothesis holds that a sample of accident severities is distributed according to the Pareto model. Although the F-N curve is widely used for providing target values and sometimes also fits of data have been carried out, this does not prove whether the data really follow a Pareto distribution.

The Pareto distribution is closely connected to the exponential distribution.

If S has a Pareto distribution

$$F(s) = 1 - (s_0/s)^a, \tag{12}$$

then S can be expressed as

$$S = s_0\exp(X_0/a) \tag{13}$$

where X_0 is a standard exponentially distributed variable, see Johnson et al. (1994). Therefore,

$$a^*\ln(S/s_0) \tag{14}$$

has a standard exponential distribution. In the model described, s_0 is known to be 0.1. If one now tests the sample

$$\{X_i = \ln(S_i/0.1),\ i = 1, .., n\} \tag{15}$$

for exponentiality (i.e. with arbitrary mean of the exponential distribution), one has tested the sample $\{S_i,\ i = 1, .., n\}$ for the Pareto distribution.

A study of Ascher (1990) has shown that the score test proposed by Cox and Oakes (1984) seem to be the best one for testing exponentiality against general alternatives. In fact, the Cox and Oakes test is a score test; it tests in the Weibull model for the shape parameter being 1. That means exponentiality since a Weibull distribution with shape parameter one is an exponential distribution.

This test is easily computed. The score statistic is defined as

$$U = n + \Sigma \log(X_i) - n\, \Sigma X_i \log(X_i)/\Sigma X_i, \tag{16}$$

where the sum Σ runs over i from 1 to n. U is an asymptotically normal with mean zero and variance

$$(I_{aa} - I_a\lambda^2/I\lambda\lambda), \tag{17}$$

where

$$I_{aa} = n + \Sigma(\lambda X_i(\log(\lambda X_i)^2, \tag{18}$$

$$I_a\lambda = \Sigma X_i \log(\lambda X_i), \tag{19}$$

$$I\lambda\lambda = n/\lambda^2 \tag{20}$$

$$\lambda = n/\Sigma X_i. \tag{21}$$

Since the X_i are easily obtained from the S_i, the application of this test is straightforward.

4 EXAMPLE

Accident data from Switzerland for Swiss railway accidents have been used. The data have been collected over the last decade. Using formula (6) for accidents with an FWSI value of 0.1 or more, the shape parameter a has been estimated to be 1.8. This is in the region of 1.5 to 2, which is frequently used (see e.g. Braband and Schäbe (2011), and to the value of two, used in Rijkswaterstaat (2002) for providing target data for group risks.

By computing the confidence interval for 95% coverage, i.e. for $\alpha = 1\%$, we arrive with the help of (9) at the interval [1.60; 2.03].

A statistical test carried out for the value "2" would therefore accept the hypothesis. This is due to the fact that, for one sample test, confidence intervals for a parameter can be used for testing, the computations being the same as for obtaining critical values for the test statistic.

The test with the test statistics U in (16) cannot be applied since the data consist of many values with $X_i = 0$, caused by the fact that there are many values with $S_i = 0.1$. Also, the severity values of accidents can sometimes be imprecise, especially when talking about seriously injured persons. This is simply caused by the process of data collection. We apply another method. We just compare the counts of accidents in the following four classes

[0.1; 0,2], [0,2; 1.5], [1.5, 2.5] and [2.5, ∞]

with the computed values for these intervals. This is done with the help of the chi-square statistic

$$H = \Sigma\, (O_k - E_k)^2/E_k. \tag{22}$$

Here, O_k and E_k denote the observed and expected numbers of events in the k-th class. H is known to have a chi-square distribution with $r - 1$ degrees of freedom. With r, the number of calluses is denoted and since one parameter is estimated from the same sample, the number of degrees of freedom is reduced. The computed test statistics is 97, which largely exceeds the critical value of 11.3 for a 1% error of the first kind. This is caused by the fact that in the smallest class, a smaller number of events has been counted that expected according to the parametric model.

5 OUTLOOK

A closer look at the data reveals, however, that while the general decaying shape suggests a Pareto distribution, there might be a better fit when approximating the distribution by a weighted sum of discrete random variables. To intensify this affect we regard Fatalities and Weighted Injuries (FWI), which are often defined by

FWI = <number of fatalities>
+ <number of serious injuries>/10
+ <number of light injuries>/100

Figure 1 shows an example based on a simulation, where the number of fatalities, serious injuries and slight injuries have been drawn for each accident as realizations of independent Poisson random numbers. The dominating number of accidents with FWI zero has been truncated.

Like in real accident data, the typical distribution shape emerges with a kind of step-like structure

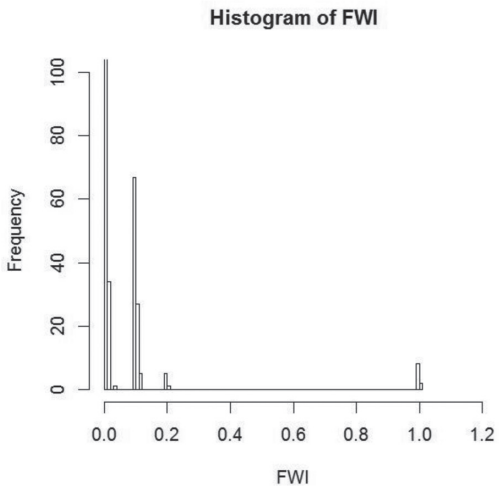


Figure 1. Typical sample FWI distribution.

beginning at 0, 0.1, 0.2 and 1.0. This is due to the fact that the majority of accidents affects only a small number of people, often only one. In practice, however, the number of fatalities, serious injuries and slight injuries would be dependent.

6 CONCLUSIONS

In this paper, we have given a theoretically well founded derivation of the distribution for the jump height of the compound Poisson process which can be used to describe counts of railway accidents. The distribution has been derived from the well-known F-N curve and turns out to be the Pareto distribution. We have used standard statistical textbooks to provide estimation and testing methods. In a practical example, we have derived the shape parameter that falls into an interval for parameters usually used for F-N curves. The distribution type, however, may in fact be more complex due to discretisation effects due the definition of FWI. This needs further research in order to come up with a distribution which fits the data and allows the derivation of optimal tests.

ACKNOWLEDGEMENT

The authors wish to thank the BAV, Bern and especially Hanns Meuli and Roman Slovák, Franziska Rexin from TU Braunschweig, and Rainer Beck, DB AG in Munich, for interesting discussions and giving the possibility to use their data on rail accidents.

REFERENCES

Ascher, S. 1990. *A survey of test for exponentiality*, Commun Statist. Meth. 19(5), 1811–1825.

Braband, J., Schäbe, H. 2011. *Statistical analysis of railway safety performanc, in the European Union*, ESREL (2011), Proceedings, Advances in Safety, Reliability and Risk Management, pp. 1783–1787.

Braband, J. Schäbe, 2013. *Assessment of national reference values for railway safety: a statistical treatment,* Journal of Risk and Reliability, 227(4) 405–410.

Braband, J., Schäbe, H., 2013. *Comparison of compound Poisson processes as a general approach towards efficient evaluation of railway safety*, Proceedings of the ESREL (2013), Safety, Reliability and Risk Analysis: Beyond the Horizon—Steenbergen et al. (Eds) 2014 Taylor & Francis Group, London, ISBN 978-1-138-00123-7), pp. 1297–1302.

Cox, D.R, Oakes, D. 1984. *Analysis of Survival Data*, Chapman & Hall, London New York.

EC 2009. *Commission Decision of 5 June 200) on the adaption of a common safety method for assessment of achievement of safety targets, as referred to in Article 6 of Directive 2004/49/EC of the European Parliament and the Council*; 2009/460/EC.

European Commission, 2009. *Commission Decision of 5 June 2009 on the adoption of a common safety method for assessment of achievement of safety targets, as referred to in Article 6 of Directive 2004/49/EC of the European Parliament and of the Council.*

European Commission, 2010. *Commission Decision of 19 July 2010 on Common Safety Targets as referred to in Article 7 of Directive 2004/49/EC of the European Parliament and of the Council.*

Johnson, N.L. Kotz, S., Balakrishnan, N. Continuous 1994. Univariate Distributions Vol. 1, 2nd Edition, J. Wiley, New York, Chichester, Brisbane, Toronto, Singapore.

Proske, D., 2008. *Catalogue of Risks*, Springer.

Rijkswaterstaat, (2002), *Normdocument veiligheid Lightrail*, v 5.0.

Sachs, L., 2003. *Angewandte Statistik*, Springer, Heidelberg.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Geospatial modelling of rail safety hazards

D.J.K. Griffin
Rail Safety and Standards Board, London, UK

ABSTRACT: RSSB has developed geospatial models (GeoSRM) of rail safety hazards across the mainline rail network in Great Britain (GB). The GeoSRM, shows how risk is distributed across the network, rather than generating a single national estimate for each type of hazard. The GeoSRM is web-based allowing users to submit queries on the risk level for specified regions, routes, hazard types, train operators, services or classes of rolling stock, and display the risk levels overlaid on a map. The pilot model of the GeoSRM is based around three hazardous events: station slips, trips & falls, railway suicides and train derailments. Station slips, trips & falls and suicides are modelled statistically with generalised linear models, taking into account geospatial variation in population characteristics and station properties. Whilst describing the GeoSRM framework in general, this paper focusses on the modelling of train derailments. This takes into consideration the geospatial variation in the frequency of derailments, the probability of derailment escalation and the consequence of any resulting derailment. Derailment causes and escalation probabilities have been linked to the underlying assets that could lead to a derailment e.g. linking derailment due to landslip to presence of cuttings. The paper shows how geospatial risk models can be developed and applied within a railway environment, and how models of this type could be used to inform decision making.

1 INTRODUCTION

Safety performance of the mainline railways in Great Britain has shown significant year-on-year improvements. While there was an average of 18.4 fatalities to passengers and workforce in the five years leading up to 1996/97, in the five years leading up to 2010/11 this figure had reduced to 9.0. This is a reduction of 51%, and is even more significant when it is considered that passenger kilometres have increased by 57% over the same period.

At the same time as safety performance has been improving, the overall cost of the rail industry has been increasing. Since 1996/97 rail industry costs have increased by 60% (at constant prices). Although some of this is a result of the increased train kilometres, it has been reported (McNulty 2011) that there is a 30% efficiency gap between the current industry costs and comparable railways elsewhere in Europe.

A certain proportion of this efficiency gap has been attributed to standards being overly conservative with respect to safety. Where standards have been changed, they often replace the requirement for a risk control with a requirement for a risk assessment to determine if the control is necessary in the given situation. By being able to identify low risk locations or routes and areas where the risk controls deliver little or no additional safety benefit, the industry could achieve significant cost and efficiency savings through the removal of unnecessary/over-prescriptive control measures. It is also increasingly difficult to introduce additional controls to reduce risk that are reasonably practicable, and in many cases they can only be justified for key high risk locations or routes (Griffin & Holloway 2012).

The GB rail industry currently relies on RSSB's Safety Risk Model (SRM) for much of its safety analysis (Dennis & Somaiya 2004). The SRM generates a national estimate of risk for each type of hazard on the network, but it does not show how the risk from these hazards is distributed across the network.

The GeoSRM is a new map-based tool for showing how risk is distributed across the rail network. To demonstrate the concept, the GeoSRM has been piloted on the Wessex route in England. The Wessex route operates a mix of services, whilst dominated by commuter services into London Waterloo station, but also longer distance services to Southampton, Bournemouth, Exeter and Portsmouth.

The pilot also considers just three distinct areas of risk:

- Train derailments
- Suicides
- Passenger slips, trips and falls at stations

These risk areas offer a varied range of hazards that depend on a wide range of spatially varying factors.

The modelling of train derailments follows similar work undertaken by Marsh & Bearfield (2008). It takes into consideration the geospatial variation in both the frequency of derailments and the consequence of any resulting derailment. Derailment causes have been linked to the underlying assets that could lead to a derailment e.g. linking derailment due to landslip to presence of cuttings. The escalation mechanisms modelled include carriages falling on their side, structural collapse and secondary collision. The geospatial factors that affect the event escalation include the train frequency on adjacent lines, presence of structures, switches and crossings and embankments.

The modelling of railway suicides is statistically based, and split into suicides at stations, suicides at level crossings and suicides at other locations. The model considers the size of the local population, characteristics of the local population such as gender, age profile, income and employment levels, health deprivation and disability, education, housing and crime. The model also takes into account train frequency and speed and features of the station such as ticket barriers, presence of staff and CCTV.

Passenger slip, trips & falls are also statistically based with a generalised linear model, accounting for the exposure of passengers to the different parts of the station such as platform, stairs, escalators and concourse. The model takes into account the mix of different types of passenger and locations with particular risk issues, e.g. high use by passengers with luggage, passengers under the influence of alcohol, or propensity for rushing.

This paper focusses on the modelling of train derailments. The next section of the paper deals with the principle of the GeoSRM model and the design decision that have to be made to make the modelling tractable. Sections 3 and 4 deal with the derailment model and the means of calculation, whilst section 5 describes the web interface for the model.

2 GeoSRM PRINCIPLE

The basic principle underlying the GeoSRM is that all risk models are pre-calculated. This enables the web querying to operate with a reasonable degree of responsiveness, as the model is not being recalculated each time the user re-queries the data. There are four basic components, the web interface, the results database, the GeoSRM database and the risk models.

The web interface allows users of the GeoSRM in train operating companies or infrastructure managers to log in to a web based tool. From this tool they can view risk results on a map, create queries and filter the results.

The results database stores all the pre-calculated results from the risk models. The web interface queries this database to generate the data to be displayed. The database contains aggregated data layers so that geospatially coarser datasets are queried where appropriate, depending on the zoom-level of the map.

The GeoSRM database stores all the data required to run the risk models. It is essentially a data warehouse with data having been sourced from a varied range of individual databases. It consists of:

- Track data, defining the track centre line of the network.
- Asset data defining the position of key risk related assets on the railway
- Train data defining the timetable and the movement of the trains across the network
- Safety data defining the rates of precursors, escalation probabilities and event data.

Of the three risk models, the suicides and passenger slips, trips & falls models are statistical and can be implemented within a spreadsheet environment. The derailment model is more complex, based on localised fault and event trees, and is implemented in C++. A schematic of the GeoSRM architecture is shown in Figure 1.

The track is divided into track sections which are explained in more detail in the following section. The derailment and suicides model calculate individual risk values for every train the passes over a track section. This enables the risk from specific causes, at individual locations for just a single train if desired. It does require a large number of individual model evaluations ($\approx 1 \times 10^9$) for the Wessex route.

Derailment risk is calculated for individual sections of track, whilst slip, trip & fall risk is calculated on a station-by-station basis. To enable both these (very different) risk types to be displayed consistently on a map, slip, trip & fall risk is mapped to the individual track sections that pass through the station.

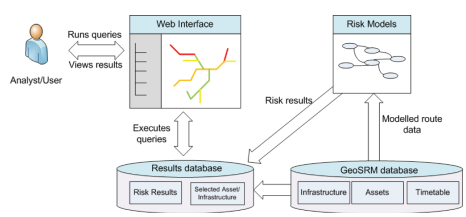


Figure 1. Schematic of the GeoSRM architecture.

2.1 *Track model*

The starting point for the geospatial risk model is the discretization of the track into sections, but first a choice had to be made in terms of which size the sections should be. Large track sections (>100 m) have the advantage that fewer sections are required to cover the network and consequently fewer model calculations. However they do have a number of disadvantages:

– The track sections may need to be represented by a sequence of spatial points to represent the curvature of the track
– More than one asset may be present within a track section, e.g. more than one set of points in a 100 m track section. This will require the derailment model to distinguish between sections with one set of points and sections with two sets of points, as the risk values will be different.
– Risk originating from a single point asset will be smoothed across the whole track section
– Assets may only exist over part of the section, i.e. an embankment might only be present over a fraction of the track section

As it is always possible to "aggregate" risk values to a coarser scale, it was decided to use relatively small track sections, and discretize on a 10 m scale. The Wessex route, which consists of approximately 2,100 km of track was discretized into 211,000 individual track sections. An example of the discretization is shown in Figure 2.

2.2 *Timetable and train data*

To understand risk it is necessary to associate each train in the timetable with the track sections.

There are nearly 3,000 trains operating over a typical day that traverse the Wessex region for at least part of their journey, which includes freight and empty coaching stock movements. The timetable specifies train movements in terms of a sequence of times at fixed timing point locations, with optional platform and routing information.

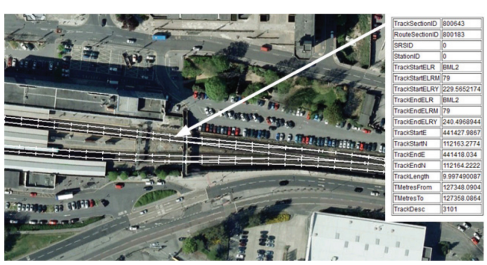


Figure 2. Track sections discretized to 10 m sections (Southampton Central station).

These timing point locations are often stations but include significant junctions en route.

Each train in the timetable was decomposed into a series of journey segments timing point location to timing point location pairs. There were approximately 1,000 distinct journey segments identified, and for each journey segment, the track sections that constitute that segment established. This task is complex, at least for GB timetables, as the timing point to timing point pairs do not necessarily define a unique set of track sections, so there may be more than one way of routing the train.

2.3 *Train loading*

Associated with each train is a "consist" (number and type of carriages) and a loading for the train (number of passengers per carriage). The train loading is taken from modelled passenger demand data, which is based on the concept of demand sections between groups of stations rather than individual stations. It does not identify individual trains but assigns loadings to groups of train. Train journey segments are mapped to these demand sections.

2.4 *Asset data*

The GeoSRM requires information regarding the position of assets on the network. The geospatial position of these assets is normally specified by a mileage along a track. This is then converted to the track sections defined within the track model as well as evaluating the geospatial coordinates of the asset. The assets considered are:

– Switches & crossings
– Level crossings
– Earthworks, such as embankments and cuttings
– Structures, such as over-bridges, under-bridges, viaducts, tunnels, culverts and retaining walls.
– Stations

3 DERAILMENTS

3.1 *Structure*

The derailment model consists of three parts:

– Causal component considering the main causes of derailments
– Escalation component calculating what happens once the train has derailed
– Consequence component which calculates the injuries to those on the train

These three components are discussed in turn in the next three sections.

3.2 *Derailment causal model*

There are 65 precursors within the causal model. These are divided into six groups of causes, namely:

- Rolling stock faults, e.g. axle failure
- Striking an object, e.g. striking items left on line by vandals
- Track faults e.g. track twist, track buckle and rail breaks
- Switch and crossing faults, e.g. points move under train
- Human errors, e.g. signals passed at danger leading to derailment
- Infrastructure failures, e.g. landslip or bridge collapse

Each precursor depends on different geospatial factors, so the causal calculations are illustrated with three examples, track twist, axle failure and landslip.

3.2.1 *Track twist*

The probability of each of these is defined by simple functions. Let $p_{i,j,k}$ be the probability of derailment for the ith track section, jth train and the kth derailment cause. Then for derailment caused by track twist ($k = TTWS$ where $TTWS$ is the index of the track twist precursor), the probability of derailment for the jth train traversing the ith track section is:

$$p_{i,j,TTWS} = \begin{cases} 2.44\times10^{-10} d_i & t_j = P \\ 8.00\times10^{-9} d_i & t_j = FP \\ 2.11\times10^{-7} d_i & t_j = FF \\ 2.44\times10^{-10} d_i & t_j = ECS \end{cases} \quad (1)$$

where d_i is the length of the ith track section and t_j is the train type of the jth train (P = Passenger, FP = Freight of passenger line, FF = Freight on freight only line, ECS = empty coaching stock). The numerical values have been derived from historical rates of occurrence of derailments due to track twist. At this stage of the model development these are national average rates, but future development will make the rates dependent on additional parameters such as track type and condition.

3.2.2 *Axle failure*

For a derailment caused by axle failure ($k = AXL$), the probability of derailment for a single track section traverse additionally depend on the length of the train which determines how many axles it has,

$$p_{i,j,AXL} = \begin{cases} 1.89\times10^{-10} d_i n_j^{AXL} & t_j = P, ECS \\ 2.11\times10^{-9} d_i n_j^{AXL} & t_j = FP, FF \end{cases} \quad (2)$$

where n_j^{AXL} is the number of axles on the train, which depends on the train length (number of vehicles) and the train class, as some trains have just two axles per vehicle.

3.2.3 *Landslip*

In a similar way, the probability of a derailment caused by landslips does not depend on train type but does depend on whether there is a cutting present at the track section,

$$p_{i,j,LNS} = \begin{cases} 2.24\times10^{-9} d_i & X_i^{Cutting} \neq 0 \\ 0 & X_i^{Cutting} = 0 \end{cases} \quad (3)$$

where $X_i^{Cutting}$ is the asset identifier for each cutting. As the track sections are small it is a suitable to treat cuttings as either present or not. In practice what will actually be known, from accident data, is the frequency of derailments f^{LNS}. This frequency has to be apportioned to each of the track sections dependent on whether there is a cutting present and the number of trains that use the track section. Equation (3) can be expressed as follows,

$$p_{i,j,LNS} = \begin{cases} \frac{f^{LNS}}{e^{Cutting}} d_i & X_i^{Cutting} \neq 0 \\ 0 & X_i^{Cutting} = 0 \end{cases} \quad (4)$$

with the distance travelled by all trains in cuttings $e^{Cutting}$ calculated as follows,

$$d_{i,j}^{Cutting} = \begin{cases} d_i & X_i^{Cutting} \neq 0 \\ 0 & X_i^{Cutting} = 0 \end{cases} \quad (5)$$

$$e^{Cutting} = \Sigma_i \Sigma_j d_{i,j}^{Cutting} \quad (6)$$

3.3 *Derailment escalation model*

The escalation model considers the sequence of events following the derailment. For this model the following are considered:

- Train is outside of clearances, so that it foul of its kinematic envelope and could strike a structure or be struck by another train infrastructure failures, e.g. landslip or bridge collapse
- Carriages fall on their side, which increases the degree of injury to the passengers on board
- Derailed train hits a lineside structure

– If train hits a lineside structure then does the structure collapse onto the train?
– Secondary collision with another train on an adjacent line.
– Do the carriages catch fire?

The event tree (Bedford & Cooke 2001, Rausand & Høyland 2004) representing the event escalation is shown in Figure 4, and each of the gates are explained in more detail in the following sections.

3.3.1 *Outside clearances*
The probability of the train maintaining clearances is a simple piecewise linear function of the speed at which the train derails. This is based on an analysis of historical accidents, with different curves for passenger & ECS trains when compared to freight. The relationship is shown in Figure 5.

3.3.2 *Carriage falls on side*
The probability that carriages fall on their side is also modelled as a function of the speed of derailment when the train is not on an embankment. If the train is on an embankment a fixed probability of 0.8 is used instead. These relationships are also shown in Figure 5.

3.3.3 *Hits structure*
For each track section, the distance to next significant structure that could collapse onto the train is determined. Where track sections are bi-directional, this distance depends on the direction that the train is travelling in. Let this distance to the structure be $d_{i,j}^{Struct}$. Assuming a constant deceleration of the derailed train, then the probability of the derailed train hitting the significant structure, $p_{i,j}^{HS}$, is given by,

$$p_{i,j}^{HS} = \begin{cases} 1 & \frac{(v_{i,j})^2}{2a} \geq d_{i,j}^{Struct} \\ 0 & \frac{(v_{i,j})^2}{2a} < d_{i,j}^{Struct} \end{cases} \quad (7)$$

where $v_{i,j}$ is the derailment speed and a is the average deceleration of a derailed train which has been estimated from historical accidents and the relationship between the derailment speed and the distance travelled in a derailed state.

3.3.4 *Structure collapses*
The probability that the structure collapses depends on the speed that the derailed train strikes the structure. This has been estimated based on the assumed average deceleration of a derailed train and again shown on Figure 4.

3.3.5 *Secondary collision*
The probability of a secondary collision depends on the time difference between the time that the train derails and the time that the next train arrives on an adjacent line. The GeoSRM is not a timetable simulation model, so this time is approximated, based on the timetable with random perturbations to ensure that the probability of a secondary collision is a smooth function. The time at which a train traverses a track section is based on the time the train departed the previous timing point, the time the train arrives at the next timing point, and an interpolation between these two times. It does not take into account the acceleration and braking characteristics of the train between these two points, if the timing points represent station stops.

The time of arrival of the next train on an adjacent line $t_{i,j}^{nxt}$ is calculated based on the timetable. Based on the train type of this train (speed and emergency braking capability) and the time to warn the approaching train, the time required for this train to stop short of the derailed train is estimated, $t_{i,j}^{w}$. The arrival time of the next train will follow a distribution to reflect the possibility of late (or early) running. It is not expected that this distribution is symmetrical, but for simplicity a symmetrical triangular distribution is assumed, based around $t_{i,j}^{nxt}$ but with a half-width t^{var}. The probability of a secondary collision is

$$p_{i,j}^{SC} = F_{Tr}\left(t_{i,j}^{w} \mid t_{i,j}^{nxt} - t^{var}, t_{i,j}^{next} + t^{var}, t_{i,j}^{nxt}\right) \quad (8)$$

where $F_{Tr}()$ is the cumulative distribution function of the triangular distribution. The choice of triangular distribution is arbitrary and difficult to justify, although with access to data on actual train movements, empirical distributions of actual train lateness could be derived in future updates of the model. A similar calculation is made for the probability of a secondary collision with the previous train, if it's running sufficiently late so that it arrives after the derailed train—although $t_{i,j}^{w}$ will be different. This is shown in Figure 5.

Two times are calculated, one for where the derailed train activates track circuits on the adjacent line automatically and an additional (longer) time if there is there is a need for verbal communication to warn the approaching train.

3.3.6 *Fire*
The probability of a fire following a derailed train depends on the sequence of events that have already occurred, but not on other location or train specific values. Table 1 lists the values currently used within the GeoSRM. These probabilities are applied to the relevant gates of the event tree displayed in Figure 3.

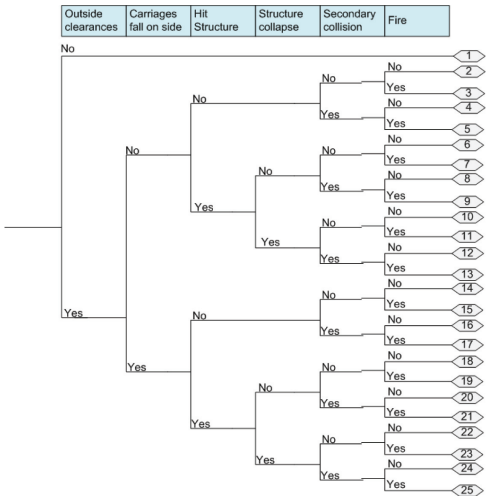


Figure 3. Event tree for the escalation model.

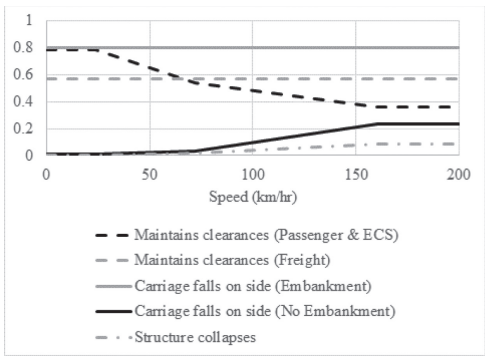


Figure 4. Relationship between probability and derailment speed for escalation events.

3.4 *Derailment consequence model*

The event tree shown in Figure 4 has 25 outcomes (leaves) for which a derailment consequence is required to be calculated. For the SRM, the derailment consequences are calculated manually from available accident history. For the GeoSRM an alternative calculation process was developed based on the concept of an injury atom (Cheng 2009). The injury atoms follow the gates of the event tree and there are 7 in total: base case, maintains clearances, carriage falls on side, hits structure, structure collapses, secondary collision and fire. Each atom is additive so that each of the 25 outcomes is composed of between 1 and 7 of the injury atoms.

Outcome 1 represents a train that derails but maintains clearances and no other escalation events occurs. This outcome has the base case injury atom only. Outcome 2 is based on outcome 1 but with the addition of the maintains clearances injury atom. Outcomes 3 and 4 are similar to outcome 2 but with the addition of the fire and the secondary collision injury atoms respectively. This process continues until outcome 25 which contains all 7 injury atoms. The order that atoms are applied does not affect the result but this requires an injury probability and severity to be defined that is additive for each group of people that are affected.

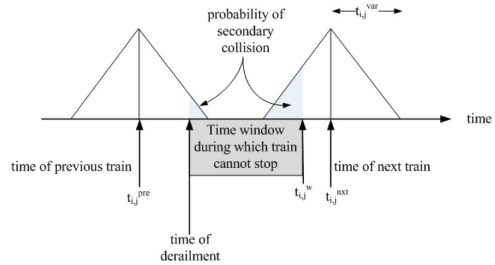


Figure 5. Calculation of the probability of secondary collision.

Table 1. Fire probabilities.

Derailed train	Secondary Train	Probability of fire
Passenger or ECS	None	0.012
	Passenger or ECS	0.03
	Freight Non hazardous	0.05
	Freight hazardous	0.1
Freight	None	0.01
	Passenger or ECS	0.03
	Freight Non hazardous	0.05
	Freight hazardous	0.1

3.4.1 *Injury probability and severity*

In any given train accident there will be a range of injuries from those that are fatalities to those that are uninjured. Injuries are classified into three broad classifications: fatal injuries (death occurring within one year of accident), major injuries and minor injuries. Major injuries are defined in RIDDOR (2013). They cover most fractures, loss of consciousness or other injuries resulting in hospital attendance of more than 24 hrs. All other physical injuries that are neither fatal nor major injuries are classed as minor injuries. Clearly as the speed of the derailment increases, the proportion of the passengers on board the train receiving fatal and major injuries increases. As the total number of passengers on the train is finite, the proportion of minor injuries will start to decrease. To represent

this relationship the consequence is represented by a probability of injury p and a severity of injuries s. Most injuries on trains are caused by secondary impacts and Bell (2001) estimates a relationship between injuries sustained on board the train and accident speed. This relationship can be approximated by a logistic function, using accident speed as a proxy variable for severity. These relationships are shown in Figure 6.

The calculation of consequence at an outcome proceeds as follows. Let C1 be an accident consequence with probability of injury p1 and injury severity s1. Then a new consequence C2 is defined in terms of C1 with the addition of an injury atom. For example consequence 15 in Figure 3 is based on consequence 14 but with the addition of the fire injury atom. The probability of injury and severity of consequence 2 (p_2 & s_2) are based on the probability and severity of consequence 1 (p_1 & s_1), with some additional contribution from the injury atom (p_a & s_a).

$$p_2 = p_1 + p_a - p_1 p_a \quad S_2 = S_1 + S_a \tag{9}$$

Equation 9 assumes that each atom add a fixed additional probability of an injury that is independent of the other atoms that form the consequence. The additional severity is also assumed to be independent of the other atoms. This would seem to be a reasonable simplification given the other uncertainty in the values for these atoms that can be derived from historical accidents.

3.4.2 *Population exposed*

To convert the injury probability and severity to a consequence requires multiplication by the number of people exposed. For derailments there are 6 population groups:

- Passengers on the derailed train
- Workforce on the derailed train
- Passengers on any train involved in a secondary collision with the derailed train
- Workforce on any train involved in a secondary collision with the derailed train

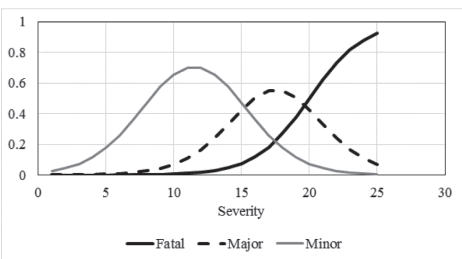


Figure 6. Probability of fatality as a function of accident severity.

- Number of passenger waiting for train at a station
- Number of members of public within 1 km of the derailed train

The last two population groups are only used for derailments occurring within a station and for large fires and explosion involving hazardous goods trains.

4 MODEL CALCULATION

4.1 *Key risk drivers*

An important aspect of the model is to be able to determine what the risk associated with some of the key influencing factors are, termed key risk drivers. These key risk drivers could be basic events of the model but could equally be other quantities that affect event escalation and consequences. For example a bridge might be a key risk driver at a location dues to its effect on both the frequency of derailments and consequence of derailments. It is also necessary that the key risk drivers can be scaled either spatially or across risk precursors, so that the key risk drivers on a route can be calculated. The measure used is the risk reduction importance measure (van der Borst, 2001). The risk reduction importance $\Delta R_{i,j,k}(x)$ for some model parameter x is the difference between risk and the risk with the parameter at some optimum value x^*.

$$\Delta R_{i,j,k}(x) = R_{i,j,k} - R_{i,j,k}(x = x^*) \tag{10}$$

For precursors, the optimum value is simply when the probability of failure is zero. For other parameters the optimum value is more difficult to determine, and has to be defined manually. For example passenger train loading is an important key risk driver at most locations, i.e. the greater the number of passengers on the train then the greater the risk. The optimum value of train loading that minimises risk is zero, but that is not a particularly useful comparison. For the GeoSRM, the optimum value for train loading is chosen so to be the minimum train loading across the network. This ensures that the risk reduction measure is always positive, but at least at one location is equal to zero. The key risk driver $K_{i,j,k}(x)$ is calculated by normalising the risk reduction measure by the risk.

$$K_{i,j,k}(x) = \frac{\Delta R_{i,j,k}(x)}{R_{i,j,k}} \tag{11}$$

The risk reduction measure can be aggregated, spatially, across trains or precursors, and the key risk driver at this aggregated level is the ratio of the

aggregated risk reduction measure and the aggregated risk.

4.2 *Asset risk*

The GeoSRM allows the risk associated with an asset to be determined. Asset risk is defined in a similar way to the risk reduction importance measure used to calculate the key risk drivers. Thus it is the difference in risk between the network with the asset and the risk from the network without the asset.

For example, a set of points is a potential cause of a train derailment, from points moving under the train say. However they can also increase the consequences from a derailment at other nearby locations. If a train derails nearby, but continues to move whilst maintaining clearances, then when the derailed train strikes the set of points, it will immediately go out of line and the consequences will be likely be more severe.

Thus the calculation of asset risk for an asset a is,

$$A(a) = \Sigma_i \Sigma_j \Sigma_k (R_{i,j,k} - R_{i,j,k}(a = \text{null})) \quad (12)$$

where a = null indicates that the asset has been removed from the model input dataset. As the calculation of asset risk requires a full computation of the model within the immediate vicinity of the asset, it is computationally expensive to undertake.

5 GeoSRM WEB INTERFACE

The GeoSRM has been developed as a web application by the University of Southampton. The interface is by default a map that can be zoomed in/out and panned as appropriate. At the moment it is not possible to view the network in a schematic view but this facility may be provided in later releases. The interface consists of three main areas.

The left hand side allows the user to filter the displayed risk, the right hand side that displays the scale and summary results, and the central map area. It is possible to filter by:

- Hazards. Such as derailments, suicide or slip, trips and falls.
- Causes. It is possible to also filter for specific causes of hazards.
- Route. The Wessex route is divided into smaller strategic route sections which can be selected individually or in combination.
- Train. It is possible to filter by both group of train services as well as by class of rolling stock
- Company. Each precursor is assigned a company that controls that risk. Some precursors are shared between two or more companies and in this case all risk controlling companies are assigned. Other companies do not control the risk but are affected by it are also assigned.



Figure 7. Screenshot of the GeoSRM web interface.

The right hand side of the interface displays the results. Results can either be displayed in absolute terms such as fatalities and weighted injuries per year, or normalised. There are a range of possible normalisers that the user can select, such as track km, route km, passenger journeys, passenger km or train km. The colour scale is automatically calculated and is log-symmetrical around some predefined reference value. This reference value sets the middle of the scale and typically could be set to the national average or average over Wessex. By setting this reference value it is easy for the user to see if the displayed risk is better or worse than average.

The central area of the map displays the risk values overlaid on a backdrop aerial imagery. Navigation controls allow the user to zoom in and out of the map. At each zoom levels, the risk values are aggregated to a suitable level to ensure that the information presented to the user is neither in too much detail or too little detail. The pre-calculated aggregation also ensures that the volume of data queried by the tool is minimised, which improves tool performance. A screenshot of the tool is shown in Figure 7.

6 CONCLUSIONS

The GeoSRM demonstrates that it is possible to develop a geospatial risk model for rail safety hazards. The data requirements for such a model are high, and challenges remain in gaining access to the data in a form that is easy to process. Work is ongoing, within Network Rail to develop a Railway Infrastructure Network Model (RINM). This will contain geospatial and schematic layers, but will also contain a logical model that will enable the mapping of trains onto the track sections a

much simpler task. It is anticipated that developing geospatial risk models will be a much more tractable task in the future.

ACKNOWLEDGEMENTS

The author would like to thank South West Trains and Network Rail for their support of this work and for supplying infrastructure data and expertise to enable the models to be developed, and also the UK Department for Transport and their funding of project "T972 Piloting a geo-referenced safety risk model for the rail network in Great Britain", which forms the basis for the work presented in this paper.

REFERENCES

Bedford, T. & Cooke R. 2001. Probabilistic Risk Analysis. Cambridge: Cambridge University Press.

Bell, H.K. 2001. Accident Consequence Modelling for the Layout Risk Method, WS Atkins.

Cheng, D. 2009. Uncertainty Analysis of Large Risk Assessment Models with Applications to the Rail Safety & Standards Board Safety Risk Model. Glasgow: Strathclyde University.

Dennis, C. & Somaiya, K. 2004. Development and Use of the UK Railway Network's Safety Risk Model, Probabilistic Safety Assessment and Management: PSAM 7—ESREL ′04.

Griffin, D. & Holloway, A. 2012. Route based risk estimation across the GB rail network using empirical Bayes methods. ESREL 2012.

Marsh, D.W.R & Bearfield, G. 2008. Generalizing event trees using Bayesian networks. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 222: 105–114.

McNulty, R. 2011. Realising the potential of GB rail, Final Independent Report of the Rail Value for Money Study, Detailed Report. Department for Transport.

Rausand, M. & Høyland, A. 2004. System Reliability Theory, Models, Statistical Methods, and Applications. Second Edition. Wiley.

RIDDOR. 2013. The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations. No 1471.

van der Borst, M. & Schoonakker, H. 2001. An overview of PSA importance measures. Reliability Engineering and System Safety. 72. 241–245.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparing the two methods for judging changes in European railways and in European nuclear safety

N. Petrek
Institute of Railway Engineering and System Safety, Technische Universität Braunschweig, Germany

H.P. Berg
Bundesamt für Strahlenschutz, Salzgitter, Germany

ABSTRACT: In 2009 a new regulation has been implemented by the European Commission which harmonizes the risk assessment process for the European railway industry. This regulation describes the Common Safety Method (CSM) and contains a process for judging the significance of a change. In the area of nuclear safety such a common regulation does not exist to date. In Germany nuclear regulations are issued by the Federal Government although the European Commission enhances efforts to create such a common framework as a reaction to accidents at the Nuclear Power Plants (NPPs) of Fukushima-Daiichi in March 2011. After discussing the regulation framework we compare both methods in detail and explain their similarities and differences and the underlying reasons and how the results can be categorized.

1 MOTIVATION

As part of the harmonization of the risk assessment process in the area of European railway industry a new concept judges the significance of a change. In our paper we will compare this approach of the so-called CSM-Process with the method applied in case of changes of equipment in NPPs. The similarities and differences between both methods are investigated and it is discussed why the method for judging changes in railways uses both risk-based and qualitative criteria in one method.

2 THE CSM-PROCESS FOR JUDGING THE SIGNIFICANCE OF A CHANGE

The CSM regulation of the European Commission (2013a) describes the whole process and defines which changes have to be considered. Article 2 of this regulation which replaces the original CSM regulation (European Commission 2009a) defines that changes may be of technical, operational or organizational nature. Organizational changes must have an impact on the operating conditions or an influence on the maintenance processes. Furthermore, the proposer of the change has to consider the impact on safety of the change. For all changes, which have an impact on safety, the proposer has to evaluate the significance of the change based on six criteria. The CSM regulation describes these six criteria in Article 4 as follows:

- failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system under assessment;
- novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new for the organization implementing the change;
- complexity of the change;
- monitoring: the inability to monitor the implemented change throughout the system life-cycle and intervene appropriately;
- reversibility: the inability to revert to the system before the change;
- additionality: assessment of the significance of the change taking into account all recent safety-related changes to the system under assessment and which were not judged to be significant.

In this context the criteria additionality is not used for judging the significance of the change like the other five criteria. It can rather be interpreted as an instruction how to consider changes, which were already implemented in the same area as the proposed change and were not significant but safety relevant. Apart from the explanation in Article 4 it does not exist any further guidance in the regulation itself how to apply the criteria and how to judge the significance of a change on the basis of the given criteria. This relates to both the

weighting of the criteria and also to the threshold above which the examined change is valuated as significant.

However, the explanation of the criteria clearly reveals that there exists the risk-based criteria failure consequence and four additional criteria, which can be qualified as qualitative. The regulations provide no reasons for the selection of these criteria. Moreover, there is no guidance how to apply both risk-based and qualitative criteria in one method.

Petrek (2014) develops a method how to judge the significance of a change on the basis of the application of all criteria which are given by the CSM regulation. The framework for judging the significance of a change is given in Figure 1. This framework is also developed and explicitly discussed in Petrek (2014). It becomes clear that the consideration of the safety relevance and the analysis of the significance of the change are only two elements of the whole process. These both elements are represented in the light blue box in Figure 1.

The proposed changes are classified in three different categories. If a change does not fall within the scope of the CSM regulation or if a change is not safety related, the CSM process does not have to be applied. However, the application of QM-Procedures is needed, if those procedures are required by the SMS of the company. Besides these QM-Procedures the CSM process distinguishes between the application of own safety procedures and the application of the harmonized CSM risk management process.

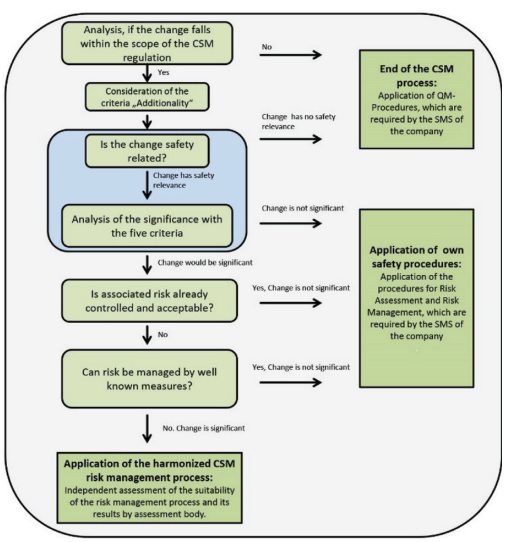


Figure 1. Caption of the framework of the CSM risk management process.

It becomes obvious that the analysis of the significance of the proposed change determines, if the harmonized process has to be applied. Only for significant changes the application of the harmonized risk management process may become necessary. In order to clarify this, further considerations are necessary. This includes the verification, if the associated risk is already controlled and thus acceptable. Only if this is not the case and the risk cannot be managed by well know measures, the proposed change is finally significant and the proposer has to apply the harmonized risk management process. But it should be emphasized that the analysis of the significance does not decide whether any risk management is necessary or not.

The main difference between the harmonized and the own risk management process is the necessity for an independent assessment of the risk management and its results in the application of the harmonized process. Against this background, the role of the qualitative criteria becomes clear. The qualitative criteria are used for the assessment, if the company already has experience with the implementation of the proposed change or not. If this is not the case, it is more likely that the change is significant and an independent assessment of the risk management process is necessary. As described earlier, this role of the qualitative criteria is not clearly given by the regulation itself.

3 JUDGING CHANGES IN NUCLEAR POWER PLANTS

The nuclear technology is, in contrast to the European rail transport, not monitored by European authorities. The licensing and supervision of nuclear installations in Europe is perceived by the respective national authorities.

At European level, so-called safety reference levels have been defined by WENRA (2008, 2013), originally in the context of the definition of safety requirements for nuclear installations of countries which are potential candidates to join the European Union. These reference levels should be adhered to by all member countries of the European Union.

In Part G of these reference levels, the safety classification of Structures, Systems and Components (SSCs) is described. The goal is to identify all safety related SSC and to classify them according to their importance for safety. Part Q reflects changes in a Nuclear Power Plant (NPP) and it is requested that no change reduces the ability of the reactor for safe operation in any form. In addition, national regulations and international agreements within the European Union are supplemented by a directive of the European Commission (2009b) which had to be implemented by July 2011 into national

law. Moreover, a draft amendment to this directive (European Commission 2013b) is under discussion which intends to describe a possible mechanism to develop harmonized European safety regulations.

The licensing and supervision of nuclear installations in Germany is the responsibility of the Federal States (Länder) who are subject of expediency supervision of the Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety (BMUB).

In addition to the German Atomic Energy Act (Atomgesetz—AtG) (2013), there exist several national requirements which have to be considered in the approval and supervision process of nuclear facilities. A recent comprehensive update of the German sub-legal nuclear regulations including interpretation has been issued (BMU 2013a and 2013b).

Basically, each NPP in Germany must have a valid operating license. An essential part of this approval is the condition of the AtG to show all changes to the plant and the operation (including changes in the organization) to the competent authority and to examine their safety relevance. Significant changes of systems according to § 7 AtG are subject to approval by the supervisory authority. The implementation of authorizations below this level is subject to a graded supervisory control depending on their safety significance.

The approach in nuclear technology is that all important equipments of a NPP are classified in terms of their safety significance, accompanied by respective requirements and specifications. At the international and national level, there is no detailed classification of SSCs. The procedural rules for the treatment of changes are regulated in operating manuals which are specific for each NPP. The operating manual is part of the approval of the competent authority to start or to continue the operation of the NPP.

In the following, the evaluation of changes in the Federal State of Baden-Württemberg which oversees in total four NPPs is exemplarily described because this Federal State has developed a concept for regulatory supervision of NPPs—the last version is issued last year (UM BW 2013)—and a supervisory manual (UM BW 2011) with a separate detailed chapter describing the regulatory plant change procedure (Landeseinheitliches Änderungsverfahren—LEÄV), already anticipating the safety requirements for NPPs (BMU (2013a).

In this supervisory manual of Baden—Württemberg changes are subdivided into three categories, designated as category A, category B or category C where category A contains the highest requirements and category C the lowest ones. If it is a change in the hardware that also requires a change of the documentation, the higher classification determines the overall classification of the change.

Figure 2 shows the procedure how to classify changes of equipment. In a first step, it must be considered whether the proposed change relates to equipment which is subject to the Atomic Energy Act. In this case it must be examined whether this change is a change in the legal sense. If yes, one has to consider whether a significant change has occurred. According to the supervision manual a change is to be regarded as significant in the legal sense if the change can have more than obviously insignificant effects regarding the safety level of the plant. In this case, the change falls into category A.

Otherwise, it must be checked whether the change is subject to the uniform change process. In this case, the change falls into the category B or category C. For example, changes to safety systems or safety-relevant systems are belonging to category B or C. The decision regarding category B or C depends on the type of change: is it only an exchange by equivalent equipment (components or systems) or leads the change to a deviation in the approved specification.

In the first case it would be a change of category C, in the second one a change of category B.

Therefore, two issues are of vital importance for the assessment of changes in this process.

One is the decision whether a change is a change in the legal sense. This is the case if the planned change is not covered by the previous approvals. If the answer is negative, no further consideration of the change is necessary.

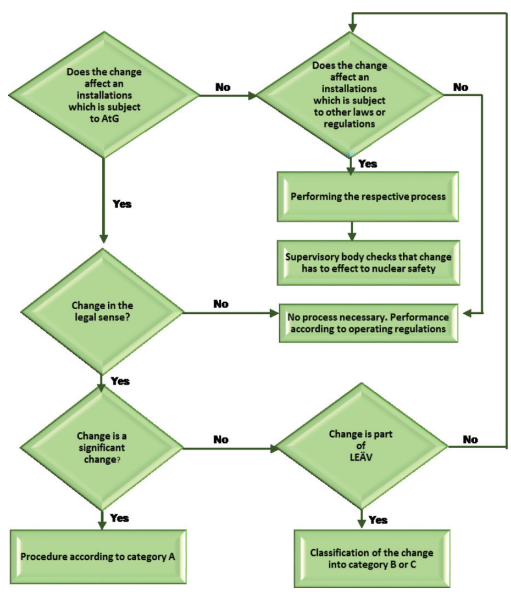


Figure 2. Procedure of classifying changes of equipment in NPPs.

In a next step it is important whether the planned change has to be classified as a significant change. The result of this assessment determines whether a change is classified into category A or category B/ C, respectively.

The importance of a change has to be assessed by comparing the actual plant state with the state after having performed the change. The decisive factor is whether and to what extent the change has safety relevance. The probability of a significant change depends on the impacted area. Changes that affect the design characteristics of the plant or the safety systems are, with a high probability, significant changes and, thus, fall into category A.

In the following it is explained which procedure depending on the classification of the change in one of the three categories is required according to (UM BW 2011).

Category A: If the change belongs to category A, an authorization procedure is required by § 7 of the Atomic Energy Act and pursuant to § 7 paragraph a permit application has to be submitted by the licensee to the supervisory body. The licensing procedure is conducted in line with the Nuclear Licensing Procedure Ordinance (2006). In addition, a probabilistic assessment is required which shows the influence of the change on the Probabilistic Safety Analysis (PSA). It must be explained why the proposed change has no effect on the PSA.

Category B: If the change belongs to category B, it must be supervised by the authority under § 19 of the Atomic Energy Act. A notification of the planned change must be submitted by the licensee to the supervisory authority. The implementation of the change can only take place if the supervisory authority has provided its written supervisory opinion that the proposed change is seen from the perspective of the supervisor as "without any concern or not subject to licensing." The supervisory authority and the technical support organisation (consulted by the regulatory authority pursuant to § 20 of the Atomic Energy Act) monitor and accompany the implementation of the planned changes. In addition, a probabilistic assessment is required as in the case of a change of category A showing the influence of the change on the PSA. It must be explained why the proposed change has no effect on the PSA.

Category C: If the change belongs to category C, it must be monitored by the authority under § 19 of the Atomic Energy Act. An examination of the changes in category C by an expert according to § 20 of the Atomic Energy Act is required. The implementation of the change can only start after the expert has finalised his supervisory report and the authority does not make any objections until the change starts. It is, however, no probabilistic evaluation required as in categories A and B.

Changes that are not subject to the procedure described above are performed by the operator according to its internal written operating procedures without participation of the authorities and experts. The supervisory authority will perform random checks on the basis of the documentation provided by the operator, if he has correctly classified the changes.

Examples of changes are listed in Berg (2011). Basically, it has to be noted that a changes also in other Federal States are classified into one of three categories; however, usually no additional probabilistic reviews have been required so far.

4 COMPARING BOTH METHODS

The detailed description in the last two chapters has shown that the basic procedure of both methods is comparable to each other. Both methods are generally used for judging technical, operational and organizational changes.

In the method of judging changes in nuclear safety the first step is the analysis if the change affects an installation which is subject to the AtG. Additionally, the procedure of Figure 2 contains the examination if the present change is a change in the legal sense. This is the case if the change is not covered by the existing approval of the NPP. For example, a technical plant modification concerning the spent fuel pool cooling using other systems than in the past.

In the CSM risk management process these both steps are enclosed by the analysis if the change falls within the scope of the CSM regulation. This analysis is described in detail in Petrek (2014). For instance a technical change is relevant for the CSM regulation if the change makes use of new technical solutions or if new risks or hazards may arise respectively if existing risks or hazards are altered due to the change.

Both methods distinguish in the described manner between relevant and irrelevant changes for the further procedure.

The next step in both methods is to analyze the significance of the change.

According to Figure 2 for classifying changes of equipment in NPPs the result of this specific step leads to the decision whether the planned change falls into category A or in category B respectively C. As already described in chapter 3 a change is to be regarded as significant if the change can have more than obviously insignificant effects regarding the safety level of the plant. Therefore, the classification of the change is based on the consideration of the safety relevance and the impacted area.

Contrary to this procedure, in the CSM risk management process of Figure 1 the analysis of the safety relevance is only the first step. If the

change is safety relevant, the proposer has to apply the further criteria to assess the significance of the change. According to chapter 2 four of these five criteria are qualitative and do not consider the change itself but rather the implementation of the change. The remaining fifth criterion failure consequence is used for a risk-based consideration of the change.

For clarification, within the procedure of the British ORR (Office of Rail Regulation) for determining the significance of a change the different perspectives of these criteria are combined in a matrix (ORR 2012). This matrix which is basically a type of risk matrix is shown in Figure 3.

The criteria novelty and complexity are interpreted as the uncertainty of outcome, which consider the likelihood that the proposed change will or will not behave as predicted. The uncertainty of outcome represents the Y-axis of the given matrix. The X-axis is defined by the risk-based criterion failure consequence. The X-axis and the Y-axis possess four different categories with the result that the matrix consists of 16 fields, while each of these 16 fields is associated with a significant change, a non-significant change or an unclear result. In case of an unclear result the proposer of the change has to apply the additional criteria monitoring and reversibility in order to determine the significance of the change. This interpretation of the criteria

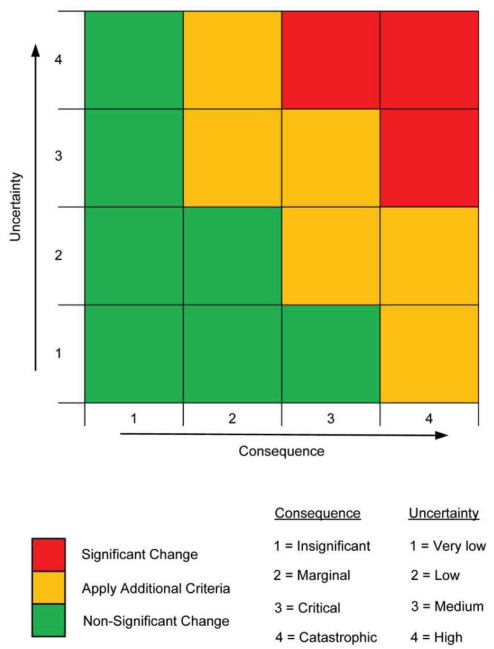


Figure 3. Procedure of the ORR for determining the significance of a change.

in the procedure of the ORR illustrates the role of the qualitative criteria, which is the consideration of the company's experience with the implementation of the change.

In contrast to this procedure, the judgment of changes of equipment in NPPs is done on a risk-based consideration. If the change is not significant, it has to be checked whether the change falls within the uniform change process. Those changes are associated with the categories B and C. The decision between both categories depends on the type of change respectively whether the change leads to a deviation in the approved specification or not. However, in contrast to the procedure of the CSM process a consideration of the existing experience with the change does not take place.

The comparison of the different categories of both methods shows that category A describes the procedure for significant changes and requires an authorization procedure for the implementation of the change. Additionally, a probabilistic assessment which shows a potential impact on the PSA is demanded. On the other hand, those changes which are rated as significant by the application of the CSM process shown in Figure 1 require an application of the harmonized risk management process and also an independent assessment by an assessment body. However, a change which is safety relevant but not significant requires the application of own safety procedures but an independent assessment is not required. In contrast, category B and C of the procedure for changes of equipment in NPPs still require a supervision by the authority respectively in case of category C a monitoring by an authorized expert. Only category B requires a probabilistic assessment which shows the potential influence on the PSA results.

While the significance of a change in the CSM process decides whether an independent assessment is required, the different categories A, B and C decide whether an authorization procedure, a supervision process or a monitoring process is required. Hence, the purpose of the CSM process shown in Figure 1 is to decide whether an independent assessment is required or not. In addition, also for safety relevant but not significant changes a risk assessment is necessary. Therefore, the CSM process does not decide whether any risk assessment is necessary or not.

5 DISCUSSION OF THE RESULTS AND CONCLUDING REMARKS

At first the comparison has demonstrated that the basis structure of both methods is similar. This concerns the initial analysis whether

the proposed change is relevant for the certain method. However, this analysis is divided into two steps within the procedure for classifying changes of equipment in NPPs.

In both methods this initial step is followed by the judgment of the significance of the change which decides what kinds of further risk management procedures are required. At this point is the main difference between both methods which is the set of the qualitative criteria in the CSM process for judging the significance of a change. It became clear that those qualitative criteria are used for the consideration whether the proposer of the change has experience with the implementation of the change.

Furthermore, the consideration of the different categories of both methods has exposed that the significance of a change in the CSM process decides whether an independent assessment is necessary. This aspect represents the main purpose of the CSM process shown in Figure 1.

In contrast, the process for judging changes in nuclear safety always requires at least a deterministic safety assessment to provide the evidence that the respective specifications and nuclear safety standards are fulfilled. Figure 2 describes how to determine the kind of participation of the authority and whether or not a probabilistic safety assessment is required. This is the reason why the method applied in the nuclear field does not contain qualitative criteria which are used for the consideration of already existing experience with the implementation of the change.

In summary, the consideration of changes is seen as a necessary part for the risk management in European railways as well as in nuclear safety.

The comparison clearly showed that there are differences in the processes regarding the role of the proposer of the change and the levels of supervision. While the CSM regulation possesses the level of independent assessment and on the other hand the application of own safety procedures without any participation of an independent assessment body, the regulations in the area of nuclear safety are more restrictive and also more prescriptive limiting the room for maneuvers for the applicant of the change. This is also visible in the fact that all three categories of changes in the nuclear field require a prescribed authorization procedure or a supervision by the authority respectively by the authorized experts but still monitored by the authority.

REFERENCES

Act on the peaceful utilisation of nuclear energy and the protection against its hazards Atomic Energy Act, Atomgesetz—AtG, 23 December 1959, as amended and promulgated on 15 July 1985, last amendment of August 28, 2013.

Berg, H.P. 2011. Classification of changes with respect to their safety significance, Presentation at *Safety in Transportation -04 of IfEV*, Technical University Braunschweig, November 2011, available on the website of IfEV in German.

European Commission. 2009a. *Commission regulation EC NO 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 63a of Directive 2004/49/EC of European Parliament and of the Council*, April 2009.

European Commission. 2009b. *Directive 2009/71/EURATOM establishing a community framework for the nuclear safety of nuclear installations*, June 25, 2009.

European Commission. 2013a. *Commission Implementing regulation EU No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation EC No 352/2009*, April 2013.

European Commission. 2013b. *Draft proposal for a council directive amending directive 2009/71/EURATOM establishing a community framework for the nuclear safety of nuclear installations*, June 13, 2013.

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety BMU. 2013a. *Safety requirements for nuclear power plants of 22 November 2012*, Federal Gazette, AT January 24, 2013 B3.

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety BMU. 2013b. *Interpretation of the safety requirements for nuclear power plants of 22 November 2012*, November 19, 2013.

Ministry of the Environment, Climate Protection and the Energy Sector Baden-Württemberg UM BW. 2011. *Regulatory Plant Change Procedure Landeseinheitliches Änderungsverfahren—LEÄV*, September 2011 currently only in German.

Ministry of the Environment, Climate Protection and the Energy Sector Baden-Württemberg UM BW. 2013. *Concept for regulatory supervision of nuclear power plants in Baden-Württemberg*. June 2013.

Office of Rail Regulation ORR. 2012. ORR guidance on the application of the common safety method CSM on risk assessment and evaluation, December 2012.

Ordinance on the Procedure for Licensing of Installations under §7 of the Atomic Energy Act Nuclear Licensing Procedure Ordinance—Atomrechtliche Verfahrensverord-nung—AtVfV of 18 February 1977, as amended and promulgated on 3 February 1995, last amendment of 9 December 2006.

Petrek, N. 2014. Konstruktion eines Verfahrens zur Signifikanzbewertung von Änderungen im europäischen Eisenbahnwesen. *Ph.D.-Thesis of the Department of Architecture, Civil Engineering and Environmental Science of the Technische Universität Braunschweig*, publication in August 2014.

Western European Nuclear Regulators' Association WENRA. 2008. *WENRA reactor safety reference levels*, January 2008.

Western European Nuclear Regulators' Association WENRA. 2013. WENRA safety reference levels for existing reactors, update in relation to lessons learned from TEPCO Fukushima-Daiichi accident, November 20, 2013.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Combination of technological and economical risk assessment using the Monte-Carlo-Simulation

F. Plinke, D. Althaus, A. Braasch & A. Meyna
Institute for Quality and Reliability Management GmbH, Wuppertal, Germany

ABSTRACT: Economical risks are directly connected with the technological risks. One major problem of a integrated technical and economical risk assessment is the identification of a suitable method, which can combine technological, safety and economical issues in one risk assessment. The Monte-Carlo-Simulation is used in both sciences (engineering & economics) and can be adapted to perform a combine risk assessment. The paper explains the Monte-Carlo-Simulation integrated in a V-model process. Via a V-model the different issues can be partitioned, analysed on a low level (component reliability, safety and price) and later combined to a complete system risk assessment.

1 INTRODUCTION

The architectures of modern systems and components record a gain in complexity and are networked with other systems to a growing extent. The result is an increase of functions, which, at the same time, imposes higher demands on their reliability.

One consequence of these complexity issues is the aggravation of a reliability analysis via classical mathematical and stochastic methods. This is essentially due to complex mathematical expressions, which cannot be solved or only at considerable effort. Furthermore, complex technical dependencies can make classical methods inappropriate. Another reason is that there is just a too high amount of components or subsystems.

The field of application of Monte-Carlo-Simulations comprises illustrating, simulating and analyzing these complex issues in technical and economic areas.

The Monte-Carlo-Simulation is a computer based simulation method that is able to model and analyse even complex interrelations by a series of simulated runs. With the help of random numbers, random events can be generated. Through much iteration of these simulated runs, an estimator can be developed which substitutes the conventional reliability analysis or other analytical calculations.

There are numerous possible fields for Monte-Carlo-Simulation operations, which can be applied for integrated analyses of systems (technical as well as economic analyses).

Selected technical fields of applications are:

- Classical reliability and safety analyses for (highly) complex systems
- Functional analyses for the investigation of degraded functional states (subsystem failures)
- Application in the area of tolerance calculation, especially for non-linear tolerances and tolerance chains
- Simulation of highly reliable systems with extremely low error probability
- Employment in early research and development stages, when a field data analysis cannot be conducted
- Integrated application in the area of product development for validating and securing the development processes.

Selected economical fields of application are:

- Analysis of technical consequences for economic issues
- Targeted risk analysis in consideration of many dynamic risk factors and objects
- Support in the drafting of contracts (especially concerning guarantee and warranty terms and conditions)
- Comparing different contractual strategies using specific simulations
- Analysis of the availability of technical units regarding to logistic questions.

2 MAINTENANCE CONTRACTS

2.1 *Contract types*

Depending on the product type different maintenance and repair strategies are disposed. A simple form for maintenance contracts are time-and-material contracts.

This standard contract type is based on real time and material overhead which is needed to repair a system. Indicating a simple calculation by the maintenance company due to the fact that every work within the repair process is charged. If no costs are capped, the risk for the maintenance company is minimal. Figure 1 describes this simple connection. In this case the "paid" line is identical with the "charged" line.

In some cases special costs are capped to a limit. If this limit is reached any additional costs cannot be charged. The implementation of a material or time cap can be important in contract negotiation. For the customer a special cap is a risk minimizing offer. On the other side if the probability for reaching the cap is very low and if the cap is reached additional costs are low as well, it can be valuable for the maintenance company to offer these types of contracts with caps.

The agreement on special caps can be generalized to a not-to-exceed contract. In this case the maintenance company cuts the costs of all time-and-material-repairs at one point, but however becoming a high risk for the operator. The customer has no additional risk at this point. Figure 2 shows the initial point and the increasing risk value.

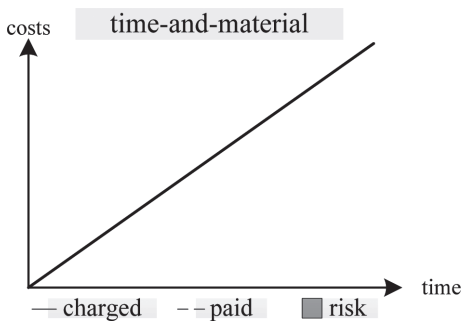


Figure 1. Time-and-material contract.

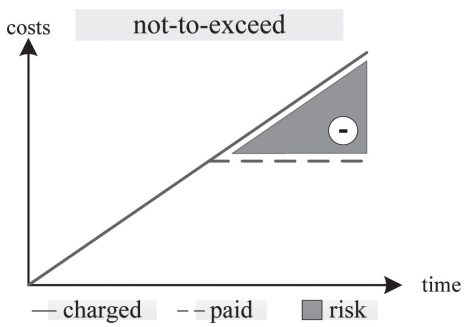


Figure 2. Not-to-exceed contract.

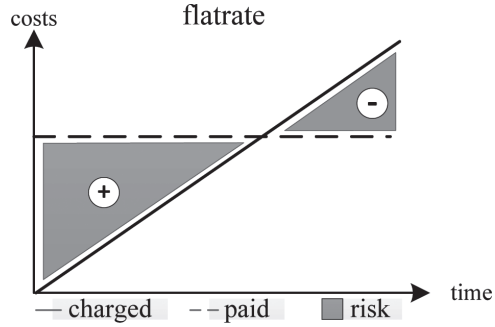


Figure 3. Time-and-material contract.

Another very popular contract type is a flatrate contract. This type is well known in many industries and also common for end-user products or services.

A flatrate based maintenance contract requires a valid period or another limited reference. This can be usage parameters, mileage, usage count or other recordable characteristics. The economical risk is distributed between the maintenance company and the customer and has the highest value in comparison to time-and-material or not-to-exceed contracts.

2.2 *Valid period*

One of the most important agreements in maintenance contracts is the valid period. Especially for high-value products with a regular call for maintenance operations the maintenance offer is a sales appeal. In the last years, e.g. in the automotive industry, the valid period of maintenance services for new cars has raised strongly. Due to different statutory provisions for implied warranty the valid periods differ in European countries.

In the automotive industry the warranty period is raised up to 8 or 10 years from single OEM's. These contracts are flatrate contracts including some caps for wear parts; nevertheless some contracts are even full flatrate contracts with no caps or exclusions.

Due to this extension of the valid period the OEM's and the suppliers are confronted with new challenges in quantifying the new economical risk.

Some of these challenges are

- Warranty costs
- Component dependencies
- Availability of spare parts
- Advances in prices for spare parts or wages
- Higher storage costs

Especially for flatrate contracts theses challenges have to be very carefully considered by the OEM and the suppliers before drawing an agreement of this type of maintenance strategy.

3 RISK ASSESSMENT METHODS

3.1 *Comparison*

To evaluate the most common methods in risk assessment regarding maintenance issues, Table 1 lists the most important properties for this kind of analyses.

Abbreviations:

- CON = Convolution
- PCA = Principal Component Analysis
- NN = Neural Network
- MCS = Monte-Carlo-Simulation

3.2 *Convolution*

Merging of single distributions via continuous or empirical convolution is one of the most common methods in simple risk analysis. For few components with continuous functions the convolution is a proper method, but cannot be used for complex systems with different kinds of data like distribution functions, qualitative data or dependencies. Since not every type of information can be transformed in a distribution function. Moreover it is possible that technical dependencies may occur. In this case the repair of one component requires the change of another. This is a common problem especially due to the failure of older parts. Because of integrated system designs the compatibility of newer versions of the same parts might not be useable with some older hardware.

Using the example of a power window actuator in a car, in some cases the change of electric motor is only possible in combination with the change of rolls and Bowden cables. According to this all components have to be available. Given the case one Bowden cable breaks, the change of one cable is possible without any further effort.

This example of technical dependencies describes the need for a flexible function. The convolution is not flexible enough to integrate such issues in a suitable way.

Table 1. Comparison of different methods regarding to their usability for maintenance issues.

	CON	PCA	NN	MCS
Cont. and discrete functions	+	–	+	+
Expert knowledge	–	–	+	+
Dynamic parameters	+	o	o	+
Techn. or econ. dependencies	–	–	o	+
Rare events	o	–	+	+
Suitable for complex systems	–	o	+	o
Suitable for censored data	o	+	o	o
Tool connectivity	+	+	+	+
Evaluable, documentable	–	–	–	+

3.3 *Principal component analysis*

The principal component analysis is common in the area of economics, to analyze the correlation of different parameters. PCA, in classical meanings, allows only normal distributed parameters and acceptable for many risk assessments as a constraint. For complex systems with exponential, weibull or other distributed components or special economical functions the PCA is not useable.

3.4 *Neural networks*

Neural networks are computational methods based on machine learning and pattern recognition. They are popular in the area of risk assessments because an (almost) unlimited number of variables and parameters can be combined to free defined outputs. One further advantage of neural networks is that in analytical correlations between the variables or parameters have not to be known. A neural network can include different kinds of information. Both continuous and discrete functions can be used as well as expert knowledge. The problem with neural networks for risk analysis is the evaluation of the results. The weighting of the connection between the neurons cannot be reviewed. In addition the correlation function, learned by the neural network can be wrong without any possibility of recognizing it. However the usage of these networks in combination with technical and economical experts presents a good option for quantifying complex risk scenarios in maintenance strategies.

3.5 *Monte-Carlo-Simulation*

The Monte-Carlo-Simulation is a computational simulation method based on random events using the weak law of large numbers. Each simulation run generates a special scenario based on random historical data. One of the advantages of the MCS is the possibility to implement dependencies and qualitative data easily. In addition, the results are comprehensible and can be stored for documentation. Filters can also be inserted directly in order to compare the effects of certain parameters. One disadvantage is the need for much calculation power to perform the simulation runs. Depending on the complexity of a technical system in combination with its economic options the duration of a MCS can be quite long. For simple cases, the MCS can be performed directly in common spreadsheet programs without additional computational algorithm software. However, for complex systems additional software is highly recommended.

4 RISK SIMULATION

The Risk simulation process consists of different steps and layers. Beginning with a system breakdown and level definitions, 3 individual MCS are combined with revenue calculations and derive of measures. Figure 4 describes this process on a general level.

4.1 *V-model*

The risk simulation differs in main parts from classical safety or reliability simulations, which are more and more common in RAMS-processes.

For risk simulations the consideration of the technical and the economical area is needed. At first a system must be described—and programmed—on a technical level. For this description it has proven to be useful to use the top-down approach. Depending on the planned simulation level the system is being decomposed to the lowest data level.

For risk and warranty analyses it is useful to start with the entire system, separating it in functional groups, further in modules and at least in single subsystems with its components. With the MCS different simulation levels are possible and can be integrated in an entire system simulation. The simulation can handle different data levels given the case one functional group, e.g. the engine in a car can only be exchanged in one unit, while another group, e.g. the braking system, can be exchanged on part or component level. In each simulation run, which is one simulated warranty event, it is determined whether a part needs to be replaced or not. The sum of all parts and systems creates a technical requirement list containing all parts which has to be exchanged. Even the kind of exchange like small repair, full repair, part exchange or full exchange can be simulated if suitable data is available. Another technical issue is that the repair or exchange of a system implies the removal of other parts or systems. Especially in modern complex products the space has to be used extreme efficiently. Due to this a simple exchange of a light can presuppose the disassembly of other systems. To predict the costs of warranty events those technical presupposes have to be applied in the risk simulation.

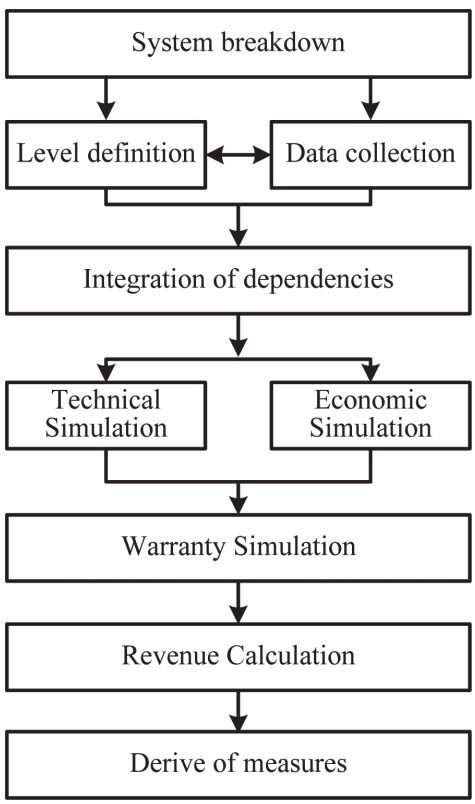


Figure 4. Risk simulation process.

In connection with the technical area, the economic area has to be combined with technical information to generated risk based results. The data needed for the economical input distributions can also be generated out of historical warranty data as well. It is very useful to transform the empirical data into distribution functions, if possible. With this transformation it is feasible to simulate the technical data with more expensive or cheaper costs than occurred in warranty data. A simulation with adapted cost distribution functions indicates the need for reviewing the adapted distribution to exclude implausible simulation results.

The empirical cost information or distribution functions are now connected with the technical requirement list from the previous step on the lowest data level. The part cost for each warranty event can now be aggregated back to subsystems, module groups and functional groups. In addition, a further query checks if the repair of single parts of a unit is more expensive than the exchange of a built unit. Via the MCS it is easy to implement and the results for all simulation runs can be extracted easily. Figure 5 shows the v-model for the MCS risk assessment approach.

Figure 5 shows only three different simulation levels.

If data is available on a higher level of detail or there are more dependency levels, the v-model can be extended accordingly.

4.2 *Input*

Many kinds of data can be programmed in the MCS. One possibility is the usage of field or test

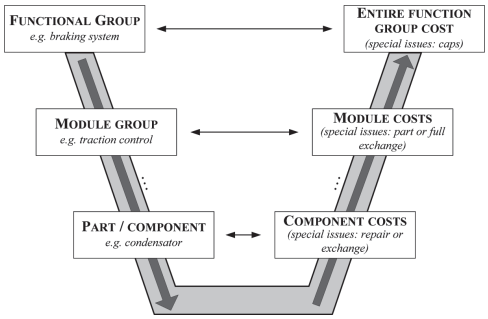


Figure 5. V-model for the technical and economical risk simulation.

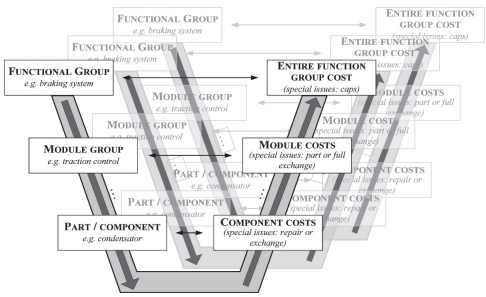


Figure 6. Multiple MCS layers.

data. Also qualitative data and expert knowledge in digital form (yes/no) can be implemented. The simulation can be transformed from the simulation in one-layer into many layers (see Fig. 6).

Different layers can be:

- usage information
- stress information
- individual market or region data
- different warranty rules
- different part versions
- different repair methods

The superposition of the different layers can be programmed via different quantiles of each layer or in different simulations, if asked for a comparison and not an inclusion of different layers.

Another important task in risk assessments is the prognosis of warranty cases and costs of new customers. Depending on different usage and stress factors (in comparison with the list of different layers) every customer has a different failure characteristic and special warranty needs. If the data is on a high quality level and contains different usage and stress information theses data can be adapted to new customers to generate a new customer profile. Also the change of the behavior of a customer can be analysed. In the automotive industry for example data from polluted or hot markets "A" can be used for other regions "C" with similar characteristics. Combined with the knowledge of the special usage behavior from a market "B" which is similar with the knowledge in "C" a customer profile for market "C" can be generated to negotiate a first warranty contract with this customer. This example illustrates the need for high quality data which presents a problem in many industries and at many levels. Due to the fact that this kind of data is not always available the MCS allows changing the simulation level of a single functional group or module very easily. If more detailed data for a special system is available the level can be adapted quickly. Additionally the new data can be used to validate and improve the results of the risk simulation.

4.3 *Revenue calculation*

The simulation of the costs of a warranty event and the statistical conclusions are only one part of the risk assessment process.

Also important is the calculation of the revenues of the warranty arrangement for the maintenance company. To consider this information a database is included in the risk simulation process, containing all warranty rules and maintenance contract details. After the cost simulation every simulation run is filtered by the revenue database which results in the real revenue of a warranty event. Beside the contract and warranty information economical company parameters like marginal returns and handling charges are included as well.

Classic parameters can be:

- Caps on components, parts, modules or systems
- Excluded material for some parts or components
- Different cost sets for special repair processes
- Dynamic parameters changed with the valid period of a maintenance contract
- Special customer parameters
- …

Due to the fact that every simulation run is checked with the revenue calculation and not the final result of the cost simulation, the revenue is also given by a distribution function, on the same level as the cost simulation. This kind of result provides a lot of possibilities for further analyses and derives of measures lowering the risk or increasing the revenue.

4.4 *Measures*

For a holistic risk assessment very flexible outputs and results are of great importance. Next to the result in kind of costs and revenues, also the amount of the contribution of every part or sub-

system to the result is needed to derive measures out of the analysis.

Therefore the MCS is very suitable due to the fact that every simulation run can be stored and analysed.

The most popular presentation of the results is the classic probability function or density. But also tornado graphs containing parts or layer information with high contributions to the entire risk analysis result are useful and can be analysed on a high detailed level. Examples of these presentations can be found in Chapter 5.

5 EXAMPLE

To describe the process disposed above this chapter contains a very simple example with some car components and parts. The values have been changed totally to illustrate the process and the presentation of the results.

In this case study three different functional groups, in one case separated in two module groups which consist of different parts, are going to be simulated (see Fig. 7). The contract type is a flatrate contract, with a valid period of 10 years. The rates are being paid in one year periods with one-tenth of the contract sum.

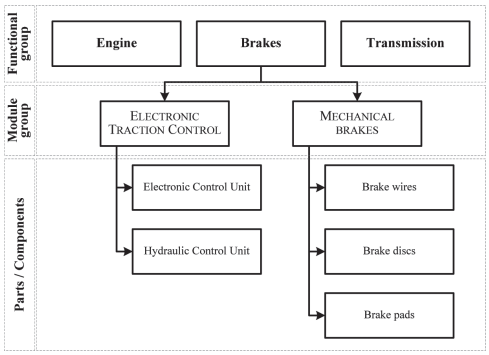


Figure 7. Structure of the example.

One simple technical dependency is given by the fact that, if one brake disc or brake pad has to be changed, the same parts of the other side of the axle have to be changed too. This is premised on safety reasons. If the condition of the brake discs or pads on one axle is clearly different the car can get out of control in full brakings.

The following technical conditions are given for this simple example. There are 3 different part conditions. Condition 1 (C1) is fully ok, only check costs accrue. Condition 2 (C2) is repairable, which means that parts have not to be changed. This condition includes an economical dependency. If the repair of a part is more expensive than the exchange, the part will be exchanged with the price of condition 3 (C3) which is defined as exchange needed.

For every part and condition the cost is defined and connected with the technical simulation of the part condition. Normally this cost information is generated on the basis of field data. In this simple example the costs for C1 and C3 are fix costs, and the costs for the repair (C2) are normal distributed via $N\sim(\mu,\sigma)$ due to the fact that not all repairs are equal in time and material expenditure. For the disc brakes, pads and wires a repair is not possible. These parts can only be C1 or C3. All technical parameters and the assigned costs are given in Table 2. Please remember, that all data for this example have been thinking up free.

The cost for the 10 year flatrate including all warranty issues mentioned above is 4.000€ including contribution margin, handling charges and so on.

Via MCS 1000 random customers are simulated with the aim to get the difference between the flatrate profits versus the warranty costs in years.

Figure 8 shows the simulated empirical distribution of the probability of the amount of warranty costs per contract.

As seen in Figure 8 the probability of a positive end of the warranty contract for maintenance company is about 50%. However, the total result for 1000 customers with a 10 year flatrate contract is clearly negative due to a negative average of the

Table 2. Technical parameters and costs for the simulation.

	P (C1)	Costs (C1)	P (C2)	Costs (C2)	P (C3)	Costs (C3)
Engine	0,89	10€	0,1	N~(5000,1000)	0,01	7.000 €
Brake—ECU	0,79	10€	0,2	N~(500, 100)	0,01	800 €
Brake—HCU	0,89	10€	0,1	N~(300, 50)	0,01	500 €
Brake—Wires	0,70	10€	0		0,30	100 €
Brake—Discs	0,40	10€	0		0,60	50 €
Brake—Pads	0,20	10€	0		0,80	20 €
Transmission	0,98	10€	0,01	N~(2000,800)	0,01	2.500 €

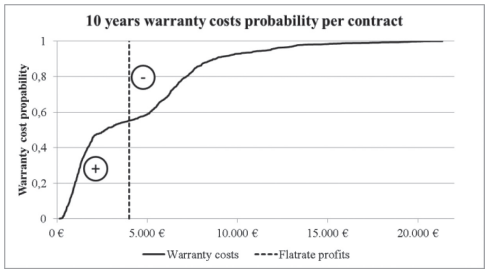


Figure 8. 10 years warranty costs probability per contract.

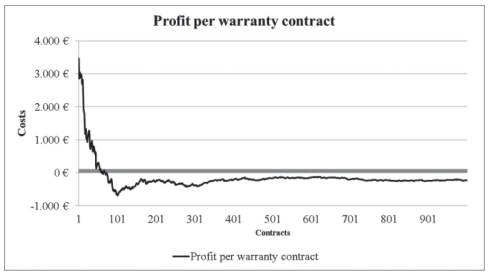


Figure 9. Average profit for all contracts.

Table 3. Summary of the economical simulation results.

	Average	Customers	Total
Flatrate profits	4.000 €	1000	4.000.000 €
Warranty costs	4.234 €	1000	4.234.888 €
Total revenue	–234 €	1000	–234.888 €

relation between costs and profit. Figure 9 shows the development of the average profit for all contracts.

As seen in Figure 5 the average profit in this simulation is almost constant at 400 simulated contracts.

The achievement of the constant value is required for the validation of the simulation results.

In total, this contract type with the given warranty issues and technical dependencies result in the total costs, profits and revenues given in Table 3.

In addition to the total results of the 10 years contract also the regression analysis is also of interest. The regression analysis describes the effect of the single technical components to the final result. The regression coefficients of the simulation for 1000 customers are given in Figure 10 and the input ranked by their effect on the Output Mean is shown in Figure 11.

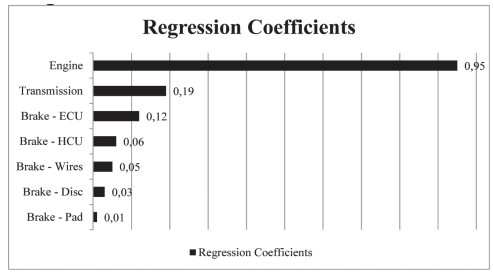


Figure 10. Regression coefficients of the simulation.

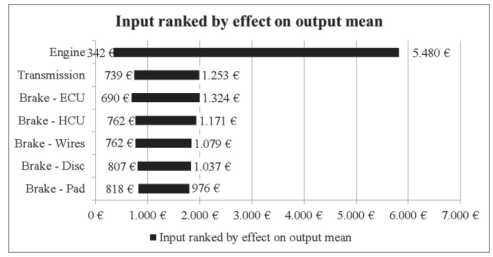


Figure 11. Input ranked by effect on output mean.

It becomes obvious that in this simple warranty cost simulation the influence of the engine status is the dominating parameter. Followed by the ECU & HCU the transmission has a lower impact than expected with regard to the warranty costs. But in combination with the high reliability, the effect is reduced strong.

The input ranked by effect on output mean is a comprehensible description of the risk parameters. The spread of the brake values is in total lower than the spread of the engine costs regarding to the output mean. The range of variation of the engine costs from min. 342€ to max. 5.480€ effect on the output mean confirms the regression analysis and adds the knowledge, that the engine maintenance is a risk but also a chance for profit maximizing.

6 SUMMARY/CONCLUSIONS

Not only technical safety and security issues can influence the risk potential of a product. Also the economical risks depending on the reliability of a product are very important for the manufacturer or the maintenance service company. New contract types are dominating the maintenance market. One example is the automotive industry which highly increasing warranty periods which new risk potential has to be transferred to the suppliers. Also flatrate maintenance contracts for end-users

become more and more popular, with new risks (and chances) for all parties involved.

In classical risk assessment approaches the technical and economical issues are analysed with different methods. The main reason for this is, in addition to the problem to get suitable data, a methodical problem. The methods to analyse technical risks are not compatible with economical issues and vice versa. This paper compares the most common and general methods for complex data analysis and manipulation. It concludes that the Monte-Carlo-Simulation is very suitable for risk assessment issues. The MCS, based on random events, can handle almost any common information (e.g. empirical, continuous, quantative data and expert knowledge). This is one of the major advantages of the simulation method due to the fact that different kinds of information are used in technical and economical issues. To perform a risk assessment with the MCS it is suitable to use an adapted v-model to connect the technical with the economical level. To get versatile outputs, MCS can be inserted in all typical statistic methods which offer a lot of possible output visualizations.

In addition the MCS is useable with conventional business laptops or notebooks and for not very complex technical systems or economical dependencies it is feasible with standard spreadsheet programs.

REFERENCES

Althaus, D.; Braasch, A.; Schlummer, M.; Meyna, A.: *Reliability and safety in full brake systems with ABS*. ESREL 2010 Conference, Rhodes, Greece.

Chan, N.; *Handbook of financial risk management.* 2013, Wiley Verlag, Hoboken. ISBN: 978-1-1185-7350-1.

Cox, L.A.: *Risk analysis of Complex and Uncertain Systems.*—International Series in Operations Research & Management Science 2009, Springer-Verlag, Boston ISBN: 978-0-387-89014-2.

Kolonko, M.: Stochastische Simulation—Grundlagen, Algorithmen und Anwendungen. 2008, Vieweg+ Teubner-Verlag/GWV Fachverlage GmbH, Wiesbaden. ISBN: 978-3-8348-9290-4.

Lee, M.-L.T.: *Risk assessment and evaluation of predictions*—Lecture Notes in statistics; 210—Proceedings. 2013, Springer-Verlag, New York. ISBN: 978-1-4614-8980-1.

Meyna, A.; Pauli, B.: *Taschenbuch der Zuverlässigkeitstechnik: Quantitative Bewertungsverfahren*. 2010, Carl Hanser Verlag, München. ISBN: 978-3-446-41966-7.

Plinke, F., Schlummer, M.; Braasch A.; Meyna, A.: *Reliability analysis with the Monte-Carlo-Method for complex systems in an early phase of development.* PSAM 11 & ESREL 2012 Conference, 25–29 June 2012, Helsinki, Finland,

Plinke, F.; Guennel, C.; Althaus, D.; Meyna, A.; *Methodical approach for analysing different stress factors by means of different usage behaviour on the basis of field data*. ESREL 2013 Conference, Amsterdam, Netherlands.

Preiss, R.: *Methoden der Risikoanalyse in der Technik.*—Edition TÜV Austria 2009, TÜV-Austria-Akademie, Wien. ISBN: 978-3-901942-09-9.

Zio, E.: *The Monte Carlo Simulation method for system reliability and risk analysis.* 2013, Springer series in reliability, London. ISBN: 978-1-4417-4587-5.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The results of a systematic study of the risks associated with the transportation of hazardous substances

D. Prochazkova, J. Prochazka & H. Patakova
Faculty of Transportation Sciences, Czech Technical University in Prague, Czech Republic

ABSTRACT: Statistics on traffic accidents annually contain a number of serious accidents involving the hazardous substances on roads and railways, which are accompanied by explosions, fires, leaks of hazardous substances into the environment, or a combination of the two to three mentioned phenomena which have impacts on the protected assets in a traffic accident site, and perhaps as a consequence of internal links and couplings they seriously damage the environment surrounding the accident site. By application of empirical data and procedures of risk engineering it was compiled the check list by which it is possible to determine the critical sites on roads and railways in advance, and it was tested specifically aimed What, If the method, by which it is possible to determine in advance scenarios of impacts of traffic accidents involving the hazardous substances and to determine critical aspects of critical sites from the viewpoint of protection of humans and other public assets.

1 INTRODUCTION

At present it comes up to increasing concern for the protection of human and to the awareness of the public there are entered the issues on security and sustainable development. It is intensifying the interest in recognition of risks and their elimination, respectively, on their elimination on the economic-social acceptable level. The current trend of research in the subject area is the integration of security features with an impact on a wide range of affected areas to complex safety solutions. Today we cannot understand the safety as partial separate segments, but we have to understand it in the complex way, that is, in its real and imaginary form, in all areas of natural or anthropogenic risks.

The basic function of the State is to ensure the security and development of human society, which is not possible without ensuring a safe space in which we live. The basis for safe community is a critical infrastructure, which is understood as a set of infrastructures ensuring the quality of life of the humans. To the critical infrastructure the transport infrastructure also belongs. Its main components are: elements such as terminals, bus stations, railway stations, airport, bridges, tunnels etc.; the traffic physical infrastructures that are made up from the liner constructions and which are important for ensuring the serviceability of a territory under normal, abnormal and critical conditions; and management systems. The subject of the paper is the protection of people from the risks associated with the carriage of dangerous substances by ground roads.

Traffic accidents involving the hazardous substances threaten the people, and therefore, there are subject to the safety management of the territory. For ensuring a safe space in which we live the current relevant international organizations (e.g. the UN, the OECD, the EU, NATO, UNECE), Governments, public administration (administrative authorities, regional and local authorities) have special programme the aim of which is to create a safe space for the 21st century. The real results obtained for the Czech Republic data are shown in next paragraphs.

2 TRANSPORT AND TRAFFIC ACCIDENTS INVOLVING DANGEROUS SUBSTANCES ON THE ROAD

Industry and economy of the countries depend on the hazardous substances that are transported from manufactures to users, to the storages of the waste etc. Hazardous substances are transported by road, rail, water, air and pipelines. Most transportation is done safely. According to the World Road Association PIARC (PIARC 2010), which has been in operation since 1909 and today brings together over 140 countries, the transport of hazardous substances in the EU countries makes up 5–8% of the total volume of traffic. PIARC has kept track of traffic accidents on the road, with the presence of hazardous substances since 30's years of the last century and since the 70's years it records their steep rise, Figure 1.

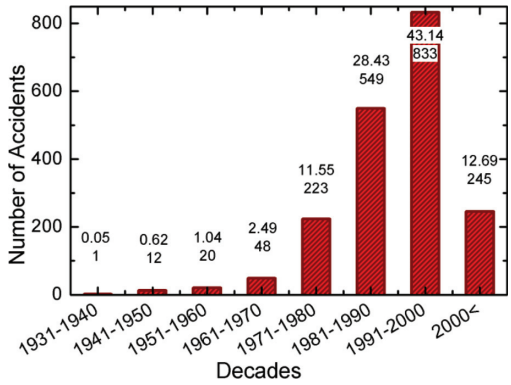


Figure 1. The number of traffic accidents involving hazardous substances (PIARC 2010).

2.1 *Hazardous substances*

Hazardous substances are chemical substances and chemical agents, which accompanies a human in everyday life. By various processes there are from them produced final products, which are part of the nutrition of human or his/her life in many domains, e.g. medicines, hygiene means and equipment, synthetic fertilizers, plastics, synthetic fibbers, etc. At the very beginning it is the mining of raw materials and their subsequent machining. It is followed by transport to the place of processing, storage, production of various intermediate products and, if necessary, transport and storage. Finally, by the various processes there are produced final products.

In each process the chemical substances behave in such a way that corresponds to their nature. Chemical substances have the same properties in the few grams and in many tunes quantities, i.e. in mega kilograms. The severity of the impacts of chemicals on the environment depends on the direct proportion of their quantity. It is, therefore, only on humans, in order to ensure the safe development and use of all chemicals and at the same time at the lowest possible rate cut their unacceptable impacts, both through highly specialized technical discipline, safety engineering and, secondly, also by shoring up the knowledge level of the society as a whole. This means that in human society is promoted a certain safety culture (Prochazkova 2011a, Prochazkova & al 2008).

2.2 *The transport of hazardous substances*

Transport of hazardous substances takes place largely on ground roads what are the liner constructions of transport infrastructure, which is a fundamental part of the critical infrastructure of the territory. They are important for ensuring the service of a given territory under conditions of normal, abnormal and critical. At present there are transported a variety of harmful and toxic chemicals used as raw materials in the industry. The amounts of these chemicals in the transport range from kilograms after dozens of tons. As the possibility of leakage of harmful chemicals in transit is the most dangerous (because in such occurrence it is a lack of specialized catch equipment, on the accident site it is not immediately trained specialized personnel and equipment for the disposal of leakages), and also it is relatively the easiest possibility of puncture of the tank in a car accident, leaks at pumping, overheating, overfill of containers, etc., it is necessary to have this domain regulated by laws, which provide rules for loading, transporting and technical requirements to transport equipment.

Transport on ground roads is according to (Prochazkova & al 2008), codified by a number of provisions, however, it is the fact that so far none legislation does not regulate the transport of chemicals in sufficient details. Therefore, in most of countries it is used a number of international regulations, which, however, are not compatible with other countries' legislations, or each other (Prochazkova & al 2008); therefore, the solution of some problems is long.

Road and rail transport is permitted only to carry dangerous goods as defined in the international treaties, which the Czech Republic is bound and which have been promulgated in the collection of laws. For rail transport, according to the Convention concerning international carriage by rail (COTIF), adopted in Bern on the May 9, 1980, the use of procedure for the international carriage of dangerous goods by rail (RID) and the uniform rules concerning the contract for international carriage of goods by rail (CIM), which regulates the international directive UIC (471-1 in); and for road transport with regard to the international agreement of the ADR (European Agreement concerning the international carriage of dangerous goods) (Prochazkova & al 2008).

2.3 *Knowledge about the accidents with the presence of hazardous substances*

Statistics of road traffic accidents annually, contain a number of serious traffic accidents involving the hazardous substances on roads and railways, which are accompanied by explosions, fires, spills of hazardous substances into the environment, or a combination of two to three phenomena, which has impacts on protected assets in a site of traffic accident and, as a result of internal links and couplings it seriously damaging the

environment and other assets in the wider area of traffic accidents' sites.

Specialized literature contains descriptions of accidents involving the hazardous substances, which caused tens of millions of dollars in damage and great loss of human lives. At accidents on the roads there are threatened humans, property and the environment, that are in the area of ground roads. Figures 2 and 3 show the impacts of the oil train accident that happened on July 6, 2013 in the town of Lac-Mégantic in Canada (Canadian Press Agency 2013). The train, consisting of 5 locomotives, one auxiliary car and 72 loaded oil tankers spontaneously started, derailed, there were several explosions, and the city was flooded with oil and large fires. It was destroyed more than



Figure 2. The impacts of the oil train accident that happened on July 6, 2013 in the town of Lac-Mégantic (Canadian Press Agency 2013).



Figure 3. The impacts of the oil train accident that happened on July 6, 2013 in the town of Lac-Mégantic (Canadian Press Agency 2013).

30 buildings, killed more than 80 people, 10 people remained unaccounted for, evacuated more than 2000 people because of the threat of toxic gases and fire. The next big train accident with presence of oil was on December 23, 2013 in North Dakota (Reuters Agency 2013). Half of the 106 carriages of the train derailed after a collision with another train. After it into the air, it raised a massive fireball. Authorities have evacuated due to heavy black smoke, the adjacent village of Casselton with 2 300 inhabitants.

Authorities ordered residents of a half mile of the remote Casselton to their homes for a time. County Sheriff at the same time recommends to people living within eight kilometres to the South and East of the accident site, to be evacuated. ***All the people in and around 16 km then it was recommended that in this time from they did not ventilate at home.*** After the crash, the causes of which have not yet been found, it went off the track 50 wagons. At least ten of them began to burn. The vicinity was clouded by impenetrable smoke.

According to the data of customs reports in the EU today they also run a trains with oil in Europe, they have 30–50 wagons, i.e. it's not about science fiction, when considering such hazards.

Therefore, the major traffic accidents involving the chemical substances are a subject to the safety management of the territory. Clarifying the causes of traffic accidents involving the hazardous substances is very complex, because it often happens that the safety data sheets, which belongs to the mandatory documentation of vehicles carrying the chemicals, are not complete or entirely absent; sometimes they are only in the language of the carrier (Prochazkova 1993).

On the basis of investigations in the USA and the UK (Lum & Reagan 1995) from the year 1985 the causes of traffic accidents on the roads are divided as follows:

- 57% of the human factor of the driver,
- 27% a combination of factor of the road and the driver human factor,
- 6% a combination of driver human factor and a factor of the vehicle,
- 3% the factor road,
- 3% a combination of factors of the road, drivers and vehicles,
- 2% the factor of the vehicle,
- 1% a combination of road and vehicle factors.

To accident origin they contribute the design of the vehicle, the speed and density of traffic, road design, environs around the road, skill and defects in the behaviour of the driver. In the professional literature, you can now find lots of models showing the factors interconnection, e.g. at work [8] it can be found simple model of the causes of traffic

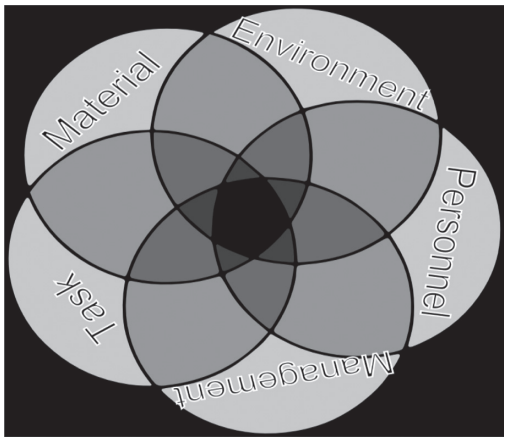


Figure 4. Causes of road traffic accidents (Canadian Centre for Occupational Health and Safety 2012).

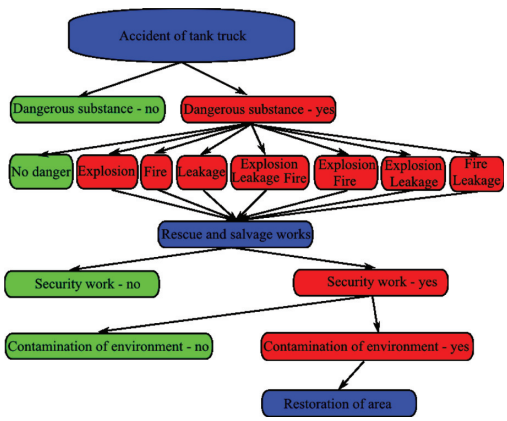


Figure 5. Process model drawn up for the needs of planning activities associated with transportation accidents involving hazardous substances (Prochazkova 2011a).

accidents involving the hazardous substances, Figure 4.

Because at transport the chemicals behave in such a way that matches their nature (Prochazkova & al. 2008), it is necessary to follow every accident involving the hazardous substances from the perspective of ensuring the safety according to the process model, which is shown in Figure 5.

3 DATA AND METHODS USED FOR PROCESSING THE DATA IN A DATABASE

On the basis of current knowledge the safe territory and safe transport in the territory can be ensured only if they are adequately managed and traded-off the risks, i.e. if it proceeds strategically, systematically and proactively (Prochazkova 2011a). Therefore, we have compiled a database of accidents involving the hazardous substances for the Czech Republic (CTU 2013).

The data in the database are evaluated through ordinary methods of mathematical statistics and by the specific methods of risk engineering, i.e. using a specially drawn up a checklist, and What, If method revealing the impacts of accidents involving the hazardous substances on public assets (Prochazkova 2011b). Application of empirical data and procedures of risk engineering the special checklist has been drawn up, which you can specify in advance the critical places on the roads and railways with regard to the transport of hazardous substances (Prochazka 2013).

4 THE RESULTS OF THE RESEARCH ON TRAFFIC ACCIDENTS INVOLVING THE HAZARDOUS SUBSTANCES

We present selected results obtained from investigation by statistic methods and one selected result obtained by risk engineering method; the other results are in the Archives (CTU 2013).

4.1 *The selected results of the statistical surveys*

The analysis of the database of traffic accidents involving the hazardous substances (CTU 2013) shows that there are carrying the different sorts of chemicals: fuel; oil; highly flammable substances; nitric acid; sulphuric acid; lactic acid; phosphoric acid; nitrates; zinc phosphates; manganese phosphates; nickel phosphates; potassium hydroxide; styrene; liquid chlorine; argon gas; formaldehyde; asphalt; lime; powdered PVC etc. There are a total of road accidents involving the hazardous substances hundreds annually and evaluated damage to property associated with the deterioration of the dangerous substance understood as goods associated with them reach hundreds of millions. Other costs are associated with the response (it is often necessary to pump over a hazardous substance, which requires special equipment and technology), clean-up, and renovation of ground roads and with the interruption of the supply chains and stopping the passenger services. These traffic accidents are also accompanied by lighter or heavier injuries of passengers and deaths, damage to roads and property in the vicinity of roads, as well as environmental damage.

On the basis of the source (CTU 2013) they have been drawn up two frequency dependences

for traffic accidents involving the hazardous substances, on the roads, Figures 6 and 7.

Figure 6 shows: the downward trend in the total number of traffic accidents involving the hazardous substances on the territory of the Czech Republic in the years 2007–2010; and the number of traffic accidents involving the hazardous substances depends on the deployment of the main traffic arteries—the most traffic accidents involving the hazardous substances falls annually on the Central Bohemian Region, which is followed by the Southern Moravia Region, Zlin Region, Vysocina Region, Usti nad Labem Region, Liberec Region, the Moravian-Silesian Region and Olomouc Region. The first figure is pleasing. The second figure is in line with the findings of the early 1990s. years (Prochazkova 1993), where as the main source of traffic accidents

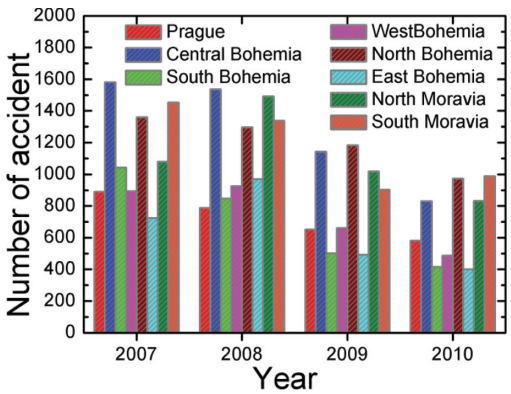


Figure 6. Frequency distribution of traffic accidents with the presence of a hazardous substance on the road for the years 2007–2010, differentiated according to regions.

involving the hazardous; substances was revealed traffic from Asia minor and the Balkans in the direction of Rotterdam, i.e. to the Europe's largest port, in which hazardous substances are translated on the ocean-going ship. This data is in its own way worrying, because the evaluation of traffic accidents involving the hazardous substances in the cited report, made at the turn of the years 1992 and 1993 proposed the need to perform measures, mainly processing and adoption of good legislation for the domain in question, in order to protect the lives and health of people and the environment in the Czech Republic.

From the data in Figure 7 it is an obvious seasonal trend in the occurrence of traffic accidents involving the hazardous substances, i.e. the largest occurrence of traffic accidents involving the hazardous substances is in the summer months, from April to June.

Recorded traffic accidents involving the hazardous substances on the Czech railways show that carrying all sorts of chemical substances: flammable solids substances, substances liable to spontaneous combustion, corrosive substances, poisonous substances and other dangerous substances and articles. The frequency distribution of traffic accidents on the rail with the presence of hazardous substances for the years 1996–2010 is shown in Figure 8. We observe that most of the accidents on the rail with the presence of hazardous substances were in 1997; their number exceeded 700. In the period 1998–2004, the annual number of accidents involving the hazardous substances increases. In the years 2006–2010 there is a decline in the annual number of accidents involving the hazardous substances and, in the years 2009 and 2010 reached under a value of 100, which may, however, be the result of a decline in industrial production, which

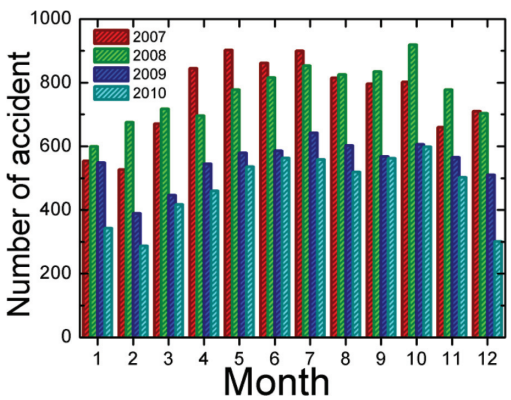


Figure 7. Frequency distribution of traffic accidents involving the hazardous substances for the years 2007–2010, differentiated according to the months.

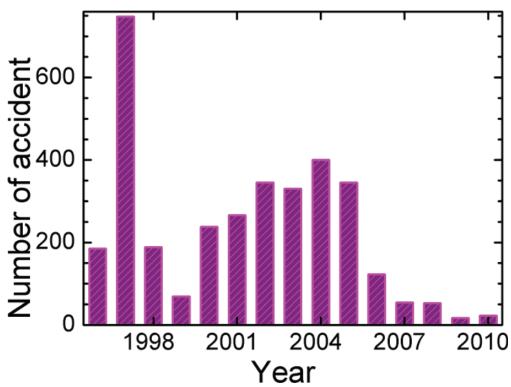


Figure 8. Frequency distribution of traffic accidents involving the hazardous substances for the years 1996–2010.

is naturally linked to the transport of hazardous substances.

Figure 8 shows the frequency distribution of traffic accidents involving the hazardous substances for the years 1996–2010. There were transported flammable, combustible and liable to spontaneous combustion, solid, toxic, corrosive, etc. substances; the most of flammable substances are fuel substances; the second place ranked traffic accidents with the presence of corrosive substances, which is very dangerous, because the substance in the release into the environment pose a great danger to surface and underground water and sewer system; a significant percentage have a traffic accident with the presence of toxic substances, which is dangerous for both people and animals, and the environment (CTU 2013). Further investigation will focus specifically on poisonous substances and explosive substances and performs the simulation possible scenarios of the impacts of accidents in places with large amounts of people and other assets of the human system to identify the places in which it is necessary to perform safeguard measures in the interest of security and further development of the people.

4.2 *Selected results obtained by the What-If method*

To illustrate, there are here the results of the method, What If for the territory in the vicinity of the intersection of the D1 highway and the road "class 1, No. 52", Figure 9, in which according to our database of accidents involving the hazardous substances (CTU 2013) there are frequent accidents with the presence of oil products (mostly fuel—gasoline). The overall look on a given site is shown in Figure 10.



Figure 9. Scheme of territory in the vicinity of the intersection of the D1 highway with the road, class 1, No. 52.



Figure 10. The overall view on the stretch of road No. 52.

The reference section of the D1 highway is located to the South of the city of Brno on 194 km from Praha. In the area it is also departure from the highway, which leads from the North to the centre of the city of Brno and to the South along the road class1, No. 52 in the direction to Vienna. In vicinity of the highway it is a shopping zone with a filling station, then the industrial zone, where mainly dominated technical services and warehouses, supplying the city of Brno. In the zone a railway trail is located. In the investigated area they are also a residential zone and the allotment, along the highway it leads the railroad, and the Leskava River, which flows into the Svratka River. On the road No. 52 in both directions, there are the tram tracks.

The assessment of impacts of traffic accident involving the oil products is performed by the What, If method that is specially modified for the safety management of the territory (Prochazkova 2011b). The results of the evaluation are listed in Table 1.

From Table 1 it follows that recovery after some damage will require a longer period of time, e.g. damage of engineering networks, groundwater contamination, damages as damage of sewer infrastructure need always longer time for renovation; e.g., traffic accident on the D1 highway near the village Kozlov in 2004 caused in the village sewer system a set of explosions that very damaged sewer system (CTU 2013) and renovation lasted several months.

Considering the results of other What, If analyses of traffic accidents with presence of hazardous substances in other urban areas (Prochazkova & al. 2013) it is necessary to solve identified problems. E.g., it is necessary to ensure the readiness of the municipalities with extended competence for overcome of consequences of great traffic accidents with the presence of hazardous substances. They must pay great attention to objects with a

Table 1. Results of What-If analysis of traffic accident with oil products, at the junction of the D1 highway with the Brno-Vienna road, class 1, No. 52, on the territory of the city of Brno. DN—the impacts of a normal traffic accident, NL—other impacts traffic accidents involving the hazardous substances (fuel, oil products); the impacts are listed in the times of 0, 3 and 12 hours and 3 days, taking the time of 0 indicates the time of the accident origin; the symbol ** indicates that no further new impact.

Protected public assets	The impacts
Human lives and health	DN: 0 h-death or injury to participants in a traffic accident, 3 h, 2 h, 3 days ***. NL: 0 h-heavy fires and explosions (highly flammable vapours create with air explosive mixture), thick smoke affects humans and damages human health—vapour with a higher concentration affect as narcotic, provoked the skin, membranes, eyes and respiratory system; 3 h—damage to health by fire with high temperatures; 12 h—damage to health by missiles in a case of leakage of oil products into the sewage and at origin of explosive clouds in the nearest vicinity (there are affected humans in the industrial zone and the shopping area, which is located in the gas station), 3 days ***. ***Numerous losses on humans live as a result of traffic accidents, the subsequent fire and explosions in the sewer system. The place is located in a densely populated area on the outskirts of Brno, where are dense drainage networks.***
Human security	DN: 0 h—stress of drivers in the traffic jam, 3 h—the growing stress of drivers, the disruption of human security in the surrounding municipalities (Moravany, Dolní Heršpice and Přízřenice) and in areas of Brno in which there are detour routes, 12 h ***, 3 days—the inconveniences caused by traffic restrictions due to damage to the ground roads. NL: 0 h-stress to the panic caused by origin of the fire and explosions in the area of the accident, 3 h—stress and panic during the evacuation of the nearby parts of the city of Brno, 12 h—fear from origin of subsequent explosions of the leaked fuel and oil substances, persistent disruption of peace in villages and in urban areas around the detour routes, 3 days ***.
Property	DN: 0 h—damage of ground road due to traffic accidents (road surface, the pillars of bridges, tramway tracks, railways and railway trail) and the buildings in surrounding, 3 h—possible disruption to production in the industrial zone, 12 h ***, 3 days ***. NL: 0 h—damage to the destruction of traffic ground road and buildings in the vicinity due to fire and explosions, 3 h—damage to the destruction of the buildings in the surrounding municipalities and city districts caused by explosions of the leaked fuel and oil substances in the sewer system, then the loss of profit of stores and operators of industrial zone in the evacuated areas, 12 h—persistent loss of profits of stores and operators in the evacuated areas, 3 days—as a result of the destruction of the monitored intersections by the explosion there are over-utilized detour ground roads and factories and plants inside the affected zone are affected by worse traffic situation. *Big losses on buildings, property and ground roads as a consequence of explosions of fuel and oil substances and petrol fumes in an accident side and in the sewer system*.
Environment	DN: 0 h—contamination of Leskava River (Leskava River flows into the Svratka River) and the soil by leakage fuel and oil substances, 3 h—damage to the flora and fauna in the contaminated waters and soils, the deterioration of the atmosphere in the villages on the detour routes, 12 h ***, 3 days—the weakening of the ecosystem due to contamination. NL: 0 h—water contamination (Leskava River flows into the Svratka River), soil and air (in the air a lot of fumes and vapours), damage of greenery due to fire, 3 h—damage to the flora and fauna in the accident site and its surrounding, the persistence of the devastating impacts of fire, 12 h—damage to air quality round the detour routes, 3 days—the weakening of the aquatic ecosystems due to the contamination of surface water and ground water, the destruction of ecosystems as a result of a fire in the accident site and its surrounding. *Long-term groundwater contamination.*
Infrastructure and technology	DN: 0 h—failure of the affected section of the D1 highway (exit 194), road, class 1, No. 52, 3 h—out of function of affected sections of ground roads, trails, 12 h detour routes overload ***, 3 days-decommissioning of the affected leg due to traffic accidents, damage to the detour ground routes due to overload. NL: 0 h—loss of function to destruction of the followed part of the D1 highway and ground road No. 52, 3 h—malfunction of the affected parts of ground roads, possible destruction of ground roads, and other infrastructures and technological facilities due to explosions of petroleum substances and overloading of detour ground routes, 12 h—loss of function of affected sections and overloading the detour ground routes, 3 days—permanent damage to affected areas due to traffic accidents, fires and explosions, damaging the detour ground routes due to overload. *Serious damage to sewers and other utility networks as a result of explosions of vapours oil substances. Paralysis of the transportation infrastructure of Brno.*

(*Continued*)

Table 1. (*Continued*)

Protected public assets	The impacts
Emergency services (police, fire, paramedics)	DN: 0 h—a reduction of the availability of the components of the Integrated Rescue System (IZS), 3 h—reduction of the availability of the IZS components, 12 h ***, 3 days ***. NL: 0 h—a reduction of the availability of the IZS components, 3 h—reduction of the availability of the IZS components, 12 h—a reduction of the availability of the IZS components, 3 days ***.
Supply chains	DN: 0 h ***, 3 h—the disruption of supplies from warehouses in part of Brno the connection of which with Brno is out of function due to damaged ground roads at traffic accident, 12 h ***, 3 days ***. NL: 0 h ***, 3 h, 12 h—disruption of the supply of the Brno from boxed warehouses, 3 days ***.

large number of people (employees and passengers at the time of travel to work and from work from residential parts; transfer to and from schools, shopping malls and medical centres) and also to sites with technologies, which may cause a domino effect. It would be useful if the municipal authorities should have any agreement with schools, hospitals and shopping centres for an emergency case, how best to handle the evacuation, because only a sucker may assume that the task will pulled off by management of objects with a large number of people, or by the Fire Department, that will have to reduce the criticality of the situation and to carry out prompt response to the explosions and fires.

5 CONCLUSIONS

For the protection of the people it is necessary to perform the separate concept of transport, based on a systemic approach that allows keeping up tempo with the technological developments of transport systems that considers the needs of people and transport serviceability, environmental protection and reduces economic damage. Public authority is necessary in co-operation with experts to define the issues which are necessary to solve and to process the relevant studies in the sense of the above recommended procedure—i.e. to determine how the protection of humans will be ensured in places with a high number of people.

After the losses and damage caused by traffic accidents caused by oil trains in the North America in 2013, it is necessary to pay more attention to safety culture and human security. In the event of traffic accidents at settled areas it is necessary to pay great attention to objects with a large number of people and also the sites with technologies, which may cause a domino effect. It would be useful if for any emergency the municipal authorities should prepare agreements with schools, hospitals and shopping centres, how best to handle the evacuation, because this is the way of human survival at emergency situations.

ACKNOWLEDGEMENTS

The authors wish to thank the CTU in Prague for the under grant SGS13/158/OHK2/2T/16, in frame of which the work was processed.

REFERENCES

Canadian Press Agency 2013. http://www.lapresse.ca.

Canadian Centre for Occupational Health and Safety 2012. *Reports on Traffic Accidents*. www.ccohs.ca.

CTU 2013. *Archives*—Database of Accidents Involving the Dangerous Substances. Praha: CTU.

Lum, H & Reagan, J.A. 1995. *Interactive Highway Safety Design Model Design: accident Predictive Module*. Public Roads Magazine. http://www.fhwa.dot.gov/publications/publicroads/95winter/p95wi14.cfm PIARC, 2010. www.piarc.org.

Prochazka, J. 2013. *A Checklist for the Assessment of the Criticality of the Selected Sites of Ground Roads*. In: Požární ochrana 2013. Ostrava: SPBI, ISBN: 978-80-7385-127-9, ISSN: 1803-1803, pp 202–204.

Prochazkova, D. 1993. *The Conclusions of The Investigation of The transport of Dangerous Substances on the Main Roads in the Czech Republic and of Road Accidents Involving The Dangerous Substances in 1991–1992*. Report for the Ministry of State control of the Czech Republic, Praha: MSK, 1993, 126 p.

Prochazkova, D. 2011a. *Strategic Safety Management of Territory and Organisation*. ISBN 978-80-01-04844-3. Praha: ČVUT, Praha, 483 p.

Prochazkova, D. 2011b. Methods*, Tools and Techniques for Risk Engineering*. Praha: ČVUT, ISBN: 978-80-01-04842-9, 369 p.

Prochazkova, D., Bumba, J., Sluka, V. & Sestak, B 2008. *Hazardous Chemical Substances and Chemical Preparations and Industrial Accidents*. Praha: PAČR, ISBN 978-80-7251-275-1, 420 p.

Prochazkova, D., Patakova, H., Prochazka, J., Prochazka, Z. & Strymplova, V., 2013. *Results of Systematic Study of Risks connected with Transport of Dangerous Substances*. In: Ochrana obyvatelstva 2014. ISBN: 978-80-7385-142-2, ISSN: 1803-7372, SPBI, Ostrava 2014, 191–194. Reuters Agency 2013. *Report 31.12.2013*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Preference risk assessment of hazardous substances road transportation

D. Rehak, A. Bernatik & P. Novotny
Faculty of Safety Engineering, VŠB-Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT: Current techniques and methods of risk assessment in the field of hazardous substances road transportation are oriented especially towards assessing the impacts of potential accidents on population and the environment. However, every subject affected has different preferences arising from the nature of his activities. While a carrier prefers maximum profit arising from safety transport, public administration authorities prefer ensuring maximum safety of population and other public estates and properties. At the same time, it is necessary to point out that current legal regulations make a significant drawback in the field of ensuring safety of hazardous substances road transportation. The above mentioned legal regulations do not require risk assessments from the road carriers of hazardous substances. Therefore, carriers do not carry out such assessments, as the data gained from accessible techniques and methods do not provide them with requested information.

Applying the multi-criteria preference risk assessment of hazardous substances road transportation brings a suitable solution to the current situation, as it lies in setting criteria by considering real threats as well as all potential areas of their impact. Subsequent implementation of weight coefficients enables the assessor to prefer his concerns, while the final risk listing provides him with requested information regarding his activities. Realizing such assessment brings complex increase in preventive safety measures in hazardous substances road transportation, since it enables the carrier to realize not only primary risks connected with possible economic loss, but also secondary risks related to the impact on population and other public estates and properties.

From the economic point of view, hazardous substances transportation is a subject of business like any other. However, in comparison with other areas of business, its impacts may be much higher and more serious. In spite of this fact, the risk assessment in the area of hazardous substances road transportation is not required by legislation within the EU. This obligation is only set for stationary sources (Directive 2012).

Moreover, hazardous substances road transportation is a very specific area with a disunited attitude within the issue of risk assessment. This attitude is a subsequence of different preferences of individual interest groups. Owners of transport companies, whose main goal is the maximization of the transport profit, have a different point of view from the public administration authorities who strive for ensuring maximum security of the given transport. There is another point of view, presented by various stakeholders, like purchasers of hazardous substances owning the security certificates or ecological activists. The consequence is a singnificantt diferentiation between the recommended (by the public administration authorities) and the eccepted (by the hazardous substances road transporters) security measures.

On the basis of the above mentioned facts, the authors present a possible solution of the given situation by means of risk assessment of hazardous substances road transportation, where each assessed subject matches identical criteria with various prefecences reflecting his or her interests.

1 MATERIALS AND METHODS

1.1 *Accidents and their impact*

In the past, there have been a number of accidents during hazardous substances transportation around the world, for emample (Oggero et al., 2006):

1. Road accident in Houstonu, USA in 1976, ammonia leakage, 6 casualties, 178 injured; Road accident in San Carlos, Spain in 1978, propylene explosion, 200 casualties,
2. Railway accident in Mississauga, Canada in 1979, LPG explosion and chlorine leakage, 200 thousand people evacuated; railway accident in Montanas, Mexico in 1981, chlorine leakage, 28 casualties, and 1000 injured.

The outcomes of the study show (Guidelines, 2005a) that the accident frequency occurring on roads and railways during hazardous substances transportation has been increasing. At the same time, the outcomes show that more than a half of

the accidents have happened on roads (63%). The most frequent impact of the accidents has been substance leakage (78%), followed by fires (28%), explosions (14%) and gas clouds (6%).

1.2 *Methods of risk assessment of hazardous substances transportation*

Risk assessment of hazardous substances transportation may be realized by means of various methods based on qualitative assessment (estimating merely the consequences of accidents) as well as complicated quantitative methods (which, apart from estimating consequences of accidents, determine probability of accident occurrence).

The European legislation neither determines nor recommends any method in this area. In spite of that, it can be stated that the most suitable methods are those like Chemical Process Quantitative Risk Analysis (CPQRA) and Chemical Transportation Risk Analysis (TRA) issued by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE).

The CPQRA method (Guidelines, 1999) serves for quantitative estimation of chemical processes risk. It uses a complex of methods in the logical process of chemical processes risk assessment by means of risk measure which is the result of risk summarization of selected undesirable accidents. Sollution is carried out in stages, starting with statement and development of undesirable events of the investigated risk realization and aiming at assessing consequences, impacts and probability of all terminal scenarious of selected undesirable events. At the same time, it includes suggestions for risk reduction. For quantification of consequences and impacts, modeling of physical-chemical processes and phenomena is used (leakages, dispersions, fires, explosions, risk receiver vulnerability—models of burst and response: concentration, function probit, heat radiation, overpressure).

The TRA function (Guidelines, 2005a) states kinds of malfunctions and its frequency for individual types of transport (pipelines, railway, road transport, boats, oceanic crafts), choice of possible accident scenarios, case studies, etc. The method may also be used for mere identification of possible risks. The TRA may help with choosing the type of transport, way of transport, possibilities of combining various types of transport, suitable transport alternatives, the most suitable containers. It can also help develop plans for solving emergencies, managing transport risks, etc. The right application of TRA within the risk management enables one to decide about an alternative way of transport, suitable route, travel limits (speed, weather, time of he day), size of consignment (the total volume), etc.

1.3 *Multicriterial assessment*

Currently there is a whole range of multicriterial assessment techniques, differing in their abilities (e.g. Figueira et al., 2005). Matematically, the decision model can be formulated in the following way (relation 1):

$$\max \quad u_i = \sum_{j=1}^{m} pm_{i,j} \cdot w_j \tag{1}$$

where utility u of variant i, defined as a sum of weighted (w) performance measures pm of the criteria j, is maximized. Definition (1) presumes that the criteria used in the decision analysis are independent of each other (Fishburn, 1965).

Matematical considering of the given assessor or specific interest groups is suitable to be realized by implementing weight coefficients of individual criteria. These weight coefficients might be set by using simple methods (e.g. the method of point llocation, the method of weighed order, the method of alkaline variant, the method of Fuller's triangle) or using more complicated methods based on pairwise comparison which support criteria hierarchy assessment. (Řehák and Šenovský, 2014). The most suitable methods based on pairwise comparison are Analytic Hierarchy Process AHP (Saaty, 2008) or Analytic Network Process ANP (Saaty, 2004), or methods based on utility function quantification or a combination of the above mentioned methods (Weil and Apostolakis, 2001).

2 RESULTS

2.1 *Preferencial risk assessment*

Preferencial risk assessment enables the assessor to implement subjective conditions into an otherwise objective process of risk evaluation. Therefore, it enables the assessor to have a partial influence on the assessment process by preferring certain coefficients to others. This part of the process is important, since every subject perceives certain risks from a different point of view, which subsequently leads to discussion among all stakeholders and to choosing the most suitable security measures.

There are three main groups of stakeholders in the field of hazardous substances road transportation that are entitled to regulate the transport safety:

1. Road carriers of hazardous substances,
2. Public administration authorities:
   a. ministry of the environment,
   b. county council,
   c. affected villages,
3. Other interest groups (e.g. purchasers of hazardous substances or ecological activists).

Preferences of the road carriers of hazardous substances are above all connected with the financial aspect of the transport. The aim of he carrier is gaining a maximum profit from the transport, which is closely connected with the transport safety. In case of an accident the carrier loses the profit as well as the transport vehicle during the repair, which prevents him from earning further profit.

On the other hand, public administration authorities preferences are based on socioenvironmental aspect. The authorities primarily try to ensure maximum safety of population and environment during hazardous substances transportation, considering economic and technological possibilities of the carrier. There are secondary preferences like transport infrastructure security or ensuring transport smoothness.

The last group is formed by other interest groups. Their preferences differ according to their relationship to the carrier. For example, purchasers of hazardous substances, who are holders of safety certificates (e.g. ISO 14 000 or Eco Management and Audit Scheme), prefer the goodwill of supplier companies. As opposed to that, ecological activists strive for maximum environment protection regardless.

2.2 *Multicriterial risk assessment of hazardous substances road transportation*

The essence of multicriterial risk assessment is the right criteria setting. In relation with risk assessment of hazardous substances road transportation, the criteria are divided into three main groups: (Řehák et al., 2014):

1. criteria related to the level of vulnerability of the subjects affected (i.e. population, environment and the road carrier's property),
2. criteria related to evaluating the level of hazardousness of the realized transportation,
3. criteria related to evaluating the level of intended security measures.

2.2.1 *Criterial vulnerability assessment*

Criteria related to assessing the level of vulnerability may be divided into three groups reflecting different vulnerability of the subjects affected:

1. criteria related to population vulnerability assessment, i.e. Occurrence of densely populated areas and Occurrence of buffer zones of water resources.
2. criteria related to population vulnerability assessment, i.e. Occurrence of protected areas and Occurrence of buffer zones of water resources.
3. criteria related to means of transport and cargo vulnerability assessment, i.e. Value of transport technology and Value of the transported cargo.

Occurrence of densely populated areas (V_{POP})—with growing density of populated areas on the hazardous substances transport route there is a potential growth of population vulnerability.

Occurrence of protected areas (V_{PRO})—with the growing number of protected areas on the hazardous substances transport route there is a potential growth of environment vulnerability.

Occurrence of buffer zones of water resources (V_{WR})—with the growing number of buffer zones of water resources on the hazardous substances transport route there is a potential growth of environment and population vulnerability.

Value of transport technology (V_{VT})—carrier's pecuniary loss caused by the damaged transport technology.

Value of the transported cargo (V_{VC})—carrier's pecuniary loss caused by the destruction of the transported hazardous substance.

2.2.2 *Hazardousness assessment criteria*

The level of hazardousness of the realized transport is assessed by means of the following criteria: Hazardousness of the transported substance, Amount of the transported substance, Average age of the transport technology, Average age of the road on the route, Driver's experience and skills and Weather.

Hazardousness of the transported substance (H_{HS})—the level of hazardousness derived from hazardous qualities of the transported substance (e.g. explosiveness, inflammability).

Amount of the transported substance (H_{AS})—the level of hazardousness derived from the amount of the transported substance.

Technical condition of the transport technology (H_{TC})—the level of hazardousness resulting from a bad condition of the transport technology.

Driver's experience and skills (H_{ES})—the level of hazardousness resulting from low experience and bad skills of the driver.

Average state of the road on the route (H_{SR})—outside influence that may have a negative effect on the safety of hazardous substances transportation.

Weather (H_W)—outside influence that may have a negative effect on the safety of hazardous substances transportation.

2.2.3 *Safety measures assessment criteria*

The level of intended safety measures is assessed by means of the criteria of Viability, Effectiveness, Financial demandingness and Time demandingness.

Effectiveness (S_E)—the ability of safety measures to minimize the effect of threat and its impact on the asset.

Feasibility (S_F)—accessibility and utilizability of technological measures to minimize the threat.

Criteria of financial and time demandingness are directly related to the criterion of viability.

Financial Demandingness (S_{FD})—accessibility of financial sources to implement safety measures.

Time Demandingness (S_{TD})—time needed for safety measures realization.

2.2.4 *Criteria specification and indexation*

Specification and indexation must follow after setting the criteria. Specification is based on listing various variants of the given criterion manifestation. Indexation is based on semi-quantitative way of assessment, with selecting a five-grade scale in this case, where 1 presents a low level of vulnerability, hazardousness or measure effectiveness and 5 stands for the highest level. Specific cases of specification and indexation of the criteria of Occurrence of densely populated areas (V_{POP}) and Occurrence of protected areas (V_{PRO}) are elaborated in Tables 1 and 2.

2.3 *Implementation of multicriterial assessment into the risk assessment process*

As it follows from the current methods analysis, the most suitable tool for the hazardous substances road transportation is the TRA method. At the same time it is important to point out that it would be suitable to modify this method with adding the multicriterial assessment, which would make the provided outcomes more suitable for specific users (see Fig. 1).

The basic presumption of successful implementation of interest groups' preferences into the risk assessment process is realistic weight estimation. Based on this, the AHP method (Saaty, 2008), which is often used in practice and reaches good results, was selected. Another significant factor for selecting this method is the fact that it contains mechanisms enabling assessment of measurement consistence by means of the quantity of Consistency Ratio (CR). This quantity indicates the degree of randomness during criteria preference measurement, when the value of 0,1 indicates an acceptable level of consistence and 0,9 corresponds to a purely random choice.

In the first step of the preferential risk assessment it was necessary to set weight of individual areas. In this case, the weight was equally divided among risk increasing areas (i.e. vulnerability and dangerousness) and the risk reducing area (i.e. safety measures). In the second step, individual areas criteria were already assessed by means of the AHP method (Saaty, 2008). For the hierarchy of the above mentioned criteria the following results were reached (see Table 3).

The above mentioned outcomes describe differences in preferences of interest groups, i.e. hazardous substances carrier, public administration authorities and ecological activists, when each of the above nemtioned has a different point of view on the road transportation. Consistence of the set weight coefficients (CR) is the most balanced at public administration authorities. On the contrary, preferences of the road carrier and ecological activists are the least consistent with criteria for setting dangerousness of threats and safety measures.

Table 1. Specification and indexation of the criterion of "Occurrence of densely populated areas".

Specification of the criterion of "Occurrence of densely populated areas"	Index value of the criterion
Population density up to 20 people/ha	1
Population density up to 40 people/ha	2
Population density up to 60 people/ha	3
Population density up to 80 people/ha	4
Population density above 80 people/ha	5

Note: Specification and indexation of this criterion follows from a Dutch manual for risk assessment, the Purple Book (Guidelines, 2005b).

Table 2. Specification and indexation of the criterion of "Occurrence of protected areas".

Specification of the criterion of "Occurrence of protected areas"	Index value of the criterion
Specifically protected areas, regional systems of ecological stability, natural and priority stations	1
Woods, orchard, wineyards, hop-field, loations with livestock breeding	2
Gardens	3
Cultivated farmland	4
Non-cultivated farmland	5

Note: Specification and indexation of this criterion follows from a Czech method of Hazard & Vulnerability Index (Vojkovská and Danihelka, 2002).

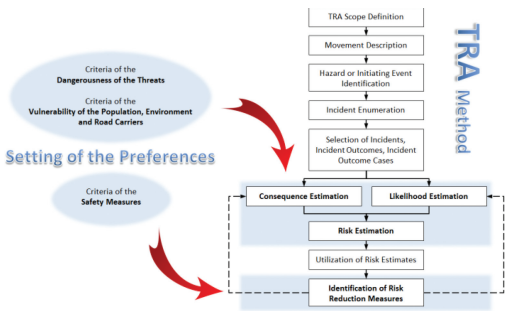


Figure 1. Implementation of preferential criteria in the TRA method.

Table 3. Results of weight calculation of criteria indicating preferences of stakeholders

Area	Area weight	Criterion	Criterion weight (hazardous substances road carrier)	Criterion weight (public administration authorities)	Criterion weight (ecological activists)
Vulnerability of the population, environment and road carriers	0,5	Occurrence of densely populated areas	0,033	0,181	0,088
		Occurrence of protected areas	0,019	0,116	0,189
		Occurrence of buffer zones of water resources	0,067	0,145	0,189
		Value of transport technology	0,252	0,029	0,018
		Value of the transported cargo	0,128	0,029	0,018
	Consistency Ratio (CR)		*0,069*	*0,032*	*0,021*
Dangerousness of threats	0,5	Dangerousness of the transported substance	0,118	0,075	0,205
		Amount of he transported substance	0,041	0,083	0,130
		Technical condition of the transport technology	0,033	0,166	0,054
		Driver's experience and skills	0,226	0,127	0,053
		Average state of the road on the route	0,036	0,034	0,031
		Weather	0,045	0,015	0,028
	Consistency Ratio (CR)		*0,119*	*0,067*	*0,140*
Safety measures	1,0	Effectiveness	0,117	0,584	0,587
		Feasibility	0,148	0,085	0,221
		Financial demandingness	0,666	0,239	0,122
		Time demandingness	0,069	0,092	0,070
	Consistency Ratio (CR)		*0,226*	*0,008*	*0,268*

This fact proves intentional and biased data manipulation in favour of the assessor.

From the set weight of criteria it is evident that road carriers positively prefer the Value of transport technology, the Value of the transported cargo, Driver's skills and experience a in the area of safety measures it is the Financial demandingness of the transport. On the other hand, public administration authorities prefer Protection of population and environment, good technical condition of technology, and high effectiveness of safety measures. The last group is represented by ecological activists who call for environment protection, low dangerousness of transported hazardous substances above all and high effectiveness of safety measures, similar to public administration authorities.

Generally speaking, it may be claimed that, as it was expected, the road carrier's preferences significantly differ from those of public administration authorities and ecological activists. At the same time, it is important to say that the carrier was forced to think more carefully about the propotional value of personal preferences connected with profit maximization and general interest connected with protection of population and environment. The outcome of such movements will be an increasing complex risk which will positively influence the carrier to realize safety measures.

3 CONCLUSION

Hazardous substances road transportation means an important risk, the assessment of which is not required by legislation. Thus, carriers often prefer maximizing profit to transport safety. However, at the same time they are aware of the fact that in case of an accident of their transport not only that the surrounding is endangered (e.g. people, property, environment), but there is also a significant financial loss caused by not delivering the cargo and transport technology damage.

A possible solution to this situation is the preferential risk assessment of hazardous substances road transportation based on modification of the TRA method, enhanced with multicriterial assessment. A method modified in such way enables stakeholders (carriers above all) to implement their own preferences into the assessment process, by doing which the final risk listing includes required information related to the given subject activity. The outcome of such assessment will then be accepting safety measures reflecting the carrier's preferences (e.g. minimization of financial loss connected with an accident), but increasing safety of surroundings and its elements.

ACKNOWLEDGEMENTS

This paper was prepared as a part of the grant project of the Ministry of the Interior of the Czech Republic under number VF20112015018, titled "Security of Population—Crisis Management".

REFERENCES

Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.

Figuiera, J., Greco, S., Ehrgott, M., Eds. 2005. Multiple Criteria Decision Analysis: State of the Art Surveys. *International Series in Operations Research & Management Science*, 78, DOI: 10.1007/b100605.

Fishburn, P.C. 1965. Independence in Utility Theory with Whole Product Sets. *Operations Research*, 13(1), 28–45, DOI: 10.1287/opre.13.1.28.

Guidelines for Chemical Transportation Risk Analysis. (2005a). New York, American Institute of Chemical Engineering, Center of Chemical Process Safety, ISBN 978-0-8169-0626-0.

Guidelines for Chemical Process Quantitative Risk Analysis. (1999). New York, American Institute of Chemical Engineering, Center of Chemical Process Safety, ISBN 978-0-8169-0720-5.

Guidelines for Quantitative Risk Assessment—Purple Book. (2005b). Amsterdam, The State Secretary of Housing Spatial Planning and the Environment (VROM).

Oggero, A., Darbra, R.M., Munoz, M., Planas, E., Casal, J. 2006. A survey of accidents occurring during the transport of hazardous substances by road and rail. *Journal of Hazardous Materials*, A133, 1–7.

Řehák, D., Danihelka, P., Bernatík, A. 2014. Criteria Risk Analysis of Facilities for Electricity Generation and Transmission. In Steenbergen et al. (eds). *Safety, Reliability and Risk Analysis: Beyond the Horizon (ESREL 2013)*, pp. 2073–2080. ISBN 978-1-138-00123-7.

Řehák, D., Šenovský, P. 2014. Preference Risk Assessment of Electric Power Critical Infrastructure. *Chemical Engineering Transactions*, Vol. 36 (in print).

Saaty, T.L. 2004. Fundamentals of the analytic network process—multiple networks with benefits, costs, opportunities and risks. *Journal of Systems Science and Systems Engineering*, 13(3), 348–379, DOI: 10.1007/s11518-006-0171-1.

Saaty, T.L. 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1), 83–98.

Vojkovská, K., Danihelka, P. 2002. Methodology for the environmental impact analysis of accidents involving hazardous substances: Hazard & Vulnerability Index (Metodika pro analýzu dopadů havárií s účastí nebezpečné látky na životní prostředí: Hazard & Vulnerability Index), Ostrava, VSB—Technická univerzita Ostrava (in Czech).

Weil, R., Apostolakis, G.E. 2001. A methodology for the prioritization of operating experience in nuclear power plants. *Reliability Engineering & System Safety*, 74(1), 23–42, DOI: 10.1016/S0951-8320(01)00064-3.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantifying MSD risks through Job Hazard Analysis

L. Dement
UL Workplace Health and Safety, TN, USA

ABSTRACT: A proper JHA requires much more than observing a job to see "if it looks hard". The purpose of this study is to break down a task into its component steps, determine the hazards associated with each step, and focus on the ergonomic connection of those hazards. In order to quantify the risks of musculoskeletal disorders, we calculated lifting tasks and compared those to minimal averages. The results indicated that multiple job tasks were in excess of the recommended weight limits for those tasks. Implementing controls is necessary for reduction of these injuries.

1 INTRODUCTION

Nearly 3 million non-fatal workplace injuries and illnesses were reported by private industry employers in 2012 (Bureau of Labor Statistics, 2013) and 4,383 workers died on the job (National Census of Fatal Occupational Injuries, 2013).

Musculoskeletal Disorders (MSDs) accounted for 34 percent of all injury and illness cases in 2012. More specifically, there were 388,060 MSDs in all sectors (private, state and local government) with an incidence rate of 38 cases per 10,000 full-time workers. Injuries and illnesses resulting from repetitive motion involving microtasks resulted in workers taking a median of 23 days away from work to recuperate. MSDs specifically involving the back accounted for 41 percent of the total MSD cases, and shoulder injuries were the most severe accounting for 14 percent of all MSD injuries. It's also important to note that ergonomic risk factors exist in all types of industries. For example, six completely different occupations accounted for more than 25 percent of MSD cases (Bureau of Labor Statistics, 2013).

Regarding Europe, according to the European Agency for Safety and Health at Work, within the EU-27, MSDs are the most common work-related health problems with 25 percent of European workers complaining of backache and 23 percent of muscular pains (EU-OSHA, 2013). Moreover, 62 percent of workers are exposed a quarter of the time or more to repetitive hand and arm movements, with 46 percent to painful or tiring positions and 25% to carrying or moving heavy loads (EU-OSHA, 2013).

Similar to the United States, a plethora of industries are affected by MSDs. The 2013 Liberty Mutual Workplace Safety Index reported the most disabling workplace injuries and illnesses in 2011 amounted to $55.4 billion in direct U.S. workers' compensation costs. This translates into more than a billion dollars spent by businesses each week on the most disabling injuries (Liberty Mutual Insurance, 2014).

Among all the workers who are injured on the job, how many thought to themselves, "I've done this job hundreds of times; I'm not going to get hurt." Until the moment happens to them and it's too late.

Unfortunately, many employees think they are doing the job correctly when in reality they are working in an unsafe manner. This is not to say that the job was done incorrectly to begin with, but over time deviations from the proper procedure can occur. When that happens, workers adapt their work methods to the ever-changing workplace. In time, this can result in at-risk work practices becoming normalized into routine procedures. In an effort of trying to correct these improper deviations, employees will look at the job as a whole and overlook crucial hazards instead of breaking the task down into its component steps. This is a common, worldwide problem.

One answer to this problem is a Job Hazard Analysis. The Occupational Safety and Health Administration (OSHA) define a JHA as "a technique that focuses on job tasks as a way to identify hazards before they occur. The JHA focuses on the relationship between the worker, the task, the tools, and the work environment" (Occupational Safety and Health Administration, 2002).

JHAs are an essential part of a comprehensive safety program. However, the JHA is often overlooked as a particularly beneficial training tool, and without it the potential for injuries and fatalities is elevated. A JHA is not just about identifying hazards and risks. It is a transformative process that illuminates how specific aspects of a job are performed, allowing workers to rate risks associated with each task and prioritize correc-

tive actions to eliminate those risks. Ultimately, it changes workers' attitudes toward their jobs.

2 PREPARATION AND INTEGRATION

It is important to understand which types of jobs are best suited for a JHA. Not all jobs necessarily need one, but many will require a JHA for a deeper appreciation of the individual tasks that comprise the job as a whole. According to OSHA, a JHA is specifically well-suited for jobs (Occupational Safety and Health Administration, 2002):

- with high injury or illness rates;
- with the potential to cause death/severe injuries or illnesses;
- in which a single error could lead to a severe accident or injury;
- that are new to an operator;
- in which there have been changes in equipment, processes or procedures; and
- that are complex enough to require written instructions.

As you're looking at the jobs that are in need of a JHA, consider the methodology. JHAs enable participants to break the task down into to detailed, component steps. JHAs help employees recognize *all* the hazards that are associated with a specific job, in turn reducing the potential for accident or injury.

There is no firmly established template or standard method for a JHA. It's important to use a plethora of methods early in the development process. Direct observation is pivotal in the early stages. It's helpful to take photographs and/or using a video camera to refresh your memory later. The more deeply a job is examined, the greater the likelihood specific hazardous components will become apparent. Interviewing the worker and reviewing the written job description is also crucial to gain a deeper insight into specific job tasks.

Often it isn't until after an injury occurs that the questions start: How did it happen? Why did it happen? Was I doing the job correctly or as I have always done it? The JHA puts a proactive spin on these questions.

It's also important to note, that JHAs can be subjective. For example, what distinguishes a "low/medium/high hazard" from one worker to another? Moreover, what happens to those workers who have pre-conceived notions regarding the job? To one employee, the task might be easy, while to another it's actually quite difficult. What about the many employees who think the job process cannot be changed or improved? This is one of the reasons we recommend involving multiple workers—so various perspectives can be shared and risk perceptions can be aligned.

2.1 *Hazard recognition*

Hazard recognition will assist in identifying perceived, existing, and potential hazards and what will happen if exposure occurs (Roughton & Crutchfield, 2008). The JHA should be designed to answer certain questions that provide insights into specific job tasks and hazards associated with the job.

For example (Occupational Safety and Health, 2002):

- What can go wrong?
- How could it happen?
- How likely is the accident to happen?
- What are the consequences?
- What can be done to eliminate the hazard or reduce it to an acceptable level?

Answers to these questions help ensure the hazard is eliminated or reduced to the greatest extent possible.

3 ERGONOMICS CONNECTION

When conducting a JHA, it's important to realize the variety of hazards that could be present. Many organizations do not effectively identify issues related to ergonomics when conducting a JHA. Breaking down specific tasks is an ideal time to consider ergonomic aspects of the job as a whole.

NIOSH defines ergonomics as, "the scientific study of people at work" (NIOSH, 2013). It is fitting the job to the person in an effort to reduce stress on the body and eliminate possible work-related injuries.

Ergonomic issues affect all types of people and occupations. Occupations such as nursing assistants and registered nurses; laborers and freight, stock and material movers; janitors and cleaners; maintenance and repair workers; and heavy and tractor-trailer truck drivers are among the most vulnerable populations, representing more than 25 percent of MSD cases. In 2012, MSD cases accounted for a median of 12 days away from work compared to nine days for all other types (Bureau of Labor Statistics, 2013).

MSDs can affect workers for sustained periods of time and can recur in the absence of intervention. With ergonomics, it's important to be aware of the risk factors that could lead to injuries. They are:

- Awkward posture
- Force
- Contact stress
- Repetitive motion
- Vibration
- Extreme temperatures

Obviously, awareness of these types of hazards is a pivotal part of the hazard reduction process. In

many instances, quantification is needed to evaluate the hazard and the associated risk, for instance, a worker is constantly bending over and picking up boxes throughout the day. The boxes may be light weight, but the repetitive process of bending over to lift them still has cumulative effects. Using the NIOSH Lifting Equation during a JHA, for example, helps employers and workers better understand body mechanics and risks associated with repetitive lifting.

4 CASE EXAMPLE #1

To better explain the ergonomics connection, let's elaborate on a specific job task that was conducted. For one example, we chose to create a JHA for a rotor inspector, specifically for MSDs. The employee's task was inspecting and stacking rotors in an automobile manufacturing facility. Throughout the day, the employee would grab a rotor from the line, lift the rotor for inspection, and carry it to a pallet three feet away. We broke the task down and to its component steps and quantified the results. The rotor itself, weighed 20 pounds (9.07 kilograms). After watching the worker for an extended period of time, we concluded that approximately six rotors were inspected and transferred per minute. After performing a few calculations, that task equaled 120 pounds per minute (54.4 kilograms) transferred and over 7000 pounds (3175 kilograms) per hour. If the employee works an eight-hour shift, he is lifting over 57,000 pounds (25,854.7 kilograms). Furthermore, from having to walk from the assembly line to the pallets, he is walking around 3.4 miles (5.47 kilometers) per shift.

After breaking this task down, it was evident that it consisted of risk factors such as repetitive motion, awkward posture and force. Quantification also assisted in determining that this job was in need of ergonomic improvements. Using the revised NIOSH lifting equation, we calculated the recommended weight limit for the rotor inspection and stacking. Specifically, we chose the worst position for the task.



The inputs for the example were as shown in the equation calculator below.

Horizontal Location Origin (in.) =	<= 10
Horizontal Location Destination (in.) =	21
Vertical Location Origin (in.) =	0
Vertical Location Destination (in.) =	0
Vertical Travel Distance (in.) =	<= 10
Angle of Asymmetry Origin (degrees) =	0
Angle of Asymmetry Dest (degrees) =	15
Frequency (lifts per minute) =	6
Duration (hrs) =	> 2 but <= 8
Coupling =	Fair
Weight of Object (lbs.) =	20

Calculate

https://www.emcins.com/losscontrol/quick_links/employee_safety_health/ergonomicsNIOSH.aspx.

After computing the total, the results showed the Recommended Weight Limit (RWL) was below the weight of the rotor.

	RWL =	LC	X	HM	X	VM	X	DM	X	AM	X	FM	X	CM
Origin	10.20	51	X	1.00	X	.78	X	1.00	X	1.00	X	.27	X	.95
Destination	4.65	51	X	.48	X	.78	X	1.00	X	.95	X	.27	X	.95

https://www.emcins.com/losscontrol/quick_links/employee_safety_health/ergonomicsNIOSH.aspx.

At the origin (assembly line) of the lift, the RWL for the lift should not exceed 10.20 pounds (4.63 kilograms) and at the destination (pallet) the RWL for the lift should not exceed 4.65 pounds (2.11 kilograms).

4.1 *Results*

The results show both, the origin and the destination, should require ergonomic controls to be implemented to reduce the stress on the worker. Lowering the frequen cy of the lift and reducing the horizontal distance of the destination would aid in making this lift safer for the employee.

Multiple studies were conducted within the manufacturing environment and all showed similar results. Although the task wasn't extremely taxing on the body for a single lift, the more lifts that were conducted throughout the day could pose serious threats to the health and well-being of the worker.

The way the task is presently being performed, the worker is at risk for MSD injuries involving the shoulder, wrist, back, and possibly the neck. Injuries such as these can pose a serious threat to workers and costs companies in lost time and worker's compensation claims.

A lift assist would be an ideal control that could be used in this specific task. The lift assist would enable the worker to use less force while picking up and placing the object in its desired location. Virtually all the force of the lift would be diminished by this simple device that can increase productivity and reduce risk of an injury.

5 CASE EXAMPLE #2

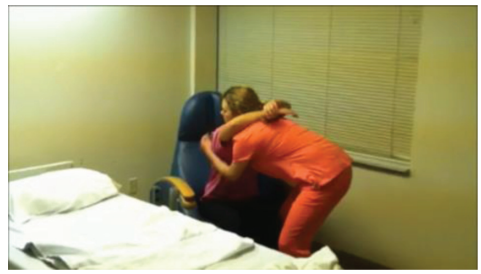
A second case that was researched was of a healthcare worker. Numerous times throughout a 12-hour shift, nurses were lifting, pushing, pulling, and transferring patients without any assistance. For this specific example, the most strenuous lift for the nurse was a patient transfer from a chair to the bed. Similar to the rotor example, when conducting a JHA it's important to recognize the ergonomic hazards that are present and could lead to MSDs.

The task in this example begins with the patient in the chair needing to be moved to the bed. In most healthcare facilities, nurses do not have assistance from other nurses or manual lifting assists. When no assistance is available, nurses will do whatever they can to make sure the job is done. This example showcases one of those dangerous tasks.

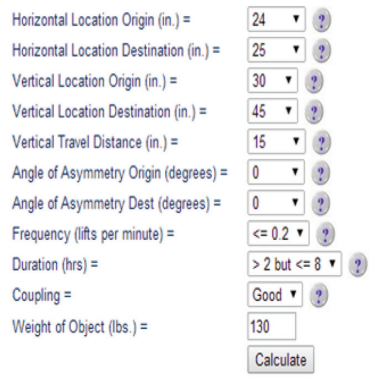
The patient weighed 130 pounds (58.97 kilograms) while the nurse weighed 140 pounds (63.5 kilograms). Initially, a back compressive force calculation was conducted to find out the force put on the lower back during the most strenuous part of the lift. The results showed the back compressive force on the nurse's lower back was 2014 pounds (913.5 kilograms), which is in excess of the desired back compressive force of 770 pounds (349.3 kilograms).

After calculating the back compressive force for the lift, we decided to run the NIOSH RLE. Although this equation is not intended for patient lifts, it can be used when certain conditions are met, such as the patient is non-combative, the amount of weight the nurse is lifting can be estimated, the lift is smooth, and the lift is fairly consistent. When used for a patient lift, the recommended weight limit changes from the regular 51 pounds to 35 pounds.

There are more variables to consider when lifting a human but to put into perspective the gravity of the lift, we studied the task and chose the most difficult part of the lift to judge. The specific step of the task chosen was as the nurse was bending over to pick up the patient.



In this example, the origin of the lift was approximately two feet away from the body and the destination was two feet one inch. After inserting the other variables, the results showed the RWL were 11.75 pounds (5.33 kilograms) at the origin and 9.96 pounds (4.52 kilograms) at the destination. The patient being 130 pounds (58.97 kilograms) was over the RWL for both tasks.



	RWL =	LC	HM	VM	DM	AM	FM	CM
Origin	11.75	35	.42	1.00	.94	1.00	.85	1.00
Destination	9.96	35	.40	.89	.94	1.00	.85	1.00

Origin	LI =	130	/	11.75	=	11.06
Destination	LI =	130	/	9.96	=	13.05

https://www.emcins.com/losscontrol/quick_links/employee_safety_health/ergonomicsNIOSH.aspx.

5.1 *Results*

The results indicate the task is in need of ergonomic controls such as team lifts and/or manual lifting assists. Reducing the risks with this given job task, and breaking the task down completely, will enable safety and health professionals to further realize the importance of worker health.

Multiple nurses and patient lifts were observed and tested for our research. As with this lift, when one nurse was lifting/pulling the patient, there was greater risk of serious injury. After monitoring nurses for a given period of time, we found many of the nurses had complaints of sore backs, necks, and shoulders.

As is, the patient would have to weigh approximately no more than 11.75 pounds for the job to be considered safe. Another option would be to implement controls such as a lift assists or team lifts when moving patients. These controls will aid in taking the majority of the weight off one individual and dispersing it between multiple nurses or the lift assist.

5.2 *Prioritizing risk*

A matrix that can be used to prioritize risk is another important tool that should be considered when creating a JHA. Risk matrices are used to evaluate the severity and probability of the incident occurring again. Although this can be subjective, it is a valuable tool in determining hazard risk. The matrix below was created for this study and determining the risk associated with specific job tasks.

Risk Matrix	Incident Severity			
Recurrence	Negligible	Marginal	Critical	Catastrophic
Extremely Improbable	L	L	L	M
Unlikely	L	L	M	M
Occasional	L	M	M	H
Probable	M	M	H	H
High Probability	M	H	H	H

5.3 *Benefits*

When properly applied, the job hazard analysis is a tool that enables workers to be more engaged in the job and aware of potential hazards. It assists with the establishment of best practices for performing tasks and implementation of effective safety controls for the specific job. The JHA should be treated as a relevant training instrument designed to raise workplace safety and health awareness. Optimally, it encourages employee engagement and assists in outlining preventative measures (Roughton & Crutchfield, 2008).

The goal for any employer should be to keep workers as safe and healthy as possible. As the JHA becomes more utilized within the organization and workers begin to become more aware of safe practices, higher productivity, lower injury rates, reduced absenteeism, and increased morale should occur. This is also going to enable more communication between the employer and employees and create a positive safety culture.

6 CONCLUSION

The findings of this research show how to quantify a task and determine how unsafe it is. Applying ergonomic principles to these tasks and many others like them, should be a priority and of primary importance for reducing the burden of MSDs in the workforce. Ergonomic issues are overlooked many times within an organization, and by actually putting a number or severity to the task, it enables employers to better understand the relationship between the ergonomic hazard and the worker.

There are many studies that have been conducted, pre- and post-, ergonomic evaluations for the healthcare and manufacturing industries. In almost all instances, the number of injuries and illnesses were reduced, the number of lost and restricted work days were reduced, and workers' compensation claims were reduced.

Overall, the results of this research depict how dangerous these "simple" tasks can be and how easy it is for musculoskeletal disorders to occur.

In both industries, we noticed repeated ergonomic risk factors that were putting workers in hazardous situations. Improper lifting, repetitive motion, awkward posture, force, and contact stress were all prevalent during these routine tasks. As these organizations began implementing JHAs and teaching proper ergonomic awareness, the number of injuries decreased and worker morale and productivity increased. For the short-term, we had positive results from the facilities that had implemented proper ergonomic controls and expect positive outcomes for the long-term as well.

We found the healthcare industry provided a more difficult conclusion. Although the results of the JHA and the quantification of the ergonomic risk factors showed major ergonomic hazards in the healthcare industry that needed to be corrected, actually making those changes in the future will be difficult. This industry deals with time constraints, shortage of nurses, and decrease in staffing ratios which leads to nurses having to do whatever it takes to get the job done; which in some instances might be getting injured performing an improper lift. Due to the majority of nurses being women and the average age being 51.5, muscle strength and intervertebral disc strength have decreased, lowering the maximum recommended weight limit and putting more workers at risk for injury (AMN Healthcare, 2013).

By breaking the task down and evaluating each step, there is a greater potential to recognize all the possible hazards associated with the specific job. JHAs aren't the most "glamorous" aspect of a safety program, but they are an excellent vehicle for training and hazard recognition. The JHA empowers workers to look at their job in a different light—a safer one—by helping them:

- prioritize the jobs and tasks to be analyzed
- break down the job
- analyze each step and identify potential hazards
- identify and implement controls to reduce/eliminate hazards

Finally, the JHA serves workers for the life of their job. These are tools that need to be re-visited and re-evaluated on a regular basis or when a change of a work process or injury has occurred. The JHA is a tool that promotes deeper thinking about the task and a greater understanding of how to rate risk, recognize hazards and work safely.

Practically speaking, the JHA is only going to be truly effective if the organization has made a genuine commitment to putting safety first. From the top down, the importance of a "safe way of life" must be at the forefront. With key elements such as hazard identification, training, employee participation, understanding the risk matrix and learning how to prioritize hazards, the JHA can be the cornerstone of any safety program and a key contributor to a culture of safety in your organization.

REFERENCES

AMN Healthcare. (2013, May 15). *2013 Survey of Registered Nurses.* Retrieved from http://www.amnhealthcare.com/uploadedFiles/MainSite/Content/Healthcare_Industry_Insights/Industry_Research/2013_RNSurvey.pdf.

Bureau of Labor Statistics. (2013, November 7). *BLS News Release*. Retrieved December 2013, from http://www.bls.gov/news.release/archives/osh_11072013.pdf.

Bureau of Labor Statistics. (2013, August 22). *National Census of Fatal Occupational Injuries*. Retrieved September 2013, from http://www.bls.gov/news.release/archives/cfoi_08222013.pdf.

Bureau of Labor Statistics. (2013, November 26). *Nonfatal Occupational Injuries and Illnesses Requiring Days Away From Work, 2012.* Retrieved 2014, from Bureau of Labor Statistics: http://www.bls.gov/news.release/archives/osh2_11262013.pdf.

EU-OSHA. (2013, September 5). *Musculoskeletal Disorders Key Facts*. Retrieved from European Agency for Safety and Health at Work: https://osha.europa.eu/en/topics/msds/index_html/facts_html.

Garg, A. (2014, January 16). *Long-Term Effectiveness of "Zero-Lift Program" in Seven Nursing Homes and One Hospital.* Retrieved from https://www.aft.org/pdfs/healthcare/zerolift0899.pdf.

Liberty Mutual Insurance. (2014, February 25). *2013 Liberty Mutual Workplace Safety Index.* Retrieved from Liberty Mutual Research Institute for Safety: file:///C:/Users/phillip.dement/Downloads/WSI%202013%20(1).pdf.

NIOSH. (2008, September 22). *Preventing Back Injuries in Health Care Settings*. Retrieved from NIOSH Science Blog: http://blogs.cdc.gov/niosh-science-blog/2008/09/22/lifting/.

NIOSH. (2013, October 7). *Ergonomics*. Retrieved 2014, from http://www.cdc.gov/niosh/topics/ergonomics/.

Occupational Safety and Health. (2002). *Job Hazard Analysis.* Retrieved from Job Hazard Analysis Publication: https://www.osha.gov/Publications/osha3071.pdf.

Occupational Safety and Health Administration. (2002). *Job Hazard Analysis*. Retrieved 2013, from https://www.osha.gov/Publications/osha3071.html.

Roughton, J.E., & Crutchfield, N. (2008). *Job Hazard Analysis.* Burlington: Elsevier Inc.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Handling epistemic uncertainty in the Fault Tree Analysis using interval-valued expert information

M. Francese
PriceWaterhouseCoopers (PWC), Rome, Italy

G.M. Galante, C.M. La Fata & G. Passannanti
Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica (DICGIM), Università degli Studi di Palermo, Palermo, Italy

ABSTRACT: Risk Analysis (RA) is a meaningful process in every industrial context, particularly referring to major hazard plants. In such sites, input reliability data are generally poor so leading to a partial or incomplete knowledge of the failure process. As a consequence, RA is always affected by the so called *epistemic uncertainty* which presence makes inappropriate the classical probabilistic approach. Therefore, the present work deals with such a kind of uncertainty in the Fault Tree Analysis (FTA) and proposes a new aggregation rule to combine the interval-valued information supplied by a team of experts about each Basic Event (BE). The aggregation leads to an interval which bounds are modelled by fuzzy numbers. Successively, such an uncertainty is properly propagated up to the Top Event (TE) in order to determine the related probability of occurrence. The approach is finally applied and discussed with relation to a Safety Instrumented System (SIS).

1 INTRODUCTION

Risk Analysis (RA) is a fundamental process to prevent accidents and other unwanted events possibly occurring during industrial process activities handling of hazardous materials. It is defined as the process of systematic use of available information in order to identify hazards and to estimate the risk (IEC 60300 1995). Depending on the accuracy required to the analysis, it can be qualitatively or quantitatively carried out. In qualitative methods no explicit quantification of the risk is obtained, whereas in the quantitative ones a numerical calculation of the risk level is addressed.

Quantitative Risk Analysis (QRA) has been in existence for many years particularly in the nuclear industry. Nowadays, QRA is widely used in aerospace, chemical process industries, petrochemical and manufacturing plants even if its detailed application can result very troublesome, time-consuming and expensive. In order to perform a quantitative risk analysis, reliability data are needed. These data have to reflect not only the design features of the employed components, but also the working environment and the adopted maintenance policy. Anyway, in major hazard plants, available reliability data are few and not well documented. As a consequence, the common way of proceeding is to make reference to similar systems/plants or to some worldwide recognized reliability databases. Nevertheless, relying on such data unavoidably affects the accuracy and the precision of the risk analysis results so making them at least questionable. Therefore, this work is focused on the characterization of the uncertainty arising from the poor available information. In literature, uncertainty arising from the intrinsic variability of the failure process under study is known as objective or aleatory uncertainty. On the contrary, uncertainty due to the lack of knowledge about the model characterizing the physical process is known as subjective or epistemic uncertainty (Hoffman & Hammonds 1994, Ferson & Ginzburg 1996, Oberkampf et al. 2004, Sentz & Ferson 2011).

The probabilistic approach is the most widely used method for characterizing both types of uncertainty. However, the purely probability-based approach to risk and uncertainty analysis can be challenged under the common conditions of limited or poor knowledge on the high-consequence risk problem, for which the information available does not provide a strong basis for a specific probability assignment (Zio & Pedroni 2013). This concern has sparked a number of investigations in the field of uncertainty representation and analysis which has led to the development of alternative frameworks that can be grouped in four main categories (Aven & Zio 2011): imprecise probability,

probability bound analysis, random sets (Dempster 1967, Shafer 1976) and possibility theory.

In the present paper, reliability information about the probability of occurrence of each *Basic Event* (BE) are supposed to be supplied by different experts in an interval form. A new aggregation rule is proposed to combine the expressed interval-valued judgments. The aggregation leads to the characterization of probabilities by means of particular intervals named *FUzzy Boundary Interval* (FuBI). Then, the propagation from BEs to the *Top Event* (TE) is performed in order to determine the FuBI related to the TE.

The remainder of the paper is organized as follows. The literature review is supplied in Section 2, whereas the proposed approach is described in Section 3. An industrial application is presented in Section 4 and conclusions are supplied in Section 5.

2 LITERATURE REVIEW

Fault Tree Analysis (FTA) (IEC 61025 1990) is the most used technique in RA to determine the logical sequence of events leading to an undesired one (i.e. the TE) that can imply the occurrence of some hazardous situations. The effectiveness of FTA strongly depends on the accuracy of BE probability estimations. However, real contexts are often characterized by a poor availability of reliability data so that the employment of the classical probabilistic approach can be misleading. Therefore, a meaningful attention has been paid by researchers to theoretical approaches alternative to the probabilistic one. In particular, the possibility theory and the evidence theory, also known as Dempster-Shafer Theory (DST), have been considered as the most promising methodologies to deal with subjective uncertainties about events. In addition, the DST suggests several combination rules to aggregate evidences coming from different sources of information (Sentz & Ferson 2002).

The DST has been mainly applied to design problems (Bae et al. 2004), whereas its application in the reliability field has not yet been widely researched. A methodology to characterize the TE probability of occurrence through the FTA and the evidence theory is proposed in (Curcurù et al. 2012). A continuous frame of discernment, coincident with the interval probability [0,1], is considered and a team of experts is asked to supply the interval-valued probability of occurrence of BEs associated to a stated basic belief mass. Then, supplied information are aggregated by means of the Dempster combination rule and propagated up to the TE. Finally, Belief and Plausibility functions are employed to estimate the uncertainty about the TE probability of occurrence. Advantages arising from using the DST to system safety prediction are outlined in (Limbourg et al. 2008). Authors propose a FTA to investigate upon whether the safety system under study can assure a fixed level of safety. Finally, authors claim that the main advantage of DST lies in its flexibility to handle expert estimates that can be merged, and updated in a comprehensible way.

The application of the possibility theory to the FTA generally reduces to the employment of the classical fuzzy numbers (Zimmermann 1991). Sallak et al. (2006a, 2006b, 2008) propose the fuzzy set theory to evaluate the Safety Integrity Level (SIL) of a Safety Instrumented System (SIS). Authors suggest a fuzzy probabilistic importance measure to identify the SIS critical components aiming at reducing the SIL uncertainty by changing the SIS configuration. A fuzzy based computer-aided FTA tool is presented by Ferdous et al. (2009a). Authors compare the robustness of the fuzzy approach to that one of the classical probabilistic method and claim that the first one is more realistic and robust in handling vague and imprecise basic event data. A hybrid method that jointly propagates probabilistic and possibilistic uncertainties is considered and compared with pure probabilistic and pure fuzzy methods for uncertainty propagation in (Baraldi & Zio 2008). The analyses are carried out on a case study concerning the uncertainties in the probabilities of occurrence of accident sequences in an event tree analysis of a nuclear power plant. A real-time risk assessment method combining Set-Pair Analysis (SPA) and fuzzy theory is proposed by Zhou (2010) and applied to installations storing flammable gas. On the base of data acquired from the safety monitoring system, the likelihood and the consequence of an accident can be evaluated in real-time. In (Ferdous et al. 2009b), fuzzy sets and evidence theory are used to an Event Tree Analysis, and the obtained results are compared to those arising from the Montecarlo simulation. In the fuzzy-based approach, the α-cut method is used to propagate the uncertainty through the tree. In the evidence theory based approach, basic belief masses of each event are aggregated by means of the classical Dempster' and Yager' rules, whereas the three-valued logic structure (Cheng 2000) is used to obtain the total evidence of consequences. Variables involved in a bow-tie representation are modelled by fuzzy numbers in (Markowski et al. 2009). The TE fuzzy probability and the fuzzy probability of consequences are calculated by employing the fuzzy arithmetic in fault and event trees respectively. In (Ferdous et al. 2013), a fuzzy-based and an evidence theory-based approaches are applied to a bow-tie analysis considering the interdependence of input events. The bow-tie approach is also proposed by Khakzad et al.

(2013) to carry out risk analysis of offshore drilling operations and compared with the Bayesian network approach. Strengths and drawbacks of each method are highlighted.

3 PROPOSED APPROACH

The present paper is focused on the implementation of the risk analysis within a major hazard plant. The main innovative aspect of the paper is the proposal of a new combination rule of information supplied by experts with relation to each BE. The aggregation step is a critical phase of the whole procedure consisting of the following steps:

1. information elicitation;
2. information aggregation;
3. calculation of the *fuzzy boundary interval* of each minimal cut-set;
4. calculation of the TE *fuzzy boundary interval*.

3.1 *Information elicitation*

Doubtless, the analyst plays a meaningful role during the information elicitation phase. In fact, the obtained information depends on the way the question is formulated. Experts are often unable to supply a single value about the BE probability of occurrence. Instead, it seems more plausible that experts can characterize each BE by means of intervals in which they estimate the related probability of occurrence could belong to.

In the context here taken into account, the hypothesis made concerns that the only available information is that arising from experts specifically operating in the plant under analysis. Such a hypothesis is particularly true in the specific context of major hazard plants which the paper is focused on.

Therefore, the analyst will ask to the few available experts a synthetic interval-valued information about the BE probability of occurrence.

3.2 *Information aggregation*

Let N be the uncertain parameter on which n experts are asked to express their own interval-valued judgment. Hence, let $N_i = [N_{iL}, N_{iU}]$ be the interval opinion of the ith expert about N, with $i = 1, \ldots, n$. Starting from n interval opinions on N, the aggregation rule reduces the total available knowledge into a single interval which bounds are modelled by means of fuzzy numbers. With relation to a different context, such a particular interval has been defined as *FUzzy Boundary Interval* (FuBI) (Nie et al. 2007). Let $\tilde{N} = [\tilde{N}_L, \tilde{N}_U]$ be a FuBI, with $\tilde{N}_L = (N_{L,Min}, N_{L,Avg}, N_{L,Max})$ and $\tilde{N}_U = (N_{U,Min}, N_{U,Avg}, N_{U,Max})$ triangular fuzzy numbers.

The proposed aggregation rule works as follows:

1. determination of the FuBI support by applying the union operator among the n interval judgments;
2. determination of the crisp part of the FuBI as the intersection among the n interval judgments;
3. assignment of the maximum membership value of the fuzzy bounds to the arithmetic mean of the n lower and n upper bounds of the interval-valued judgments.

Let being so, the bounds of the FuBI, namely $\tilde{N}_L$ and $\tilde{N}_U$, are calculated by means of equations (1)–(6):

$$N_{L,Min} = \min_{i=1,..,n} \{N_{iL}\} \tag{1}$$

$$N_{L,Avg} = \frac{1}{n}\sum_{i=1}^{n} N_{iL} \tag{2}$$

$$N_{L,Max} = \max_{i=1,..,n} \{N_{iL}\} \tag{3}$$

$$N_{U,Min} = \min_{i=1,..,n} \{N_{iU}\} \tag{4}$$

$$N_{U,Avg} = \frac{1}{n}\sum_{i=1}^{n} N_{iU} \tag{5}$$

$$N_{U,Max} = \max_{i=1,..,n} \{N_{iU}\} \tag{6}$$

In order to clarify the structure of the FuBI, Figure 1 reports a simple example of aggregation where two experts are involved.

Therefore, the classical interval representation of the aggregated opinion is limited to the agree-

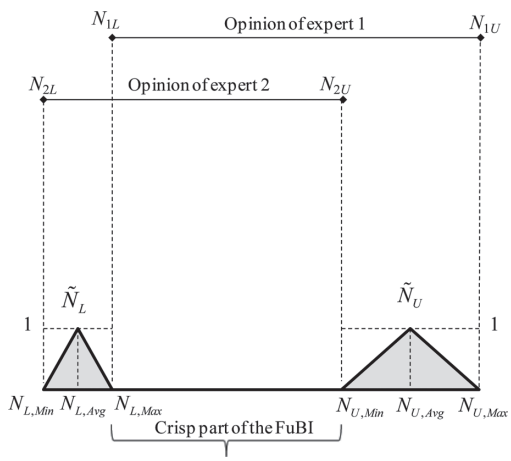


Figure 1. FuBI of the uncertain parameter N.

ment among experts and obtained by the intersection operator, whereas fuzzy numbers are associated to the disagreement part. The way the agreement and the disagreement parts of expert information are handled during the combination phase leads to the FuBI. The aggregation rule is based on the assumption that the interval-valued expert opinions about each BE have a not empty intersection. Namely, it is plausible the existence of an interval on which experts agree. The condition about the small number of involved experts together with that one regarding their specific field of expertise fully support the assumption of not disjoint interval-valued judgments. Analytically, the existence of a not empty intersection is expressed by the following equation:

$$\max_i\{N_{iL}\} < \min_i\{N_{iU}\} \tag{7}$$

As a consequence, there is not any intersection between the lower and the upper fuzzy bounds of the aggregated interval.

Furthermore, experts are supposed to have the same credibility so that equal weights are assigned to them during the aggregation phase. However, if different weights w_i could be assigned to each expert i, equations (2) and (5) turn into:

$$N_{L,Avg} = \frac{\sum_{i=1}^{n} w_i \cdot N_{iL}}{\sum_{i=1}^{n} w_i} \tag{8}$$

$$N_{U,Avg} = \frac{\sum_{i=1}^{n} w_i \cdot N_{iU}}{\sum_{i=1}^{n} w_i} \tag{9}$$

The way the proposed aggregation rule is formulated assures that:

1. the concordance among expert opinions is saved by means of the intersection operator that results into the crisp part of the FuBI;
2. the uncertainty associated with the discordance part of the expert opinions is expressed by means of fuzzy numbers.

Commonly, within the arithmetic interval approach, judgments combination is performed by the classical mean, union or intersection operators. The mean and the intersection operators lead to a reduction of the aggregated interval, namely some values that sources of information consider as possible are ignored. Otherwise, by the union operator the aggregated interval expresses the highest level of uncertainty of the aggregated judgments. In the classic fuzzy approach, each interval information supplied by experts represents the support of a fuzzy number. The choice of the membership function implies an arbitrary alteration of the original information available to the analyst. Let being so, one believes that the suggested aggregation rule modifies the poor available information as less as possible, hence representing a valid alternative to the classical aggregation approaches based on the interval arithmetic or the fuzzy set theory. Furthermore, in comparison with the DST approach, the one suggested here is easier both for the required information and the computational aspect. Therefore, it seems more suitable and applicable to industrial contexts.

3.3 *Calculation of the fuzzy boundary interval of each minimal cut-set*

Once expert assessments with regard to each BE have been aggregated, the next step consists in the determination of the fault tree minimal cut-sets (Rausand & Høyland 2004), together with the calculation of the related probability of occurrence. Let j be a generic BE belonging to the minimal cut-set z, and N_j the related probability of occurrence. Therefore, N_z (i.e. the probability of occurrence of the minimal cut-set z) can be obtained as follows:

$$N_z = \prod_{j=1}^{m} N_j \tag{10}$$

where m is the total number of BEs, supposed to be independent, within the minimal cut-set z. Bearing in mind that the aggregated interval on a generic BE j within z is expressed by means of a FuBI (i.e. $\tilde{N}_j$), as a consequence even N_z is a FuBI. Therefore, equation (10) turns into:

$$\begin{aligned}\tilde{N}_z &= [\tilde{N}_{zL}, \tilde{N}_{zU}] = \prod_{j=1}^{m} \tilde{N}_j = \prod_{j=1}^{m} [\tilde{N}_{jL}, \tilde{N}_{jU}] \\ &= [\tilde{N}_{1L} \otimes \tilde{N}_{2L} \otimes \cdots \otimes \tilde{N}_{mL}, \tilde{N}_{1U} \otimes \tilde{N}_{2U} \otimes \cdots \otimes \tilde{N}_{mU}]\end{aligned} \tag{11}$$

where $\tilde{N}_z$ is the FuBI of the probability of occurrence of the minimal cut-set z. Equation (11) is solved by applying the classical fuzzy arithmetic (Klir & Yuan 1995). In particular, in the present paper the α-cut method is used. Hence, for each level $\alpha \in [0,1]$, the fuzzy lower and upper bounds of the minimal cut-set z, namely $\tilde{N}_{zL}$ and $\tilde{N}_{zU}$ are calculated as follows:

$$\begin{aligned}[N_{zL}^{\alpha}, N_{zU}^{\alpha}] &= \prod_{j=1}^{m} [N_{jL}^{\alpha}, N_{jU}^{\alpha}] \\ &= [N_{1L}^{\alpha} \cdot N_{2L}^{\alpha} \cdot \ldots \cdot N_{mL}^{\alpha}, N_{1U}^{\alpha} \cdot N_{2U}^{\alpha} \cdot \ldots \cdot N_{mU}^{\alpha}] \\ \forall\ \alpha &\in [0,1]\end{aligned} \tag{12}$$

3.4 *Calculation of the TE fuzzy boundary interval*

Once the FuBI of minimal cut-sets have been determined, the TE's FuBI (i.e. $N_{TE}^{\sim}$) is calculated by using the rare events approximation formula:

$$N_{TE}^{\sim} = [\tilde{N}_{TE\,L}, \tilde{N}_{TE\,U}] = \sum_{z=1}^{c} N_z^{\sim} = \sum_{z=1}^{c} [\tilde{N}_{zL}, \tilde{N}_{zU}]$$
$$= [\tilde{N}_{1L} \oplus \tilde{N}_{2L} \oplus \cdots \oplus \tilde{N}_{cL}, \tilde{N}_{1U} \oplus \tilde{N}_{2U} \oplus \cdots \oplus \tilde{N}_{cU}] \quad (13)$$

being c the total number of TE's minimal cuts.

Therefore, using the α-cut method, the fuzzy lower and upper bounds of the TE's FuBI, namely $\tilde{N}_{TE\,L}$ and $\tilde{N}_{TE\,U}$ are calculated as follows:

$$[N^{\alpha}_{TE\,L}, N^{\alpha}_{TE\,U}] = \sum_{z=1}^{c} [N^{\alpha}_{zL}, N^{\alpha}_{zU}]$$
$$= [N^{\alpha}_{1L} + N^{\alpha}_{2L} + \cdots + N^{\alpha}_{cL}, N^{\alpha}_{1U} + N^{\alpha}_{2U} + \cdots + N^{\alpha}_{cU}]$$
$$\forall\ \alpha \in [0,1] \quad (14)$$

Since the top event' FuBI could be difficultly understandable by risk managers or surveillance Authorities, a crisp interval is derived by applying a defuzzification operator to the TE fuzzy lower and upper bounds. For this purpose, the Center of Area (COA) method is applied (Bojadziev & Bojadziev 1995).

4 APPLICATION OF THE METHODOLOGY TO A SAFETY INSTRUMENTED SYSTEM

The proposed methodology has been applied to a SIS in order to evaluate the *Probability of Failure on Demand* (PFD) of a Safety Instrumented Function (SIF).

The international standard ISA-TR84 (ISA-TR84 Part 1, 2002) describes various methodologies for the determination of the PFD. In particular, three techniques, simplified equations (ISA-TR84 Part 2 2002), fault tree analysis (ISA-TR84 Part 3 2002), and Markov modelling (ISA-TR84 Part 4 2002, ISA-TR84 Part 5 2002), can be used to model the interaction and functionality of basic components of a SIS in order to determine the PFD. Anyway, such a standard disregards the uncertainty associated with the input reliability data of SIS components. On the contrary, the proposed methodology, applied to the base case example reported in the ISA-TR84 Part 3, takes into account such an uncertainty and propagates it up to the TE.

In Figure 2 a simplified representation of the system process diagram is reported.

Table 1 synthesizes the system devices and the corresponding BE number. Three experts are here supposed to be involved, each one expressing his/her own judgment about the PFD of SIS components. The bounds of the interval information have been randomly generated around the value reported in the standard. Such values are reported in Table 2, and rounded off at the second meaningful number. The fuzzy bounds of the corresponding aggregated interval, namely the FuBI, are synthesized in Table 3.

The 11 minimal cut-sets of the fault tree are reported in Table 4.

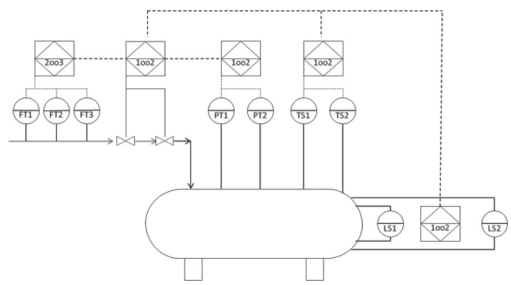


Figure 2. Case example process diagram.

Table 1. Device description and corresponding basic event.

Device	Basic Event (BE)
Pressure Transmitters (PT)	1, 2
Temperature Switches (TS)	3, 4
Level Switches (LS)	5, 6
Logic solver (E/E/PE)	7
Solenoid valves	8, 10
Block valves	9, 11
Flow Transmitters (FT)	12, 13, 14

Table 2. Interval-valued PFD of basic events supplied by three experts.

	Expert		
BE	Expert 1	Expert 2	Expert 3
1, 2	[6.0E-3, 1.8E-2]	[5.0E-3, 1.7E-2]	[6.0E-3, 1.6E-2]
3, 4	[1.7E-2, 6.6E-2]	[1.1E-2, 5.6E-2]	[1.5E-2, 6.2E-2]
5, 6	[1.2E-2, 4.0E-2]	[1.0E-2, 3.8E-2]	[9.0E-3, 3.3E-2]
7	[2.0E-3, 8.0E-3]	[2.0E-3, 9.0E-3]	[2.0E-3, 8.0E-3]
8, 10	[6.0E-3, 1.7E-2]	[4.0E-3, 2.5E-2]	[5.0E-3, 1.7E-2]
9, 11	[6.0E-3, 2.0E-2]	[5.0E-3,1.7E-2]	[4.0E-3, 2.0E-2]
12, 13, 14	[8.0E-3, 1.7E-2]	[6.0E-3, 2.3E-2]	[7.0E-3, 2.0E-2]

Table 3. Aggregated PFD of basic events.

	Fuzzy lower bound			Fuzzy upper bound		
BE	Min	Avg	Max	Min	Avg	Max
1	5.00E-3	5.67E-3	6.00E-3	1.60E-2	1.70E-2	1.80E-2
2	5.00E-3	5.67E-3	6.00E-3	1.60E-2	1.70E-2	1.80E-2
3	1.10E-2	1.43E-2	1.70E-2	5.60E-2	6.13E-2	6.60E-2
4	1.10E-2	1.43E-2	1.70E-2	5.60E-2	6.13E-2	6.60E-2
5	9.00E-3	1.03E-2	1.20E-2	3.30E-2	3.70E-2	4.00E-2
6	9.00E-3	1.03E-2	1.20E-2	3.30E-2	3.70E-2	4.00E-2
7	2.00E-3	2.00E-3	2.00E-3	8.00E-3	8.33E-3	9.00E-3
8	4.00E-3	5.00E-3	6.00E-3	1.70E-2	1.97E-2	2.50E-2
9	4.00E-3	5.00E-3	6.00E-3	1.70E-2	1.90E-2	2.00E-2
10	4.00E-3	5.00E-3	6.00E-3	1.70E-2	1.97E-2	2.50E-2
11	4.00E-3	5.00E-3	6.00E-3	1.70E-2	1.90E-2	2.00E-2
12	6.00E-3	7.00E-3	8.00E-3	1.70E-2	2.00E-2	2.30E-2
13	6.00E-3	7.00E-3	8.00E-3	1.70E-2	2.00E-2	2.30E-2
14	6.00E-3	7.00E-3	8.00E-3	1.70E-2	2.00E-2	2.30E-2

Table 4. Minimal cut-sets.

Minimal cut-sets	Events in the cut
1	1, 2
2	3, 4
3	5, 6
4	8, 10
5	8, 11
6	9, 10
7	9, 11
8	12, 13
9	12, 14
10	13, 14
11	7

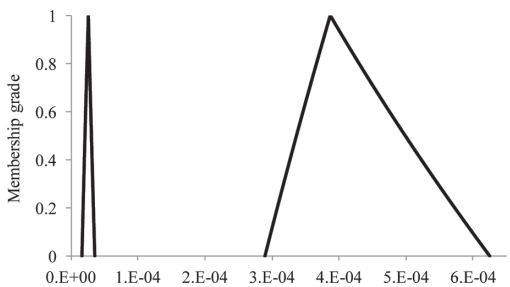


Figure 3. FuBI related to the probability of occurrence of the 5th cut.

As example, the following figure (Fig. 3) shows the FuBI related to the 5th minimal cut-set.

Finally, Figure 4 shows the TE's FuBI, which defuzzified lower and upper bounds are 2.59E-3 and 1.65E-2 respectively.

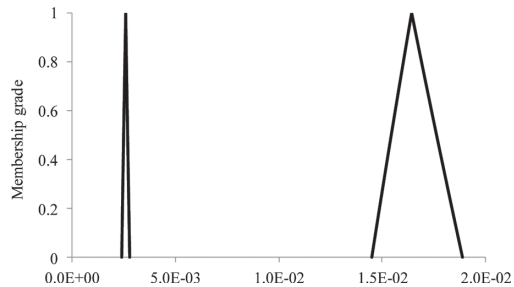


Figure 4. FuBI related to the probability of failure on demand of the SIF.

5 CONCLUSIONS

In the present paper, a new aggregation rule is suggested in order to characterize Basic Events (BEs) by means of a single aggregated interval. Such an interval has been defined as *FUzzy Boundary Interval* (FuBI). In particular, the classical interval representation of the aggregated opinion concerns the concordance among experts, and obtained by the intersection operator, whereas the fuzzy number bounds are associated to the disagreement part. In other words, the uncertainty of each expert about the BE probability of occurrence is modelled by an interval judgment, whereas the further uncertainty arising from the disagreement among experts turns into two fuzzy numbers that bound the aggregated interval.

After performing the aggregation step, the classical fuzzy arithmetic is applied to the FuBI bounds of BEs belonging to the Top Event (TE) minimal cut-sets in order to obtain the TE's FuBI.

Finally, bounds of the TE's FuBI are defuzzified in order to obtain a classical interval. Such an interval can represent a more meaningful and useful information for both the plant risk managers and the surveillance Authorities than that one arising from the classical approach to FTA. In fact, the latter characterizes the TE probability of occurrence by means of a single value that, if on the one hand is easily usable, on the other hand gives to results a certainty that is at least questionable. Instead, considering the uncertainty where it effectively arises from, namely in the probability of occurrence of BEs, and its propagation through the fault tree up to the TE, seems to be a more informative approach.

Furthermore, one believes that the suggested aggregation rule is able to adequately synthesize the available information. In fact, the intersection operator allows at taking into account the concordance among expert judgments and results into the crisp part of the FuBI, whereas the uncertainty associated with the discordance is expressed by means of fuzzy numbers. Furthermore, the totally available information is saved and results into the support of the FuBI associated with each basic event.

REFERENCES

Aven, T. & Zio, E. 2011. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. *Reliability Engineering & System Safety* 96(1): 64–74.

Bae, H.R., Grandhi, R.V. & Canfield, R.A. 2004. An approximation approach for uncertainty quantification using evidence theory. *Reliability Engineering & System Safety* 86: 215–225.

Baraldi, P. & Zio, E. 2008. A combined Monte Carlo and possibilistic approach to uncertainty propagation in event tree analysis. *Risk Analysis* 28(5): 1309–1326.

Bojadziev, G. & Bojadziev, M. 1995. Fuzzy sets, fuzzy logic, applications. *World Scientific Publishing Co Pte Ltd*. Singapore.

Cheng, Y. 2000. Uncertainties in fault tree analysis. *Journal of Science and Engineering* 3(1): 23–29.

Curcurù, G., Galante, G.M. & La Fata, C.M. 2012. Epistemic uncertainty in fault tree analysis approached by the evidence theory. *Journal of Loss Prevention in the Process Industries* 25: 667–676.

Dempster, A.P. 1967. Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics* 38(2): 325–339.

Ferdous, R., Khan, F., Veitch, B. & Amyotte, P. 2009a. Methodology for computer aided fuzzy fault tree analysis. *Process Safety and Environmental Protection* 87: 217–226.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P. & Veitch, B. 2009b. Handling data uncertainties in event tree analysis. *Process Safety and Environmental Protection* 87: 283–292.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P. & Veitch, B. 2013. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. *Process Safety and Environmental Protection* 91: 1–18.

Ferson, S. & Ginzburg, L.R. 1996. Different methods are needed to propagate ignorance and variability. *Reliability Engineering & System Safety* 54: 133–144.

Hoffman, F.O. & Hammonds, J.S. 1994. Propagation of uncertainty in risk analysis assessments: the need to distinguish between uncertainty due to lack of knowledge and uncertainty due to variability. *Risk Analysis* 14(5): 707–712.

IEC 60300-3-9 1995. Risk analysis of technological systems.

IEC 61025 2006. Fault Tree Analysis (FTA).

ISA Standard, Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques Part 1: Introduction, TR84.00.02-2002, Part 1, 2002. *ISA-The Instrumentation, Systems, and Automation Society*. Research Triangle Park, NC.

ISA Standard, Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations, TR84.00.02-2002, Part 2, 2002. *ISA-The Instrumentation, Systems, and Automation Society*. Research Triangle Park, NC.

ISA Standard, Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of a SIF via Fault Tree Analysis, TR84.00.02-2002, Part 3, 2002. *ISA-The Instrumentation, Systems, and Automation Society*. Research Triangle Park, NC.

ISA Standard, Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques Part 4: Determining the SIL of a SIF via Markov Analysis, TR84.00.02-2002, Part 4, 2002. *ISA-The Instrumentation, Systems, and Automation Society*. Research Triangle Park, NC.

ISA Standard, Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques Part 5: Determining the PFD of SIS Logic Solvers via Markov Analysis, TR84.00.02-2002, Part 5, 2002. *ISA-The Instrumentation, Systems, and Automation Society*. Research Triangle Park, NC.

Khakzad, N., Khan, F., Amyotte, P., 2013. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. *Safety Science* 57, 108–117.

Klir, G., Yuan, B., 1995. Fuzzy Sets and Fuzzy Logic: Theory and Applications. *Prentice Hall*.

Limbourg, P., Savić, R., Petersen, J. & Kochs, H.D. 2008. Modelling uncertainty in fault tree analyses using evidence theory. *Proc IMechE Part O: Journal of Risk and Reliability* 222(3): 291–302.

Markowski, A.S., Mannan, M.S. & Bigoszewska, A. 2009. Fuzzy logic for process safety analysis. *Journal of Loss Prevention in the Process Industries* 22: 695–702.

Nie, X.H., Huang, G.H., Li, Y.P. & Liu, L. 2007. IFRP: A hybrid interval-parameter fuzzy robust programming approach for waste management planning under uncertainty. *Journal of Environmental Management* 84: 1–11.

Oberkampf, W.L., Helton, J.C., Joslyn, C.A., Wojtkiewicz, S.F. & Ferson, S. 2004. Challenge problems: uncertainty in system response given uncertain parameters. *Reliability Engineering & System Safety* 85: 11–19.

Rausand, M. & Høyland, A. 2004. System Reliability Theory: Models, Statistical Methods, and Applications. *John Wiley & Sons, Inc. Publication*. Hoboken, New Jersey.

Sallak, M., Simon, C. & Aubry, J.F. 2006a. Evaluating Safety Integrity Level in presence of uncertainty. In: *Fourth International Conference on Safety and Reliability*.

Sallak, M., Simon, C. & Aubry, J.F. 2006b. On the use of a new possibilist importance measure to reduce Safety Integrity Level uncertainty. In: *Fourth International Conference on Safety and Reliability*.

Sallak, M., Simon, C. & Aubry, J.F. 2008. A Fuzzy Probabilistic Approach for Determining Safety Integrity Level. *IEEE Transactions on Fuzzy Systems* 16(1): 239–248.

Sentz, K. & Ferson, S. 2002. Combination of Evidence in Dempster-Shafer Theory. *Report of Sandia National Laboratories Technical*. Report no. SAND2002-0835. Albuquerque, New Mexico.

Sentz, K. & Ferson, S. 2011. Probabilistic bounding analysis in the Quantification of Margins and Uncertainties. *Reliability Engineering & System Safety* 96: 1126–1136.

Shafer, G., 1976. A mathematical theory of evidence. Princeton: Princeton University Press.

Zhou, J. 2010. SPA–fuzzy method based real-time risk assessment for major hazard installations storing flammable gas. *Safety Science* 48: 819–822.

Zimmermann, H.J. 1991. Fuzzy set theory and its application. 2nd revised ed. Kluwer Academic Publishers.

Zio, E. & Pedroni, N. 2013. Risk analysis: Literature review of methods for representing uncertainty. *Foundation for an Industrial Safety Culture*. Toulouse, France.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Expressing and communicating uncertainty and bias in relation to Quantitative Risk Analysis

F. Goerlandt & J. Montewka
Department of Applied Mechanics, Marine Technology, Research Group on Maritime Risk and Safety, Aalto University, Espoo, Finland

ABSTRACT: In the field of risk analysis, there is a recent focus on foundational issues regarding concepts, terminology and perspectives on risk and there are recent calls on research on how to describe risk. Much of the recent work highlights the importance of uncertainty, and a number of methods have been proposed to assess and communicate uncertainty. This paper starts from an uncertainty-based conceptualization of risk and an existing framework for assessing uncertainty. An overview of propositional attitudes shows that, apart from uncertainty, risk assessment primarily involves the attitude of acceptance. Reflecting on the difference between belief and acceptance, it is argued that often, it is possible to also describe evidential biases. The assessment of bias is subsequently taken as an extension of the existing uncertainty-based risk perspective. Finally, a number of tools are outlined to assess the strength of evidential support and for assessing the direction of bias, both on the level of individual probability assignments and on the overall risk model level. Unlike earlier methods, we assess the various types of evidence separately, showing more transparently what kind of evidential support various probability assignments have.

1 INTRODUCTION

There have been a number of calls for increased focus on foundational issues in risk analysis, addressing concepts, principles and methods when assessing, managing and communicating risk (Aven 2012a).

In this paper, the uncertainty-based risk perspective by Aven (2010) and the framework to assess and communicate uncertainty by Flage and Aven (2009) is taken as a starting point. Reflecting on the nature of the types of propositional attitudes typically found in risk assessments, we propose a modification to the qualitative uncertainty assessment methodology by Flage and Aven (2009) and an extension of the evidence assessment to also include bias, as suggested by Rosqvist and Tuominen (2004).

The paper is organized as follows. Section 2 outlines the adopted uncertainty-based risk perspective and the existing framework to express uncertainty by Flage and Aven (2009). In Section 3, the various propositional attitudes found in risk assessments are considered, indicating that acceptance, along with uncertainty, are the foundational attitudes in risk assessments. In Section 4, an extended uncertainty/bias risk perspective is outlined. In Section 5, a qualitative evidence assessment scheme is proposed, accounting both for uncertainty and bias in line with the suggested risk perspective.

2 UNCERTAINTY-BASED RISK PERSPECTIVE AND UNCERTAINTY ASSESSMENT SCHEME

Recent discussions on foundations of risk analysis have identified a need to clearly distinguish between the concept of risk and ways to describe risk (Aven 2012a). A plethora of risk definitions and concepts is known to exist (Hampel 2006, Aven 2012b), e.g. based on probability (Kaplan 1997), expected values (Campbell 2005), events (Rosa 2010) or uncertainty (Aven and Renn 2009).

For our present purposes, we define the risk concept in line with Aven (2010): "Risk is uncertainty about and severity of the consequences of an activity with respect to something that humans value".

We take the risk description suggested by Flage and Aven (2009) as a starting point, and write (where the symbol "~" means "is described by"):

$$\text{Risk} \sim (A, C, U \mid BK) \quad (1)$$

Here, risk is described by events A and consequences C. The assessor expresses his uncertainty U about the occurrence of A and C based on a background knowledge BK available to him.

Several measures of uncertainty U exist (Helton and Johnson 2011), but for our present purposes we focus on degrees of belief / subjective probabilities P_s as an expression of outcome uncertainty.

A central concern of Aven (2010) is that these subjective probabilities are not perfect representations of uncertainty, because important uncertainties may be hidden in the background knowledge.

Aven (2010) argues that such uncertainties should be made explicit, from which he arrives at a risk description:

$$\text{Risk} \sim (\text{A, C, Ps, EU} \mid \text{BK}) \quad (2)$$

Flage and Aven (2009) suggest following qualitative classification of the strength of evidential support:

Significant uncertainty: one or more of these apply

i. the phenomena involved are not well understood; models are non-existent or known/ believed to give poor predictions
ii. assumptions represent strong simplifications
iii. data are not available, or are unreliable
iv. lack of agreement/consensus among experts

Minor uncertainty: all of these apply

i. the phenomena involved are well understood; models are known to give predictions with the required accuracy
ii. assumptions are seen as very reasonable
iii. much reliable data are available
iv. broad agreement/consensus among experts

Moderate uncertainty exists when conditions are between those of significant and minor uncertainty. Naturally, the classification of these uncertainties in minor, moderator or significant are case-specific and subject to the judgment of the assessor, but the above guidelines are meant to make the reasoning process of the analyst explicit.

In addition to the qualitative uncertainty assessment, the risk description by Flage and Aven (2009) also considers sensitivity S, which relates to the change in the relevant calculated risk measures conditional to changes in the uncertain quantities. This leads to a risk description:

$$\text{Risk} \sim (\text{A, C, Ps, EU, S} \mid \text{BK}) \quad (3)$$

Following classification is adopted for sensitivity:

Significant sensitivity:
Relatively small changes in base case values result in altered conclusions (e.g. exceeded acceptance criteria)

Moderate sensitivity:
Relatively large changes in base case values needed to bring about altered conclusions

Minor sensitivity:
Unrealistically large changes in base case values needed to bring about altered conclusions.

The classification of evidential support in terms of significant, moderate or minor uncertainty as described above provides a good starting point for extending the risk assessment beyond probabilities. However, we find some areas for improvement in the work by Flage and Aven (2009).

First, we find value in providing a qualitative assessment of the various types of evidence per se, which can be rated by an assessor. This approach identifies explicitly which evidence actually is available for the assignment of a subjective probability to the considered variable of interest. The approach by Flage and Aven (2009) in our view leads to some inconsistencies. E.g. when no data is available but the models are based on very well established theories, the classification by Flage and Aven (2009) leads to moderate or even significant uncertainty. However, it is possible that even when no data is available at all to the assessor, the models are so accurate that the uncertainty regarding the evidence is minor.

Second, Flage and Aven (2009) refer to models, assumptions, data and expert judgment as sources of evidence in the background knowledge. However, in characterizing these as evidence for making the assessment, we find it beneficial to consider what propositional attitudes are relevant in the assessor's consideration of these data, models, assumptions and expert judgments as pieces of evidence in making judgments on probabilities.

In particular, a more elaborate discussion on propositional attitudes will indicate that apart from evidential uncertainty, it may also be valuable to consider evidential biases.

3 PROPOSITIONAL ATTITUDES

In the philosophical literature, a distinction is made between several attitudes one can have regarding a proposition. The formalism of propositional attitudes stems from a need for conceptual clarity regarding what sort of attitude or stance one takes regarding a statement (Schwitzgebel 2010). The generic structure of a propositional attitude is as follows:

$$\text{S A that P} \quad (4)$$

The formalism captures an individual's mental state of having some attitude, stance, take or opinion about a proposition or about the potential state of affairs in which that proposition is true (Schwitzgebel 2010). The above structure constitutes of a subject S, an attitude A and a proposition P. For example, in the sentence "the assessor hopes that he will complete the report on time", S refers to "the assessor", A refers to "hopes" (i.e. an attitude expressing a desire concerning a given outcome) and P refers to "he will complete the report on time." Note that

implicitly, it is understood that the attitude A is expressed at a given time t. This further implies that at another time t^*, a subject's attitude toward the proposition may be different. The subject-bound nature of propositional attitudes furthermore shows that different subjects may have different attitudes toward the same proposition P.

In the following sections, a number of important propositional attitudes are briefly considered. It should be noted that the exact philosophical characterization of these propositions is a major challenge for philosophers, with e.g. long-standing debates on the exact nature of knowledge (Lemos 2007). The outlines given below should therefore primarily be seen in a stipulative sense, with the aim of making these broadly different attitudes more in focus in foundational literature on risk assessment, which is (in the authors' view unfortunately) uncommon at present: in standard textbooks on risk assessment, such distinctions are not made (Aven 2010, Bedford and Cooke 2001, Jordaan 2005).

3.1 *Belief*

The attitude of belief (B) can be characterized as follows (Schwitzgebel 2010):

S beliefs that P
if and only if
S has the mental state that P is true.

Beliefs are common attitudes in epistemological contexts, and generally are taken to be truth-oriented. Whether or not a belief is trustworthy depends primarily on the amount and reliability of the offered justification.

Take the following example: "the operator beliefs that the valve is closed". Here, the operator has the mental state that the valve is closed, but this does not mean that the valve really is closed. When asked, he may justify his belief e.g. by saying that the computer system indicates that the valve is closed and that he has just made an inspection during which he has seen that the handle of the valve showed a closed position. Nonetheless, the operator may be wrong in his belief, e.g. when the interior mechanism of the valve is actually cracked, such that the valve leaks.

3.2 *Knowledge*

Clearly, much has been written about the concept of Knowledge (K), and there are major philosophical difficulties in exactly characterizing what knowledge is (Lemos 2007). For our purposes, we adhere to the standard epistemological conceptualization as Justified True Belief (JBT), which can be formalized as a propositional attitude as (Schwitzgebel 2010):

S knows that P
if and only f
(a) S beliefs that P
(b) S has a justification for the belief
(c) P is true

In this account, knowledge clearly is truth-oriented as the propositional attitude is a stronger version of belief, as the proposition is actually true. Note that for S to know P, S must be able to provide a justification.

Take the following example: "the analyst knows that the square of the hypotenuse in a right triangle is equal to the sum of the squares of other sides". This is the well-known Pythagorean theorem, which the analyst may be well-justified to believe as there are no less than 370 proofs for the proposition (Loomis 1968).

Taking however the previous example "the operator beliefs that the valve is closed", the justification provided by the operator may be wrong without him realizing this, see Section 3.1. The valve may in fact really be closed, but neither the indication of the computer system, nor the position of the lever provides the same kind of certainty of justification as the mathematical proof of the Pythagorean theorem. The operator may have very strong justification for his belief, and even if the value really is closed, it is questionable if he can know this in the strict sense of knowledge as justified true belief. Metaphysically, the valve may indeed be closed, but for the operator, the inner mechanism of the valve is not accessible to verify the closed position (and were he to open it, the proposition would be false).

Such considerations naturally lead to the attitude of uncertainty.

3.3 *Two attitudes of uncertainty*

Several conceptualizations of uncertainty exist, often made in light of the nature of the problems dealt with. Levin (2006) proposes an analytical taxonomy of uncertainty, in line with the structure of the propositional attitudes. He distinguishes Outcome Uncertainty (OU) and Evidence Uncertainty (EU).

S is at time t outcome uncertain whether P
if and only if
(a) S believes that either P or ¬P may be true, and
(b) the truth-value of P is non-determinate at t

S is evidentially uncertain whether P
if and only if
(a) S believes that either P or ¬P may be true,
(b) S lacks knowledge of a determinate proposition e_n, and
(c) e_n stands in an evidential relation to P

It should be noted that Levin (2006) acknowledges that this definition should account for the notion that several (i.e. more than two) potentially

true propositions should be considered in uncertainty, and that the reliance on determinism in the definition poses some unresolved metaphysical challenges.

Also, it should be noted that the primary attitude in both OU and EU concerns belief. Thus, while the subject entertains rival hypotheses as being potentially true, of which he is not certain which one to believe exclusively, he has a truth-oriented attitude towards these.

Take the following example: "the operator is uncertain whether a leak will occur from the valve". First, it should be noted that this example concerns a future state of the world, which is at present non-determinate. The operator finds himself in a state of outcome uncertainty. He believes on the one hand that no leak will occur, but as he cannot be certain about future states of the world (such propositions have no true value), he must leave the option open that a leak will occur.

The operator weighs his beliefs according to the evidence available to him. If the computer system indicates a closed valve and if he sees that the lever is on the "closed" position, he has evidence to support the belief that no leak will occur during his watch. However, he lacks knowledge about the maintenance performed on the valve. In line with statement (b), this implies that the operator is in a state of evidential uncertainty because the maintenance clearly has a relation to the possibility of a leak.

3.4 *Degree of belief as an attitude of outcome uncertainty*

The attitude of outcome uncertainty naturally leads to the attitude of Degree of Belief (DB) as:

S beliefs that P to a degree p
if and only if
S beliefs that ¬P to a degree 1-p

It is seen that a subject S can express his outcome uncertainty OU in terms of a degree of belief concerning the truth-content of P.

As with outcome uncertainty, the primary attitude is belief: the subject beliefs P to a degree p. Hence, S is not uncertain about p. This is important, as the subjective degree of belief, also known as subjective probability (Aven and Reniers 2013), is not uncertain for S.

However, S may have poor evidence for making his assignment of degree of belief p. This does not act as an uncertainty about p, but as an uncertainty regarding the evidence on which his assignment of p is based.

The separation between outcome and evidential uncertainty as conceptual attitudes is thus equivalent to a separation between degrees of belief and the strength of evidence for assigning the degrees of belief. Such distinctions between judgment and evidence for judgment are important in the discussion on the risk description in Section 4.

For the assessor, his assigned value of p is not uncertain (he believes it), but this does not mean that the value p is actually true. Other assessors may assign another value p^* which they believe to truly represent their attitude towards P. The assignment of p is a personal judgment, without any reference to the existence of a "true" value p_t. A more elaborate discussion on subjective probability is given by Aven and Reniers (2013).

3.5 *Acceptance*

Acceptance (A) is a very different propositional attitude than the so far considered ones. We adopt the definition and interpretation by Elliott and Willmes (2012):

S accepts that P
if and only if
S presupposes P for specific reasons in the deliberation

Acceptance differs on a number of crucial accounts from belief. One cannot believe at will, whereas acceptance is under one's voluntary control. Furthermore, the degree to which a proposition is worthy of belief depends only on the available evidence, whereas accepting it is context-dependent.

Unlike belief, knowledge and uncertainty, acceptance does not imply any commitment of the subject S that the proposition P is true or even truth-oriented.

The key aspect of definition (A) is the notion of 'specific reasons'. Acceptance is highly context-bound: the reasons for which A is accepted in a first context may not be sufficient for its acceptance in another. In addition, the reasons for acceptance are not necessarily (exclusively) of epistemic nature. This means that the reasons for acceptance may involve value judgments, e.g. when a conservative judgment is invoked as a reason for acceptance.

Take following example: "The assessor accepts that the load-carrying capacity of the crane is 500 kN". Clearly, there may be epistemic justification (reasons) for this acceptance, for instance that calculations using beam theory indicate a capacity of 535 kN. However, the assessor may be justified in invoking value judgments to accept a lower capacity in the calculations than the first estimate of 535 kN. Depending on the purpose of the analysis, i.e. depending on the context, it can be reasonable to value a conservative estimate about which uncertainty is minimized over a possibly more accurate estimate about which uncertainty is

higher. The assessor may do this, because he prefers a calculation which is "on the safe side"—clearly a value judgment. Such a judgment may however be acceptable depending on the aim of the analysis.

More generally, in modeling environments, it is often needed to accept certain assumptions or simplifications. The kinds of assumptions and simplifications made (conservative or optimistic) ultimately rely on non-epistemic value judgments rather than on epistemic justification.

The nature of the justification of the attitude towards a proposition thus has implications as to whether or not there are values involved.

3.6 *Acceptance of evidential bias*

In our context, we define bias as the difference between what is accepted and what is believed, in line with the underlying ideas of Rosqvist and Tuominen (2004). We furthermore define the attitude of Accepting an Evidential Bias (AEB) as follows:

S accepts an evidential bias with regards to e_n
concerning P
if and only if
(a) S accepts that e_n
(b) S beliefs that e_n^*
(c) e_n stands in relation to e_n^*
(d) e_n stands in an evidential relation to P

The central characteristic of accepting an evidential bias is thus that a subject S is prepared to make statements concerning P based on evidences which he does not truly believe. Rather, he accepts evidences, the justification of which may involve value-laden reasons. Yet, the subject is aware of this situation and is able to describe the bias in terms of whether he beliefs that the bias is conservative, realistic or optimistic.

3.7 *Schematic overview*

The brief outline of the propositional attitudes in the preceding sections is summarized according to a number of central characteristics in Table 1.

The overview of characteristics of the various propositional attitudes clearly shows that there are important differences between the attitudes. Belief-based attitudes B, K, OU, EU and DB aim at truth, either an absolute truth as in K or a subjective truth as in B, OU, EU or DB, whereas the attitude of acceptance does not involve a reference to any truth per se. Acceptance depends on the context, whereas beliefs and knowledge do not.

A central characteristic of uncertainty and degrees of belief as opposed to belief, knowledge and acceptance is the simultaneous entertainment of different, mutually exclusive hypotheses regarding a proposition. In belief, knowledge and acceptance, the focus is on one particular proposition. In an attitude of accepting evidential biases regarding a proposition, a subject entertains two different propositions: the believed evidential proposition versus the accepted evidential proposition. This is not the same situation as with uncertainty because in uncertainty, one entertains simultaneous beliefs regarding one and the same proposition.

Table 1. Central characteristics of propositional attitudes.

Characteristic	B	K	OU	EU	DB	A	AEB
Truth-oriented	Y	Y	Y	Y	Y	N	N
Actually true	N	Y	N	N	N	N	N
Dependent on subject	Y	N	Y	Y	Y	Y	Y
Several alternatives	N	N	Y	Y	Y	N	N
Proposition in future	Y	N	Y	Y	Y	Y	Y
Proposition in past/ present	Y	Y	Y	Y	Y	Y	Y
Epistemic justification	Y	Y	Y	Y	Y	Y	Y
Non-epistemic justification	N	N	N	N	N/Y	Y	Y
Context-dependent	N	N	N	N	N/Y	Y	Y

Concerning the element of time, all propositional attitudes except knowledge (defined as justified true belief) can be applied to propositions related to the future, as there is broad agreement among philosophers that statements regarding the future have no truth-content (Hartnack 1959). All attitudes can be applied to propositions related to past or present.

An important distinction exists between belief-based attitudes (B, K, OU, EU, DB) and acceptance-based attitudes (A, AEB). This involves the role of non-epistemic values as justification for the type of attitude taken to a proposition. In the belief-based attitudes, the value judgments of a subject are irrelevant because whether or not one takes something to be true does not depend on whether one sees value in taking it to be true. In contrast, in acceptance-based attitudes, values do play a role as supporting justification. This is related to the attitude of acceptance more being tied to a particular action in a particular context, rather than aiming at the discovery of a true value.

Concerning degrees of belief (subjective probabilities), these may or may not involve values depending on what types of justification (epistemic vs non-epistemic) are invoked as evidential statements on which the degree of belief is based. If these evidential statements only concern attitudes of knowledge, beliefs or evidential uncertainty, non-epistemic values are not present in the

underlying justification of the degree of belief. If however there are attitudes of acceptance and acceptance of evidential bias present in the justification of the degree of belief, these degrees of belief do rely on values.

4 EXTENDED UNCERTAINTY/ BIAS RISK DESCRIPTION

Our recommended risk description can be schematically summarized as follows:

$$\text{Risk} \sim (A, C, P_s, EU, EB, S \mid EJ, NEJ) \quad (5)$$

The risk description is largely similar as the one presented by Flage and Aven (2009), focusing also on the expression of degrees of belief regarding the occurrence of events A and consequences C, using subjective probabilities P_s. As in their framework, evidence uncertainty (the strength of evidential support for the assignment of P_s) and sensitivity S is considered.

However, the methodology for assessing the strength of evidence for assigning subjective probabilities is modified and apart from evidential uncertainty, we also propose a method to assess evidential biases. The assessment of bias is also suggested by Rosqvist and Tuominen (2004) and Rosqvist (2010).

In the above risk description, the assessor makes a judgment regarding his degree of belief P_s about the occurrence of the event A based on the evidence available to him, which enables him to provide a justification J, i.e. P(A|J). This evidence may consist of data, models, theories and judgments. As discussed in Section 3, there exists a variety of propositional attitudes regarding evidential propositions. Evidence can be believed, known or accepted.

Furthermore, there often is a form of evidential uncertainty for the assessor in relation to evidential propositions. Finally, it is possible that the assessor has accepted data, models or judgments the justification of which is (partly) based on values. Hence, the justification may not only of Epistemic nature (EJ), but also may involve of Non-Epistemic nature (NEJ). Hence, the risk description is not necessarily value-free, depending on the nature of the reasons because of which a particular propositional attitude is adopted regarding the evidences. A qualitative assessment of evidential biases can make such value-laden considerations explicit.

Table 2 provides a classification of the various possible attitudes in the evidential categories. It is seen that for all types of evidence, it is possible to accept it as a basis for assigning a degree of belief P_s. For all types of evidence, there may be evidential uncertainty present to lesser or greater degree. In contrast, beliefs and knowledge (defined as justified true belief) are not always appropriate attitudes towards evidence. Some examples will illustrate these points.

Table 2. Propositional attitudes in evidential propositions acting as evidence for the judgment of a degree of belief.

Evidence type	B	K	EU	A	AEB
Data	N	N	Y	Y	Y
Mathematical model	Y	Y	Y	Y	Y
Engineering model	N	N	Y	Y	Y
Theory	Y	Y	Y	Y	Y
Judgments	Y	Y	Y	Y	Y

Experimental or empirical data is, using the concepts of Section 3, typically not believed or known, because it is not in the strict sense true. Experimental data obtained in laboratory conditions can typically be considered reliable, but e.g. accident data or data obtained from accident reports can be based on poor classifications, unreliable or incomplete to varying degrees. Hence, there may be evidential uncertainties related to data, and it may be biased e.g. when severe accidents are believed to be rather well reported, whereas minor accidents and incidents may be underreported.

Mathematical models can be believed and even known, involving no evidential uncertainty. Consider e.g. the Pythagorean theorem: this is a mathematical piece of knowledge. Other mathematical models, e.g. numerical solutions to differential equations, may be accepted rather than believed, and there may be evidential uncertainty e.g. related to the adopted discretization in the numerical solution.

Engineering models typically are not really believed as they represent a simplification of a real system. Models are not true, but are useful in a given context and can thus be accepted. In complex models, there can be evidential uncertainty related to the model structure and parameters. Biases may also be present, e.g. when conservative modeling simplifications are adopted.

Theories may be believed, known or accepted depending on the field of application. Mathematical theories may constitute knowledge, whereas psychological theories, e.g. theories of human error occurrence, may be accepted. There may be evidential uncertainties in theories.

Expert judgments may constitute of beliefs, e.g. a belief regarding the closed position of a valve. If this belief is actually true, it also is knowledge. However, judgments may also be uncertain, e.g. if different experts disagree about their beliefs.

Furthermore, judgments may be accepted, e.g. we may actually believe that not all cars in a crossroad have exactly two passengers, but we may accept this because it is simpler and because we take it that it is a conservative number.

5 TOTAL RISK PICTURE

The risk description of Eq. 5 leads to a systematic look beyond the assigned probabilities, as in the scheme by Flage and Aven (2009). It differs in the tools applied to systematically assess the evidence, and it extends the work by Flage and Aven (2009) by also considering evidential biases.

5.1 *Schematic overview of total risk picture*

The total risk picture consists of a probability model, where subjective probabilities are assigned to events and consequences. This can be achieved using event/fault trees or Bayesian networks.

Apart from the probabilistic risk measurement, a sensitivity analysis is made, identifying the elements in the model to which the risk measure is most sensitive. For those probabilities to which the model is most sensitive, a qualitative assessment of the strength of justification and the direction of bias is made. Finally, the sensitivities, strengths of justification and (when relevant) the direction of biases are grouped in a set of matrices, showing the overall picture of sensitive model elements and their epistemic and non-epistemic justification.

5.2 *Probability evidence assessment scheme*

The total risk picture constitutes subjective probabilities and sensitivities, along with a qualitative description of the strength of evidence and the direction of bias.

A proposed evidence assessment scheme for the evidential support for a subjective probability $P_s(A \mid EJ,NEJ)$ is presented in Table 3, accounting both for epistemic and non-epistemic justification. The scheme may be used to make explicit what type of evidence the assigned probability value is based on, as well as how strong that evidence is believed to be. When relevant, the direction of bias inherent in the evidence can be judged by the assessor.

Naturally, the assigned value in the evidence assessment scheme is in itself a judgment by the assessor. This inherent subjectivity could be an obstacle in communication, but the very nature of risk assessment under the adopted risk perspective is a subjectivist one, see e.g. Aven and Renn (2009).

The real value of the evidence assessment scheme is to increase transparency in the assessment, to make explicit what the various judgments are based on in a systematic manner.

Table 3. Evidence assessment scheme for a particular subjective probability P_s, H = high, M = medium, L = low, C = conservative, R = realistic, O = optimistic.

RISK MODEL ELEMENT "A"				
Strength of evidence	H		M	L
Data				
Completeness				
Reliability/accuracy				
Amount				
Model/theory				
Phenomenon understood		x		
Level of detail		x		
Accuracy of prediction			x	
Judgments				
Expertise of assessor				
Consensus				
Overall score		x		
Evidence bias	C		R	O
Data				
Reporting completeness				
Measurement bias				
Model/theory				
Type of simplifications		x		
Judgments				
Type of assumption				
Overall score		x		

The example assessment scheme concerns a probability which is derived from calculations with an engineering model of a system which is relatively well understood, which is modeled in a high level of detail and leading to reasonably accurate predictions. The evidence bias assessment shows that the type of simplifications is moderately conservative.

Hence, the probability P_s is on based on evidence with low uncertainty and a moderately conservative bias, as also indicated in the table.

The example shows that uncertainty can be minor even if only one type of evidence is available. In case no models or data is available and the assigned probability is purely based on expert judgment, the level of expertise and the degree of consensus may still lead to the conclusion of relatively minor uncertainty related to the probability value.

5.3 *Risk model evidence assessment scheme*

Once the strength of epistemic justification and the direction of evidential bias are qualitatively assessed for the sensitive probabilities in the risk

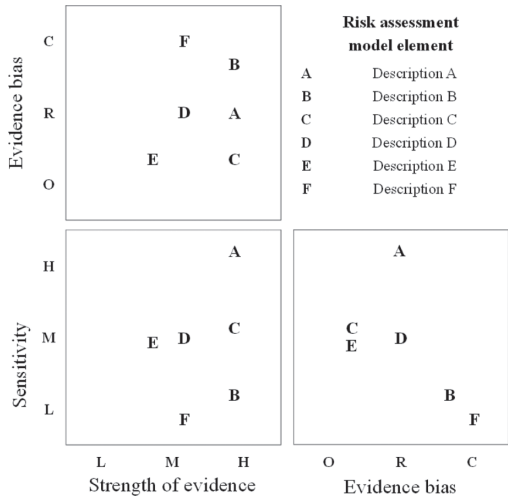


Figure 1. Aggregate risk model evidence uncertainty, bias and sensitivity assessment.

model, this information is aggregated as illustrated in Figure 1.

On the top-right corner, the various risk assessment model elements, i.e. the various subjective probabilities in the risk model, are identified. These are subsequently mapped according to their sensitivity values and their aggregate score in terms of epistemic and non-epistemic justification in a set of matrices.

The aggregation of the strength and possible direction of bias of evidential support for the probabilities in the model, along with the sensitivity score provide insight in the overall evidential support and direction of bias of the entire risk model.

A decision maker could utilize this qualitative assessment along with the quantified risk measures based on probabilities to evaluate how confident he can be about the risk measures. When e.g. an ALARP decision criterion is applied for evaluating the risk acceptability, the broad qualitative assessment guides the decision maker in establishing that the risk is positioned in a given area.

6 CONCLUSION

Informing decisions using risk assessments requires a broad, informative and transparent risk picture. Starting from an uncertainty-based risk perspective, we have outlined an existing framework for expressing and communicating uncertainty related to QRA.

While we find merit in the existing approach, we have proposed a modification to the methodology to qualitatively assess the strength of evidence. Our method directly assesses the strength of the various types of evidence relevant for making the various probability judgments in the risk model, which avoids possible inconsistencies in the existing approach.

Moreover, a more in-depth focus on what kind of attitudes are possible towards evidential statements shows that apart from evidential uncertainty, also evidential biases may be systematically assessed.

The detailed evidence assessment for the various probabilities of which the risk model consists is subsequently aggregated with the sensitivity score, providing a broad insight in the importance of various elements in the risk description, increasing the transparency of the risk assessment.

ACKNOWLEDGEMENTS

The work in this paper is prepared as a methodological support to the risk assessment developments in the WINOIL-project, funded as part of the ENPI Programme. This Programme is co-funded by the European Union, the Russian Federation and the Republic of Finland.

REFERENCES

Aven T. 2008. Risk analysis: assessing uncertainty beyond expected values and probabilities. *Wiley, pp. 206*.

Aven T. 2010. On how to define, understand and describe risk. *Reliability Engineering & System Safety 95*(6):623–631.

Aven T. 2012a. Foundational issues in risk assessment and risk management. *Risk Analysis 32*(10):1647–1656.

Aven T. 2012b. The risk concept—historical and recent development trends. *Reliability Engineering & System Safety 99*:33–44.

Aven T. Reniers G. 2013. How to define and interpret a probability in a risk and safety setting. *Safety Science 51*(1):223–231.

Aven T, Renn O. 2009. On risk defined as an event where the outcome is uncertain. *Journal of Risk Research 12*(1):1–11.

Bedford T, Cooke R. 2001. Probabilistic risk analysis: foundations and methods. *Cambridge University Press*, pp. 393.

Campbell S. 2005. Determining overall risk. *Journal of Risk Research* 8:569–581.

Elliott K., Willmes D. 2012. Cognitive attitudes and values in science. *Philosophy of Science Association 23rd Biennial Meeting*.

Flage R, Aven T. 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliability & Risk Analysis*: Theory and Application 2*(13):9–18.

Hampel J. 2006. Different concepts of risk—a challenge for risk communication. *International Journal of Medical Microbiology* 296:5–10.

Hartnack J. 1959. Knowledge of the future. *Philosophical studies (Minneapolis) 10*(6):89–96.
Helton J.C., Johnson J.D. 2011. Quantification of margins and uncertainties: alternative representations of epistemic uncertainty. *Reliability Engineering & System Safety 96*(9):1034–1052.
Jordaan I.J. 2005. Decisions under uncertainty: probabilistic analysis for engineering decisions, *Cambridge University Press*, pp. 657.
Kaplan S. 1997. The words of risk analysis. *Risk Analysis 17*(4):407–417.
Lemos N. 2007. An introduction to the theory of knowledge. New York, *Cambridge University Press,* pp. 244.
Levin R. 2005. Uncertainty in risk assessment—contents and modes of communication. *Royal Institute of Technology, Stockholm*.
Loomis E.S. 1968. The Pythagorean proposition. *The National Council of Teachers of Mathematics*.
Rosa E.A. 2010. The logical status of risk—to burnish or to dull. *Journal of Risk Research 13*(3):239–253.
Rosqvist T., Tuominen R. 2004. Qualification of Formal Safety Assessment: an exploratory study. *Safety Science 42*(2):99–120.
Rosqvist T. 2010. On the validation of risk analysis—a commentary. *Reliability Engineering & System Safety 95*(11):1261–1265.
Schwitzgebel E. 2010. Belief. Stanford Encyclopedia of Philosophy, available at http://plato.stanford.edu/entries/belief/.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safety analysis and CFD dispersion simulation of cryogenic release in a deep underground large scale cryogenic installation

E.C. Marcoulaki, A.G. Venetsanos, M. Konstandinidou & I.A. Papazoglou
National Centre for Scientific Research "Demokritos", Athens, Greece

ABSTRACT: This work considers a large installation for neutrino physics experiments, located in specially constructed caverns 1400 meters underground. The installation includes a specially designed heat insulated tank hosting 50 ktons (fudicial mass) of cryogenic argon. The main safety concern stems from the possibility that cryogen may be released from its containment and cause temperature and oxygen concentration conditions that jeopardize human health and/or the cavern integrity. The paper discusses the adopted safety measures and systems, presents CFD dispersion results simulating the uncontrolled release of the cryogen in the underground space, and assesses the potential hazards for the personnel and the cavern.

1 INTRODUCTION

There is significant evidence that very large volume underground neutrino observatories will enable fundamental discoveries in the field of particle and astroparticle physics. Many European national underground laboratories with high technical expertise are currently operated with forefront smaller-scale underground experiments, and there is currently a lot of activity worldwide on the construction of a large-scale facility. The heart of these observatories is a detector consisting of specialized sensitive detection devices submerged into a detector medium. Neutrinos interact with the detector medium, and the particles produced are analyzed to establish the neutrino characteristics. The detector medium can be purified water, liquid argon or organic scintillators.

The analysis presented here is part of an excessive multiyear design study elaborated by a large consortium of neutrino physicists and European construction companies, within the projects LAGUNA (2008–2011) and LAGUNA-LBNO (2011–2014) funded by the European Commission. Among other issues, the study considered (a) the selection of an appropriate location and the conduction of geomechanical investigations, (b) the design and costing of the excavation of underground caverns and tunnels, (c) the design and costing of a tank and its construction plan to host the liquid argon, (e) the design, construction and costing of the detector equipment, (f) the design and costing of on ground and underground processes to fill the tank with argon and (g) to maintain argon at the desired conditions etc. Safety issues have been granted significant attention from the beginning of this study. Several types of risks have been identified and registered, and specific measures were proposed to prevent and mitigate them. More information can be found at the LAGUNA website.

This paper presents in brief the safety assessment of the underground installation at normal operation. In particular, the focus here is on the argon dispersion following a cryogenic release of gaseous argon in the underground premises. The paper is organized as follows. Section 2 gives a general description of the underground installation. Section 3 discusses briefly the quantitative risk assessment leading to the evaluation of accident frequencies. Section 4 presents the phenomenology analysis using CFD simulations of the argon dispersion. Section 6 concludes the work.

2 GENERAL DESCRIPTION OF THE INSTALLATION

The neutrino detector consider here is a specially designed and heat insulated tank with gross capacity 52,300 m^3 filled with cryogenic argon. The tank, and associate processes for argon re-condensation and filtration, as well as cavern air-conditioning, will be located in specially excavated caverns 1400 m underground (see Fig. 1a). The caverns will be at a copper and zinc mine at Pyhäsalmi in central Finland (see Fig. 1b). The location selection was based on various criteria, including the excellent rock characteristics, the absence of nearby nuclear plants and hence of neutrons, the depth of the mine, the low seismicity and the distance from CERN. The latter is ideal for the study of accelerated neutrinos



Figure 1a. Pyhäsalmimine, central Finland.

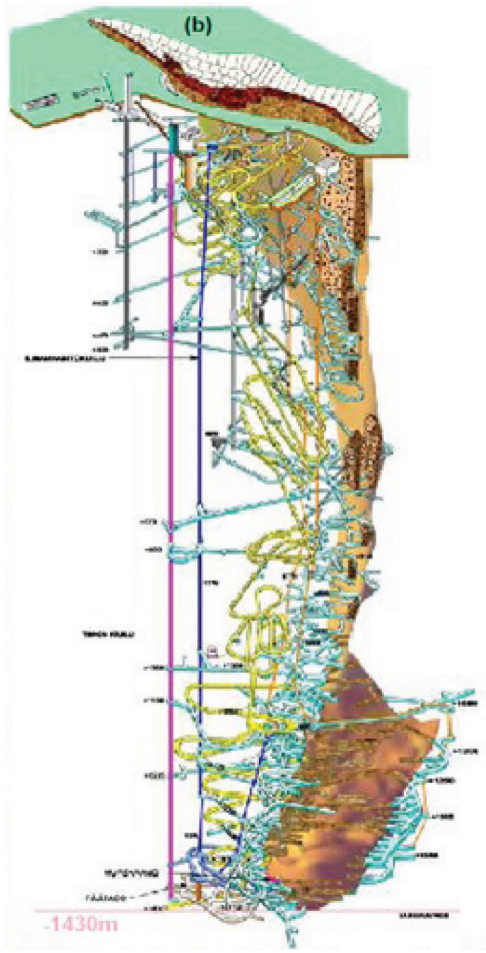


Figure 1b. Present mine layout (http://laguna.ethz.ch).

generated at CERN and aimed towards a detector at Pyhäsalmi. Information on the site selection and characteristics is publicly available in the LAGUNA project deliverables.

At –1400 m (see Fig. 1b) three large caverns will be excavated, suitable for hosting two 50 kton f.m. liquid argon tanks and one 50 kton f.m. liquid scintillator tank (tank caverns). Smaller adjacent caverns will host the process unit equipment (process unit caverns). The tank caverns will be isolated from the process unit caverns and the rest of the mine using lock doors.

The LAGUNA-LBNO project team has provided detailed designs on the location, sizing, cost and equipment types of the on ground facilities and the shafts used for technical infrastructure (like piping, electricity wires). This information is published at the LAGUNA website in strict confidence. The process flow sheet, the argon tank and process unit sizes, the temperature and pressure conditions etc used in the present analysis are also found at the website. In particular, the present work is based on the geotechnical designs and rock mechanical analysis conducted by Kalliosuunnittelu Oy Rockplan Ltd, the tank design and calculations elaborated by Technodyne International Ltd and Rhyal Engineering Ltd, and the liquid handling process design proposed by Sofregaz SA.

The detector medium is argon, kept at cryogenic conditions and vapor-liquid equilibrium at 87 K and 1265 mbar. A detector network and appropriate instrumentation to measure neutrino interactions with argon atoms will be immersed in the argon liquid inside the tank. A ventilation system (pressurizer) and a cavern heating system will work in parallel to maintain the conditions in the tank cavern at 22°C and 1250 mbar.

The neutrino experiments require argon liquid of particularly high purity, so argon liquid will be taken from the tank and processed in a set of filtration units. The argon boil-off produced inside the tank due to heat influx in the tank will be recondensed in heat exchanger units that use nitrogen as coolant. The argon cooling system will also include expansion and compression units arranged in loops that aim to cool down, re-condensate and

reuse the nitrogen coolant, and a nitrogen storage vessel.

The ventilation and heating system units, the pumps, motors and turbines for fluid transmission and processing, and the filtration units will be located in the processes cavern, next to the tank cavern. The heat generated by the instrumentation in the tank cavern and all the equipment located in the process cavern will be rejected finally into the surface atmosphere through a specially built Service Water Cooling System (SWCS). Presently the design of this system comprises a motor driven cooling tower using cooling water from the nearby Lake Pyhäjärvi, and a pipeline running several hundred meters through the rock to transmit the water underground. In case of overpressure in the argon tank, the water cooling system is able to transmit the released argon gas to the mine surface atmosphere.

3 QUANTITATIVE RISK ASSESSMENT

The main concern when storing large quantities of cryogenic argon in a confined space stems from the possibility that Liquid Argon (LAr) may be released from its containment, evaporate, and (a) reach concentrations that can expel oxygen from the air and/or (b) result to extremely low temperatures in the confined space. Two main areas exist where argon is contained and there is a possibility of a Loss of Containment (LOC) and a subsequent release of argon:

a. Tank cavern: Main cavern with the cryogenic argon tank
b. Process unit cavern: Process area where argon is cooled/condensed (if it is in gas phase), filtrated and returned to the argon tank.

A safety analysis along with a Quantitative Risk Analysis (QRA) has been performed based on the existing design details. The QRA includes:

a. an assessment of the various accident sequences leading to Ar release;
b. an estimation of their frequencies; and
c. a calculation of the consequences of Ar release using CFD tools.

This paper discusses briefly the analysis elaborated for tank overpressure, leading to the estimation of accident frequencies, and presents in more detail the CFD results for argon release owning to overpressure in the tank. The release is in the gas phase and can occur either inside the tank cavern, or in the process units cavern, or at the surface of the mine. At this stage of the design, there is lack of information on the precise geometry and equipment arrangement of the process cavern, therefore, only releases in the tank cavern can be simulated. Note that, this is part of the work elaborated on the system quantitative risk assessment, and more information is available in the LAGUNA-LBNO project website.

3.1 *Overpressure and associate safety measures*

Increase of the internal pressure can cause an increase of the stress on the containment exceeding its design limits and resulting in LOC. In the present installation, the critical design feature that might cause a LOC owing to overpressure is the roof of the tank. Its design requires that the overpressure inside the tank with respect to the pressure in the cavern does not exceed the 25 mbarg. It is assumed that, causes that result in a gauge pressure greater than 25 mbarg will result in LOC and in particular in a small break at the gaseous phase of the argon. The pressure increase can be relieved through a set of pressure relief valves (PSVs) installed on the tank. The released Ar is then transferred to the Ar-processes cavern, from where it is transferred to the mine surface through the SWCS and a piping system.

Argon is kept at Vapor-Liquid Equilibrium (VLE) at cryogenic conditions using a cooling system, to remove the heat influx from the cavern air to the argon contained in the tank. Any heat imbalance can cause an increase in the tank internal pressure, leading to LOC and argon release. The heat imbalance may be caused by either an increase in the heat influx or a decrease in the heat removal capacity. Heat flux into the cryogen from the environment will vaporize the liquid and potentially cause pressure build-up in cryogenic containment vessels and transfer lines. Cryogenic fluids have small latent heats and expand 700 to 800 times to room temperature, so even small heat inputs can cause significant pressure increase.

Table 1 reports the safety functions and the safety measures incorporated in the design to prevent

Table 1. Safety measures and safety systems.

Safety functions	Primary safety systems
Maintain heat influx into LAr within design limits	Argon tank insulation
Maintain pressure within tank below the maximum acceptable level	Argon re-condensation system Operator's action to switch off instrumentation
Maintain cavern conditions	Cavern ventilator system Cavern heating system
Relieve extra pressure	Set of tank relief valves
	Support safety systems
	Service water cooling system Electric power

pressure difference beyond the design limit, and the mitigating measures to relieve overpressure and preserve the containment integrity. Systems that directly serve a safety function are called Primary Safety Systems (PSS). For successful operations, the PSSs sometimes depend on other systems that provide support services to them, called Support Safety Systems. Their operation is also safety significant, but only through the impact they have on the operation of the PSS.

3.2 *Accident sequences and frequency of Ar release*

Accident sequences are sequences of events that lead to LOC integrity and hence to argon release. An accident sequence consists of an initiating event that challenges the safety functions/systems of the installation, and of additional events representing either hardware failures and/or human actions that collectively result in a LOC. For the safety systems described above, accident sequences are obtained using Functional Block Diagrams and the associated Event Trees (Papazoglou, 1998).

The results of the event tree analysis are summarized in Table 2. Detailed calculations can be found at the LAGUNA project website. In the case of overpressure in the argon tank, argon gas can be released to the mine surface atmosphere through the pressure safety valves and the service water cooling system. The frequency of such an event has been estimated at 5.74×10^{-1}/year or once every 21 months. This mainly comprises the frequencies of loss of the argon pump in the re-condensation system. The loss of the operating nitrogen loop and the loss of insulation make up for just 1% of the frequency for argon release to the surface. Increasing the reliability of the argon gas pumping system can reduce significantly the expected frequency of this type of release. The frequency of argon release inside the tank cavern owing to overpressure, is almost once every 7 months. This frequency is notably high, but only 17% of this value is attributed to initiating events other than the failure of SWCS components.

The quantitative risk assessment results indicated lack of redundancy in the fluid handling processes. It was, therefore, recommended that the final design incorporates redundancy in the service water cooling system, as well as in the argon side of the re-condensation system. This could reduce the expected frequency of LOC due to overpressure by two to three orders of magnitude. It is noteworthy that, the literature for double walled refrigerated LNG containments suggests a frequency for failure of the roof and vapour release in the order of 3.5×10^{-9}/hr (HSE, 2012). This is the order of magnitude for the contribution of those systems that contain redundancy, like the cavern atmosphere regulating systems, the nitrogen coolant side of the re-condensation system and the loss of insulation events.

4 CFD DISPERSION SIMULATION

4.1 *Assumptions and the modelling strategy*

The ADREA-HF CFD code (Venetsanos et al., 2010) used here has been extensively validated in handling transient dispersion problems involving two-phase cryogenic leaks of fluid heavier than air.

Table 2. Frequencies for loss of containment owning to overpressure.

		Conditional probability of Ar release in			Frequency (hr^{-1}) of Ar release in		
INITIATOR is LOSS of	Frequency (hr^{-1})	Tank cavern	Process area	Surface of mine	Tank cavern	Process area	Surface of mine
LOOP	1.00×10^{-5}	1.5×10^{-4}	3.8×10^{-2}	–	1.50×10^{-9}	3.80×10^{-7}	–
SWCS pump	3.10×10^{-4}	3.65×10^{-3}	8.3×10^{-1}	–	1.13×10^{-6}	2.57×10^{-4}	–
SWCS HX	3.60×10^{-5}	3.76×10^{-3}	9.4×10^{-1}	–	1.35×10^{-7}	3.38×10^{-5}	–
Operating pressurizer train	1.00×10^{-5}	2.00×10^{-8}	–	5.00×10^{-6}	2.00×10^{-13}	–	5.00×10^{-11}
Cavern heating system	3.10×10^{-4}	6.80×10^{-10}	–	1.70×10^{-7}	2.11×10^{-13}	–	5.27×10^{-11}
Ar pump	3.10×10^{-4}	8.60×10^{-4}	–	2.10×10^{-1}	2.67×10^{-7}	–	6.51×10^{-5}
Operating N2 train	5.00×10^{-5}	2.60×10^{-5}	–	6.40×10^{-3}	1.30×10^{-9}	–	3.20×10^{-7}
Insulation loss type 1	9.12×10^{-7}	2.60×10^{-5}	–	3.90×10^{-2}	2.37×10^{-11}	–	3.56×10^{-8}
Insulation loss type 2	1.14×10^{-7}	2.30×10^{-4}	–	5.70×10^{-2}	2.62×10^{-11}	–	6.50×10^{-9}
Insulation loss type 3	7.98×10^{-8}	4.50×10^{-4}	–	1.10×10^{-1}	3.59×10^{-11}	–	8.78×10^{-9}
Insulation loss type 4	3.42×10^{-8}	4.00×10^{-3}	–	9.96×10^{-1}	1.37×10^{-10}	–	3.41×10^{-8}
TOTAL	–	–	–	–	1.54×10^{-6}	2.92×10^{-4}	6.55×10^{-5}

The ADREA-HF code solves 3D conservation equations for mixture mass, the three Cartesian mixture velocities, the mixture enthalpy and the argon mass fraction. Thermodynamic equilibrium is assumed between phases (HEM model). In this work, the working fluid is a mixture of air and argon. The mixture can be in two-phase flow conditions. The Peng-Robinson equation of state is used to describe argon physical properties (Poling et al., 2001). The computational grids are Cartesian. The irregular cavern/tank geometry is described using the porosity approach, embedded in the CFD code. The argon tank is assumed as solid in all performed simulations. The modelled free volume between tank and cavern is equal to the actual free volume. Regardless of the orifice area, the leak source is assumed to be a single point. The flow direction is fixed, and the flow velocity depends on the orifice area and the volumetric flow rate. The volumetric flow rate depends in turn on the fluid mass flow rate and the conditions (i.e. pressure, temperature, fluid phase).

4.2 *Cavern geometry and tank data*

The tank geometry is defined by two cylinders, the inner and the outer, and is symmetrical in the z-axis. Only the outer tank geometry is used in the CFD calculations. The cavern consists of three sections: a small cylinder (tank base) at the bottom, an elliptical cylinder in the middle, and an ellipsoid part (dome) at the top. The cavern is symmetrical in the x-z and y-z planes. Figure 2 presents the cavern and tank geometry, and the respective dimensions of the cavern and tank components. In reality the tank is placed on a structure made of concrete blocks. The present analysis assumes a solid cylindrical base bellow the tank and free space between the tank base and the cavern bottom.

The calculations of the temperature profiles within the cavern walls tank into account the physical properties of the rock surrounding the cavern. The CDF simulations require a fixed thickness for the cavern wall layer. In the present simulation, this thickness is taken equal to 6 m. Outside this layer the rock temperature is constant and equal to the bulk temperature of the cavern rock. The bulk rock temperature is equal to the temperature of the air occupying the cavern when the accident occurred and the argon was released (i.e. at t = 0). The initial conditions in the cavern before the release are 295 K and 1250 mbara.

4.3 *CFD dispersion results*

The type of release considered here involves the leak of gaseous argon from the tank roof.

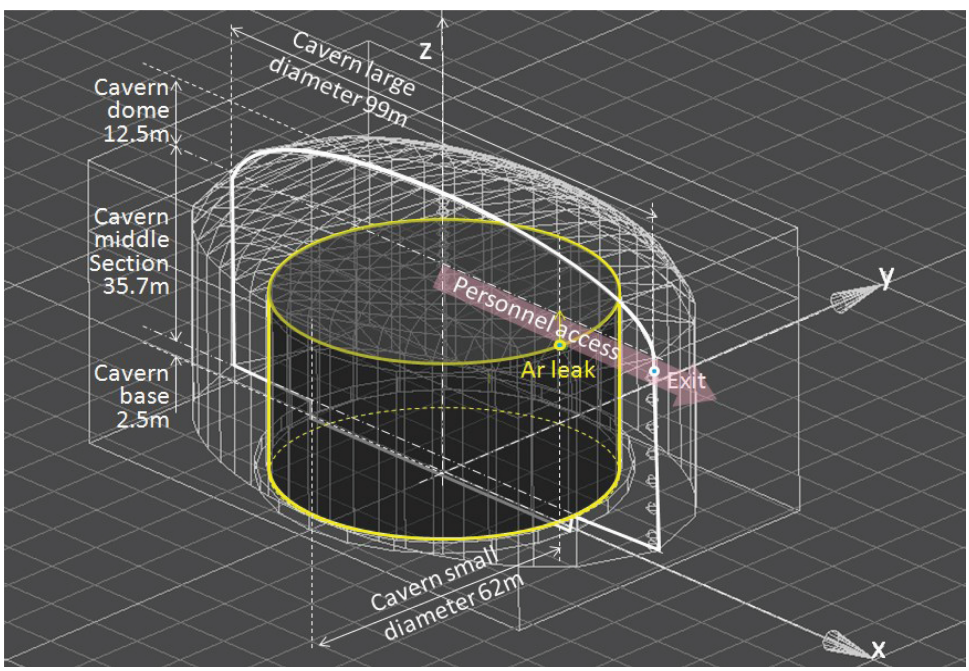


Figure 2. Tank cavern and argon tank geometry.

Table 3 presents the characteristics of this release category. The release location has been set on the cross-section of the top of the outer tank perimeter and the large cavern diameter, on the personnel evacuation route. As the exact location of a break cannot be determined, the location selected here represents the worst case scenario for the personnel safety. The argon mass flow rate is determined based on the initial gas exit velocity determined by the pressure difference and the gas density, and the assumed equivalent break diameter set equal to the boil-off pipe diameter.

Figure 3 gives the argon concentration contours at 1 hour after the release occurrence. The oxygen concentrations are calculated assuming that air consists of 20% oxygen and the gas mixture of air and argon is ideal at this pressure and temperature range. The contours show that one hour after the onset of the release, oxygen is well above 18%.

Table 3. Argon release characteristics.

Parameter name	Value
Orifice diameter	0.244 m
Initial argon flow rate	1.667 kg/s
Argon flow rate slope	0 kg/s^2
Leak location x-axis	27.5 m
Leak location y-axis	0 m
Leak location z-axis	32.5 m
Direction of leak	Upwards, vertical
Argon temperature	89.35 K
Argon pressure	1275 mbara
Argon phase	Saturated vapor
Number of cells (y-symmetry assumed)	44,559
Cell volume (near source)	0.625 m^3

The pressure, argon concentration and temperature profiles in various locations in the cavern free volume during the first 50 hours after the leak occurs are illustrated in Figures 4, 5 and 6, respectively. Concentration and temperature sensors are placed at different heights above the centre of the tank, on the cavern walls near the (x,y) location of the leak and at the (x,y) location of the exit. The exact location of the pressure sensor is near the dome centre. Unlike temperature and concentration, pressure should not change significantly between different locations in the cavern so only one sensor is sufficient. Concentrations are volumetric, so, in ideal gas mixtures, the same numbers hold for molar concentrations.

Figure 5 shows that in the centre of the cavern above the tank the argon concentrations remain below 10% during the first 24 hours, and take two days to go over 20%. Near the cavern walls around the tank the concentrations are significantly higher and reach 10% argon within 5 hours, and 20% within 8 to 10 hours. Therefore, oxygen concentrations are predicted to remain over 18% for a day above the tank and for 5 hours at lower heights. Based on the above concentration results, there is no problem of asphyxiation for this type of release at least up to 5 hours after the release.

4.4 *Qualitative analysis of dispersion results*

The CFD simulations assume that the release rate from a break in the roof of the tank will remain constant for over 50 hours. Clearly, this assumption is not realistic. Figure 4 shows that the pressure inside the tank cavern increases at a rate of 27 mbar/hour. Even if the pressure inside the tank were to remain constant at 1275 mbara (the pressure at t = 0), the cavern pressure will increase from

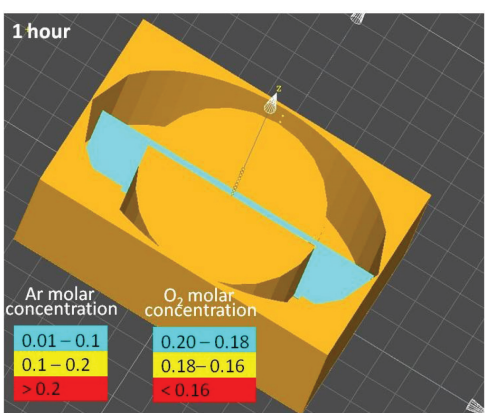


Figure 3. Argon molar concentration contours in the tank cavern at 1 hour after the release.

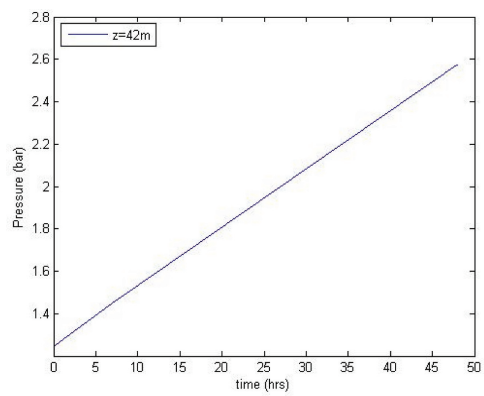


Figure 4. Pressure profile at (x,y,x) = (0,0,42 m) in the tank cavern during the first 48 hrs after the release.

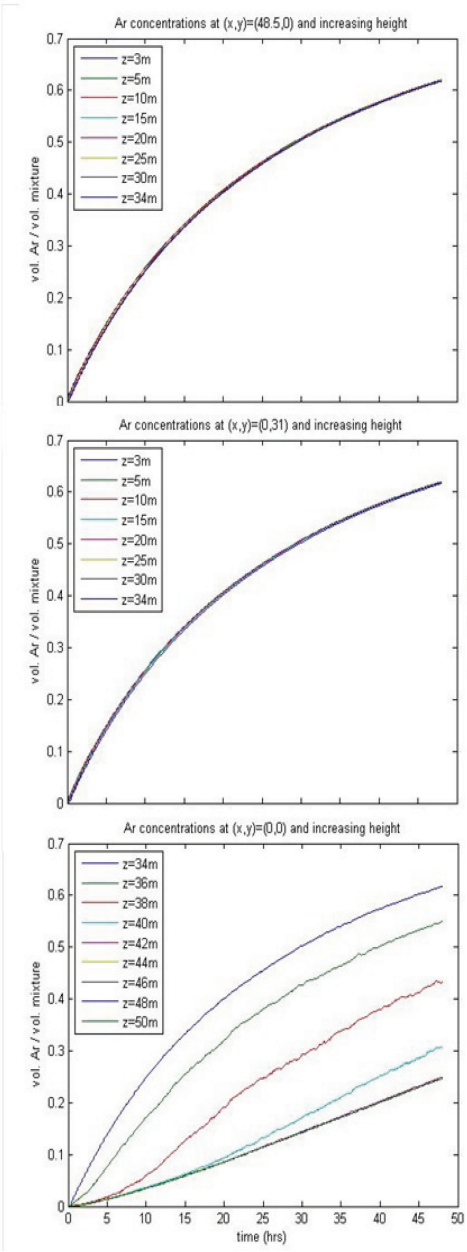


Figure 5. Argon concentration profiles at various locations in the tank cavern during the first 48 hrs after the release.

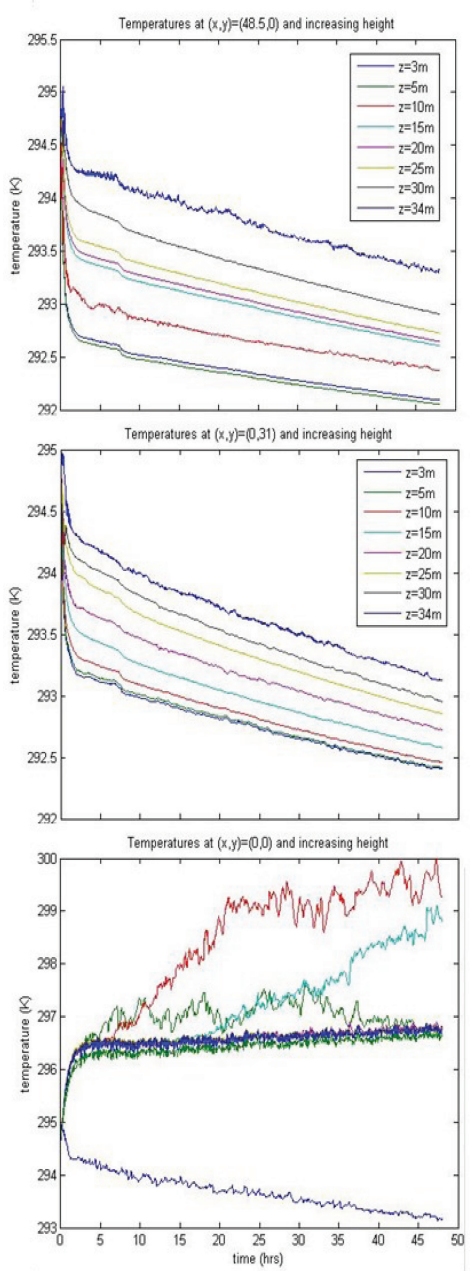


Figure 6. Temperature profiles at various locations in the tank cavern during the first 480 hrs after the release.

1250 mbara to the tank value within about 1 hour. This will effectively stop the release of Ar gas. This time frame is underestimated, since the decrease in pressure difference will reduce the mass rate of Ar release, yielding lower rate of cavern pressure increase. Hence equalization of the pressures will take place later than one hour.

It can therefore be concluded that, if there is personnel inside the cavern when an overpressure break occurs, for at least one hour the conditions

are not dangerous to health and they have adequate time for evacuation.

What will happen after the pressure equalization is questionable since it is not certain what will happen with the re-condensation system. Since the temperature in the cavern remains above 290 K, the heat influx in the tank does not change significantly, so the boil-off remains the same. If the pressure inside the tank increases, a quantity of argon will be released, the pressure in the cavern will increase and the release will stop again. If for some reason the gauge pressure inside the tank drops below –25 mbarg there might be further damage to the roof because of implosion.

Figure 6 presents the predicted temperature profiles. Both the steady-rate-release analysis and the qualitative consideration of the most realistic cases indicate that the temperatures in the cavern won't fall below 290 K.

5 CONCLUSIONS

This paper briefly presented a part of the safety analysis and quantitative risk assessment conducted for an underground installation involving the storage and processing of over 50 ktons cryogenic argon. The installation design is part of an ongoing Pan-European effort to construct a very large scale observatory for particle and astroparticle physics experiments.

The main safety concern in this facility is the loss of containment and the release of the cryogen in the underground premises. Such releases could lead to oxygen deficiency and freezing temperatures, and, therefore, be hazardous for the health of personnel present in the facility. In addition, exposure of the cavern walls to extremely low temperatures for long time periods may alter the rock properties, thus entail significant risks to the cavern integrity.

The study discussed here included a detailed evaluation of accident frequencies and dispersion simulations of argon release due to tank overpressure. The possible release scenarios involve gaseous argon leak inside the tank cavern or the adjacent process cavern. The frequency analysis indicated that there is room for improvement in terms of the fluid handing processes, and suggested specific modifications to increase the system reliability.

The dispersion simulations involved the use of a Computational Fluid Dynamics (CFD) tool suitable for handling Three Dimensional (3D) transient dispersion problems involving two-phase cryogenic leaks of fluid heavier than air. Results are presented for the case of argon gas leak inside the tank cavern due to tank overpressure. A second scenario involving release in the process cavern could not be considered at this stage due to lack of information on the geometry and configuration of the process cavern. The simulation results indicate that the considered release category does not entail risks for human hazards or the underground construction.

Note that, further analysis, not presented here, involves additional types of cryogen release, including the analysis of: (a) a medium size break releasing liquid argon due to rupture of a pipe carrying argon from the tank to the filtration units, and (b) a major failure of the tank resulting in large break (probably along seam lines) also releasing liquid argon. This work is available at the LAGUNA website.

The safety and risk assessment analysis will benefit from the results of an ongoing site investigation (by other members of the LAGUNA-LBNO consortium) will enable a better understanding of how the cavern rock walls will respond when exposed to extremely low temperatures or extremely high pressures for long time periods.

ACKNOWLEDGEMENTS

The authors acknowledge financial support from the European Commission, project LAGUNA-LBNO "Design of a pan-European Infrastructure for Large Apparatus studying Grand Unification, Neutrino Astrophysics and Long Baseline Neutrino Oscillations", EC GA 284518, FP7-INFRASCTRUCTURES-2011-1.

REFERENCES

HSE Health and Safety Executive. Failure rate and event data for use within land use planning risk assessments. Document ID: HSE PCAG chp_6 K Version 12—28/06/12. Available at: http://www.hse.gov.uk.

LAGUNA Deliverables of LAGUNA (GA 212343) and LAGUNA-LBNO (GA 284518) European Commission projects. Available at: http://laguna.ethz.ch:8080/Plone.

Papazoglou, I.A. 1998. Functional block diagrams and automated construction of event trees, Reliability Engineering & System Safety 61 (3): 185–214.

Poling BE, Prausnitz JM, O'Connell JP, *Properties of Gases and Liquids*, 5th ed, McGraw Hill,

Venetsanos, A.G., Papanikolaou, E. & Bartzis, J.G. 2010. The ADREA-HF CFD code for consequence assessment of hydrogen applications. International Journal of Hydrogen Energy 35 (8): 3908–3918.

Reliability and safety based system design

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

European survey on safety methods application in aeronautic systems engineering

A. Berres, H. Schumann & H. Spangenberg
German Aerospace Center, Lilienthalplatz 7, Braunschweig, Germany

ABSTRACT: After gaining working experience by many years of learning, safety experts work in interdisciplinary teams, sometimes companywide or as a hired specialist. Planes are usually used and maintained over decades. Both scenarios require a safety data exchange over a long time to support development and maintenance. Addressing those needs a survey was developed to evaluate application of safety methods and tools in context of a European project. Based on engineering knowledge and the survey findings, we will show an approach combining system and safety engineering needs. Also recommendations are made for methods and tools applicable for an early integration of safety method. This reduces risk and save cost of projects.

1 INTRODUCTION

Unfortunately, thinking of system errors, defects or failures is not a likeable part of systems engineering. Especially within damaged systems, the loss of resources or lives is at stake. Most engineers are used to develop system functionality and solve problems by finding adequate design solutions without considering the risks (N.G. Leveson 2002). Also the separation for safety and systems engineering during the development worsens the problem. In consequence, the application of safety methods is considered or introduced late in the design process. Furthermore, uncovered requirements and design solutions, not satisfying the required system functionality, are the consequences. Regarding (INCOSE 2011), about 85% of costs are committed within the design stage. Also, requirement changes lead to design changes and costs have to be multiplied by factor 6 during design, by 100 in development and by 1000 in production or test stages (INCOSE 2011).

Cost reduction is possible if safety requirements are considered as early as possible in the development process. Therefore, development phases and applied safety methods have to be understood. With our expertise in systems engineering research projects, we have a clear idea, which methods should and can be applied during early development phases (Berres, Schumann, and Escher 2012). However to help engineers, we would like to follow a pragmatic approach and try to understand which methods and tools were applied during development.

It was decided to start with the development of a survey across the Actuation 2015 partners to find out, which tools for safety assessments are used in industry and academia and may be relevant candidates for further investigation. The identified tools were used to perform a data exchange using our system model PREMISE (H. Schumann and A. Berres 2011). Our system model enabled us to show the early integration of safety methods into the development process in the Actuation 2015 project.

This paper describes the development of the questionnaire, its technical implementation and, of course, the evaluation of the survey results.

1.1 *Actuation 2015*

Before starting with the conducted questionnaire, the project context has to be understood to evaluate the gathered results for the aerospace domain.

Actuation 2015 is a European collaborative research and development project. The project aims to develop and validate a common set of standardized, modular, and scalable Electro Mechanical Actuator (EMA) resources for all actuators and all types of aircraft (Actuation 2015). Safety critical functions for flight control, high lift, landing gear, door, thrust reverser have to be developed.

Actuation 2015 coordinated by Goodrich Actuation Systems SAS gathers 53 partners, including the European key players in the aircraft industry. The consortium includes:

- main European players in actuator and component suppliers
- European players of the business, regional and commercial aircraft industry
- European standardization authorities (CEN)
- Research and test centers from all over Europe, with international reputation in aircraft equipment

development, with past and recognized experience on many aircraft programs (A350, F7X, etc.)
- Universities from several European countries, each of them internationally recognized for the quality of their scientific work, in the field of electric actuation standardization. Several of them have long-term relationship with both aircraft manufacturers and equipment providers.
- SMEs—ten SMEs work in Actuation 2015 and cover a wide range of activities (software, manufacturing and assembly, R&T and test centers, R&T project support).

Considering the project partners and the project goal by conducting the survey, both systems engineering and safety experience of the partners cover the need to find tools and methods for an early integration of safety methods into model based systems engineering.

2 A EUROPEAN SAFETY SURVEY

Various lifecycles of systems engineering are shown in (INCOSE 2011). Identifying applicable safety methods to consider safety methods as early as possible requires the definition of development stages and also the assignment of those methods to the stages. According to (NLR 2013) and in respect to (INCOSE 2011), the following stages are considered for the safety survey: Requirements definition (RD), Preliminary Design (PD), Conceptual Design (CD), Detailed Design (DD), System Design (SD).

For being able to define applicable safety methods, the available methods for systems engineering had to be analyzed. Over the last years, NLR collected more or less all known safety methods and put them into a database (NLR 2013). About 750 methods or techniques are listed therein. Based on the database list, only methods applicable to aircraft and aviation were considered for the survey. However, the database returns 321 safety methods for both applications. To reduce the number of methods, an expert voting was conducted. Safety experts voted the methods impact according to systems engineering stages. The voting of safety methods for the defined development stages adds up as follows:

Requirements design

RHA	Requirements Hazard Analysis
SRCA	Safety Requirements Criteria Analysis

Preliminary design

PSSA	Preliminary System Safety Assessment
PHA	Preliminary Hazard Analysis

Conceptual design

PHL	Preliminary Hazard List

Detailed design

CCA	Common Cause Analysis
BFM	Beta-factor method
CRA	Criticality Analysis or Criticality Matrix
DD	Dependence Diagrams
DMEA	Damage Mode and Effects Analysis
FHA	Functional Hazard Assessment
F(a)HA	Fault Hazard Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FMES	Failure Modes and Effects Summary
FTA	Fault Tree Analysis
GFCM	Gathered Fault Combination Method
QCT	Quantified Causal Tree
RBD	Reliability Block Diagrams
SM	Shock Method
SSA	System Safety Assessment
SSHA	Subsystem Hazard Analysis
CCD	Cause Consequence Diagrams
CCA	Cause Consequence Analysis
CCFA	Common Cause Failure Analysis
CMA	Common Mode Analysis

System Design

CCA	Common Cause Analysis
BFM	Beta-Factor Method
DD	Dependence Diagrams
QCT	Quantified Causal Tree
SM	Shock Method
CCFA	Common Cause Failure Analysis
ESD	Event Sequence Diagrams
ETA	Event Tree Analysis
KTT	Kinetic Tree Theory
SHA	System Hazard Analysis

2.1 *Developing the questionnaire*

Based on the safety methods classification, we started to build the questionnaire. To gain valid answers which methods are applied and which methods are pragmatic, we had to answer the following questions:

2.1.1 *Did we find the relevant persons?*

To evaluate the possible impact of an answer, the experience of the participants was considered. Therefore, we designed questions to gain an understanding of the safety experience and expertise in applying safety methods of the answering person.

2.1.2 *Did we identify the relevant processes and standards?*

Known standards and processes as well as their importance and application among users have to be understood. Standards which have to be considered in the future shall be identified.

2.1.3 *Did we find the right applied methods?*

Based on the found classification, we have to ask engineers the following question: “Do you

apply the identified methods during the assigned development stage". Self-developed research safety methods and tailored methods which are derived from standard methods are also to be identified.

2.1.4 *Which tools are applied for the identified methods?*

To understand the requirements of data exchange among tools by using an integrated design model, we need to identify the tools which are used to apply the safety methods. Our main goal is to support the most applied methods and tools, to help engineers during their daily work.

Answering the shown questions lead to 31 questions which compose the "Actuation 2015—safety method questionnaire". A non-functional goal was: A participant shall spend only 15–20 minutes for the survey. The achievement of this requirement was internally proven by our colleagues.

2.2 *Building an online survey*

After creating the questionnaire, we decided to use an online survey approach. Thus, we can gather and evaluate the data faster than using the classical approach by sending "pdf"—questionnaire mails.

By choosing to conduct anonymous survey, privacy and intellectual property issues of the Actuation 2015 members were assured. Furthermore, experts who work under confidential rules were encouraged to exchange their experience.

The main benefits of conducting an online survey are the easy way to deploy the survey and to create electronic reports. They lead to an efficient evaluation of the survey.

2.3 *Selecting of survey technology*

2.3.1 *Requirements on survey technology*

During the development of the questionnaire, the following requirements were identified. The requirements are needed to be able to select the right survey platform.

1. The survey shall be done once and only for this project, reuse of the questionnaire is not necessary.
2. Allowing a user group of max. 300 people.
3. A number of about 50 questions shall be possible, regard to: time spending for the survey shall take only 15–20 min.
4. The survey shall be anonymous to encourage all members to participate.
5. Easy to create, with an easy to understand user interface, to reduce the costs creating the survey.
6. Different possibilities to create questions like single choice, multiple choices, free text.
7. Getting predefined reports after survey.
8. Export report data shall be possible, including the answers of single participants. The export shall support *.csv files to evaluate the data by MS Excel.
9. Survey engines shall be hosted by external providers.

2.3.2 *Market investigation*

An analysis via the internet was done to find suitable platforms (BDC 2013, Survey Software Review 2013, IdealWare 2013, and Ohio State University 2013). We identified more than 30 possible engines. Only the most interesting engines were selected. To be able to understand the capabilities and the functionality of the platforms according to our requirements, a short overview of each platform is given.

SurveyMonkey (SurveyMonkey 2013) is an online hosted survey tool for basic and commercial surveys. The "Free" version might be useful for very small and informal surveys to collect 10 questions and 100 responses per survey. It is limited for customization of the survey look. The "Select" version offers unlimited questions and responses, customizability, skip logic and the ability to export Excel and PDF files. The package's folder structure and "search by title" feature makes it easy to navigate through many surveys. Reports are minimal, but they allow you to export results to another application to do more serious analysis. Higher end "Gold" and "Platinum" versions offer advanced logic features, like question and answer piping, randomization and text analysis for open responses.

SurveyGizmo (SurveyGizmo 2013) offers a low-cost solution with some advanced features. It supports 1000 responses per month, and basic logic as well as a range of more advanced packages. At all levels, SurveyGizmo offers basic piping, fully customizable survey look and feel and the ability to embed images and videos hosted on your own website. More advanced levels offer many randomization options, question options, questions per survey page, and pages themselves, skip logic and more. SurveyGizmo offers an API for integrating survey functionality into websites, blogs and other applications.

QuestionPro (QuestionPro 2013) provides a professional and a free version for creating online surveys. The free version includes: online surveys, micro polls and Ideascale, a feedback collection and voting platform. Also gadgets like Google Analytics and Twitter integration is available. It has a simple wizard approach to create and edit surveys with a large number of question types available. The free version allows an unlimited number of responses, making it ideal for surveys which are small in scope but large in audience, instead it is limited by number of surveys (2) and questions per survey (10).

Murvey (Murvey 2013) helps you create, publish, and manage online surveys easily than you have ever seen before. Murvey is a cloud-based web service that lets you conduct online surveys from a simple and efficient user interface. Creating and publishing the survey only takes a few minutes. Great looking reports can be created as soon as responses start coming in to your survey.

LimeSurvey (LimeSurvey 2013) is a free and open source survey package appropriate for non-profits, looking for advanced survey logic and analysis features. Its range of features includes full customization of survey look and feel, support for 40 different languages, piping, skip logic, a library of available survey questions and blast emailing. The tool has a large support community and is under active development. This is an open source package that can be downloaded for free, installed on your own web server, and customized to your needs by a developer with knowledge of PHP/MySQL. Although the tool itself is free, be prepared to bear the costs for your own web hosting, and the time it takes to properly install, configure, customize and support this product on your own.

Only free or basic versions of the survey platforms where used for our evaluation to reduce cost. To choose the best platform, (Table 1) shows the evaluation of each tool with regard of our requirements.

Shown in Table 1, all tools offer most of the required functionality. SurveyMonkey, SurveyGizmo and QuestionPro provide all required functions by their commercial version only. LimeSurvey covers most of the requirements, but does not provide the infrastructure for the survey. Setting up the required infrastructure was unfortunately not possible in time because of the high effort. Therefore, only Murvey covered all requirements without limitations and was selected for the survey.

2.4 *Implementing the survey*

The implementation of the survey was easy and done in less than 4 hours. To create the survey, mainly the following three types of questions were required.

Table 1. Tool requirements coverage.

Requirement tool	1 2 3 4 5 6 7 8 9
SurveyMonkey	X X O X X X X O X
SurveyGizmo	X X O X X X X X X
QuestionPro	X X O X X X X X X
Murvey	X X X X X X X X X
LimeSurvey	X X X X X X X X O

2.4.1 *Question with single choice*

To create the "single choice question", the question had to be copied from the questionnaire into the question row (grey). Then, possible answer choices had to be copied into the choice field. The created question is shown in Figure 1.

2.4.2 *Question with multiple choice*

A multiple choice question (Fig. 2) can be created like a single choice question. But by selecting the multi choice button, the character of the questions is changed. In the case that additional information is needed, an "other" field can be added. A free text field provides space for an answer, like other standards, given by the participant.

2.4.3 *Question with free-text answer*

In rare cases, a free text answer is necessary. Therefore, a free text field can be used. By selecting the option free-text, copying and pasting the question text into it, the question is easily created (Fig. 3). It is recommended to minimize such questions to reduce the evaluation effort.

After creating all questions from of the questionnaire, a theme can be selected to choose the appearance of the survey. Also an entry text can be realized to introduce the purpose of the survey.



Figure 1. Implementation of single choice questions.

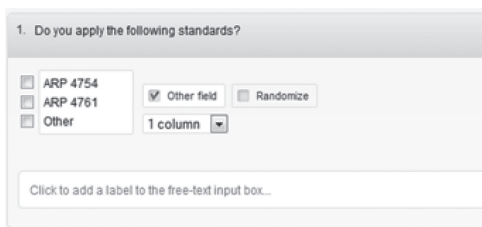


Figure 2. Implementation multiple choice questions.



Figure 3. Implementation of free text answer questions.

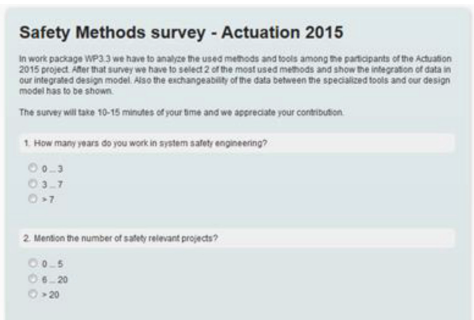


Figure 4. First questions of the online survey.

The following image Figure 4 shows the first questions of the implemented survey.

3 SURVEY REPORT

To conduct the survey, the process was split into two phases. The first phase was a test phase with 30 selected members. Goal of this phase was a test to estimate the number of replies we could expect. Therefor all project member were asked to attend. Our goal was to reach about 10% of the project team. Before starting the survey, the first test group was prepared, by sending the prepared questionnaire. Additionally the purpose of the survey was described. After two weeks, the phase was finished by reaching the goal. Also part of this phase was the evaluation of the questionnaire. The test group was asked to send a feedback. The replies of the test group showed, only minimal adjustments of the questions were required.

After the first phase, the next phase was started. Therefor all project members were asked to contribute to the survey. Again the questionnaire was sent for preparation. A week later, the link to the survey was sent. Because of the holidays took place during the survey time, it was decided to extend the planned two week time span to a month.

The survey was conducted during August and September 2013. All members of Actuation 2015 with a technical background like research, system design or development, were asked to join the survey. As a first result of the survey, only members with a technical background answered. Also, in one case a pdf was send due to technical problems.

3.1 *Did we find the relevant persons?*

As shown in Figure 5, 27% of the members with technical background participated in the survey, by means of filling out or declining the participation.

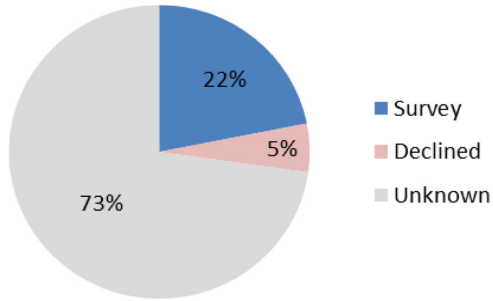


Figure 5. Distribution of participants.

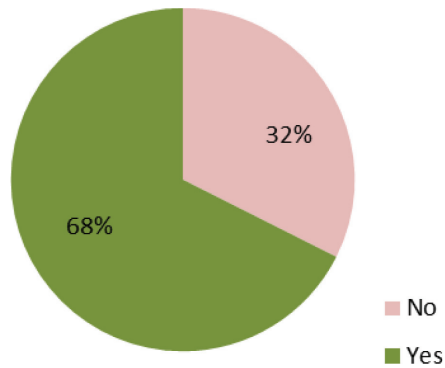


Figure 6. Safety experience.

To distinguish participants with and without safety experience, it was offered to answer only the first question and to leave all others unanswered for participants without experience. Figure 6 shows the distribution of participants with and without experience. Related to Figure 6 and regarding an amount of 68% of participants with safety experience, ~15% of the team with technical background answered the survey while gained safety experience.

To classify the level of experience in beginner, experienced and expert levels, data was classified by years of safety experience, the number of projects attended and a self-assessment of the participant. In Figure 7 the classification results are shown. About half of the participants had gained beginner experiences, i.e. less than 3 years safety experience and less than 5 projects attended. The rest is split equally into experienced with 5–20 years and safety experts with more than 20 year experience and more than 7 projects attended.

The field of work was additionally analyzed. In Figure 8 the expected distribution is shown. Most of the participants work in the field of research, because of the research nature of the project.

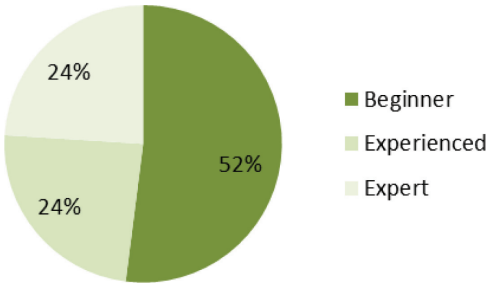


Figure 7. Distribution of safety experience.

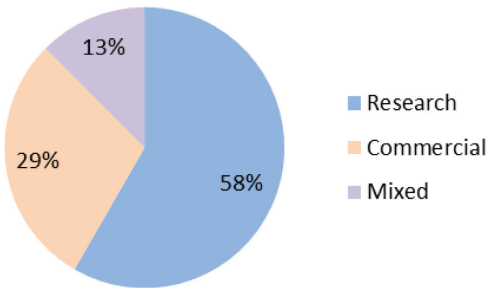


Figure 8. Participants field of work.

In summary about 22% of the project team answered the survey. A good mix of research and industrial experience was found. The participants mainly work in the field of research with a good knowledge of applied standards. They develop new methods, like method driven approaches. At least the participants are experienced in applying safety methods.

3.2 *Applying safety methods*

Regarding the question "Did we find the right applied methods and processes?", analysis of the application of safety standards and methods was done.

In the survey, the following in aerospace mainly employed standards like DO-178b, DO-178c, ARP4754 and ARP4761 were given. In Figure 9 the applied standards are depicted. Also the additionally application of special standards, like ARP 4763 and Mil882, is shown.

Next question to be answered was, to analyze the number of applied methods among the development stages. Figure 10 shows the number of participant applying methods in each development stage.

Unexpected were the results of Concept and System Design stage. One reason may be a different understanding of development stage definition,

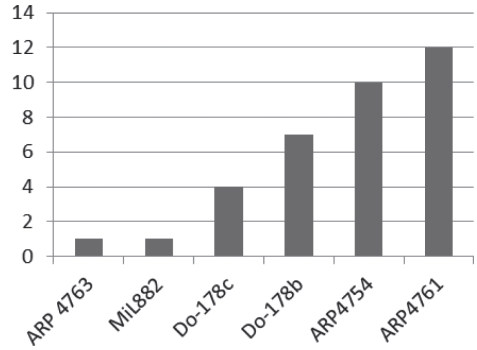


Figure 9. Number of participants applying safety standards.

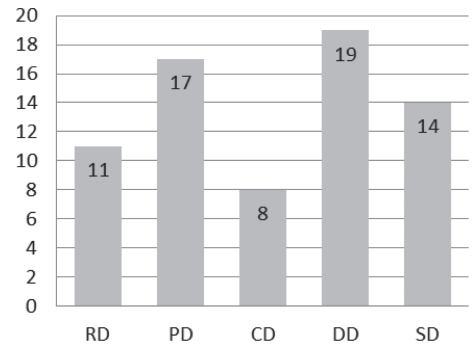


Figure 10. Number of participants applying methods.

applied in systems and safety engineering. Also a reason could be, the different definitions in the applied standards. With regard to (INCOSE 2011), the understanding of what is covered by a development stage depends on the development process. By our expierience made in different domains like aerosapce, aircraft and automotive, merging of stages is recommended. Therefor from the safety engineering perspective Preliminary and Concept Design are merged into a Concept stage and Detailed and System Design into a Detailed stage. This merge is proposed as a safety system engineering process. The number of participants applying safety methods for this recommodation is shown in Figure 11.

Shown in Figure 10, also and according to our expectation, the amount of participants applying safety methods in the early stages is less than in later development stages. This may lead to uncovered safety requirements in the ongoing development process.

Did we find the right methods?

In Chapter 2, applicable methods for each development stage were presented. To validate our classification and assignment of those methods, the

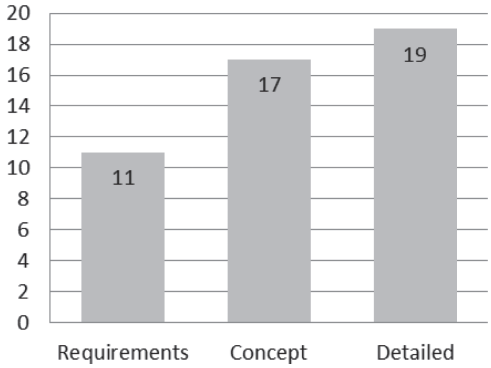


Figure 11. Number of participants applying methods for the recommended merge of development stages.

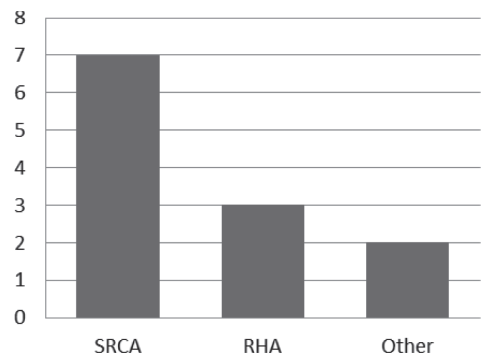


Figure 12. Participants applying methods in requirement stage.

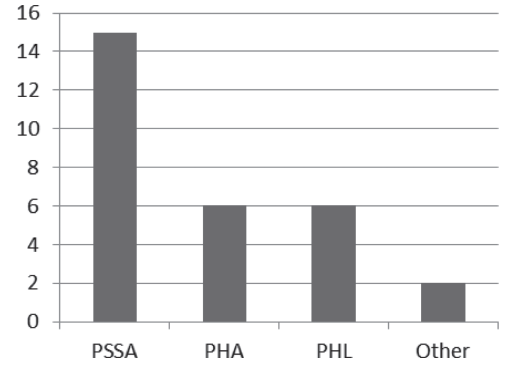


Figure 13. Participants applying methods in concept stage.

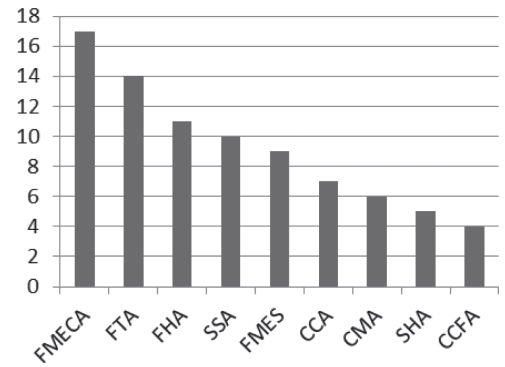


Figure 14. Participants applying methods in detailed stage.

survey answers had to be analyzed. Unfortunately, in the cases that other than the given methods are applied, participants did not mention those methods.

Figure 12 shows the number of participants applying the proposed method during the requirement stage. Besides, only two methods where proposed: SRCA and RHA. SRCA is the most applied method and shall be considered as standard method for the requirement stage.

Regarding the recommended merging, the Concept stage depicted in Figure 13 shows the number of participants applying PSSA, PHA, PHL or other methods. As shown PSSA has a wide user basis: therefore this method is recommended during the concept stage. Note that for the PSSA several methods like FTA and CCA (Common Cause Analysis) are used which are also depicted in Figure 14.

In opposition to the first two stages the detailed stage contains a wide set (~ 30) of applicable methods. The results for detailed stage are presented in Figure 14. As expected nearly all proposed methods were used by the participants, but only methods applied by a minimum of 4 users were presented.

FMECA is the most applied method during detailed stage. This bottom up method can be performed on functional level. But normally it will be performed on part level. On the other hand the second most applied method is FTA. This top down method is usually performed on functional level. One of those methods is recommended, depending on a top down or bottom up development strategy. Applying both methods during a safety assessment leads to coverage validation. In case any function or part is not covered by FMECA or FTA this will be recognized. To complement the safety assessment in this stage additional methods are necessary. Which methods shall be applied, depends on the safety requirement demand by the employed standard.

3.3 *Which tools are applied?*

The safety goals of the applied methods during requirements and concept design are identification

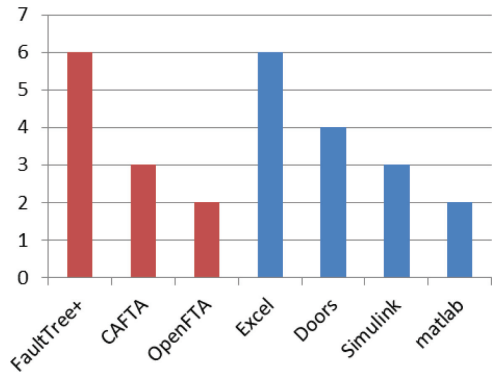


Figure 15. Applied tools.

of hazards, events or risks at system level. Also the assignment of those hazards, events or risks to functions or system elements is required. These methods can be implemented by the use of tables. Common tools providing these functionalities are Doors or Excel. (J. Langheim 2010) shows both tools are used in safety projects. An exchange of data among those tools and our system model PREMISE are implemented easily and shown in (H. Schumann 2010).

Some methods applied during the detailed design like FMECA or FHA can also be implemented in Excel or Doors (Total Quality Management 2013). But others are more complex like FTA. During this analysis a Fault Tree has to be constructed. Implementation of Fault Trees in Excel or Doors is possible but the maintenance is hard and error prone. Therefor a set of tools exists especially for FTA shown in Figure 15.

A little surprise was Matlab and Simulink tool, because those tools are usually applied in systems exploration (Vanderperren and Dehaene 2006). On the other hand implementing a safety method for example risk evaluation on batteries are easily made as shown in (C.G. Wang 2013).

4 CONCLUSION

The survey showed which safety methods are considered in the systems engineering process. But it was also shown that there is a tendency starting late applying safety methods. According to INCOSE 2011, the project risk and effort can be reduced by a factor of 10–1000 by regarding safety requirements early in systems engineering process.

Additionally it was depicted, that most of the methods and standards are well known and applied by experienced engineers. However, new research related methods were applied late or even not. Thus, methods like model based development provide a solution for long term support in development and maintenance.

By defining a systems safety engineering process with three stages, we recommend applying top down safety methods, like SCRA and FTA. Furthermore in the late development stages, bottom up methods like FMECA comply this process. Combining top down and bottom up approaches in the development strategy, a validation is possible. Therefore, by identifying hazardous events of system functions in FTA and identifying hazards and their causes on part level in FMECA, coverage is possible. Also uncovered functions or system parts are detectable.

The recommended tools for safety assessment during the requirements stage are table based tools like Excel or Doors. Both tools are well known in the engineering domain. In the later stages, Matlab Simulink may be used for the evaluation of system and safety aspects. Depending on applied safety methods, specialized tools, comply the safety analysis in those stages.

According to the survey results, the fault tree analysis is the most applied method by safety engineers. Based on this result and the applicability of this method, a demonstrator for data exchange among tools using PREMISE system model was realized. The presentation of this work would exceed this paper and will be presented in an additional publication.

REFERENCES

Actuation 2015, 2013, ACTUATION 2015 Towards the next generation of aircraft, http://www.actuation2015.eu/, accessed on 10/2013.

BDC, 2013, How do Internet survey tools help?, http://www.bdc.ca/EN/solutions/smart_tech/tech_advice/free_low_cost_applications/Pages/internet_survey_tools.aspx, accessed on 10/2013.

Berres A., H. Schumann, S. Escher, 2012, Modellbasierter Systementwurf: Generierung von Fault-Trees, DLRK 2011.

IdealWare, 2013, A Few Good Online Survey Tools, www.idealware.org/articles/fgt_online_surveys.php; accessed on 10/2013.

INCOSE, 2011, Systems Engineering Handbook v. 3.2.2.

Langheim J, Guegan B, Maillet-Contozet L, et al., 2010 System architecture, tools and modeling for safety critical automotive applications—the R&D project SASHA, ERTS 2010, Toulouse, France, 19–21 May.

Leveson N.G., 2002, System Safety Engineering: Back To The Future, Aeronautics and Astronautics Massachusetts Institute of Technology.

LimeSurvey, 2013, www.limesurvey.org, accessed on 10/2013.

Murvey, 2013, www.murvey.com, accessed on 10/2013.

NLR, 2013, Safety Methods Database, Version 1.0, 4 March 2013,

QuestionPro, 2013, www.questionpro.com, accessed on 10/2013.

Schumann H. et al., 2010, Concurrent Systems Engineering in Aerospace: From Excel-based to Model Driven Design, 8th Conference on Systems Engineering Research, Hoboken NJ.

Schumann H., A. Berres, 2011, Modellbasierter Systement wurf mit dem PrEMISE-Modell, Tag des System sengineering 2011 Hamburg.

Survey Software Review, Free survey software comparison chart 2012, www.survey-reviews.net; accessed on 10/2013.

SurveyMonkey, 2013, www.surveymonkey.com, accessed on 10/2013.

SurveyGizmo, 2013, www.surveygizmo.com, accessed on 10/2013.

The Ohio State University, A survey of survey tools, wac.osu.edu/workshops/survey_of_surveys/, accessed in 10/2013.

Total Quality Management, Excel-Tool FMEA-Formblatt, http://www.tqm.com/service/download/excel-tool-fmea-formblatt, accessed in 10/2013.

Vanderperren Y., Wim Dehaene, 2006, From UML/SysML to Matlab/Simulink: current state and future perspectives, DATE '06 Proceedings of the conference on Design, automation and test in Europe: Proceedings.

Wang C.G. et al., 2013, A New Method to Detect Voltage Sag Based on Wavelet Energy Entropy, Applied Mechanics and Materials, Chapter 22: Power Grid and Smart Grid Technologies, Pages 2254–2258.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Semi-formal static and dynamic modeling and categorization of airport checkpoints

P. Renger, U. Siebold, R. Kaufmann & I. Häring
Fraunhofer Ernst-Mach-Institut, Efringen-Kirchen, Germany

ABSTRACT: Airport check points are vital infrastructure for secure and safe air transport. They consist of an ever increasing number of components. Also the interactions between the checkpoint components as well as the checkpoint itself and external systems are expected to further increase in the future, e.g. if profiling and more risk based methods are applied. As a basis of analyzing airport checkpoints with respect to security and safety a sufficient system understanding is a prerequisite. The Systems Modeling Language (SysML) is used to accomplish that, which is a system engineering adaption of the Unified Modeling Language (UML). We show how static and dynamic properties of airport checkpoints are modeled using SysML. Aiming at an overall modeling of different airport checkpoint designs, we model a generic airport checkpoint design using SysML. The model comprises standard airports as in operation at many airports today. Throughout the paper, we give a broad outlook how these semi-formal models are applied to new ACP concepts as for example proposed by the famous "airport of the future" project as well as distributed checkpoints, where parts of the screening happens "on the fly" by stand-off screening equipment without intrusion for the passenger.

1 INTRODUCTION

Triggered by the rise of hijacking in the 70 s and the events of September 11th, ever intensified regulations for airport security came into effect, e.g. 107th Cong (2001), European Commission (2002), (2008). Despite the fact that the International Civil Aviation Organization (ICAO) adopts standards and recommendations for the aviation sector, the laws concerning airport security are predominantly national (Nelson and Walker, 2011). This circumstance together with the increased security level has a huge impact on passengers and the aviation business and those businesses that depend on air transport. (Schiphol Group, 2009, AIC Europe, 2010).

Health concerns, loss of privacy and time consuming procedures and queues lead to a negative passenger experience at Airport Check-Points (ACPs). AIC Europe (2010) reported that for European airports security accounts for 35% of airport operation costs. The EU-funded international collaboration project XP-DITE (XP-DITE Project, 2013) is dedicated to the above issues, approaching the ACP from a system level point of view.

This paper does not restrict consideration and modeling of ACPs to the limited number of systems currently compliant with regulations from the EU or the US American Transport Security Administration (TSA). The static and dynamic semi-formal modeling approaches proposed in this paper enable the assessment of future, alternative ACP designs, taking into account common performance indicators and deviations from current regulations. The goal behind the research is also to understand and develop future ACP concepts with the help of the presented modeling techniques and in a second step with executable models to assess the performance of these concepts.

Section 2 reviews the state of the art of airport checkpoint modeling and simulation. Section 3 presents roughly the semi-formal system modeling language. Section 4 shows and explains modeling of conventional and innovative ACP systems. Section 5 concludes and gives an outlook.

2 STATE OF THE ART IN AIRPORT CHECKPOINT SECURITY MODELING

Looking at the literature for airport security, we notice that there are many books treating the very popular subject of terrorism, which always implies aviation security. Also books treating only the subject of aviation security are available (Sweet, 2002) (Seidenstadt and Splane, 2009). A scientific approach to measure, optimize or assess the security or performance of the airport or subsystems like the security checkpoint on an integrated

overall system level is not really covered in the scientific literature.

There are various commercial products available to model and simulate performance of economic and operational aspects. Manataki and Zografos (2010) and (2009) modeled an airport terminal as a flow model with UML for this purpose. Other works focus on time performance of functional areas in the airport. Van Landeghem and Beuselinck (2002), Soolaki et al. (2012) and Nyquist and McFadden (2008) tried to optimize the boarding time while Hsu et al. (2012), van Dijk and van der Sluis (2006) and Park and Ahn (2003) tried to improve the check-in procedure.

2.1 *Airport security analysis tools*

Some regulators have developed their in-house solution for software based assessment of the ACP security level [personal communication]. These tools simulate operational aspects like throughput but also security aspects, e.g. detection rate and compliance with current regulations. Usually these tools have a Monte Carlo approach in common, using several instances of a passenger type with distributions for carried threats and other relevant attributes. TSA developed a Security Checkpoint Optimizer (SCO) software to simulate operational and security performance (Wilson et al., 2007). All these tools have the drawback that the components are thought as statistically independent and no human factors with regard to the ACP staff are taken into account, obviously a major model restriction.

Driven by the Homeland Security, MITRE, a not-for-profit organization chartered to work in the public interest, developed an agent-bases Simulation for the whole airport security. The simulation is covers the attack on an airport. The checkpoint is a part of the whole airport security and registered travelers and other passengers are considered differently (Weiss, 2008).

2.2 *Security screening*

For ACPs, the research seems to be strongly driven by the TSA policy. Papers published in journals often show a connection to a regulation or standard rolled out by the TSA. After the events of 9–11 the TSA required the airports to screen 100% of the checked baggage. This led to a number of publications to help solving this problem with time and budget that is in accordance with the economic requirements (Hafizogullari et al., 2003, Jacobson et al., 2005a, Jacobson et al., 2005b, Leone and Liu, 2003, Sahin and Feng, 2009). The paper from Sahin and Feng (2009) introduces prescreening of passengers to optimize the checked baggage screening. de Barros and Tomber (2007) and Holguín-Veras et al. (2012) used discrete event simulation to examine the checkpoint performance and its impact on design and operation of airport terminals.

Prescreening is another security measure introduced by the TSA that influenced many publications. There was already research in this direction from Jacobson et al. (2001). Along with discussions about the different systems introduced by the TSA, researchers tried to quantify the benefit of prescreening for the security process. Lazar Babu et al. (2006) used linear optimization to assign passengers to different screening procedures with the aim to minimize the risk while the capacity of the screening devices is restrained. This approach assumes that every passenger poses the same risk to the system. The works of Nie et al. (2009), McLay et al. (2006) and McLay et al. (2010) assign a varying thread probability. An example with two lanes with strong and normal checks is done by Nie et al. (2012). Nikolaev et al. (2007) used a greedy heuristic for passenger grouping to minimize the risk with a precedent step in which the security devices are set up restrained by space and budget.

Evolutionary optimization is a less commonly applied mathematical approach. But it allows to optimize cost, delays and risk of a check point at the same time (Concho and Ramirez-Marquez, 2012). Others like Olapiriyakul and Das (2007) used queuing theory to measure time consumption for screening and determine the required staff and equipment. Wang and Zhuang (2011) used also the queuing theory to minimize the waiting lines and game theory to simulate the passengers reaction on waiting lines. To propose better check point designs, Leone and Liu (2011) used the queuing theory to measure the performance defined as screening time of different check point designs. Those standard designs are purposed by the TSA in an older version of the Checkpoint Design Guide, now replaced by (TSA, 2009).

2.3 *Integrated view on the security checkpoint*

Within the work discussed, the level of resolution of airport checkpoints ranges from system level, where the whole checkpoint is characterized by a number of attributes, to component level.

All the publications named above have in common that only one aspect of the ACP is assessed. No publication takes an integrated approach to ACP performance. Modeling presented here aims at an integrated approach, also as basis for simulations, i.e. to cover costs (which includes all operational and capacity aspects), compliance with regulations (which cover all aspects of security), and finally

customer satisfaction. An even more thorough and holistic approach would also include the ethical dimension, which is not always directly linked with passenger satisfaction. The publication which covers cost and security is the one from Nikolaev et al. (2007). The above described approach from (Concho and Ramirez-Marquez, 2012) already covers partly each performance area.

2.4 *Research approach*

Using SysML, this paper models not only the structure and function of current ACP concepts but also possible future configuration as discussed for example in the checkpoint of the future from the International Air Transport Association (IATA).

The purpose of the modelling is to lay the basis of an integrated ACP performance prediction, considering all performance aspects along with security.

The basis of the analysis of ACPs are their models that employ OMG's System Modeling Language (OMG, 2010).

3 SEMIFORMAL SYSTEM MODELING

3.1 *General*

There are many modeling languages that are dedicated to the modeling of systems. The Object Process Methodology (OPM) applies a holistic approach to model complex systems. Main elements of OPM are objects, processes and states (Dori, 2002). It is also one of the state of the art system modeling languages (Grobshtein et al., 2007).

The Architecture Analysis & Design Language (AADL) focuses on the modeling of systems that have to fulfill requirements regarding the demand of space, energy and memory. Therefore it supports the estimation of performance, reliability, and schedulability (Feiler et al., 2006, SAE Aerospace, 2004).

AltaRica is a modeling language that mainly uses hierarchical nodes that contain states and transitions (Griffault and Point, 2006). Among other things it can be used to analyze concurrent processes (Arnold et al., 2000).

3.2 *State of the art in modeling security systems*

SysML is one of the latest semi-formal modeling languages and developed by the Object Management Group (OMG). Derived from a subset of UML and extended with components for system engineering it is a promising candidate for a widely used standard modeling language for complex systems. (Weilkiens, 2008). We have selected SysML to model the airport checkpoint within the overall ACP evaluation approach mainly because of its multi-disciplinary application domain, graphical representation and general acceptance.

SysML was developed to model huge complex systems like an airplane. It is proven to be useful for system design and development. There are books describing system engineering with SysML (Weilkiens, 2008, Debbabi et al., 2010) as well as papers (Hause et al., 2005).

In SysML, the diagram elements for requirements modeling are a completely new extension of UML. Soares et al. (2011) describe requirements modeling for software-intensive systems and propose some extensions to the SysML requirements modeling tools.

Other publications focus more on specific aspects of SysML or system engineering. Some authors focuse on an aspect of SysML like activity modeling. Bahill and Szidarovszky (2009) compared several methods for model driven design including various aspects of SysML and Lopes et al. (2011) used it for the system engineering of smart grids.

Also whole product service systems were modeled, including not only the product understood as engineered system but also the customer service provided to the end user (Durugbo, 2012). Geyer (2012) uses SysML for performance-oriented sustainable building design and showed generic models of typical requirements, design structures and flows of energy and resources. This already shows the applicability of SysML for system analyses.

Beside the main use of SysML in the design and modeling of complex systems, numerous publications describe the use of SysML for system analysis regarding safety our security issues. David et al. (2010) describe a method to assess how the functional design process is linked to reliability techniques with automated model analysis of the SysML model. Grunske and Joyce (2008) used SysML to provide a quantitative security evaluation for component based systems. They created modular attack trees for the components in the system and also transferable attack probabilities between the components to explore vulnerabilities in multiple system components.

SysML does not provide the utilities to test the system or validate it against the requirements. Therefore Linhares et al. (2007) proposed to complement the modeling with petri nets and validate it with the TINA toolbox. A very useful approach when it comes to simulation is the mapping/connection between a conceptual model and the computational process or

simulation program. McGinnis and Ustun (2009) showed this concept using SysML and Arena. Pedroza et al. (2011) presented AVATAR as a SysML environment for the verification of safety and security properties in embedded systems.

3.3 *Requirement analysis and use cases*

To model a system in SysML, which is in our case the airport checkpoint, it is crucial to formulate the purpose or the main function of the system. In case of an ACP this is clearly given. The airport checkpoint should execute screening and inspection procedures to identify dangerous objects in cabin baggage and on persons. This main use case leads to a lot of follow-up requirements. But there are also other SysML use case diagrams like a possible intervention of a law enforcement officer for alarm resolution. In our work we focus on the screening of passengers and their belongings.

3.4 *Block diagrams*

Block diagrams are used to model all components within the system and the relations between them. The block definition diagram (bdd) in SysML defines features of blocks and relationships between blocks such as associations, generalizations, and dependencies. It captures the definition of blocks in terms of properties and operations, and relationships such as a system hierarchy or a system classification tree. A special block named constraint is used to model the constraints on properties of the system.

The internal block diagram (ibd) in SysML captures the internal structure of a block in terms of properties and connectors between properties. A block can include properties to specify its values, parts, and references to other blocks (OMG, 2010). The ibd shows in what role (instances) the elements of the bdd are used in the system.

3.5 *SysML behavior diagrams*

Additional to the structure of the model, diagrams are needed to express the behavior of the ACP. We mentioned briefly the use case diagrams which give the behavior of the system with regard to actors outside the system. Use cases specify the general interaction of the system with a specific user.

The activity diagram (act) shows in more detail what happens inside the system during the operation. It describes which actions are executed and what kind of information or condition has to be fulfilled that lead to the next action. The actions can be operations defined in a block and/or just another activity. The level of detail depends on the model purpose.

Another view on the behavior of the system is the state machine diagram (stm). It describes the configuration of the system with regard to its attribute values. Each set of possible attribute values make up one state. The state machine diagram names some of these states and gives information on what conditions and events lead to another state.

The sequence diagram describes the flow of control between actors and systems (blocks) or between parts of a system. This diagram represents the sending and receiving of messages between the interacting entities called lifelines, where time is represented along the vertical axis. The sequence diagrams can represent highly complex interactions with special constructs to represent various types of control logic, reference interactions on other sequence diagrams, and decomposition of lifelines into their constituent parts (OMG, 2010).

4 SEMIFORMAL MODEL OF AIRPORT CHECKPOINTS

4.1 *Airport checkpoint structural model*

The ACP is a combination of interacting screening and logistical components. The core elements the detection devices to screen people and their baggage for prohibited items. To make screening possible in an organized way and as fast as possible, multiple additional components, here after called logistical components are necessary. Examples are desks for divesting, queuing stanchions or all sorts of barriers. For the operation of an ACP various staff members with different tasks need to be present at the ACP.

4.1.1 *ACP elements in a block definition diagram*

There are many possible main categories of ACP elements. To understand the function of each element a block diagram can be used to group and categorize them.

The ACP as a whole can be modeled by a central block with several connections to subsystems and components, as well as flow ports, in this case two, indicating the passenger flow through the ACP. The important point to notice is that the block definition diagram does not show an actual instance of a system but the elements and their relations in a potential instance of the system.

For one thing, there are subsystems connected with a composition to the ACP. The subsystem called lane is connected via an aggregation to the ACP. The components themselves are connected with a generalization to the block screening device. All detection devices have several attributes and operations they share that are expressed with the generalized component. In addition to the attributes

the detection devices have in common, each device has attributes specific to its technology.

Several components build up a lane. As a component could also exist on its own, the connection to the lane is an aggregation. In contrast, a lane cannot exist on its own because it is dependent on the existence of the ACP. This is expressed by the connection with the ACP in form of a composition.

There are components directly connected to the ACP or first aggregated to a lane and within this subsystem part of the ACP. The idea behind that way of modeling is that some elements like personnel or private screening areas are shared over the whole ACP and therefore over several possible lanes, whereas the elements in a lane are not shared and only used and functioning in the context of a subsystem.

In addition to the components having a screening function, there are structures used to encircle the ACP, organize passenger flow and screening processes. These are also generalized, indicating the similar tasks they fulfill in the ACP.

The path elements through the ACP are special because these are not actual physical elements but an abstract concept to plan and analyze possible ways of the passengers through the ACP. When used for simulation, these model elements are quite important for flow and queuing analysis. The path is connected with a composition to the ACP, which is quite clear because dissolving the ACP would make the path disappear or rendering the concept of paths useless. On the other hand, the path shares some properties with the block logistical structures, as it is also used to guide and control passenger flow.

4.1.2 *Simple ACP lane in an internal block diagram*

In Figure 1. the internal block diagram of a simple ACP is shown. It represents those aspects of an ACP which are commonly seen at airports by regular passengers.

The internal block diagram shows the elements of a system in their role they have to fulfill in the considered instance of an ACP. In this case it is a small ACP consisting only of one lane with some extra elements. The components are instances of their block representation. Each instance fulfills a specific task in the overall system. In the shown example this is the case for the block screener. Depending on the position in the system the screener has to fulfill different tasks.

The block queuing area is also used two times in the ACP. One lane is for priority passengers and the other one for all other passengers. Obviously this leads to shorter waiting times for priority passengers. Both groups share a divesting area, where the flow of passengers and their belongings

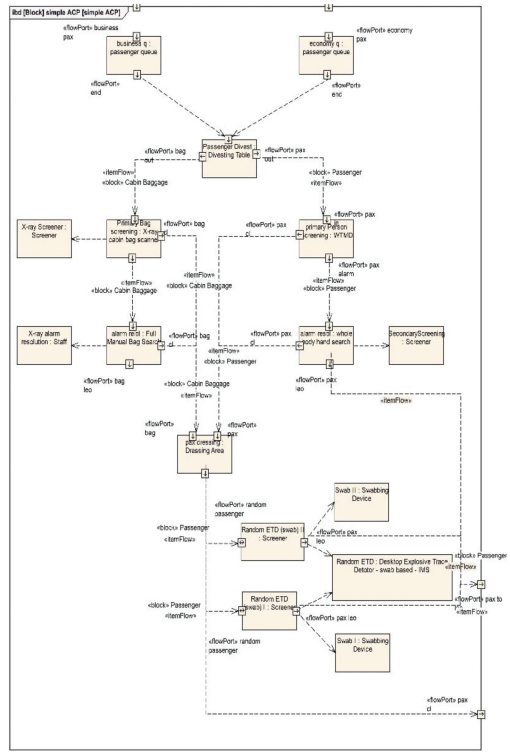


Figure 1. SysML internal block diagram of standard airport checkpoint.

is divided. The baggage goes through an X-ray machine. The X-ray machine depends on a screener as indicated with the arrow symbol used for such a relation between two blocks. After the X-ray there is either an alarm resolution or the baggage is available at the dressing area. If the alarm resolution fails, a Law Enforcement Officer (LEO) takes over and the baggage leaves the ACP not cleared.

On the other path parallel to the baggage the person is first screened with a metal detector. If necessary an alarm resolution is executed by a staff member doing a pat down. If the alarm is not resolved, the passenger leaves the ACP as not cleared and is handed over to the LEO.

Otherwise the passenger reclaims the baggage at the dressing area, where the two paths for passenger and baggage meet. Leaving the dressing area, the passenger is either chosen to be screened for explosive traces or he can move on undisturbed to the gate. The trace detection is performed by two screeners, each using a swabbing device. Together they use the actual trace detector. The passenger is either handed over to the LEO if an alarm was raised or the passenger can proceed to the gate.

The ibd shows the path of passengers and/or bags through the ACP including the junctions and joints. The flow ports indicate both the item, i.e. passenger or bag flowing through, and the status, e.g. alarm cleared.

Thinking already of evaluating the model of the ACP, it is very useful to determine all possible paths a passenger and its belonging can pass. There are blocks with more than one flow port with an outward direction. For simulation some decision logic or probability must be given, determining which flow port is passed by the flow element. In addition to that information, every block has a processing time and capacity in terms of the number of objects it accepts. With the ibd and the mentioned information, first system analysis methods and performance predictions are already supported by the system data modeled with SysML. The data can be used for running a Monte Carlo simulation with a sufficient number of passengers for computing for instance throughput. If queuing theory should be applied the problem of synchronizing the passenger and baggage flow has to be solved first. These examples show that the modelling suffices for the application of performance and security assessment methods.

4.2 *Airport checkpoint behavior modeling*

In the previous section the structure of a simple ACP was presented. Assuming that each component acts independently from the others, the internal block diagram and the description of the components and its attributes are a good basis for a simple analysis and also for running such a model.

In reality the screeners and components react on each other and alter their behavior according to the output of other checkpoint elements. This concept is even more present in so called new and innovative ACPs as discussed in projects like the IATA checkpoint of the future. The present paper does not discuss such ACP concepts with respect to operational or security aspects.

The paper aims at presenting SysML as a modeling tool to represent both structure and behavior, respectively. The structure was discussed in the previous section and in the following sub subsections an activity diagram, a state machine diagram as well as a sequence diagram are shown.

The behavior diagram not presented in this paper is the use case diagram. However this is usually used together with requirements modeling more likely in the planning phases. We focus on SysML modeling for system analysis and evaluation rather than requirements modeling.

4.2.1 *Activity diagram of a simple ACP*

In the activity diagram of the generic ACP, see Figure 2, the principle of independent screening

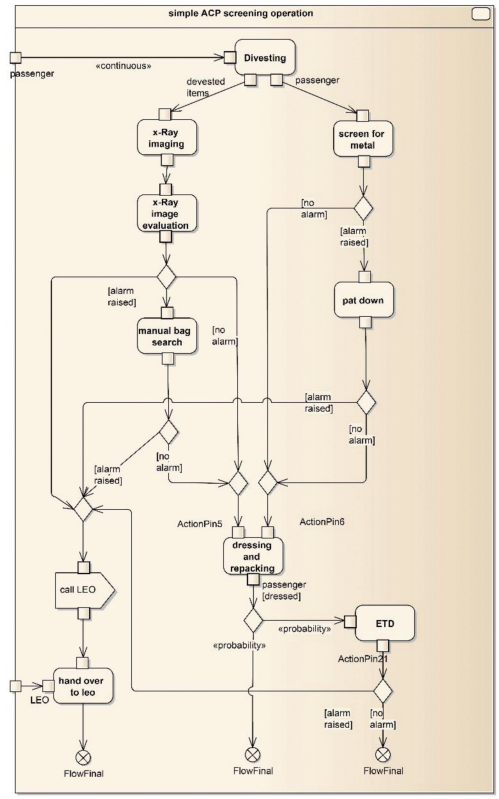


Figure 2. SysML activity diagram of standard airport checkpoint.

equipment lead to nearly no additional information compared to the internal block diagram. The structure of the activities and the connections resembles the one seen in the ibd. As already pointed out in the introduction to this section, this is the case because each component has a single purpose in the ACP and acts independent from the other subsystems in the checkpoint.

The activity diagram adds some information to the process like specifying a continuous input stream of passengers. In the internal block diagram some blocks have one input and two outputs. The flow ports there show the object passing through, however, the logic of the decision is not part of that diagram. The words “probability” or “alarm” and “no alarm” beside the diverging paths indicate the logic behind the decision.

4.2.2 *Sequence diagram for an ACP with sensor fusion on data level*

As explained along with the internal block diagram of a simple ACP lane, the current detection devices do not communicate with each other and each

system provides an independent result with respect to the operation of other components.

In the future, more complicated systems are desired to achieve a more diverse screening process, which reacts on results of other components. Also several results of different screening components are expected to be combined to find a better judgment concerning the status of a screened object, while reducing false alarms. This also allows a faster flow through the ACP as there is no alarm decision after every screening device but only if information has cumulated. If alarm resolution components are less distributed and separated from the main passenger stream, more than it is usual today, the hope is that a significant amount of passengers could go much faster through the ACP.

The sequence diagram of Figure 3 shows the function of such an ACP. The involved components are lined up at the top of the diagram. Each component has a live line attached to it. Between the live lines, arrows indicate signals sent between components. There are arrows indicating synchronized and not synchronized signals. When time advances, the arrows are attached to the life line farther towards the bottom of the diagram.

The diagram describes how the components send their screening information to a central unit. This unit requests a decision on alarm resolution from an extra component. This is the core function of an ACP with sensor fusion on data level.

Additionally, there is the necessity to recognize the passenger at each step in the screening process to make sure that the results of the screening is attached to the right person. Therefore the passenger has to register himself at the entrance of the ACP. Leaving the ACP the result of the screening process is requested and either the exit gate opens and the passenger proceeds to his gate or the passenger is led to a place where alarm resolution is performed. The sequence diagram indicates this decision with a box containing both versions of the behavior divided by a dotted line.

The use of data fusion allows another type of ACP. The function of this ACP is presented in the following sub subsection.

4.2.3 *Activity diagram of a distributed ACP*

In a (theoretical) distributed ACP people move more freely. One realization could be achieved by registration every passenger upon entering and

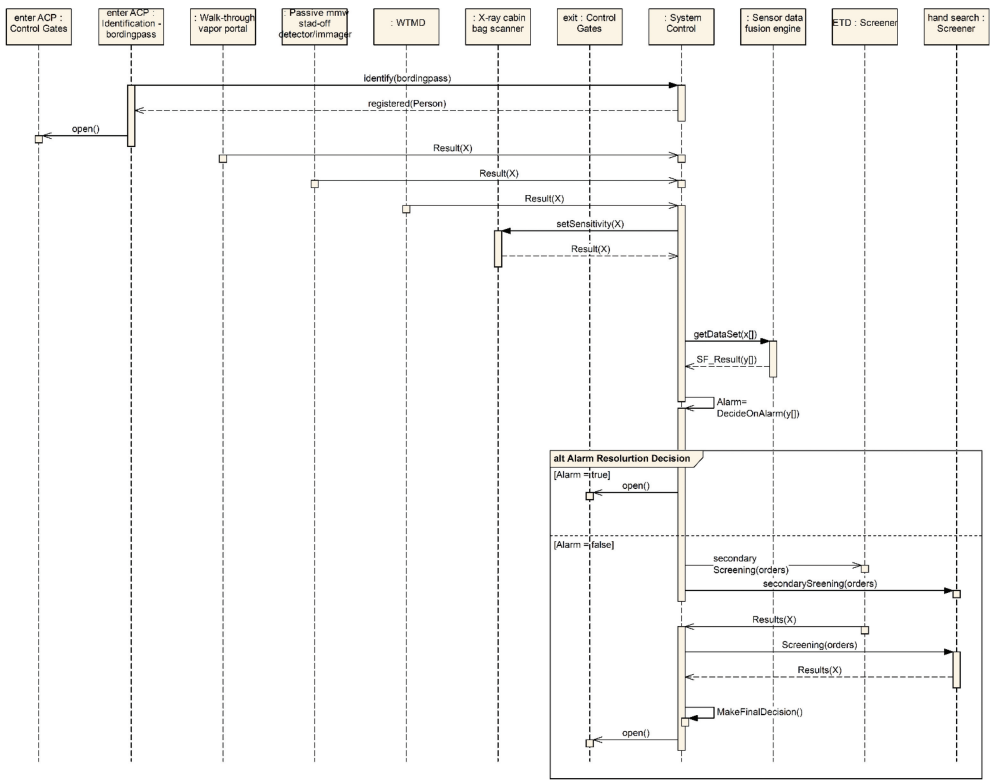


Figure 3. SysML sequence diagram of ACP with sensor fusion on data level.

exiting the *screening* area and making a final decision on alarm resolution upon request from the overall screening system. The screening area itself could be any confined space accessible to the passenger inside the airport, e.g. the check-in hall, commercial area, or passenger lounge.

The screening areas might be equipped with several stand-off detections devises used to screen the people while present in the screening area. Additionally people could be tracked (e.g. biometrically) to connect screening results with persons' identities. A centralized processing unit could merge the results and decides if a further, more thorough screening (e.g. conventional ACP screening) is necessary when leaving the screening area.

The process is modeled with a SysML activity diagram in Figure 4. In this diagram we use the Accept Event Action and Send Signal Action elements to illustrate the communication with the continuous screening part and the exit control mechanism. Parallel to the passenger proceeding to the screening area, the process of tracking and screening is started. This actions are surrounded by an interruptible activity region and are going on till the signal of a leaving passenger is received. This stops the screening and tracking and causes

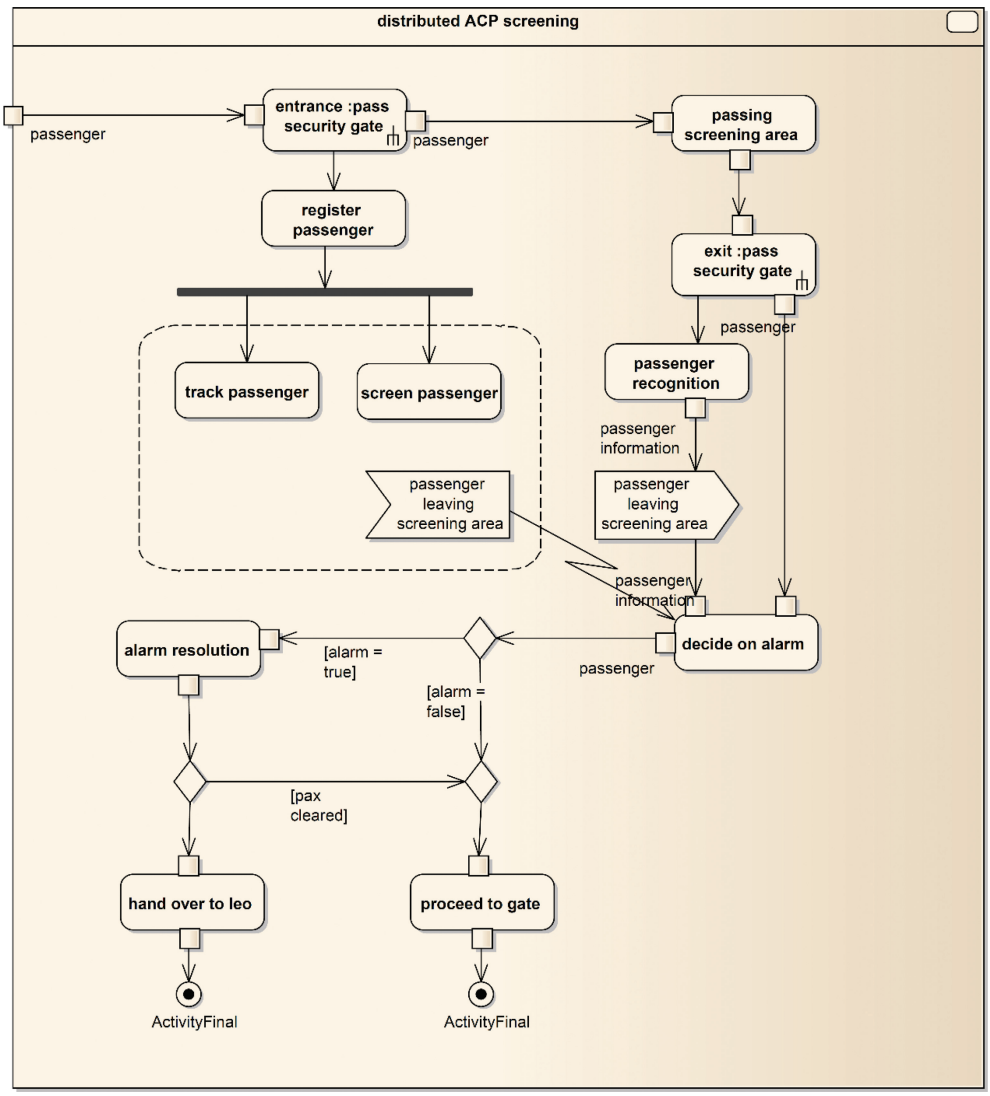


Figure 4. SysML activity diagram showing the passenger handling in a distributed ACP.

the action "decide on alarm resolution" to be executed.

Furthermore the concept of a Call Behavior Action, indicated by the little fork under the action name is used for the activity entering the control gate. This activity consists again of various actions modeled in a separate activity diagram. This is quite useful when modelling reoccurring sets of activities in a condensed way in the context of the overall process.

4.2.4 *State machine diagram to determine passengers' screening status*

One of the security concepts of an airport checkpoint is that screened people are strictly separated from people that are not yet screened. This is an obvious way to exclude the exchange of prohibited items between passengers. In a distributed ACP it is the standard situation that at any time passengers with different screening status can meet each other and also can exchange items. This problem has to be solved by using a screening area with a relative low density of persons (e.g. multiple path-like geometries) and by continuously updating the state of the passengers.

Figure 5 shows a state machine diagram of a single passenger. The state machine diagram keeps track of the state of the passenger with respect to two different screening methods and the passenger tracking while moving around in the screening area.

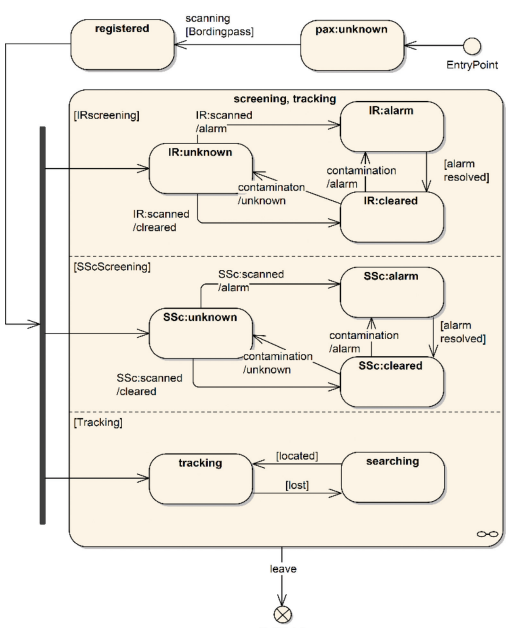


Figure 5. SysML state machine diagram for the passenger sta-tus, while being screened in a distributed ACP.

The logic displayed in the diagram is that if passengers come too close to one another, the passenger with the better screening status switches to the state of the person just met. The process of screening competes with this mechanism that people 'contaminate' each other. Every time a passenger passes by a detection device and nothing is found the passenger state improves again. So the concept of distributed checkpoint works only if people are faster cleared than they can contaminate each other. This could also mean to remove problematic passengers from the screening area.

A prerequisite to this kind of handling the passenger is that the system has to know the location of the passenger at all times. The passenger screening state switches back to unknown if the tacking system has lost the passenger for a significant amount of time.

5 CONCLUSION AND OUTLOOK

The paper gave an overview of modeling and simulation efforts in the domain of airport checkpoints and an overview of SysML modeling in domains close to the airport operation and security.

We focused on the static SysML modeling of a classical airport checkpoint and the dynamic modeling of more modern airport checkpoint designs. In particular, we showed how to model dynamic screening sensor data fusion using SysML sequence diagrams. We used SysML activity and state machine diagrams to model the behavior of a distributed airport checkpoint.

We will elsewhere give further SysML diagrams relevant for the checkpoint of the future and distributed checkpoints. We showed how information for typical current security and performance modeling approaches can be extracted from the presented SysML models. To this end, we are planning to employ the SysML models in future work.

The overall goal is that various performance areas can be assessed and optimized against each other with the help of underlying SysML models.

REFERENCES

107TH CONG. 2001. *Aviation and Transportation Security Act (Passed Congress/Enrolled Bill version)* [Online]. Available: https://www.govtrack.us/congress/bills/107/s1447/text.

AIC EUROPE 2010. An Outlook for Europe's Airports: Facing the Challenges of the 21st Century.

Arnold, A., Poin, G., Griffault, A. & Rauzy, A. 2000. The AltaRica Formalism for Describing Concurrent Systems. *Fundamenta Informaticae*, 109–124.

Bahill, A.T. & Szidarovszky, F. 2009. Comparison of dynamic system modeling methods. *Systems Engineering,* 12, 183–200.

Concho, A.L. & Ramirez-Marquez, J.E. 2012. A mathematical framework for passenger screening optimization via a multi-objective evolutionary approach. *Computers and Industrial Engineering,* 62, 839–850.

David, P., Idasiak, V. & Kratz, F. 2010. Reliability study of complex physical systems using SysML. *Reliability Engineering & System Safety,* 95, 431–450.

De barros, A.G. & Tomber, D.D. 2007. Quantitative analysis of passenger and baggage security screening at airports. *Journal of Advanced Transportation,* 41, 171–193.

Debbabi, M., Hassaïne, F., Jarraya, Y., Soeanu, A. & Alawneh, L. 2010. Systems Modeling Language. *Verification and Validation in Systems Engineering.* Springer Berlin Heidelberg.

Dori, D. 2002. *Object-Process Methodology—A Holistic Systems Paradigm,* Berlin, Heidelberg, New York, Springer-Verlag.

Durugbo, C. 2012. Integrated product-service analysis using SysML requirement diagrams. *Systems Engineering*, n/a-n/a.

EUROPEAN COMMISSION 2002. Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security. *In:* PARLAMENT, E. & UNION, R. D.E. (eds.) *2320/2002.*

EUROPEAN COMMISSION 2008. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Feiler, P., Gluch, D. & Hudak, J. 2006. The Architecture Analysis & Design Language (AADL): An Introduction. Carnegie Mellon University.

Geyer, P. 2012. Systems modelling for sustainable building design. *Advanced Engineering Informatics*.

Griffault, A. & Point, G. 2006. On the partial translation of Lustre programs into the AltaRica language and vice versa. Laboratoire Bordelais de Recherche en Informatique.

Grobshtein, Y., Perelman, V., Safra, E. & Dori, D. Systems Modeling Languages: OPM Versus SysML. International Conference on Systems Engineering and Modeling—ICSEM'07, 2007. Haifa, Israel.

Grunske, L. & Joyce, D. 2008. Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profiles. *Journal of Systems and Software,* 81, 1327–1345.

Hafizogullari, S., Bender, G. & Tunasar, C. Simulation's role in baggage screening at the airports: A case study. 2003, 1833–1837.

Hause, M., Thom, F. & Moore, A. 2005. Inside SysML. *Computing and Control Engineering,* 16, 10–15.

Holguín-Veras, J., Xu, N. & Bhat, C. 2012. An assessment of the impacts of inspection times on the airline industry's market share after September 11th. *Journal of Air Transport Management,* 23, 17–24.

Hsu, C.-I., Chao, C.-C. & Shih, K.-Y. 2012. Dynamic allocation of check-in facilities and dynamic assignment of passengers at air terminals. *Computers & Industrial Engineering,* 63, 410–417.

Jacobson, S., Kobza, J. & Easterling, A. 2001. A Detection Theoretic approach to Modeling Aviation Security Problems using the Knapsack Problem. *IIE Transactions,* 33, 747–759.

Jacobson, S.H., Mclay, L.A., Kobza, J.E. & Bowman, J.M. 2005a. Modeling and analyzing multiple station baggage screening security system performance. *Naval Research Logistics,* 52, 30–45.

Jacobson, S. H., Mclay, L.A., Virta, J.L. & Kobza, J.E. 2005b. Integer programming models for deployment of airport baggage screening security devices. *Optimization and Engineering,* 6, 339–359.

Lazar babu, V.L., Batta, R. & Lin, L. 2006. Passenger grouping under constant threat probability in an airport security system. *European Journal of Operational Research,* 168, 633–644.

Leone, K. & Liu, R. 2011. Improving airport security screening checkpoint operations in the US via paced system design. *Journal of Air Transport Management,* 17, 62–67.

Leone, K. & Liu, R.R. 2003. Measures of effectiveness for passenger-baggage security screening. *Transportation Research Record,* 1822, 40–48.

Linhares, M.V., De oliveira, R.S., Farines, J.M. & Vernadat, F. 2007. Introducing the modeling and verification process in SysML. *12th IEEE International Conference on Emerging Technologies and Factory Automation*, 344–351.

Lopes, A.J., Lezama, R. & Pineda, R. 2011. Model Based Systems Engineering for Smart Grids as Systems of Systems. *Procedia Computer Science,* 6, 441–450.

Manataki, I.E. & Zografos, K.G. 2009. A generic system dynamics based tool for airport terminal performance analysis. *Transportation Research Part C: Emerging Technologies,* 17, 428–443.

Manataki, I.E. & Zografos, K.G. 2010. Assessing airport terminal performance using a system dynamics model. *Journal of Air Transport Management,* 16, 86–93.

Mcginnis, L. & Ustun, V. 2009. A simple example of SysML-driven simulation. *Proceedings of the 2009 Winter Simulation Conference (WSC 2009)*, 1703–1710.

Mclay, L. A., Jacobson, S.H. & Kobza, J.E. 2006. A multilevel passenger screening problem for aviation security. *Naval Research Logistics (NRL),* 53, 183–197.

Mclay, L.A., Lee, A.J. & Jacobson, S.H. 2010. Risk-Based Policies for Airport Security Checkpoint Screening. *Transportation Science,* 44, 333–349.

Nelson, R. & Walker, K. 2011. International Standardization of Air Passenger and Cargo Screening. Available: http://csis.org/publication/international-standardization-air-passenger-and-cargo-screening.

Nie, X., Batta, R., Drury, C.G. & Lin, L. 2009. Passenger grouping with risk levels in an airport security system. *European Journal of Operational Research,* 194, 574–584.

Nie, X., Parab, G., Batta, R. & Lin, L. 2012. Simulation-based Selectee Lane queueing design for passenger checkpoint screening. *European Journal of Operational Research,* 219, 146–155.

Nikolaev, A.G., Jacobson, S.H. & Mclay, L.A. 2007. A sequential stochastic security system design problem for aviation security. *Transportation Science,* 41, 182–194.

Nyquist, D. C. & Mcfadden, K.L. 2008. A study of the airline boarding problem. *Journal of Air Transport Management,* 14, 197–204.

Olapiriyakul, S. & Das, S. 2007. Design and analysis of a two-stage security screening and inspection system. *Journal of Air Transport Management,* 13, 67–74.

OMG 2010. OMG Systems Modeling Language (OMG SysML™).

Park, Y. & Ahn, S. B. 2003. Optimal assignment for check-in counters based on passenger arrival behaviour at an airport. *Transportation Planning and Technology,* 26, 397–416.

Pedroza, G., Apvrille, L. & Knorreck, D. 2011. AVATAR: A SysML Environment for the Formal Verification of Safety and Security Properties. *2011 11th Annual International Conference on New Technologies of Distributed Systems (NOTERE)*, 10 pp.-10 pp.10 pp.

SAE AEROSPACE 2004. Architecture Analysis & Design Language (AADL). *SAE Aerospace*.

Sahin, H. & Feng, Q. 2009. A mathematical framework for sequential passenger and baggage screening to enhance aviation security. *Computers & Industrial Engineering,* 57, 148–155.

SCHIPHOL GROUP 2009. Anual Report. Amsterdam: Schiphol Group.

Seidenstadt, P. & Splane, F.X. 2009. *Protecting Airline Passengers in the Age of Terrorism*, Praeger Frederick A.

Soares, M.D., Vrancken, J. & Verbraeck, A. 2011. User requirements modeling and analysis of software-intensive systems. *Journal of Systems and Software,* 84, 328–339.

Soolaki, M., Mahdavi, I., Mahdavi-amiri, N., Hassanzadeh, R. & Aghajani, A. 2012. A new linear programming approach and genetic algorithm for solving airline boarding problem. *Applied Mathematical Modelling,* 36, 4060–4072.

Sweet, K.M. 2002. *Terrorism and airport security,* Lewiston, Queenston, Lampeter, The Edwin Mellen Press Ltd.

TSA 2009. Checkpoint Design Guide (CDG). Transportation Security Administration.

Van dijk, N.M. & Van der sluis, E. 2006. Check-in computation and optimization by simulation and IP in combination. *European Journal of Operational Research,* 171, 1152–1168.

Van landeghem, H. & Beuselinck, A. 2002. Reducing passenger boarding time in airplanes: A simulation based approach. *European Journal of Operational Research,* 142, 294–308.

Wang, X. & Zhuang, J. 2011. Balancing congestion and security in the presence of strategic applicants with private information. *European Journal of Operational Research,* 212, 100–111.

Weilkiens, T. 2008. Systems Engineering with SysML/UML: Modeling, Analysis, Design. Burlington: Morgan Kaufmann.

Weiss, W.E. 2008. *Dynamic Security: An Agent-Based Model for Airport Defense*.

Wilson, D., Pryor, R., So, S.A. & Roe, E.K. 2007. Security checkpoint optimizer simulation tool for passenger screening prototyping. *2007 Winter Simulation Conference*, 2384–2384.

XP-DITE PROJECT. 2013. *XP-DITE: Accelerated Checkpoint Design Integration Test and Evaluation* [Online]. Available: http://www.xp-dite.eu/ [Accessed 17.06.2014 2014].

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Achieving safe designs through evaluation of options at the conceptual level of safety system design

E. Alijagic & V.N. Dang
Paul Scherrer Institute, Villigen, Switzerland

ABSTRACT: When designing a safety system according to IEC61508/61511, after the risk/hazard analysis step that produces a set of Safety Functions (SFs), the designer is obligated to execute a number of additional steps. Some of these steps are:

– Allocating the target Safety Integrated Level (SIL) (or Risk Reduction Factor RRF) for each SF,
– Developing the Safety Requirement Specification (SRS),
– Developing safety system concept design and
– Verifying that the concept design meets the target SIL.

Given the set of SFs, the designer typically generates a number of options in the concept phase. These options are clearly constrained by the way both SFs and their RRFs are specified. This has consequences for the subsequent lifecycle's steps too. When considering protection against a single consequence of different severities by multiple SFs, it may be beneficial for generating the concept design proposals to allow for variations in the RRFs while keeping the overall risk reduction below a tolerable level. Allowing variations in the RRFs could help to achieve cost savings in the associated design proposal. These savings can then be reinvested to achieve additional tightening of the SFs within this new design option.

The aim of this paper is hence twofold: (1) to show how variations in the RRFs affect the design options, and (2) to introduce a rough cost model to discriminate between the options on cost basis. We demonstrate the method using a case study.

1 INTRODUCTION

A safety system is needed for the purpose of mitigating a risk or bringing the process to a safe state if a dangerous process failure occurs. The system provides the protection through a number of safety functions. The Risk Reduction Factor (RRF) and Probability of Failure on Demand (PFD) are the primary variables used to specify the safety robustness of such a function. These factors, once fixed, affect the designer's decisions in subsequent design steps regarding the architectural constraints (IEC61508, IEC62061, ANSI/ISAS84.01) as well as corresponding testing/maintenance procedures. Except for trivially simple safety system architectures, the factors alone are generally not sufficient to realistically address the implementation, maintenance, and testing costs for additional design options made through the lifecycle.

It is widely accepted (Sallak et al. 2007) that optimization methods are necessary to determine attributes such as redundancy and reliability parameters in order to maximize the safety.

When generating cost-effective design options (Amari 2006), the designer typically poses questions such as which vendor to choose, how to keep the overall availability of safety functions at maximum, and how to keep overall design costs at minimum. In this respect, the designer would like to have a methodology that effectively controls the costs in the early design phases. Although he follows rigid guidance from the standards' lifecycles when designing the system, there are still opportunities where decision making may have different cost impacts without jeopardizing safety.

When assessing the risk R^{EUC} for the baseline system, the designer is tasked to address each hazard category separately and systematically (IEC60812, IEC61508). Per category, he first determines the tolerable risk level R^{tol}. Then moves to identifying and quantifying the risk contributors (hazardous situations). After deciding how to provide the necessary protection by safety functions, RRF and PFD targets are allocated.

The process of RRF allocation necessitates (IEC61508) quantification of the failures in the underlying process in the first place. Subsequently, the designer continues with selection of the physical components for the safety functions.

The method proposed in this paper refers to a safety system implemented by a single layer of protection. The purpose is to give a methodology

that helps the designer with selection of RRF and PFD targets that minimize the design cost without jeopardizing the required safety level target.

It is also presumed that the redundancy of components within a safety function is:

- realized by components with same PFD meaning that the same PFD is allocated to all components within a component system.
- implemented independently. As common cause failures are major problems for high-reliability safety systems that depend on redundancy, an insufficiently independent implementation of such components can severely reduce the overall availability of the safety function. Where necessary, the redundant components are diversified to combat the system's vulnerability on common mode and common cause factors.

Given a cost profile for a component from a system, the methodology for the designing a safety function is established through the following steps:

1. Obtaining RRFs for the safety functions and transferring them to their components (S, LS, A) PFD targets,
2. Translation of the safety functions' PFD targets to the components' PFD targets,
3. Calculation of the components' redundancies that respects adopted cost profile.

The method is validated using a case study introduced in the last chapter of this paper.

2 COMPUTATIONAL FRAMEWORK

2.1 *Mathematical preliminaries*

The improvement in safety provided by the to-be–designed safety system, can be formulated as an improvement in the reliability of the safety system components. This reliability can be improved (Kuo & Wan 2007) either by incremental improvements in component reliability or by provision of redundant components in parallel. As emphasized in (Kuo et al. 2001) it then may be advantageous to preventively increase the component reliability to some level and provide redundancy at that level. Unfortunately, increasing the targets to anticipate for uncertainties in the subsequent design phases may push the designer against the limits of the technology where some components become extremely costly to manufacture and/or test. On another side, more channels clearly introduce more costs per channel but since each component in a redundant setting needs a lower RRF target allocated, the component's cost could be much lower than a single component's one to which a large RRF is imposed. Hence, depending on adopted components cost profiles, there is a room for trading-off between costs and redundancy without jeopardizing safety.

Presuming that individual risks R_i, $i = 1, ..., N$ associated to the consolidated hazardous situations are known, the overall baseline risk is simply

$$R^{EUC} = \sum_{i=1}^{N} R_i \tag{1}$$

where it is assumed that the independent and uncorrelated risk sources are obtained after the grouping. Since the risk of the unprotected system is the product of the Frequency (F) of the failures and the Loss (L) of the consequence i.e.

$$R_i = F_i L_i,\ i = 1, ..., N$$

the practitioner may choose to reduce each individual risk through the frequency or the loss.

By deciding to target the frequencies of the failures, the designer produces PFD targets for the safety functions associated to the individual risks. The risk reduction equation under consideration when reducing risks is

$$\frac{R^{EUC}}{\alpha} = \sum_{i=1}^{N} \frac{F_i L_i}{\alpha_i}, \quad \alpha := \frac{R^{EUC}}{R^{tol}}\ . \tag{2}$$

where (α_i, $i = 1, ..., N$) are the risk reduction factors related to the elemental risks. This problem does not have a unique solution and, hence optimization may help to find factors that are in some sense more preferable than others.

For example, optimization can be used to find the RRF such that

$$\frac{R^{EUC}}{\alpha} = \sum_{i=1}^{N} \frac{F_i L_i}{\alpha_i}, \quad \min_{\alpha_i} \left\{ \sum_{i=1}^{N} \alpha_i \right\}.$$

This optimization problem has the following solution

$$\alpha_i = \alpha \frac{\sqrt{F_i L_i}}{R^{EUC}} \sum_{i=1}^{N} \sqrt{R_i},\ \ i = 1, ..., N \tag{3}$$

Since the designer chooses to reduce the elemental risks by changing their frequency only, it can be easily seen that α_i, $i = 1, ..., N$ are of no use unless all losses are the same. The formula (3) fails to produce different targets for the same individual risks whose frequencies differ. Rescaling the factors from the optimization problem then may come into rescue. We reformulate the optimization problem as:

$$\frac{R^{EUC}}{\alpha}=\sum_{i=1}^{N}\frac{L_i}{\alpha_i/F_i},\quad \min_{\alpha_i}\left\{\sum_{i=1}^{N}\frac{\alpha_i}{F_i}\right\} \tag{4}$$

where, instead of R_i, $i=1, ..., N$, losses L_i, $i=1, ..., N$ are used. Then, the formula (3) becomes

$$\alpha_i=\alpha\frac{F_i\sqrt{L_i}}{R^{EUC}}\sum_{i=1}^{N}\sqrt{L_i},\quad i=1, ..., N \tag{5}$$

such that we may define:

$$PFD(SF_i)=\frac{1}{\alpha_i},\quad i=1, ..., N. \tag{6}$$

We take a short aside from the mainline to demonstrate that α_i, $i=1, ..., N$ are not necessarily equal when the individual risks are equal. For simplicity, assume the case $N=2$ and $R_1=R_2$. Then:

$$\alpha_1=\frac{\alpha}{R^{EUC}}(R_1+F_1\sqrt{L_1L_2}),$$

$$\alpha_2=\frac{\alpha}{R^{EUC}}(R_2+F_2\sqrt{L_1L_2}).$$

The calculated factors demonstrate that, under condition $R_1=R_2$, it follows that $\alpha_1=\alpha_2$ if and only if $F_1=F_2$. Also, by comparing these RRFs one concludes that $F_1>F_2$ implies $\alpha_1>\alpha_2$. Or, when translated to the PFD terms, $F_1>F_2$ implies $PFD(SF_1)<PFD(SF_2)$.

The objective function from the latter optimization problem then becomes:

$$\frac{R^{EUC}}{\alpha}=\sum_{i=1}^{N}F_iL_iPFD(SF_i).$$

Since each safety function is implemented by sensor, logic solver and actuator components, the designer must allocate PFD targets to them as well. These PFD are related via the so-called inclusion—exclusion formula

$$PFD(SF_i)=PFD(S_i)+PFD(LS_i)+PFD(A_i),\quad i=1, ..., N \tag{7}$$

where the terms associated to the cut-sets of the components' failure spaces are excluded as postulated in the introduction.

When allocating the PFD targets to the components the designer should also be concerned about the design costs. Each component has its own cost profile that depends on its PFD. It could then be beneficial to choose a design option that minimizes the costs without affecting required safety targets.

The search for a more cost-effective design for a set of safety functions can be formulated as an optimization task. That is, the PFD targets as well as the components' redundancies can be obtained by solving a multi-optimization task:

$$\frac{R^{EUC}}{\alpha}=\sum_{i=1}^{N}F_iL_i\left\{PFD(S_i)+PFD(LS_i)+PFD(A_i)\right\},$$

$$\min_{\substack{PFD(S_i)\\+PFD(LS_i)\\+PFD(A_i)}}\left\{\sum_{i=1}^{N}\frac{1}{F_i\left\{\begin{array}{l}PFD(S_i)\\+PFD(LS_i)\\+PFD(A_i)\end{array}\right\}}\right\},$$

$$\min_{\substack{PFD(S_i),\\PFD(LS_i),\\PFD(A_i),\\N_{S_i},N_{LS_i},N_{A_i}}}\left\{\begin{array}{l}\displaystyle\sum_{i=1}^{N}N_{S_i}C_{S_i}\left(\frac{1}{\sqrt[N_{S_i}]{PFD(S_i)}}\right)\\ \quad+N_{LS_i}C_{LS_i}\left(\frac{1}{\sqrt[N_{LS_i}]{PFD(LS_i)}}\right)\\ \quad+N_{A_i}C_{A_i}\left(\frac{1}{\sqrt[N_{A_i}]{PFD(A_i)}}\right)\end{array}\right\} \tag{8}$$

where parameters $C_{S_i}, C_{LS_i}, C_{A_i}, i=1, ..., N$ are uniformly increasing component cost functions on the RRF factors associated to sensors, logic solvers, actuators from SF_i, $i=1, ..., N$ and $N_{S_i}, N_{LS_i}, N_{A_i}$, $i=1, ..., N$ are the redundancies of the components.

Obviously, the solution of problem (8) depends on the choice of the component cost functions. Typical cases assume exponential cost functions. Such an assumption makes obtaining closed forms for the parameters difficult due to the transcendent functional dependencies between the variables. For this reason the designer is forced to look for other possibly suboptimal but more practical methods.

One should notice that the candidates for the components' PFD targets from the objective function are related exclusively to a single component. Hence multiplicity of components plays no role when determining the PFD targets for safety functions. This observation makes possible to split the optimization (8) into two subsequent optimizations:

$$\frac{R^{EUC}}{\alpha}=\sum_{i=1}^{N}F_iL_iPFD(SF_i),$$

$$\min_{PFD(SF_i)}\left\{\sum_{i=1}^{N}\frac{1}{F_iPFD(SF_i)}\right\},$$

and then to find PFD for the components and their redundancies such that the cost

$$\sum_{i=1}^{N} N_{S_i} C_{S_i}\left(\frac{1}{\sqrt[N_{S_i}]{PFD(S_i)}}\right) + N_{LS_i} C_{LS_i}\left(\frac{1}{\sqrt[N_{LS_i}]{PFD(LS_i)}}\right) + N_{A_i} C_{A_i}\left(\frac{1}{\sqrt[N_{A_i}]{PFD(A_i)}}\right) \tag{9}$$

of the overall design is minimized. To obtain a suboptimal solution to the second minimization we adopt the following assumption which is a frequently used 'rule-of-thumb':

(AS) More expensive components get larger PFDs

By allowing assumption **(AS)**, one may take

$$\begin{aligned} PFD(S_i) &:= k_{S_i} PFD(SF_i), \\ PFD(LS_i) &:= k_{LS_i} PFD(SF_i), \\ PFD(A_i) &:= k_{A_i} PFD(SF_i) \end{aligned} \tag{10}$$

where the factors k_{S_i}, k_{LS_i} and k_{A_i} are defined as:

$$k_{S_i} := \frac{C_{S_i}\left(\frac{1}{PFD(SF_i)}\right)}{C_{SF_i}\left(\frac{1}{PFD(SF_i)}\right)}, \quad k_{LS_i} := \frac{C_{LS_i}\left(\frac{1}{PFD(SF_i)}\right)}{C_{SF_i}\left(\frac{1}{PFD(SF_i)}\right)},$$

$$k_{A_i} := \frac{C_{A_i}\left(\frac{1}{PFD(SF_i)}\right)}{C_{SF_i}\left(\frac{1}{PFD(SF_i)}\right)}$$

and

$$C_{SF_i}\left(\frac{1}{PFD(SF_i)}\right): = C_{S_i}\left(\frac{1}{PFD(SF_i)}\right) + C_{LS_i}\left(\frac{1}{PFD(SF_i)}\right) + C_{A_i}\left(\frac{1}{PFD(SF_i)}\right), \quad i = 1, \ldots, N.$$

Straightforward substitution of these PFDs into (7) shows that they are admissible candidates as, by construction

$$k_{S_i} + k_{LS_i} + k_{A_i} = 1, \quad i = 1, \ldots, N.$$

Since the design targets are now created for the components from each safety function, minimization of cost functional (9) now reduces to minimizations per each component. That is, the required minimal redundancies follow from:

$$\begin{aligned} &\min_{N_{S_i}}\left\{N_{S_i} C_{S_i}\left(\frac{1}{\sqrt[N_{S_i}]{k_{S_i} PFD(SF_i)}}\right)\right\}, \\ &\min_{N_{LS_i}}\left\{N_{LS_i} C_{LS_i}\left(\frac{1}{\sqrt[N_{LS_i}]{k_{LS_i} PFD(SF_i)}}\right)\right\}, \\ &\min_{N_{A_i}}\left\{N_{A_i} C_{A_i}\left(\frac{1}{\sqrt[N_{A_i}]{k_{A_i} PFD(SF_i)}}\right)\right\}, \\ &i = 1, \ldots, N. \end{aligned} \tag{11}$$

Further cost reductions are usually made in the post optimization step of the design where it is decided what to share among the actual components. Generally, a single logic solver is shared amongst the safety functions. Sharing sensors or actuators is strongly problem-dependent and depends on the choice taken for safety functions.

2.2 *Sensitivity of the components PFDs on changes in $PFD(SF_i)$ around the given initial $PFD(SF_i)$*

When attempting to gain additional costs savings, the operator typically decides to slightly change the PFD targets for safety functions. By varying these targets he hopes to come out with a less costly design. We show that, in fact, this will not introduce additional cost savings under Assumption **(AS)**. To demonstrate this, it is sufficient to take any PFD from (10) and evaluate its relative sensitivity to changes in $PFD(SF_i)$ around the initial $PFD(SF_i)$. We perform this on RRF terms α_i and obtain:

$$\frac{\partial k_{S_i}}{\partial PFD(SF_i)} \times \frac{k_{S_i}}{PFD(SF_i)} = \frac{\partial\left(\frac{C_{SF_i}(\alpha_i)}{C_{S_i}(\alpha_i)} - 1\right)^{-1}}{\partial \alpha_i} \times \frac{C_{S_i}(\alpha_i)\left(C_{SF_i}(\alpha_i) - C_{S_i}(\alpha_i)\right)^2}{\alpha_i\left(C_{SF_i}(\alpha_i)\right)^3}$$

where the first term is infinitesimally small since it is a derivation of a slowly varying function at initial α_i and the second term is bounded. Hence,

$$\frac{\partial PFD(S_i)}{\partial PFD(SF_i)} \times \frac{PFD(S_i)}{PFD(SF_i)} \approx 1.$$

Therefore we state the following conclusion that requires further elaboration:

(C) Factors k_{S_i}, k_{LS_i} and k_{A_i} can be regarded as constants around the initial $PFD(SF_i)$. Hence, $PFD(S_i)$, $PFD(LS_i)$ and $PFD(A_i)$ are approximately linear functions of $PFD(SF_i)$.

Conclusion **(C)** is true if the adopted components' cost models are all continuous functions on the range of variations around the initial $PFD(SF_i)$ for all components from the safety function. Consequently, **(C)** is always true when the cost models accommodate the continuous cost profiles. Typically, the component price within more realistic cost profiles changes in jumps as the component's performance changes. The locations of the jumps may differ among components as well. As a result, deciding to significantly increase the initial PFD of one of the safety functions causing abrupt cost reductions for other components is compensated with a decrease in the initial PFD for the other safety functions. When a discrete cost profile is shared amongst the components of the same type (a very good approximation used in process industry), then this decrease leads to a disproportionate increase of the component costs for the other safety functions that ultimately outweighs the cost savings realized for the first safety function. Obviously, conclusion **(C)** is not necessarily true when all components accommodate different cost profiles.

Accordingly, the designer's attempt to increase the PFD of some safety functions and decrease those of the others can not lead to lower costs then those associated to the initial $PFD(SF_i)$ calculated by (5) and (6) unless all components accommodate different cost profiles. This is due to the adopted cost functional from (4) that gives minimal RRF factors optimally adjusted to the risk frequencies of the individual risks.

We close this chapter by introducing a generic component cost model used in the examples throughout the rest of this paper.

2.3 *Component costs model and the cost of redundant implementation*

A cost model; $C_x(\alpha)$, depending on a risk reduction factor α for a (generic) component $x \in \{S, LS, A\}$ is introduced according to the following specification:

– When no risk reduction is required then $\alpha = 1$ and $C_x(\alpha = 1) = 0$.
– For a small α (but larger than 1) there will be some initial component cost; $C_x(\alpha = 1+) = C_x^{start}$
– When the redundancy of a component is fixed, then an increase in α always implies an increase in $C_x(\alpha)$.

This specification for the cost function describes typical situations that occur in practice. Although it is generally accepted (Rao et al. 1999) in most research that a component's cost function follows an exponential closed model, we adopt a more realistic, rough model that features piecewise constant cost functions over the RRF's intervals.

On the top of Figure 1 the dependency of a cost on RRF factor is shown for the following specification

$$C_x(\alpha) = \left\{ \begin{array}{c} 200,\ 1 < \alpha \le 80, \\ 350,\ 80 < \alpha \le 150, \\ 500,\ 150 < \alpha \le 1200, \\ 5000,\ 1200 < \alpha \le 10000, \\ 15000,\ 10000 < \alpha \end{array} \right\}. \tag{12}$$

Such cost profiles are typical in practice, where the price of a product is kept constant for a large range of selected performance.

When the protection is redundantly implemented with N_x identical components, then $N_x\sqrt{\alpha}$ is the minimal required robustness for each component in the redundant setting to guarantee the same level of safety.

Thereby:

$$C_{x,N} := N_x C_x\left(\sqrt[N_x]{\alpha}\right) \tag{13}$$

is the cost of this redundant configuration. On the bottom of Figure 1, cost (13) of redundant setting is shown on basis of cost model (12).

It is worth of mentioning that $C_{x,N}$ does not necessarily have a global minimum. This is due to

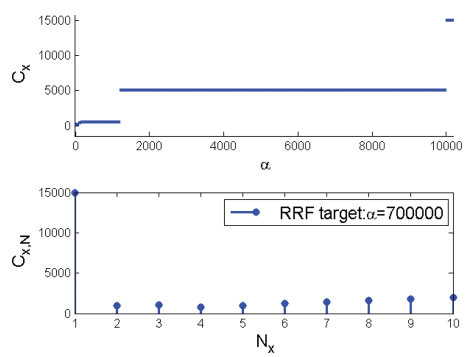


Figure 1. A component cost function (top) and the costs of its redundant setting (bottom) for RRF target set to 700000.

discontinuities in the cost function where, for some target RRFs, successively calculating roots causes the discrete jumps into other RRF regions that may be much more cost beneficial even for a larger number of components. No matter what cost function is given, for sufficiently large redundancy, the component cost will start to increase. It is therefore important to consider a sufficiently large range of N_x before concluding which value leads to a minimal component costs. To determine a sufficiently large search space for such N_x, it suffices to take N such that $\sqrt[N]{\alpha}$ belongs to the first cost level of the cost function. Any further increase of N leads to uniform cost increase since $\sqrt[N]{\alpha}$ can not escape the first cost level.

In the case of cost function $C_x(\alpha)$, the minimum costs for the target α=700000 are achieved for $N_x = 4$ with the resulting cost $C_{x,N=4} = 800$.

3 METHODOLOGY STEPS APPLIED ON A CASE

3.1 *Description of the case*

In this case we presume that three safety functions are needed to provide the risk reduction from $R^{EUC} = 9502000$ of the base-line system to the tolerable risk level $R^{tol} = 13.5743$. The RRF factor that corresponds to this reduction is $\alpha = 700000$. The individual risk levels and their associated frequencies are assumed as in Table 1.

Generally, the component cost profiles differ for each component. We restrict ourselves to the cases where each component group have approximately the same costs for their required performance level. This assumption somewhat simplifies the problem but does not narrow the scope of application.

We adopt the following cost profiles for each component:

– Sensor;

$$C_S(\alpha) = C_x(\alpha), \tag{14}$$

– Logic solver;

$$C_{LS}(\alpha) = \begin{cases} 100, 1 < \alpha \le 10 \\ 5000, 10 < \alpha \le 1000 \\ 50000, 1000 < \alpha \le 10000 \\ 70000, 10000 < \alpha \le 100000 \\ 100000, 100000 < \alpha \end{cases} \tag{15}$$

Table 1. The individual risk data assumed for the case.

R1, F1	R2, F2	R3, F3
500000, 30000	2000, 40000	9000000, 100000

– Actuator;

$$C_A(\alpha) = \begin{cases} 1000, 1 < \alpha \le 500, \\ 3500, 500 < \alpha \le 1500, \\ 25000, 1500 < \alpha \le 30000, \\ 30000, 30000 < \alpha \end{cases}. \tag{16}$$

3.2 *Step 1: obtaining PDF(SF_i), i = 1,2,3 targets for the safety functions*

A set of $PDF(SF_i)$, $i = 1,2,3$ for the set of the safety functions is obtained using formulae (5) and (6). We then, use

$$PDF(SF_i) = \left[\alpha \frac{F_i \sqrt{R_i / F_i}}{R^{EUC}} \sum_{i=1}^{N} \sqrt{R_i / F_i} \right]^{-1}, \quad i = 1,2,3 \tag{17}$$

and substitute the risk data introduced earlier. This calculations produce the targets found in Table 2.

3.3 *Step 2: translation of the safety function PFD target to the components' PFD targets*

The designer now proceeds with a determination of the PFD targets for the components from each safety function. As before, let $C_{S_i}(\alpha_i), C_{LS_i}(\alpha_i), C_{A_i}(\alpha_i)$ be the costs associated with the components from safety function SF_i to which RRF target $\alpha_i = \{PFD(SF_i)\}^{-1}$ is imposed.

The designer now uses (10) to calculate PFD targets for each component group. These targets are provided in Table 3.

These component PFD targets are then used to obtain minimal redundancies for each component from three safety functions.

Table 2. PFD targets for the three safety functions.

PFD(SF1)	PFD(SF2)	PFD(SF2)
8.0355E-06	1.1003E-04	1.0374E-06

Table 3. The PFD targets for each component group.

	PFD(SF1)	PFD(SF2)	PFD(SF3)
Sensors	8.3126E-07	6.8769E-06	1.0732E-07
Logic solvers	5.5418E-06	6.8769E-05	7.1544E-07
Actuators	1.6625E-06	3.4385E-05	2.1463E-07

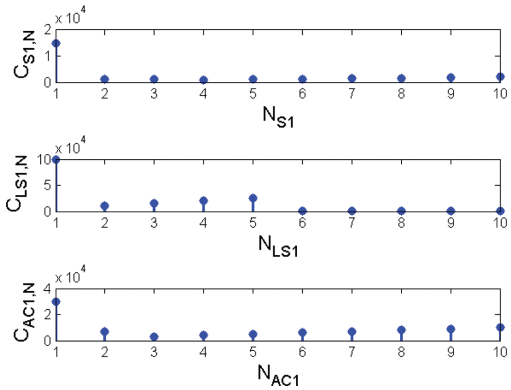


Figure 2. Minimal redundancies that determine the architecture for the first safety function.

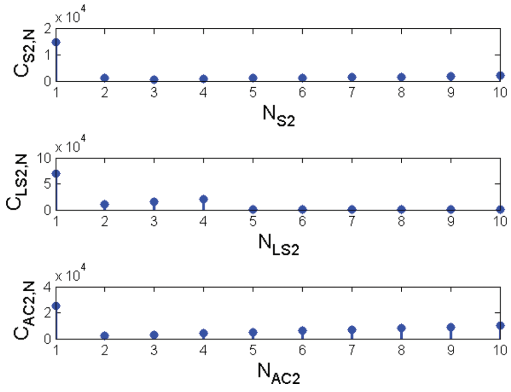


Figure 3. Minimal redundancies that determine the architecture for the second safety function.

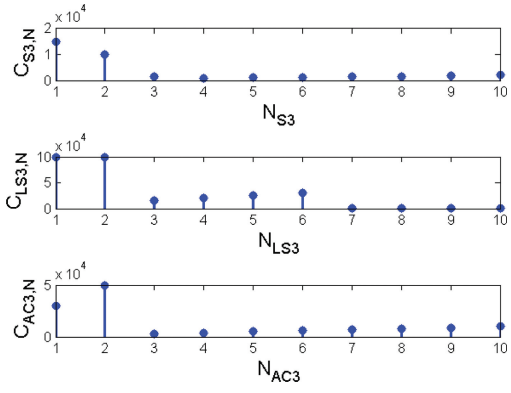


Figure 4. Minimal redundancies that determine the architecture for the third safety function.

3.4 *Step 3: calculation of the component redundancy that respects adopted component cost profiles*

We proceed with evaluation of minimal redundancies for each component group. By plotting the costs along with redundancy, one can determine which architecture has minimal costs.

Finally, component subsystem costs are listed in Table 4 along with the component redundancies within the subsystem. For the given data targets it follows that the design costs equal 12000.

The cost optimal architecture of the safety functions is shown in Figures 5, 6 and 7.

As the part of the post optimization procedure conducted on the current case to obtain additional

Table 4. The costs of the design. The costs represent the lumped investment costs per component subsystem (redundancies counted).

	Design costs		
	SF1	SF2	SF3
Sensors/red.	800/4	600/3	800/4
Logic solvers/red.	600/6	500/5	700/7
Actuators/red.	3000/3	2000/2	3000/3
	Total: 12000		

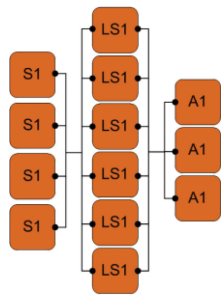


Figure 5. Cost optimal architecture for the first safety function.

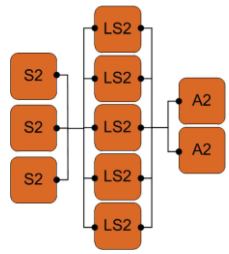


Figure 6. Cost optimal architecture for the second safety function.

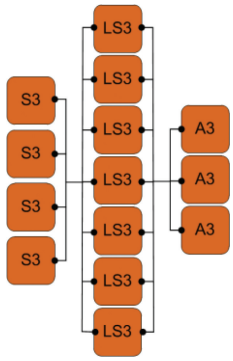


Figure 7. Cost optimal architecture for the third safety function.

cost savings, the designer typically decides to share the logic solvers among the safety functions. This requires an additional robustness increase for the logic solvers to adequately combat the risk of multiple safety functions failure due to a single point of failure. This topic, however is beyond the scope of this paper.

4 CONCLUSIONS

Despite the rigid requirements imposed by the safety standards, the safety system designer still possesses some flexibility when selecting components for the safety functions as well as their PFDs. When in the process of generating and implementing design proposals, the budget limitations play a considerable role in component selection. In this respect however, the safety standard offers no guidance. When no proper measure for the effort is given, the designer is likely to strive to deliver the safe system against high costs. It was our intention to provide a methodology for a PFD allocation for safety functions and their components that can be used in conjunction with the standard's imperatives to produce a design proposal that respects the budget costs without jeopardizing safety.

In this paper we provide the designer with a three-step workflow on how to allocate PDFs to safety functions' components that respects the components' costs profiles in order to obtain a more cost-effective design. In the first step, we show how to avoid taking disproportionate decisions when allocating PFDs to the safety functions. In the second step, using the components' cost profiles we show how to translate the SFs' PFD targets to their respective component subsystems. The third step is concerned about finding cost-optimal redundancy for a component subsystems.

The cornerstone for this method is provided by the initial RRF/PFD allocation procedure used to correct the designer's decisions by obtaining a safe design with minimal performance requirements for the safety functions. By showing that components' PFD targets are weakly sensitive on changes in the PFD of their safety function around the initial PFD targets when Assumption **(AS)** is adopted, the designer's efforts to vary the initial PFDs for safety functions become obsolete. In other words, the initial PFD as obtained by (17) guarantee the minimal design costs.

The reach of the methodology is limited to the safety systems:

1. whose safety functions are independently implemented and
2. use single layer of protection to provide the required risk reduction.

A natural extension of the methodology should address the cost-optimal designer's decision making in case of multiple layers of protection as well as safety systems whose safety functions share components.

REFERENCES

Amari S. 2006. *Optimal Systems*, A chapter from *Springer Book of Engineering Statistics*, pp. 1039–1064, Springer-Verlag Berlin Heidelberg.

ANSI/ISAS84.01 1996. *Application of Safety Instrumented Systems for the process control industry,* Instrumentation Society of America (ISA), Durham US.

IEC60812 2006. *Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA),* 2nd Ed., International Electrotechnical Commission IEC, Geneva.

IEC61508 2010. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES),* 2nd Ed., International Electrotechnical Commission IEC, Geneva.

IEC62061 2005. *Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems,* 1st Ed. International Electrotechnical Commission IEC, Geneva.

ISO13849-2 2012. *Safety of machinery—Safety-related parts of control systems—Part 2: Validation,* International Organization for Standardization, Geneva.

Kuo W. & Wan R. 2007. *Recent Advances in Optimal Reliability Allocation*, Computational Intelligence in Reliability Engineering (SCI) 39, pp. 1–36, Springer-Verlag Berlin Heidelberg.

Kuo W., Prasad V.R., Tillman F.A. and Hwang C.L. 2001. *Optimal Reliability Design: Fundamentals and Applications*, Cambridge University Press, Cambridge.

Rao S.V. M, Dawande M. and Rajgopal J. 1999. *Optimal Reliability Allocation with Discrete Cost-Reliability Data for Components*, Journal of Operations Research, Volume 47, Issue 6, pp. 899–906, Catonsville.

Sallak M., Simon C. and Aubry J.–F. 2007. *Optimal Design of Safety Instrumented Systems—A Graph Reliability Approach*, Proceedings of 7ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita, Tanger, Maroc.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Conventional correlation factors in the safety analysis of stochastic systems

O. Lukoševičienė
Institute of Mechanical Science, Vilnius Gediminas Technical University, Vilnius, Lithuania

A. Kudzys
Member of Science of Lithuanian Academy, Lithuania

ABSTRACT: The implantation of simple engineering techniques in time-dependent survival probability predictions of structural and technical systems as stochastic systems of events is discussed. A possibility to avoid complicated multidimensional integrations in a probabilistic safety analysis of stochastic systems with perfectly ductile components is based on the approaches of Transformed Conditional Probabilities (TCP) and Conventional Correlation Vectors (CCV). Dynamic (time-dependent) autosystems of extreme events of particular single and mixed ductile elements are treated as correlated components of static stochastic systems with m random failure modes. The unsophisticated and fairly exact prediction of the probability-based reliability of stochastic systems of events is demonstrated by numerical examples and histograms of their reliability indices.

1 INTRODUCTION

The reliability of structural and technical systems should always be defined for some reference period. The failure of a series system (Fig. 1, a) is caused by the first brittle component fracture. Therefore, a series system with m elements is in failure state whenever any of its elements has failed. When components of this system are ductile, it can continue to operate at reduced reliability indices of components.

A parallel system (Fig. 1, b) consisting of perfectly ductile elements can fail only when all of its contributory units have reached their limit states. Therefore, the reliability of parallel systems can be increased significantly. It can be said that the strongest component m of a parallel ductile system must survive all extreme situations (Dey and Mahadevan, 2000). Components of multi-states series-parallel systems are composed of fixed numbers m_1 of individual elements and m_2 of parallel subsystems formed from ductile elements (Fig. 1, c).

For static series and parallel structural and technical systems as systems of events, the safety or failure regions are conditioned, respectively, by unions and intersections of survival or failure probabilities of ductile components the number of which m depends on a number of random discrete failure modes. Thus, the dynamic (time-dependent) probability-based reliability indices β_k of stochastic systems may be obtained by the complicated failure modelling of their stochastically dependent elements and subsystems.

Therefore, the exact probabilistic analysis of multidimensional integrals of traditional dynamic stochastic systems of events is very difficult and sometimes not feasible. Therefore, the computer programs adopting the bi-model bounds for system reliability were proposed (Estes and Frangopol 1998).

The total failure probabilities of parallel and series systems as the intersections and unions of these probabilities in m modes may be expressed, respectively, as:

$$P\left(\bigcup_{k=1}^{m} F_k\right)_{ss} = P\left[\bigcup_{k=1}^{m}\left(X_k \le -\beta_k\right)\right]_{ss} \approx 1-\Phi_m\left(-c,\rho\right) \quad (1)$$

$$P\left(\bigcap_{k=1}^{m} F_k\right)_{ps} = P\left[\bigcap_{k=1}^{m}\left(X_k \le \beta_k\right)\right]_{ps} \approx \Phi_m\left(c,\rho\right) \quad (2)$$

where X_k (k = 1, 2, …, m) and β_k are the jointly normal random variable and reliability index for k-th element of systems, $\boldsymbol{\rho}$ is a correlation matrix. The computation of system probability of failure by Eqs. (1) and (2) involves the integration of multivariate normal distributions.

Improved computational methods for probabilistic analysis of systems were proposed by Mori &

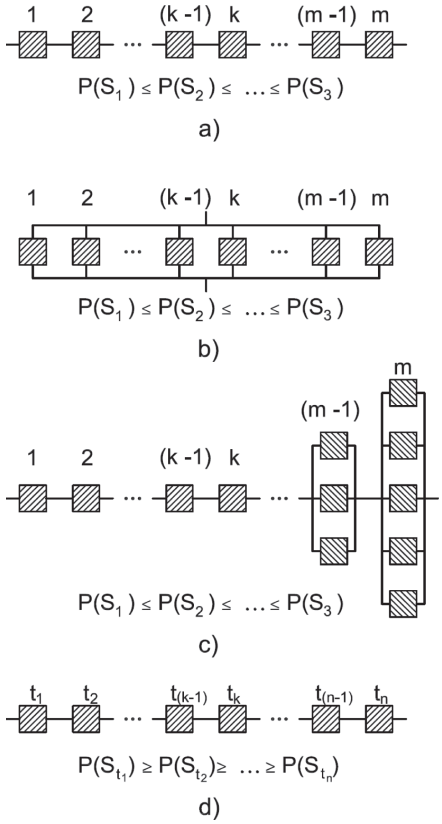


Figure 1. Schematic representations of static stochastic series (a), parallel (b) and series-parallel (c) general systems of events and dynamic autosystems (d).

Ellingwood (1993), Melchers (1994), Ditlevsen (1997), Mori & Kato (2003), Ahammed & Melcher (2005). These improvements are inconvenient for designers due to their mathematical complexity.

According to Pandey (1998 a, b), An & Pandey (2002), Pandey & Sarkar (2002) and Yuan & Pandey (2006), this computation can be simplified, when the multidimensional joint normal distribution is represented as a product of m conditional probabilities approximating by one-dimensional normal distribution. According to this method of the Product of Conditional Marginal (PCM), Eqs. (1) and (2) may be rewritten as:

$$P\left(\bigcup_{k=1}^{m} F_k\right)_{ss} \approx 1-\prod_{k=1}^{m}\Phi\left(c_{k|(k-1)}\right) \tag{3}$$

$$P\left(\bigcap_{k=1}^{m} F_k\right)_{ps} \approx \prod_{k=1}^{m}\Phi\left(c_{k|(k-1)}\right) \tag{4}$$

where $c_{k|(k-1)}$ represents a conditional normal fractile obtained by assuming that the conditional variable $X_{k|(k-1)} = X_k \left| \bigcap_{i=1}^{(k-1)} X_i \le c_i \right.$ is normally distributed. Thus, the Product of Conditional Marginal (PCM) method may be treated as a simplified computational method.

The probabilistic reliability systems of events are analysed by Žiba (2000). The analysis is based on the concepts of entropy as defined in information theory and applied to probability theory. The recommended approach allows concentrating the system analysis only on important failure modes and connects uncertainty, redundancy and robustness of systems of events. Despite this approach, the system analysis leads to complicated computations.

Kang *et al.* (2003) suggested the calculation of failure probabilities of complicated parallel and series systems, including a reliability analysis of offshore platforms, to base on the concept of Equivalent Linear Failure Modes (ELFM).

Levitin *et al.* (1998) and Levitin (2004) extends the Universal Generating Function (UGF) technique of the multistate system analysis to the format when the performance distributions of some elements depend on the states of other elements. This useful new heuristic methodology may be used by researchers and some designers.

The probability $P\left(R_S \ge E_l\right)$ means that total system capacity R_S is higher than extreme demand levels E_l. Thus, according to Ramirez-Marquez *et al.* (2004), the heuristic genetic algorithm and methodology of UGF for Multistate Series–Parallel Systems (MSPS) may be approximated and developed.

According to Li *et al.* (2007), it is possible to transform a computation of reliability parameters, using the joint probability density functions of safety margins of system components.

Song & Kang (2009), Kang & Song (2010) suggest to compute the failure probabilities of system of events by simplified matrix procedures, using the Matrix-based System Reliability (MSR) method. However, the presented analysis of large systems with different reliability and dependency of components is difficult. MSR, like the above-mentioned PCM, UGF and other methods, are hardly translated into everyday design reality and cannot be treated as universal design approximations.

According to available data of demonstrated methods, the exact and approximated reliability analysis of systems with correlated components requires multivariate integrations procedures and therefore is very difficult and sophisticated. The main task of this paper is to present for designers new unsophisticated concepts and uniform methodological analytical formats on probability-based

approaches for reliability predictions of structural and technical systems as systems of events.

2 SAFETY OF PERFECTLY DUCTILE SYSTEMS

2.1 *Ductile autosystems as components of general systems*

In the probability-based analysis of structural and technical systems, the simplified but exact applied predictions of dynamic reliability indices of particular elements are very relevant. An autosystem consisting of normal or oblique sections, connections and deflections as a dynamic (time-dependent) highly correlated decreasing series stochastic system (Fig. 1, d) belongs to a single element of a system of events and characterizes its changes in random durability (the ability to preserve its efficiency for a long period of time). Now, the values of deterministic parameters of a durability of elements due to their deteriorating and ageing are assessed and presented at design codes or standards by deterministic implicit recommendations and related with long-term experience of designers.

Any autosystem is a highly correlated series system of particular elements and their durability parameters are related to reliability indices. However, the values of safety and durability indices may be objectively defined only by fully probability-based concepts and models because probabilistic approaches allow us explicitly predict uncertainties of analysis parameters and design models.

The safety margin of time-dependent hierarchical stochastic performance processes of particular perfectly ductile elements (Fig. 1, d) may be expressed as:

$$Z_{tk} = g\left(\mathbf{X}_{tk}, \boldsymbol{\theta}\right) = g\left(\theta_R R_{tk} - \boldsymbol{\theta}_E \mathbf{E}_{tk}\right) \tag{5}$$

where $\mathbf{X}_{tk}$ and $\boldsymbol{\theta}$ are the vectors of basic and additional variables representing respectively random resistances R_{tk} (responses) and action effects $\mathbf{E}_{tk}$ (demands) of particular elements effected by extreme actions and design model uncertainties at cut t_k of finite decreasing sequence of survival probabilities $\mathrm{P}(S_{t1}) \geq \mathrm{P}(S_{t2}) \geq \ldots \geq \mathrm{P}(S_{tk}) \geq \ldots \geq \mathrm{P}(S_{tn})$. Thus, in an autosystem analysis, several dynamic safety margins are included. The vector $\mathbf{E}_{tk}$ depends also on redistributions of actions.

2.2 *Instantaneous and total survival probabilities of dynamic ductile autosystems*

According to the concept of Transformed Conditional Probabilities (TCP) (Kudzys *et al.* 2009, 2010, 2013), the instantaneous failure probability of a stochastic ductile autosystem at time t_k, assuming that analyzed element was safe at time less than t_k, may be written as follows:

$$P\left[Z_{tk} \leq 0\right] = P\left[F_{tk} \left| \bigcap_{ti=t1}^{t(k-1)} S_{ti} \right.\right] \approx 1 - P\left(S_{tk}\right) \times \left(1 + \rho_{k|f}^{x_k} \left[\frac{1}{P\left(S_{tk}\right)} - 1\right]\right) \tag{6}$$

where F_{tk} and S_{tk} denote the failure and survival probabilities of single particular elements at time t_k;

$$\rho_{k|f}^{x_k} = \left(\frac{1}{k-1}\sum_{i=1}^{(k-1)} \rho_{ki}\right)^{x_k} \tag{7}$$

is the bounded conventional correlation factor of a quadratic matrix between safety margins of autosystem elements as a member of conventional Correlation Vector (CCV) written in the form:

$$\boldsymbol{\rho} = \left[1, \rho_{2|1}^{x_2}, \ldots, \rho_{k|1\ldots(k-1)}^{x_k}\right] \tag{8}$$

when the vector $\boldsymbol{\rho} = 0$ or $\boldsymbol{\rho} = 1$, the proposed Eqs. (12), (14) and (15) give accurate solution.

Basic correlation coefficients between system elements may be calculated by the equation:

$$\rho_{ki} = \rho\left(Z_{tk}, Z_{ti}\right) = \frac{Cov\left(Z_{tk}, Z_{ti}\right)}{\boldsymbol{\sigma} Z_{tk} \times \boldsymbol{\sigma} Z_{ti}} \tag{9}$$

where σZ_{tk} and σZ_{ti} are the standard deviations of safety margins Z_{tk} and Z_{ti} calculated by Eq. (5). Their components $\rho(R_{tk}, R_{ti})$.

The bounded index of a conventional correlation factor may be expressed as:

$$x_k = P\left(S_{t1}\right) \times \left(\frac{4.5 - 4 \times \rho_{kf}}{1 - 0.98 \times \rho_{kf}}\right)^{\nu_k} \tag{10}$$

where its index

$$\nu_k = \frac{\sum_{ti=t2}^{tk} P\left(S_{tk}\right)}{\left(k-1\right) \times \left(k + 2\beta_k^2 - 15\beta_k + 30\right)^{1/2}} \tag{11}$$

helps us evaluate an effect of survival probabilities of system elements $P(S_{tk}) = \Phi(\beta_k)$ on the bounded index by Eq. (10) when a reliability index of k-th element is equal to β_k.

According to probabilistic format presented in Eq. (6), the total survival probability of particular

elements as dynamic ductile autosystems with n components may be presented as:

$$P_{as}(S) = P_{as}\left[\bigcap_{tk=t1}^{m} S_{tk}, \exists S_{tk} \le S_{t(k-1)},\ k \in [1,n]\right]$$

$$= 1 - \begin{bmatrix} P(F_{t1}) \bigcup P(F_{t2}|S_{t1}) \bigcup \dots \\ \dots \bigcup P\left(F_{tk}\left|\bigcap_{tk=t1}^{t(k-1)} S_{t(k-1)}\right.\right) \bigcup \dots \\ \dots \bigcup P\left(F_{tn}\left|\bigcap_{tn=t1}^{t(n-1)} S_{t(n-1)}\right.\right) \end{bmatrix}$$

$$\approx P(S_{t1}) \times P(S_{t2}) \times \left\{1 + \rho_{2|f}^{x_2}\left[\frac{1}{P(S_{t2})} - 1\right]\right\} \times \dots$$

$$\dots \times P(S_{tk}) \times \left\{1 + \rho_{k|f}^{x_k}\left[\frac{1}{P(S_{tk})} - 1\right]\right\} \times \dots$$

$$\dots \times P(S_{tn}) \times \left\{1 + \rho_{n|f}^{x_k}\left[\frac{1}{P(S_{tn})} - 1\right]\right\}$$

$$\approx P(S_{t1}) \times \prod_{k=2}^{n}\left(P(S_{tk}) \times \left\{1 + \rho_{k|f}^{x_k}\left[\frac{1}{P(S_{tk})} - 1\right]\right\}\right) \quad (12)$$

where the bounded conventional correlation factor, $\rho_{k|f}^{x_k}$, is expressed by Eq. (7) and n is the number of extreme events.

2.3 *Survival probabilities of static series and parallel ductile general systems*

The safety margins of performance functions of components of static general systems are:

$$Z_k = g(\mathbf{X}_k, \boldsymbol{\theta}) = g(\theta_R R_k - \boldsymbol{\theta}_E \mathbf{E}_k) \quad (13)$$

Analogically to Eq. (12) and following the same probabilistic approaches, the total survival probability of static series (Fig. 1, a) and series-parallel (Fig. 1, c) ductile general systems with m components (autosystems) may be defined as:

$$P_{ss}(S) = P_{ss}\left[\bigcap_{k=1}^{m} S_k, \exists P(S_k) \le P(S_{(k-1)}),\ k \in [1,m]\right]$$

$$= 1 - P_{ss}\left(\bigcup_{k=1}^{m} F_k\right)$$

$$\approx P(S_1) \times \prod_{k=2}^{m}\left(P(S_k) \times \left\{1 + \rho_{k|f}^{x_k}\left[\frac{1}{P(S_k)} - 1\right]\right\}\right) \quad (14)$$

where m is the number of random discrete failure modes or conventional autosystems as single elements and mixed components of systems; $\rho_{k|f}^{x_k}$ is the bounded conventional correlation factor assessed by Eq. (7).

The total survival probability of static parallel ductile general systems (Fig. 1, b) with m components may be presented as:

$$P_{ps}(S)$$

$$= 1 - P_{ps}\left[\bigcap_{k=1}^{m} F_k, \exists P(F_k) \le P(F_{(k-1)}),\ k \in [1,m]\right]$$

$$\approx 1 - P(F_1) \times \prod_{k=2}^{m}\left(P(F_k) \times \left\{1 + \rho_{k|f}^{x_k}\left[\frac{1}{P(F_k)} - 1\right]\right\}\right) \quad (15)$$

$P(S_k)$ from Eq. (14) and $P(F_k)$ from Eq. (15) denote the survival and failure probabilities of ductile autosystem $k = 1 \dots m$ at time t_k. For parallel general systems the demand vector $\theta_E \mathbf{E}_k$ corresponds to failure state after statical redistribution of actions.

The generalized reliability indices of series and parallel systems of events is presented as:

$$\beta_{ss} = \Phi^{-1}[P_{ss}(S)] \quad (16)$$

$$\beta_{ps} = \Phi^{-1}[P_{ps}(S)] \quad (17)$$

where $\Phi^{-1}[\bullet]$ is the inverse cumulative distribution function of the standard normal distribution of their survival probabilities $P_{ss}(S)$ by Eq. (14) and $P_{ps}(S)$ by Eq. (15).

The design documents recommended by the Joint Committee on Structural Safety (JCSS, 2000) are acknowledged as the progressive probabilistic model code in the design of structural members and their systems. According to these documents, the reliability index of structures is related to the consequences of failure classes when the target value is equal to β_t = 3.3–4.3 (EN 1990, 2002; ISO 2394, 1998). Particular elements and members of the structure may be designed on the same higher or lower reliability index as for the entire structure. However, there exist recommendations to use the so-called "thrifty and advanced" method in design practice. These recommendations are based on decreased target reliability index $\beta_{STR} = \beta_t \prod_{i=1}^{6} \gamma_i = 2 - 2.5$. They are included in the Lithuanian National Standard STR 2.05.03:2003. Therefore, the failure probabilities of structures of buildings and civil engineering works may increase inadmissibly by 100–500 times.

3 NUMERICAL EXAMPLES

3.1 *Series autosystem with 5 and 20 components*

Consider series autosystems with n equireliable and equicorrelated components (An & Pandey, 2002). At all failure modes cases the same reliability index $\beta_{tk} = 4.0$ and the same value 0.1 or 0.95 for correlation coefficients between the failure modes are assumed. Reliability indices of these series autosystems calculated by three methods are presented in Table 1 and Figure 2, when the number of their failure modes n is equal to 5 and 20.

Table 1. The values of reliability indices of series autosystems calculated by different methods.

The number of failure modes, n	ρ_{ki}	Design methods: TCP + CCV by Eq. (12)	Numerical integration (An & Pandey, 2002)	PCM by Eq. (4)
5	0.1	3.6031	3.6013	3.6013
	0.95	3.7922	3.7901	3.6036
20	0.1	3.2299	3.2238	3.2237
	0.95	3.2927	3.2540	3.2273

3.2 *Series systems with four reliability indices of components*

According to Zhao *et al.* (2007) consider a series system with four failure modes in which the first-order reliability indices have been obtained as $\beta_1 = 2.5$, $\beta_2 = 2.5$, $\beta_3 = 3.0$, $\beta_4 = 3.5$ and the correlation coefficient between every pair of failure modes is assumed to be $\rho = 0.86$. The results for the system reliability index are presented in Table 2. The reliability index of a series system calculated using

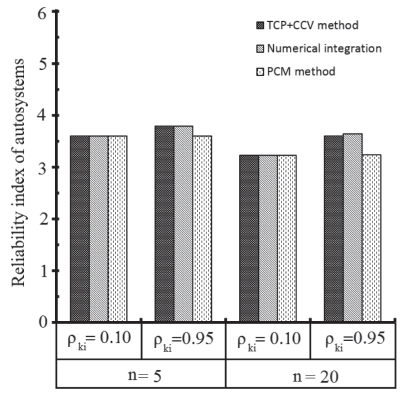


Figure 2. Comparison of reliability indices of series autosystems consisted of 5 and 20 components.

Table 2. Calculation results of series system reliability index, β_{ss}, by Eq. (16).

Bounds	Design methods: Zhao et al. (2002)	Feng's	Ditlevsen's	Numerical integration	TCP + CCV by Eq. (16)
Lower	2,333	2,331	2,351	2,330	2,327
Upper	2,317	2,311	2,273		

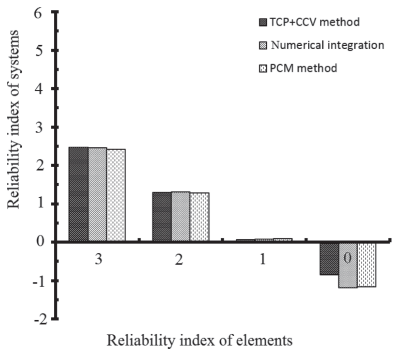


Figure 3. Reliability indices, β_{ss}, by Eq. (16) for series general systems.

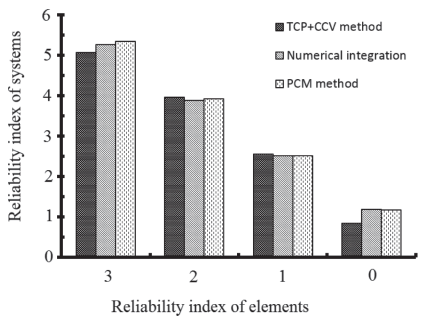


Figure 4. Reliability indices, β_{ps}, by Eq. (17) for parallel general systems.

the method TCP + CCV by Eq. (16) is close to the solution obtained through numerical integration.

3.3 *Series and parallel general systems with equireliable elements*

The analysis of reliability indices of series and parallel systems with 6 equireliable elements, the reliability index of which is $\beta = 0–3$ (Pandey 1998 a, b) are shown in Figure 3 and 4, respectively. The correlation coefficients are given in product form, i.e. $\rho_{ki} = \lambda_k \lambda_i$, $k \neq i$, and $\lambda_i = \sqrt{(13-2i)/12}$, $k,i = 1, 2, \ldots, 6$.

The conventional correlation factors of autosystems are: $\rho_{2|1} = 0.8292$, $\rho_{3|21} = 0.6963$, $\rho_{4|321} = 0.5567$, $\rho_{5|4321} = 0.4041$ and $\rho_{6|54321} = 0.2155$. They can be calculated using the matrix of basic correlation coefficients and Eq. (7).

The illustrative examples show that the results of system analysis obtained by the proposed TCP + CCV method are very close to the probabilistic data computed by exact but sophisticated numerical integration and PCM methods based on complicated integration formats.

4 CONCLUSIONS

The simplification of methodology of probability-based analysis and prediction of reliability indices of time-dependent structural and technical systems as systems of extreme events may be related to the autosystem concept. It is very useful and possible to separate the formats of probabilistic analysis of dynamic series autosystems with single and mixed particular elements (normal and oblique sections, connections, deflections) from static series, parallel and series-parallel systems consisting of autosystem components.

The proposed approaches allow us to simplify the mathematical format, if the prediction of survival probabilities and reliability indices of sustainable series, parallel and series-parallel systems are based on the additional concepts of Transformed Conditional Probabilities (TCP) and Conventional Correlation Vectors (CCV). They help us avoid of complicated multidimensional integrations both in a safety analysis of general systems and their autosystem components.

A separated reliability analysis of structural and technical systems into dynamic by Eq. (12) and static by Eq. (14) or (15) parts helps designers to simplify probabilistic calculations. The presented unsophisticated probability-based approaches, design models and calculation equations may be convenient for many practitioners and can stimulate designers to use the full probabilistic methods in their practice more actively and effectively.

ACKNOWLEDGMENT

The first author would like to express their gratitude to the Research Council of Lithuania for the Postdoctoral fellowship. Postdoctoral fellowship is being funded by the European Union Structural Funds project "Postdoctoral Fellowship Implementation in Lithuania".

REFERENCES

Ahammed, M. & Melchers, R.E., 2005. New bounds for highly correlated structural series systems. *ICCOS-SAR*, Millpress, Roterdam: 3656–3662.

An, Y. & Pandey, M.D., 2002. Evaluation of an approaximate method for multinormal integration. *The 4th Structural Specialty Conference of the Canadian Society for Civil Engineering. June 5–8, 2002*. p. 10.

Dey, A. & Mahadevan, S., 2000. Reliability estimation with time-variant loads and resistances. *Journal of Structural Engineering*, 126(5).

Ditlevsen, O., 1997. Structural reliability codes for probabilistic design—a debate paper based on elementary reliability and decision analysis concepts. *Structural Safety* 19(3): 253–270.

EN 1990, 2002. Eurocode-Basic of structural design. CEN, Brussels.

Estes, A.C. & Frangopol, D.M., 1998. RELSYS: a computer program for structural system reliability. *Structural Engineering Mechanics,* 6(8): 901–019.

ISO 2394, 1998. General principles on reliability for structures. Switzerland.

JCSS, 2000. Probabilistic model code: Part 1—Basis of design. Joint Committee on Structural Safety, 2000. p. 65.

Kang, H. & Zhang, X., Wang, F., 2003. A reliability analysis method of offshore platforms. *Proceedings of the thirteenth International offshore and polar engineering conference Honolulu, Hawaii, USA, May 25–30, 2003*. 469–472.

Kang, W.H. & Song, J., 2010. Evaluation of multivariate normal integrals for general systems by sequential compounding. *Structural Safety,* (32): 35–41.

Kudzys A. & Lukoševičienė O., 2009. On the safety prediction of deteriorating structures. *Mechanika* (78), p. 5–11.

Kudzys, A. & Kliukas R., 2010. Probability-based design of spun concrete beam-columns. *Journal of Civil Engineering and Management,* 16(4): 451–461.

Kudzys, A. & Lukoševičienė, O., 2013. Conventional Stochastic Sequences in Reliability Assessments and Predictions of Structural Members, *11th International Conference on Modern Building Materials, Structures and Techniques, MBMST 2013, Procedia Engineering,* 57: 642–650.

Levitin, G. & Lisnianski, A., Ben-Haim, H., Elmakis, D., 1998. Redundancy optimization for series–parallel multi-state systems. *IEEE Transactions on Reliability* 47(2): 165–172.

Levitin, G., 2004. A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliability Engineering & System Safety,* 84: 285–292.

Li, J., Chen J.B., Fan W.L., 2007. The Equivalent extreme event and evaluation of the structural system reliability. *Structural Safety,* 29: 612–620.

Melchers, R.E., 1994. Structural system reliability assessment using directional simulation. *Structural Safety,* 16: 23–39.

Mori, Y. & Ellingwood, B.R., 1993. Time-dependent system reliability analysis by adaptive importance sampling. *Structural Safety,* 12(1): 59–73.

Mori, Y. & Kato, T., 2003. Multinormal integrals by importance sampling for series system reliability. *Structural Safety,* 25: 363–378.

Pandey, M.D. & Sarkar, A., 2002. Comparison of a simple approximation for multinormal integration with an importance sampling-based simulation method. *Probabilistic Engineering Mechanics,* 17: 215–218.

Pandey, M.D., 1998a. A simple approach to multinormal integration with applications to the system reliability computation. *Civil Engineering and Environmental system,* 15: 89–105.

Pandey, M.D., 1998b. An effective approximation to evaluate multinormal integrals. *Structural Safety*, 20: 51–67.

Ramirez-Marquez, J. & Coit, D.W., 2004. A heuristic for solving the redundancy allocation problem for multistate series-parallel systems. *Reliability Engineering & System Safety,* 83(3): 341–349.

Song, J. & Kang, W.H., 2009. System reliability and sensitivity under statistical dependence by matrix-based system reliability method. *Structural Safety,* 31: 148–156.

Yuan, X.X. & Pandey, M.D., 2006. Analysis of approximations for multinormal intyegration in system reliability computation. *Structural Safety,* 28: 361–377.

Zhao Y.G. & Zhong W.Q., Ang A. H-S., 2007. "Estimating joint failure probability of series structural systems". *Journal of Engineering Mechanics,* 133: 588–596.

Žiha, K., 2000. Redundancy and robustness of systems of events. *Probabilistic Engineering Mechanics*, 15: 347–357.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safety-based approach in multifunctional building design

A. Taraszkiewicz & M.K. Gerigk
Gdańsk University of Technology, Gdańsk, Poland

ABSTRACT: The modern trend in design of the public buildings is to create multifunctional environments in one building, hosting a variety of functions. Multifunctional buildings entertain large number of visitors. The complexity and vulnerability of this type of public space are the main reasons to use within their design process the performance based approach including the recognition of hazards. Safety and reliability approach is now used in structural design and assessment. The paper presents safety-based approach used in the architectural design on the example of multifunctional building. The holistic method of design proposed in the paper considering hazards scenarios and management is presented and compared with the traditional design process based on the civil engineering codes.

1 INTRODUCTION

1.1 *Tendencies*

Organization of contemporary city reveals a trend to build multifunctional structures. The aim of the article is to present the necessity to improve the safety based approach in multifunctional building design. In the time of rapid development of urban spaces it is significant that the use of the land is rather intensive. In consequence, new built architecture in cities is represented by multipurpose facilities. In recent years more and more demanding structures are designed, built and operated to satisfy the increasing needs of the society (Arangio 2012). The reason to provide more detailed safety in multipurpose systems is avoiding unpredictable to cause negative influence.

1.2 *The case context*

Multifunctional buildings created today are designed in a traditional way, which is based on master plans and building codes. It may not be sufficient in relation with safety performance for complex structural systems.

Current actions in built environment are focused around the sustainable development (World Commission on Environment and Development 1987). Actual project should take social, economical and environmental factors. Safety approach is an integral component of any field relative to actual standard of development.

2 GENERAL DEFINITIONS

2.1 *Multifunctional building*

Multifunctional building is a structure that contains at least two functions in the functional programme. Multipurpose buildings are typical for the metropolitan area usage. In general multifunctional building contains a large amount of functions, mixed-use spaces that create a complex system. Multifunctional building allows to use the urban space in more efficient and compact way. The priority objective for such type of building is conservation of the city area and improvement of the quality of urban space. Furthermore, complex functional system allows to provide more economic communication, cheaper technical infrastructure, easy accessibility of services and counteracting chaotic urban sprawl.

The goal for multifunctional building is to create a new model of environment and user friendly urbanization.

2.2 *Complex system*

From the architectural point of view the system represented by a building is defined by its functions. A multifunctional building is a complex structure internally. At the same time it is also a part of the wider system in relation to the external context.

The external context, the built environment, comprises the urban design, land use, transportation system, and encompasses patterns of human activity within the physical environment (Handy & Boarnet 2002).

2.3 *Safety-based approach*

Safety is complementary with the level of risk. The common definition of risk (associated with hazard) is a combination of the probability that hazard will occur and the (usually negative) consequences of that hazard. The consequences can be expressed

in material damage or in loss of human life (Suddle 2001). Safety-based approach is necessary to improve usefulness of built environment. Safety methods are successfully applied in many practical fields connected with architectural design like: complex systems (Zio 2009); logistics (Nowakowski & Werbińka 2009); transportation including maritime and multimodal transportation (Soares & Teixeira 2001) (Abramowicz-Gerigk 2006) (Abramowicz-Gerigk & Burciu 2008) (Abramowicz-Gerigk & Burciu 2013) (Gerigk 2004) (Gerigk 2005) (Gerigk 2006) (Gerigk 2008) (Gerigk 2012); where the influence of achieved research is present in practical project designs.

Risk assessment in civil engineering design is now considered as principal rule to evaluate the consequences of building projects. There is a crucial importance of placing safety at the earliest possible stage in the project planning (Visscher et al. 2006).

3 MULTIFUNCTIONAL SYSTEM SAFETY

3.1 *Design and assessment process*

Designing a multifunctional building is a complex process. There are many factors that have an impact in the planned structure. In the life cycle of a project design the following phases are to be considered:

– concept phase,
– design phase,
– construction phase,
– exploitation phase,
– disposal phase.

In each phase the safety assessment is required. Moreover, life cycle of the project is a dynamic process in its character, so the safety assessment needs to be updated when the new hazards can appear. As it is shown in Figure 1. hazardous situation can be revealed in each phase of a design process. Each hazardous situation has its priority and importance to be resolved. It is important to resolve any hazardous situation in time to avoid overlapping, what could cause unpredictable losses.

The following stakeholders participate in the design and assessment process, when the building's essential functions and the infrastructure are defined (Nilsson & Hees 2012):

– building owner,
– tenants,
– facility staff,
– occupants,
– neighbors,
– municipality,
– regulators,
– designer,
– risk manager,
– insurer,
– fire brigade.

The final structure of the design and assessment process depends on their decision and understanding.

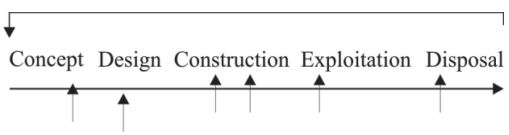


Figure 1. Multifunctional system life cycle scheme with emerging hazardous situations.

3.2 *Internal functional system*

Every function included in the structure plan must be located in the place, where it should work properly in the entire system. Recently the mixed-use buildings take the form of muli-level structures.

The base to define the outcome structure is the multifunctional building functional system. The income for determining the functional programme are the requirements defined by the developer as well as the location context. The example of the multifunctional program is presented in Table 1.

Multifunctional building design consists of a number of projects in various technical fields and a specification dependent on functional programme. The location of a function system helps to define the rest of the important subsystems. There are the following integrated subsystems:

– Construction system,
– Lighting control system,
– Electric power control system,
– HVAC (Heating, Ventilating and Air
– conditioning) system,
– Security and observation system,
– Access control system,
– Fire alarm system,

Table 1. Functional programme.

Level	Function
…	…
–2	Garage
–1	Garage, subway, logistics
0	Public communication, gastronomy, shopping
1	Fitness, art gallery, cinema
2	Offices, business
…	…

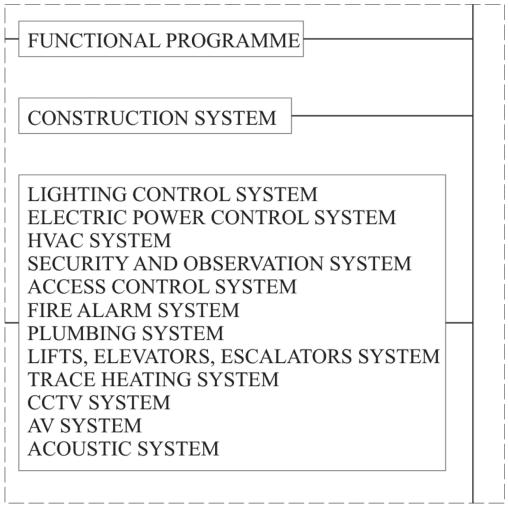


Figure 2. Internal functional system scheme.

– Plumbing system,
– Lifts, elevators, escalators system,
– Trace heating system,
– Closed-Circuit Television (CCTV),
– AV (audio-video) system,
– Acoustic system,
– Other engineering systems.

All the mentioned above systems (Doukas & Patlitzianas 2007) must be integrated with the basic architectural project.

The internal functional system of a multipurpose building can be defined as a compact structure formalized in horizontal and vertical directions.

3.3 *External functional system*

The internal functional system is dependent on the external system. The outside space of the building is the context, where multipurpose interior environment goes smoothly to exterior and is connected with different types of access. All the internal subsystems are supplied from the outside city supply systems.

Describing the external system it is necessary to mention the environmental conditions which in most cases have a significant and direct impact on the building performance. The external system components are as follows:

– Social infrastructure,
– Technical infrastructure,
– Transportation infrastructure,
– City logistics supply system,
– Waste disposal,
– Weather conditions.

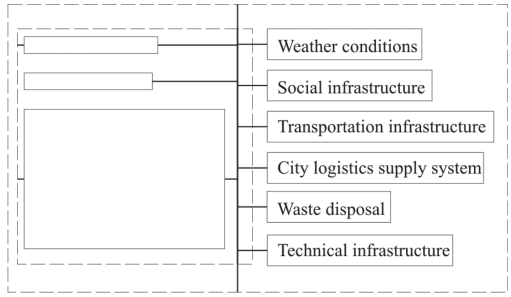


Figure 3. External functional system scheme.

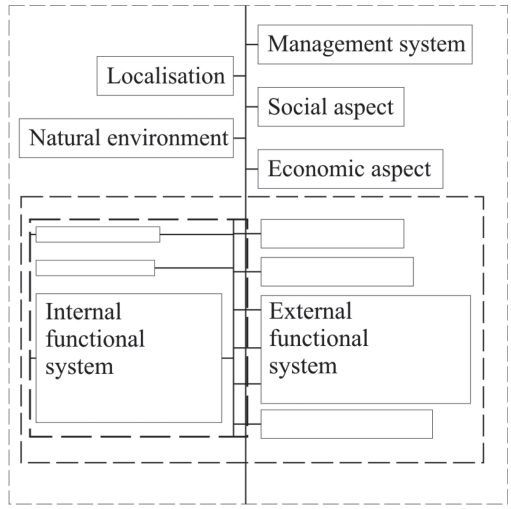


Figure 4. Environment system scheme.

3.4 *Environment*

Looking from the outside, it is easy to observe the integrity of the inside and outside. Creating a multifunctional safety-based system it is important to take into account elements related to each one of the subsystems. Environmental factors which have the influence on the building are as follows:

– Internal functional system,
– External functional system,
– Management system,
– Localization,
– Social aspect,
– Economic aspect,
– Natural environment.

3.5 *Safety approach in architectural design*

In the architectural design process the implementation of the safety criterion should be the priority.

Architectural design coordinates all factors which affect the structure of a multifunctional building. The success of the project depends on good coordination of the project as well as proper system management in each life cycle phase. Safety criteria for an architectural design are significant for the outcome of the process. The most important criteria are:

– Aesthetics,
– Functionality,
– Performance,
– Reliability,
– Design for minimum risk.

The safety-based approach in the design process refers to the elimination of the identified hazards or reduction of the associated risk through design. The risk should be evaluated with respect to people using the building, internal and external functional systems.

Greater complexity in the system increases the possibility that design faults will occur and emerge into the final product (Stephans 2012). According to (Stewart & Melchers 1997) the system failure of engineered structures may be defined as either structural collapse, functionality or serviceability failure. Moreover, it appears that human errors during the planning and design phases as well as construction phase are considered to be the most frequent. The DIN 1055 code declares, that human errors are not considered due to control processes and training. Human errors are not included in the design process. The systems view of human error regards errors and adverse events as a function of a system of interacting parts, any or all of which could present opportunities for preventing and correcting errors (Expert Working Group on Human Factors in Latent Print Analysis 2012).

4 HOLISTIC METHOD IN DESIGN

4.1 *Traditional design*

Traditional design is based on restricted requirements of building codes, law and local master plan. Taking into account only the measures listed above the project team can work out the new design. After the evaluation, when the design meets all the requirements it is ready to be realized. Developers usually should be aware of the design information and limits (Visscher et al. 2006).

In the traditional design the needs of a client or developer were the only sufficient factors for the design team to lead the project and the most important criteria were the investment cost and time.

This traditional approach never meets all the necessary requirements for example with respect to the emergence of the building. Disregard to the strategic criteria can have effect of reducing safety and reliability of the system.

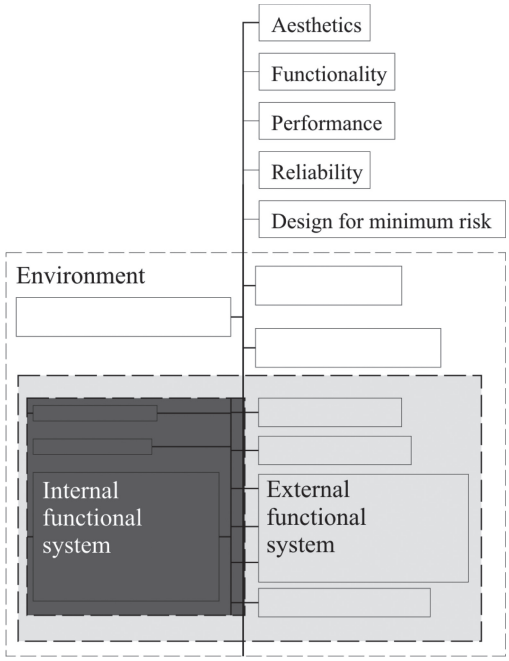


Figure 5. Multifunctional building design scheme.

Traditional approach is based on codes. Standardization and rules improve the design process, but it is not possible for them to manage the whole fluent processing.

4.2 *Multifunctional building design*

Multifunctional building design requires taking the safety-based approach into the design process with more attention. The fundamental quality of holistic method in the multifunctional building design is to reach the general system scope. The outcome of the process, that is multifunctional building design, should be fluently working system, where the functions do not interfere with respect to each other.

Defining the basic parameters of the multifunctional building design may result in its more efficient use. Optimizing durability should be the basis for each architectural project.

5 CONCLUSIONS

Traditional design is based on restricted requirements of building codes. The actual trend in public utility buildings indicates the necessity to improve the safety-based approach in their design.

The safety-based approach applied in architectural design of the multipurpose buildings puts more responsibility on the designer and allows him to use his creativity much more efficient avoiding hazardous solutions. The formal description of the architectural project is difficult in its aesthetic aspects, however the formal description of the functional aspects can have positive influence on the final result as we all appreciate and admire a beauty coming from orders, comfort and safety.

REFERENCES

Abramowicz-Gerigk, T., 2006. Determination of Safety Factors for Ship Berthing Operations. Proceedings and Monographs in Engineering, Water and Earth Sciences. In (ESREL 2006). London: Taylor & Francis/Balkema, 2737–2742.

Abramowicz-Gerigk, T. & Burciu, Z., 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. In & F.L.P. eds., C. Guedes Soares, ed. (IMAM 2013). London: Balkema, 699–704.

Abramowicz-Gerigk, T. & Burciu, Z., 2008. The risk analysis of harbour operations. In C.G.S. & J.B. eds., S. Martorell, ed. (ESREL 2008). London: Balkema, 3343–3350.

Arangio, S., 2012. Reliability based approach for structural design and assessment: performance criteria and indicators in current European codes and guidelines. *International Journal of Lifecycle Performance Engineering,* 1(1), 64.

Doukas, H. & Patlitzianas, K., 2007. Intelligent building energy management system using rule sets. Building and ….

Expert Working Group on Human Factors in Latent Print Analysis, 2012. Latent Print Examination and Human Factors: Improving the Practice through a Systems Approach.

Gerigk, M., 2006. A method for assessing hazards, risks and safety of damaged ships at sea. In (ESREL 2006). London: Balkema, 2783–2790.

Gerigk, M., 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. In (IMAM 2012). London: Balkema, 715–719.

Gerigk, M., 2005. Challenges of modern assessment of safety of ships in critical conditions. In (IMAM 2005). London: Taylor & Francis/Balkema, 1529–1536.

Gerigk, M., 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. (ESREL 2008), 4, 3303–3310.

Gerigk, M., 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. Polish Maritime Research, 11(1 (39)), 8–13.

Handy, S. & Boarnet, M., 2002. How the built environment affects physical activity: views from urban planning. *American Journal of Preventive Medicine*, 23(2), 64–73.

Nilsson, M. & Hees, P. Van, 2012. Analysis of fire scenarios in order to ascertain an acceptable safety level in multi-functional buildings. In 9th Int'l. Conf 2012 Proceedings & Case Studies. Hong Kong.

Nowakowski, T. & Werbińka, S., 2009. On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing*, 6(4), 364–378.

Soares, C.G. & Teixeira, A.P., 2001. Risk assessment in maritime transportation. Reliability engineering and System Safety, 74, 299–309.

Stephans, R., 2012. System safety for the 21st century: The updated and revised edition of system safety 2000.

Stewart, M. & Melchers, R.E., 1997. Probabilistic Risk Assessment of Engineering Systems, London: Chapman & Hall.

Suddle, S., 2001. Safety of construction in intensive use of space. Proceedings of Congress Risk Analysis.

Visscher, H., Suddle, S. & Meijer, F., 2006. Analysing safety risks when constructing over public spaces. In 3rd International SCRI Symposium. University of Salford, 483–495.

World Commission on Environment and Development, 1987. Our Common Future, Oxford.

Zio, E., 2009. Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Management of controls of fire protection systems in Switzerland

E. Nachtigall & S. Metzger
Quantum Brandschutz GmbH, Basel, Switzerland

ABSTRACT: Fire protection systems play an increasingly important role in resolving fire safety challenges. Fire protection systems interact with each other and with other safety and security related systems in a huge network. Together with growing demands and continuous technical development this leads to a rising complexity of such systems. Controls of fire protection systems are predominantly of static nature and neither considers the dynamic nature of fire nor the interactions between systems. Thus, the potential of fire protection systems is not yet fully realized and utilized. Controls of fire protection systems are therefore often planned, implemented and modified in an inconsistent manner. This paper shows how the controls of fire protection systems can be planned, implemented and tested to respond adequately to fire safety aims and to meet the safety demands of society. For this purpose a comprehensive approach to manage the controls of fire protection systems concerning the life cycle phases of buildings based on current Swiss regulations has been developed. The main groups of stakeholders and their special roles and responsibilities in this process are shown. Clear identification of processes, best practice approaches and planning instruments to support the technical and management processes are presented.

1 INTRODUCTION

Nowadays, modern fire alarm systems are much more than devices for fire detection and alarming the fire brigade. In modern buildings these complex instruments of fire protection systems can have the following functions:

- Fire detection (automatic and manual)
- Control of fire protection and building service systems
- Interaction with building safety and security systems
- Alarm/Inform (local and fire brigade)
- Evacuation of people

Because of different functions a fire alarm system can have multiple dependencies to other technical systems. Some examples are shown in Figure 1.

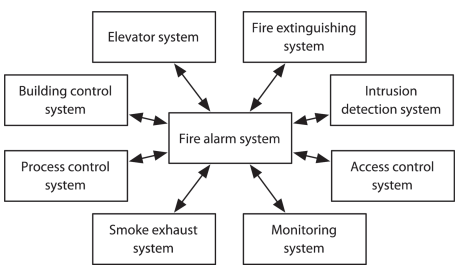


Figure 1. Examples of dependencies of technical systems to fire alarm system in buildings.

Usually a fire alarm system has numerous dependencies to other safety and security related systems (e.g. fire extinguishing, intrusion detection, access control and smoke exhaust systems). Due to safety and/or security reasons also non safety and security related systems (e.g. elevator, building control, process control and monitoring system) can be connected to a fire alarm system. This is based on the fact that many seemingly non safety and security related systems can become very relevant during complex emergency situations or scenarios (Nachtigall & Klingsch 2011).

2 CONTROLS OF FIRE PROTECTION SYSTEMS

Fire protection systems in buildings usually have many sensors, control units containing complex control logic and actuators. In most cases this complexity can be reduced to a simple control chain to demonstrate the interrelations (Burns 2001).

A usual control chain in fire protection systems containing a sensor, a control unit and an actuator is show in Figure 2.

In this example a sensor (e.g. an automatic fire detector) is activated by combustion products such as smoke, heat or combustion gases. After activating the control unit (e.g. a fire alarm or detection system), it initiates programmed Controls of Fire Protection Systems (CFPS) or activates other actuators in the building. An actuator is for example a

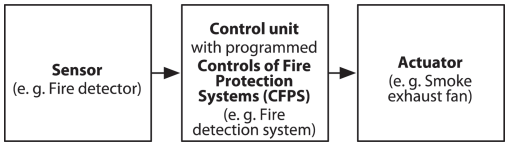


Figure 2. Control chain in fire protection system.

smoke exhaust system that ensures that the defined fire safety goals can be reached.

In modern large buildings usually a fire alarm system, sometimes with thousands of sensors and many different fire safety related and other building service systems are used. For mastering this complexity and also for planning and maintaining the CFPS in some countries (e.g. Switzerland) the following instruments are used:

- Report
- Matrix
- Plan/Visualisation
- The report usually includes the following contents:
- Introduction, description of the project and main boundary conditions
- Life and fire safety goals taken from the fire safety report
- Goals of CFPS to support life and fire safety goals
- Basics: Regulations and guidelines, plans and other documentation
- Basic and detailed description of CFPS
- Zoning of the building
- Detailed CFPS for all fire protection systems and other relevant safety and security related systems and non safety and security related systems
- Mode of alarm
- Conclusion

Another important tool to plan CFPS is the matrix or fire safety matrix. A matrix with only very few elements for an exemplary area or zone is shown in Figure 3.

A matrix represents logical connections between fire safety related sensors and actuators. In this context, the X in a cell of the matrix implies that the specific interaction described in the function cell occurs. For instance, upon activation of the sprinkler or an automatic fire alarm detector in the considered area the fire department is alerted and the smoke exhaust system is activated.

This simple matrix exemplifies the most important relationships in CFPS. More complex schemes can be necessary for large modern buildings, usually containing many different fire protection systems and other relevant safety and security related systems. In many cases CFPS are static and do not

Controls of Fire Protection Systems in area ... / Sensor/Switch ...	Actuator/System ...	Fire alarm system	Fire brigade alarm	Smoke exhaust system	Smoke exhaust fan	HVAC system	Venting system	Other systems
Automatic fire detector			X		X		X	
Manual fire detector			X					
Sprinkler			X		X			
	Function		activate		activate		deactivate	...

Figure 3. Matrix with CFPS for an exemplary area.

consider the time or dynamic interactions between systems (Jost 2005). To overcome those limitations, a model for the dynamic control of fire protection systems was developed (Nachtigall 2013c).

The final instruments of planning CFPS are special plans or visualizations. These instruments typically provide information for CFPS in floor plans. The plans can be used to visualize areas with common CFPS, as well as location of actuators and its activation function.

These three information instruments form the basis for a complete planning of the CFPS. To understand the planning process of CFPS first the life cycle of a building and the corresponding fire safety services have to be explained.

3 LIFE CYCLE OF A BUILDING AND FIRE SAFETY SERVICES

A basis for the provision of engineering services in civil engineering is in Switzerland the SIA 112 (Swiss Norm 508 112). This norm, developed by the Swiss Society of Engineers and Architects (SSEA) presents and explains performance phases for the life cycle of a building. The different main- and subphases of these performance phases are shown in Figure 4.

The SSEA main performance phases start with strategic planning (1) followed by preliminary studies (2). In this two main phases a wide range of fire safety consulting services are usually performed in subphases (11–22).

In project planning phase (3) fire safety planning in subphases (31–33) and fire safety engineering methods are performed. It bears repeating that the early involvement of the fire safety engineer is crucial for the success. In tender phase (4) tender monitoring (41) to optimize costs of all fire safety systems and services can be done.



Figure 4. Life cycle of a building, SSEA-performance phases and fire safety services.

The implementation phase (5) is crucial to costs and on time commissioning of technical building equipment and the whole building. In this phase such fire safety services as construction supervision, quality assurance (51–53) and fire safety engineering methods (52–62) can dramatically reduce construction costs, enables the flexible use of the building and ensure the realization of planed life and fire safety.

The switch from implementation phase (5) to management phase (6) is the most challenging part in the whole life cycle of a building. Therefore the put into the operation of fire protection systems and implementation of CFPS in subphases (52–53, 61–62) are very important (SSEA 2013). Well-known and best-executed processes of the commissioning and put into operation are crucial for success and cost certainty.

In management phase (6) also fire prevention (61) and support during renovation subphase (62) by experienced fire safety companies in those fields are important to support or improve a high level of fire safety (Hasofer & et al. 2007). Periodic checks, maintenance and adjustments of already implemented CFPS in subphases (61–62) help also to sustain the intended fire safety level.

4 CONTENT BASED PLANING PROCESS OF CONTROLS OF FIRE PROTECTION SYSTEMS

Based on the presented life cycle of a building following planning process for CFPS in different phases with corresponding subphases are necessary:

Phase 33: The process of creation of CFPS report usually contains the following steps:

- Analysis of CFPS from the fire safety report containing:
  Examination of available documents, and conduct a rough analysis
  - Identification of specific features of the building and its fire control systems
- Creation of CFPS report with focus on:
  - Setting the control policies with the principal
  - Create the building-specific concept CFPS (1st version of the CFPS report)

Phase 51: Creation of CFPS matrix containing:

- Create the CFPS matrix (1st version of the CFPS matrix) based on the CFPS report
- Examination of the draught fire case control by the principal

Phase 52: Updating of the CFPS documents:

- Adjusting the CFPS report (2nd version of the CFPS report)
- The CFPS report and matrix to be submitted to the authority and approved by the latter
- Customizing and finalizing the CFPS report (3rd version of the CFPS report)
- Customizing and finalizing the CFPS matrix (2nd and 3rd version of the CFPS matrix)
- The programming of the fire alarm system by the fire alarm systems suppliers as defined by CFPS report and matrix (both 3rd version)

Phase 53: Integral Tests: For the successful commissioning of the building facilities the following steps of the integrals tests (which include preparation, implementation and documentation) are necessary:

- Start meeting with the leaders of the principal, fire alarm systems suppliers and other stakeholders
- Create the test program
- Presentation and discharge of the test program by the authority
- Performing integral tests
- Documentation of the tests with protocols and fault lists
- Adaptation of the CFPS documents

5 STAKEHOLDERS AND THEIR ROLES FOR CONTROLS OF FIRE PROTECTION SYSTEMS

Besides the shown planning process of CFPS the information level and qualification level of stakeholders of the process are important for successful implementation of CFPS. Therefore a stakeholder-centered approach to planning of

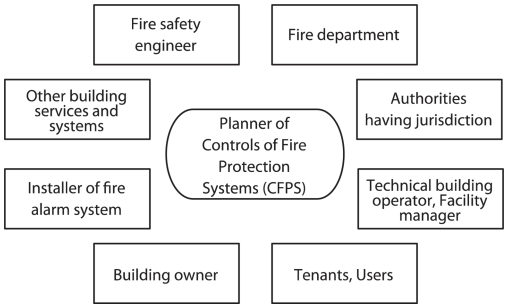


Figure 5. Different stakeholders of processes for CFPS.

CFPS is necessary. Such stakeholder-centered approach with its stakeholders to planning of CFPS is shown in Figure 5.

By far the most important role to plan and maintain CFPS is the planner of CFPS. He must communicate and get the necessary information from other technical designers and stakeholders.

At the beginning of the planning process the fire safety engineer or the author of the fire safety report must be consulted. For the best practice the fire safety engineer is the same person or at least a person in the same organization as the planner of CFPS. This is because CFPS are to support and to implement integrated fire protection systems and to reach the life and fire safety goals, which has, been carried out in fire safety report.

The needs of the fire department and authorities having jurisdiction are to be considered by the planer of CFPS. In most cases those two stakeholder groups controlling the whole process.

Consultations with planers and builders of building services and fire alarm system are also necessary. Other stakeholders such as tenants and users as well as the technical building operator or the facility manager have also to cooperate with. All important information must be communicated to those stakeholder groups.

6 MODULES FOR CONTROLS OF FIRE PROTECTION SYSTEMS

Besides the pervious considering of content based planning process of CFPS and description of stakeholders who are usually involved in the process, modules for CFPS are to develop. These modules oriented model can help to understand the process of planning of CFPS not only based on content or documents introduced before but also based on modules, which contain actions and documents. A modules oriented management system for processes to planning CFPS is shown in Figure 6.

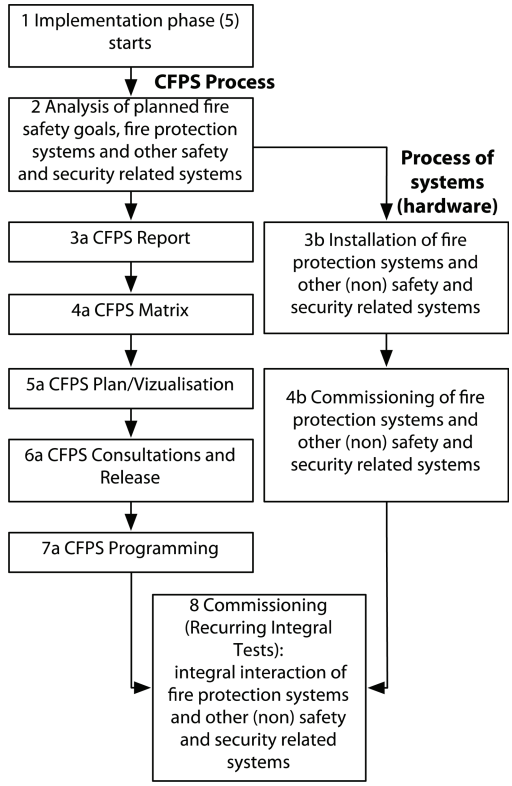


Figure 6. Management system modules of processes for CFPS.

At the beginning of the implementation phase an analysis of planned fire safety goals, fire protection systems and other (non) safety and security related systems is performed.

At this point two parallel processes start. The first process is the planning and implementation process of CFPS. The second process is the process for installation and commissioning of technical systems in the building.

The modules of CFPS process, which is in the focus of this paper, contain the following the steps:

- Creating the CFPS report (3a)
- Creating the CFPS matrix (4a)
- Creating CFPS plans or visualization (5a)

Then the process steps of consultations and release process (6a) followed by the process of programming (7a) CFPS are usually performed. After this in process step (8) both parallel processes are integrated again in integral test. Those important tests are necessary to show correct integral interactions of fire protection systems and other (non) safety and security related systems, which could be

relevant for life and fire safety. Needless to say that this process step must be repeated after changes of technical systems or after about two or three years to show the correct interactions of those systems which are crucial for life and fire safety.

The presented modules for CFPS are derived from regulations provided by the Swiss VKF (Association of Cantonal Fire Insurers; German: Vereinigung Kantonaler Feuerversicherungen) (VKF 2008), (VKF 2007).

In Switzerland at different companies, which provide services in fire, safety planning and engineering as well as in planning of CFPS the presented or similar processes are successfully developed and used.

7 FURTHER DEVELOPMENT OF CONTROLS OF FIRE PROTECTION SYSTEMS

The following key points are essential for the success in fire safety services and especially in CFPS services:

- Strategic focus on integral fire safety engineering
- Consistent operational excellence in fire safety engineering and CFPS
- Constant improvement
- High quality services on-time
- Customer centricity
- High employee engagement

These influencing factors are general in nature and meet many situations and service-oriented companies (Hess 2012). However, they are necessary for a sustainable development of companies in this field. The better the company in those key points is situated, the more likely it is possible to implement the presented management system of CFPS successfully.

Beside the implementing of the introduced management system the following points could became relevant in future for the processes interrelated with CFPS:

- Model the building and fire scenarios with the help of Computer Fluid Dynamics (CFD) including dynamic interactions of fire protection of systems (Mahdavi 1996)
- Development of software tools around the planning processes of CFPS to automate and improve the quality of processes (Männchen 2012), (Merz & et al. 2010), (Lieb & Gerhardt 2004)
- Implementation of functional safety methods in fire protection systems to achieve the life and fire safety goals quantitatively (Börcsök 2007), (IEC 2010), (Meyna & Pauli 2010), (Nachtigall 2013b)
- Development of systems approach or a special systems theory of fire safety (Ropohl 2012), (Nachtigall 2013a)
- Embedding the processes of fire safety in the overall risk management (ISO 2011)
- Further development of appropriate standards for CFPS and recurring integral tests (SSEA 2013), (VDI 2005), (GOST 2011), (Ernst & et al. 2014), (Lucka 2014)

8 CONCLUSIONS

First of all the paper introduces the concept of Controls of Fire Protection Systems (CFPS) used in Switzerland. Main documents for planning CFPS such as CFPS report, matrix and plans and their most important contents are presented.

Then the paper introduces and explains different fire safety services in the life cycle of a building. This life cycle is based on phases and subphases, which are used in Switzerland to structure the processes in civil engineering. According to the findings in the paper fire safety services should be offered during the whole life cycle to reach and optimize the intended level of life and fire safety.

After introducing the fire safety services approach based on the life cycle content based planning process of CFPS is presented. Also the main stakeholders and their roles for CFPS process are shown.

Furthermore management system modules of processes for CFPS derived from regulations in Switzerland are characterized and discussed.

Finally some indications for companies to succeed in fields of fire safety services as well as possible further developments of CFPS are given.

The paper presents processes for management of controls of fire protection systems, which are used in Switzerland. To handle the growing complexity in safety and security related systems in civil engineering and special in fire protection systems a comprehensive approach is identified. The discussed management system based on modules can also be implemented in other countries. Positive experiences of application of presented management system in modern and complex buildings are available and can be used for further development.

REFERENCES

Börcsök, J. 2007. Functional Safety—Basic Principles of Safety-related Systems. Heidelberg: Hüthig.

Burns, R. S. 2001. Advanced Control Engineering. Butterworth Heinemann.

Ernst, A. Nachtigall, E. Nagel, B. 2014. Vollprobentest und Wirkprinzipprüfung -Vergleich mit der Schweiz. Feuertrutz Magazin 2.2014.

GOST 2008–2011. GOSTR 53195 Functional safety of building/erection safety-related systems, parts 1–5.
Hasofer, A.M. & et al. (2007). Risk Analysis in Building. Fire Safety Engineering. Amsterdam: Elsevier.
Hess, E. 2012. Grow to Greatness—Smart Growth for Enterpreneural Businesses. Stanford university press.
IEC 2010. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, All Parts.
ISO Entwurf, 2011. DIN ISO 31000 Risikomanagement. Grundsätze und Leitlinie.
Jost, J. (2005). Dynamical Systems, Examples of Complex Behaviour. Springer.
Lieb, R.D. & H.J. Gerhardt 2004. Die Bedeutungder Ausführungsplanung und Bauüberwachung im Brandschutz bei komplexen Steuerungsvorgaben. VIII. Baurecht und Brandschutz-Symposium.
Lucka, F. 2014. Warum standardisiert Gebäudetesten? Die neue VDI 6010 Blatt 3. Feuertrutz Magazin 2.2014.
Mahdavi, A. ca. 1996. Toward a simulation-assisted dynamic building control strategy. Department of Architecture, Carnegie Mellon University, Pittsburgh, PA, USA.
Männchen, C. 08/2012. Brandfallsteuermatrix professionell managen. TGA Fachplaner.
Merz, H. & et al. 2010. Gebäudeautomation Kommunikationssysteme mit EIB/KNX, LON und BACnet. Fachbuchverlag Leipzig im Carl Hanser Verlag.
Meyna, A. & B. Pauli (2010). Zuverlässigkeitstechnik—Quantitative Bewertungsverfahren. München: Hanser.
Nachtigall, E. 2013a. Dynamic Control of FireProtection Systems. Ph.D. thesis, University of Wuppertal.
Nachtigall, E. 2013b. Functional Safety in Civil Engineering: On the example of the GOST R 53195 Functional safety of building/erection safety-related systems. in: Standards and Quality.
Nachtigall, E. 2013c. Systems Analysis Methodsfor Consideration of Fire Safety. in: Science and Safety 1 (6).
Nachtigall, E. & W. Klingsch 2011. Perspektivenanlagentechnischer Komponenten im ganzheitlichen Brandschutz. in: Sicher ist sicher—Arbeitsschutz aktuell 04, 160–163.
Ropohl, G. 2012. Allgemeine Systemtheorie. Einführung in transdisziplinares Denken. Edition sigma.
SSEA 2013. SSEA 2046 Merkblatt: Integrale Testsvon Gebäudetechniksystemen, draft.
VDI 2005. VDI 6010 Technical safety installations Systems-overlapping functions, All Parts.
VKF 2007. Brandschutz-Merkblatt, Gewährleistung der Betriebsbereitschaft von Brandmeldeanlagen (BMA). Forum für technischen Brandschutz, Schweiz.
VKF 2008. Brandschutzerläuterung. Gewährleistung der Betriebsbereitschaft von Brandfallsteuerungen (BFS).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Electronic components with time-dependent failure rates—reasons, values and consequences

P. Zeiler, O. Koller & B. Bertsche
Institute of Machine Components, University of Stuttgart, Stuttgart, Germany

ABSTRACT: For reliability calculation of electronic components, handbooks are typically used. The calculation shows a high level of uncertainty and usually has no direct relationship to a physical damage mechanism. Moreover, the calculation procedure assumes constant failure rates. A power module (integrated in electric and hybrid vehicles) and an electrolytic capacitor were used to examine whether this assumption is universally valid. The physics of failure of both exemplary electronic components showed that the dominant failure mode had a significantly increasing failure rate. This demonstrates that the general assumption of constant failure rate for electronic components is not permissible. It has wide-ranging consequences for reliability and safety analysis of these components and their specification. The influences of an increasing failure rate on the proper specification of a component are shown. Furthermore, the influences on preventive maintenance, functional safety and availability are considered.

1 INTRODUCTION

The reliability calculation of electronic components is typically done based on handbooks. The handbooks calculate constant failure rates based on exponential distribution which are adjusted for the particular environmental conditions and individual loads.

Using the example of a power module (integrated in electric and hybrid vehicles) and an electrolytic capacitor, it will be examined whether this approach is universally valid. A Weibull analysis of test results for this component showed a significantly increasing failure rate due to mechanical stresses caused by thermal cyclical of the component during operation. The test analysis for aluminium electrolytic capacitors showed a similar result.

This demonstrates that the assumption of a constant failure rate is not permissible in general. The modelling of the failure behaviour by an exponential distribution is obviously not correct for components with increasing failure rate. The use of a time-dependent failure rate in the model, applying the Weibull distribution, has wide-ranging consequences for reliability and safety analysis of these components and their specification.

The commonly used specification parameters can lead to dramatically misleading component reliability and safety over the specified life time. This will be demonstrated by investigating the influence of different increasing failure rates on the reliability and safety characteristics and specification parameters. An adequate specification parameter for components with time-dependent failure rates will be defined. The effect of preventive maintenance to limit the failure rate will be illustrated. The influence on functional safety and the procedure to specify the availability will be noted.

This paper is organized as follows: In chapter 2 some basics and definitions are provided. Chapter 3 describes the commonly applied procedure to calculate the reliability of electronic components. Electronic components with time-dependent failure rate are presented in chapter 4, followed by the consequences in chapter 5.

2 BASICS & DEFINITIONS

In the following some definitions and basic explanations are summarized which are essential for the topic of the paper.

2.1 *Reliability*

The reliability $R(t)$ of a component is the probability that, when operating under stated environmental conditions, the component will perform its intended function adequately for a specified interval of time t (Bertsche 2008).

The mathematical description is based on the probability density function (pdf) $f(t)$, the failure probability $F(t)$ described a cumulative distribution function (cdf), with $f(t) = \mathrm{d}F(t)/\mathrm{d}t$, the reliability $R(t) = 1 - F(t)$ and the failure rate $\lambda(t) = f(t)/R(t)$.

The failure rate is a conditional probability, as it describes the probability to fail in an infinitesimal time interval dt at time t under the condition that the observed element has survived until time t.

The expected value of life time τ is defined as

$$MTTF = E(\tau) = \int_0^\infty t\, f(t)\,\mathrm{d}t = \int_0^\infty \big(1 - F(t)\big)\,\mathrm{d}t\,, \qquad (1)$$

which is the mean life time $MTTF$ (Mean Time To Failure).

A quantile is defined as the value which is undercut by a given probability α. The α-quantile Q_α of a cdf $F(\bullet)$ is defined as

$$Q_\alpha = F^{-1}(\alpha). \qquad (2)$$

2.2 *Exponential distribution*

Starting from an initial value the pdf of the exponential distribution decreases monotonic according to an inverse exponential function. The pdf is given by (Bertsche 2008)

$$f(t) = \lambda \cdot e^{-\lambda t}, \quad t \geq 0 \text{ and } \lambda > 0\,, \qquad (3)$$

with the constant failure rate λ as the only parameter, i.e. the probability of failing in an interval is independent of the time elapsed up to the beginning of the interval. This memory-less property makes the distribution mostly inapplicable to describe sufficiently the failure behaviour of mechanical components, like aging and wear-out.

The mean life time described by the exponential distribution is

$$MTTF = \frac{1}{\lambda}. \qquad (4)$$

2.3 *The Weibull distribution*

The usual description of the failure behaviour of mechanical or automotive components is provided by the three-parameter Weibull distribution (Bertsche 2008), with the pdf

$$f(t) = \frac{b}{(T - t_0)}\left(\frac{t - t_0}{T - t_0}\right)^{b-1} e^{-\left(\frac{t-t_0}{T-t_0}\right)^b}, \quad t \geq t_0 \geq 0 \qquad (5)$$

with shape parameter b, scale parameter T and failure-free time t_0. For $t_0 = 0$ one speaks of a two-parameter Weibull distribution. With $b = 1$ and $t_0 = 0$ the Weibull distribution is reduced to the exponential distribution with $\lambda = 1/T$.

It is obvious that the failure rate of a Weibull distribution is a function of time

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{b}{T - t_0}\left(\frac{t - t_0}{T - t_0}\right)^{b-1}, \qquad (6)$$

which could depict all three sections of the well-known bath tub curve depending only on the shape parameter.

2.4 *Bath tub curve*

The failure rate λ(t) will change over the component life time of a population as shown in Figure 1.

The bath tub curve generally emerges through superposition of three typical failure modes and is therefore subdivided into the following sections:

- Section I of a decreasing failure rate ($b < 1$) represents early failures due to material or manufacturing defects. Quality control and initial component testing usually help to avoid this kind of failures. Actuarial statisticians call this section of the curve "infant mortality".
- Section II of a constant failure rate ($b \cong 1$) represents random failures caused by sudden stresses, extreme conditions e.g. like over-voltage regarding electronic components, handling errors, etc. In actuarial terms this could be equated to the accidents encountered by a population of individuals on a day-to-day basis. This section of the bath tub curve is usually assumed in the reliability calculation of electronic components, see chapter 3.
- Section III of an increasing failure rate ($b > 1$) represents wear-out or aging failures. Here the failure rate increases as equipment deteriorates. For mechanical components like bearings, gearwheels or shafts there is knowledge about the Weibull parameters in this section (Bertsche 2008). With this, the curve progression in this section of the bath tub curve is well-known.

During component development, one tries to increase the reliability of the component systematically, i.e. to avoid early failures (pre-aging) and delay the beginning of wear-out and aging failures as far as possible.

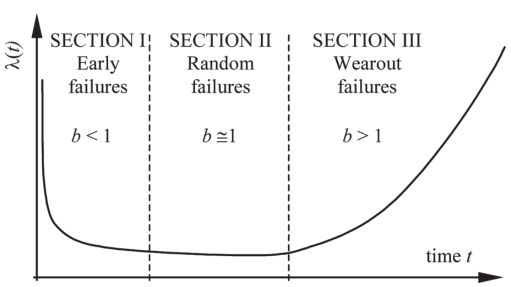


Figure 1. Failure rate λ (t) over component life time.

2.5 *Availability*

For a component which is repaired after failure or maintained the availability is used as parameter. The availability $A(t)$ is defined as the probability that a component is operating satisfactorily at time t (Bertsche 2008).

3 RELIABILITY CALCULATION OF ELECTRONIC COMPONENTS

According to IEEE (2003) component reliability is determined from field or test data, from physical failure modelling (physics of failure), or using so-called handbooks.

For reliability calculation of electronic components, handbooks are typically used (Koller et al. 2011). The handbooks calculate constant failure rates based on exponential distribution. The exponential distribution corresponds to a Weibull distribution with shape parameter $b = 1$. Therefore only random failures are described in section II of the bath tub curve, which are characterized by a constant failure rate.

Handbooks for predicting reliability list basic or fundamental failure rates for electronic components that have been obtained from empirical field or test data evaluations. The basic or fundamental failure rates are adjusted for the particular environmental conditions and individual loads on components using multiplicative or additive factors (Koller et al. 2011).

The first handbook for predicting reliability, now in widespread use, is the MIL-HDBK-217 standard (MIL-HDBK-217F Notice2 1991). It also uses field data to determine empirical failure rates and a multiplicative model for adjusting basic and fundamental failure rates to individual component loads. The model in the MIL-HDBK-217 standard assumes a linear relationship

$$\lambda_p = f(\lambda_b, \pi_1, \pi_2, \ldots, \pi_n) = \lambda_b \cdot \pi_1 \cdot \pi_2 \cdot \cdots \cdot \pi_n . \quad (7)$$

Here λ_p describes the predicted failure rate of the element, based on the individual load, λ_b describes the basic failure rate, and π_i describes the adjustment factors for the given boundary conditions. The adjustment factors take environmental factors such as the temperature and humidity into consideration. The individual loads, such as current flow or operating voltage, are also incorporated in the adjustment factors. In some cases, variables that describe load strength, such as component quality, are also included when setting the adjustment factors.

The adjustment factors for the active load are typically physically motivated and depend on just a single variable. To describe the temperature dependency of the failure rate, for example, the Arrhenius equation is used, see Equation 8 (MIL-HDBK-217F Notice2 1991). According to Arrhenius, this equation from physical chemistry describes the dependency of reaction speed on the temperature

$$k = A \cdot \exp\left(\frac{-E_A}{R\vartheta}\right). \quad (8)$$

The reaction speed constant k is calculated using the following parameters: A is a pre-exponential adjustment factor, E_A is the activation energy, R stands for the general gas constant, and ϑ is the absolute (thermodynamic) temperature. This Arrhenius equation is then used to define the adjustment factor that describes the temperature dependency of the failure rate. The adjustment factor (MIL-HDBK-217F Notice2 1991) from Equation 9 thus includes the failure rate acceleration factor between an increase in temperature ϑ and the failure rate λ

$$\pi_\vartheta(\vartheta) = \exp\left(-\frac{E_A}{R}\left(\frac{1}{\vartheta[°C] + 273.15K} - \frac{1}{298K}\right)\right). \quad (9)$$

The activation energy E_A is parameterized using field failure data. As can be seen in Equation 9, the temperature adjustment factor takes on the value 1 for a temperature of $T = 298$ K. This corresponds to the temperature at which the basic failure rate was determined.

When using handbooks for reliability analysis, a common criticism is that the calculation has a high level of uncertainty. An investigation in (Jensen 1995) of the calculation of the failure rate for a 64 K memory module showed that failure rates calculated using 5 different handbooks varied by a factor of 6.

Failure rates in the handbooks typically have no direct relationship to a physical damage mechanism. As a rule, several damage mechanisms may actually be summarized in one failure rate (Poech 2010). For this reason, a reliability calculation based on handbooks cannot provide any deeper understanding of the damage mechanisms in the product, and it is difficult to derive any potential optimizations in the development process. Rather, this reliability calculation is based on purely empirical relationships.

4 ELECTRONIC COMPONENTS WITH TIME-DEPENDENT FAILURE RATE

Chapter 3 showed that reliability analyses of electronic components typically use handbooks.

They assume constant failure rates. Using the example of a physically motivated approach for determining the reliability of a power module and an electrolytic capacitor, it will be examined whether this approach is universally valid.

4.1 *Power modules*

Power modules are integrated in electric and hybrid vehicles, for example, in order to connect the transistors of the power electronics to the heat sinks. The use of power modules is typical for power levels above one kilowatt (Hensler 2012). Power modules have electrical, mechanical, and thermal functions. The silicon chip, the bonds, and the copper layer form the electrical circuit. This electrical circuit is insulated from the rest of the module by means of an electrical insulator (typically ceramic). The insulation is applied to a heat spreader that ensures that heat is distributed uniformly within the module and that the heat is thus dissipated away from the chip. The heat spreader is typically made of copper and also provides mechanical stabilization. It is connected to the heat sink by a so-called thermal grease, and the heat sink in turn is cooled by means of a cooling medium (air or liquid).

The principle configuration of a power module is shown in Figure 2.

4.1.1 *Physics of failure*

Because the power modules contain materials with different thermal expansion coefficients, cyclical warming and cooling of the component during operation causes mechanical stresses induced by thermal strain in and between the individual connection layers. For the example of an application in electric and hybrid vehicles, the temperature cycles arise due to brief, intense currents in the power modules, such as during the recuperation processes, when vehicle braking energy is converted to supply to the vehicle electrical system. Figure 3 shows an example of the temperature increases of a hybrid vehicle in the New European Driving Cycle (NEDC).

Because of this cyclical thermal load, the solder layers can be considered as critical layers, because they are typically located between two materials with different thermal expansion coefficients and have to compensate for the stresses that arise. Because these stresses that occur will inevitably lead to crack formation and ultimately to failure over the life of the component, the fatigue strength and thus the reliability of the power module plays a decisive role.

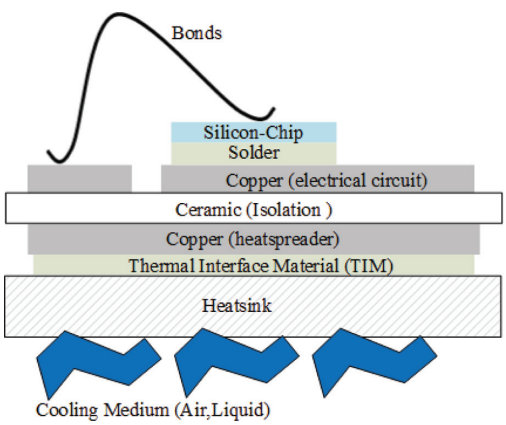


Figure 2. Configuration of a power module.

4.1.2 *Exemplary results*

In (Lutz et al. 2011), tests of the reliability of these power modules were performed and published. Five repeat tests were performed for a load level at a defined temperature rise. The failure data from this test were used to perform a Weibull analysis of the failure data. The result of the Weibull analysis is shown in Figure 4.

When evaluating the failure data shown in Figure 4, the resulting shape parameter is between

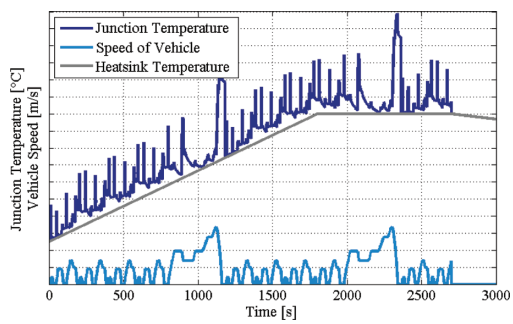


Figure 3. Junction temperature curve for a hybrid vehicle.

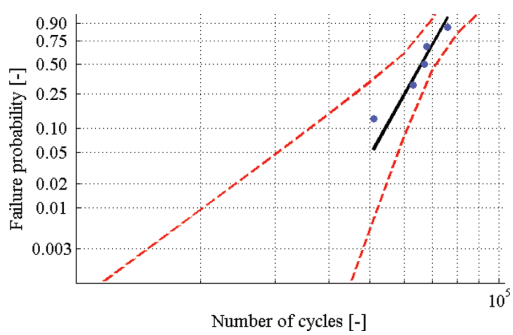


Figure 4. Failure data of a transistor on a power module.

$b = 4.49$ and $b = 10.49$ using a confidence interval of 90%. For a confidence level of 50% a shape parameter of $b = 6.86$ was determined. The shape parameter is significantly greater than the shape parameter of $b = 1$ used in the handbooks.

4.2 *Electrolytic capacitors*

Other experiments on the physical failure behaviour of electronic components have had similar results regarding their failure behaviour (Gerling 2011).

In (Perisse et al. 2004) the failure behaviour of aluminium electrolytic capacitors was investigated. The results showed, that the reliability calculation by using the exponential distribution subject to major inaccuracies. The use of the Weibull distribution with a shape parameter greater than 1 provides significantly better results.

The physics of failure is related to the time-dependent evaporation of the electrolyte. This evaporation process depends on several parameters like voltage, current and temperature (Perisse et al. 2004).

The result of the regression using the Weibull distribution is shown in Figure 5. The resulting shape parameter is between $b = 2.06$ and $b = 4.32$ using a confidence interval of 90%. For a confidence level of 50% a shape parameter of $b = 2.98$ was determined.

4.3 *Concluding remarks*

The physics of failure of both exemplary electronic components showed that the dominant failure mode had a significantly increasing failure rate. The root cause of such a failure mode can be either caused by cyclic thermal load or by forces based on electromagnetic or electrostatic phenomena. The root cause leads to cyclic stresses in the material or to micro movements e.g. micro bending. A cyclic bending leads to stresses in the material as well.

A similar situation can be observed for the packaging. Here e.g. mechanical vibrations of the application can lead to movements of the circuit board or of individual components. Mechanical stresses are consequently induced in the materials of the packaging. Sensitive elements are the bonding wires and the solder connections.

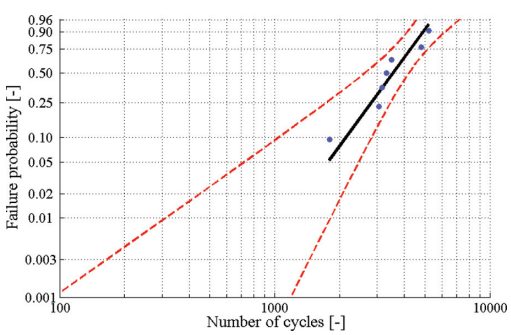


Figure 5. Failure data of an electrolytic capacitor.

These cyclic mechanical stresses lead to fatigue or ageing of the concerned materials. Crack formation or wear-out is a typical failure mode that can be observed. These failure modes are common if mechanical components are considered. This does not surprise as the principle failure mechanism is purely on the material mechanical side.

This demonstrates that the assumption of an exponential failure behaviour is permissible only for a small section of the component life which is characterized by a constant failure rate, the so-called 'useful life' (Denson 2006). In no way can the general assumption be made that the failure behaviour of electronic components can principally be modelled by a constant failure rate.

Rather, for reliability analysis of electronic components all significant failure modes need to be considered. On the one hand there are the failure modes based on electrical overstress which normally indeed show a constant failure rate. But on the other hand there are mechanical failure modes of parts inside the electronic component or its packaging which exhibit an increasing failure rate, i.e. a time-dependent failure rate.

5 CONSEQUENCES

The use of a time-dependent failure rate instead of using a constant failure rate has wide-ranging consequences. Subsequently, several topics are given to illustrate the influence of the time-dependent failure rate. It is assumed that the failure behaviour with time dependent failure rate is described by a Weibull distribution (see section 2.3). In the following sections the situation with constant failure rate is given first. Then the situation with time-dependent failure rate is described. The principal effects are illustrated by varying the shape parameter from $b = 1$ (i.e. constant failure rate) as a reference over $b = 2$, 3, 4 up to 5 (i.e. increasing time-dependent failure rates).

5.1 *Influence on specification*

For a constant failure rate, the specification can be done by two parameters:

- expected value *MTTF or*
- constant failure rate λ

Both parameters are equivalent as there is a fix relation between them, as described by Equation 4.

For a time-dependent failure rate, the specification is quite different. Subsequently, two principal situations are explained.

5.1.1 *Identical MTTF*

Given that the same expected value *MTTF* shall be specified for a component with time-dependent failure rate this would lead to the following consequences, as shown in Figure 6 for an exemplary *MTTF* of 50,000 h. As a reference the dotted line for $b = 1$ shows the corresponding constant failure rate of $2 \cdot 10^{-5}$ 1/h. For values of $b > 1$, the increasing failure rate can be observed. Compared to the constant case, for small life times the failure rate is below the reference value. But for life times at around *MTTF* or higher, the failure rate can be significantly higher. At *MTTF* for $b = 5$ the resulting failure rate is approximately 3 times higher compared to the reference rate. This can be potentially critical.

5.1.2 *Maximum failure rate*

The specification parameter *MTTF* is only useful for constant failure rates as the risk of failure is constant as well. With an increasing failure rate *MTTF* only describes the expected value, but not the distribution of the risk of failure. Therefore, it can be necessary to specify a maximum risk of failure, as shown in Figure 7.

Given that the same maximum failure rate shall be kept until time 50,000 h, in this example the value of $\lambda = 2 \cdot 10^{-5}$ 1/h, it will lead to different scale parameters T for the Weibull distribution and different expected values *MTTF* as well.

Figure 8 shows that for the given assumption, the *MTTF* of the Weibull distributions with $b = 2$ and higher are considerably higher than the *MTTF* for the constant failure rate. That means for the same maximum failure rate a more demanding *MTTF* would need to be specified.

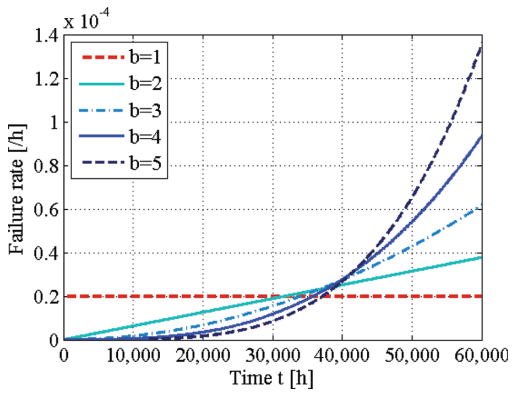


Figure 6. Failure rates for different shape parameters (with identical *MTTF* = 50,000 h).

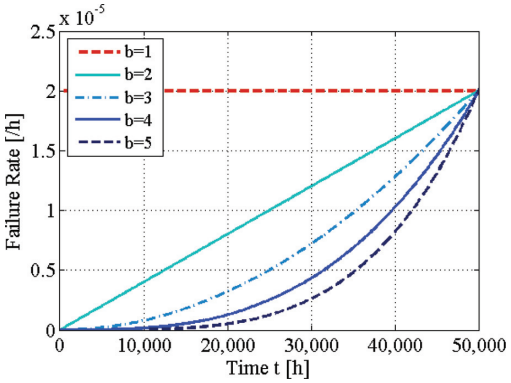


Figure 7. Different failure rate progressions (with identical maximum failure rate at 50,000 h).

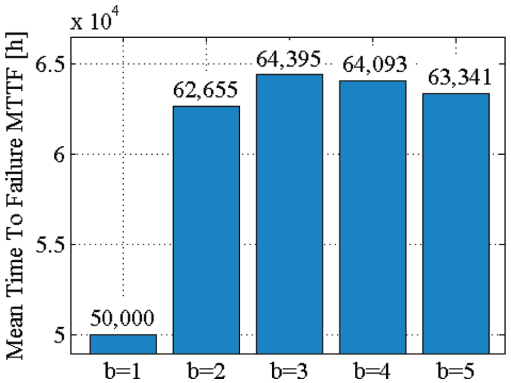


Figure 8. *MTTF* for different shape parameters (with identical maximum failure rate at 50,000 h).

5.1.3 *Influence on B_x life time*

The failure probability at the life time specified with the parameter *MTTF* is 63.2% for a constant failure rate (i.e. Weibull shape parameter $b = 1$) or approximately 50% for an increasing failure rate (e.g. Weibull shape parameter $b = 3.5$). That means, at this time half (or even more than the half) of the component's population are expected to be failed. Because of this, the *MTTF* as a specification parameter is often criticized.

Therefore, the B_x life time is applied as appropriate specification parameter, which defines the time at which a failure probability of x % is reached. Depending on the application a specification of a B_1, B_5 or B_{10} value is common. It is assumed that the same failure probability of 63.2% shall be reached at time 50,000 h. Figure 9 shows the corresponding failure probability distributions $F(t)$ for shape parameter b = 1, 2, 3, 4 and 5. It can be seen that the failure probability of 10% is

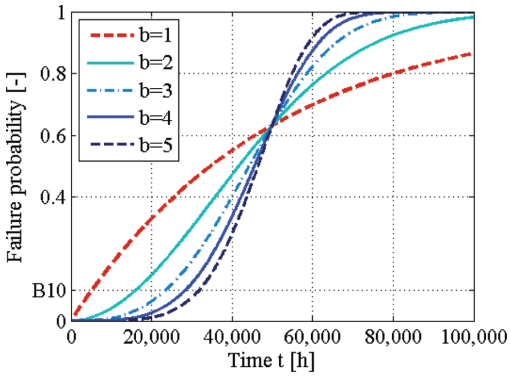


Figure 9. Influence of shape parameter b on B_{10} life time.

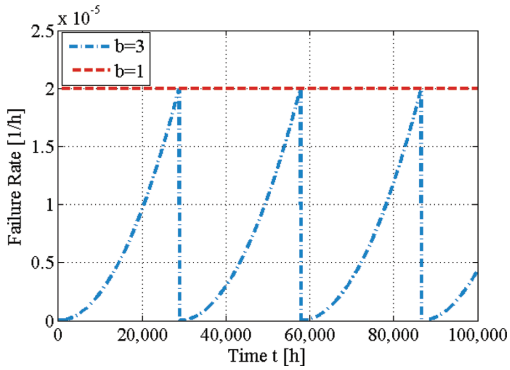


Figure 10. Limiting the failure rate by preventive maintenance.

reached at different life times depending on the shape parameter.

For $b = 1$ the B_{10} life time of 5,268 h is relatively low. In comparison the B_{10} life time of 31,879 h for $b = 5$ is high. It can be seen that the spread of the B_{10} life times is significantly high. That means, for increasing b the B_{10} life time specification is higher under these conditions.

5.2 *Influence on preventive maintenance*

For components with constant failure rate there is no benefit by performing preventive maintenance actions, if the maintenance action is the replacement of an old by a new component. As a new component has the same failure rate as a component which is operated for many hours, the risk to fail in a specific time interval stays the same.

For components with increasing failure rates, the situation is quite different. Here, replacing a component by a new one has an influence on the failure rate. Two principal situations are possible.

5.2.1 *Limiting the failure rate*

The replacement interval can be determined in order to keep the time-dependent failure rate within a specific limit. This strategy is shown in Figure 10 for a component with a Weibull distributed failure behaviour with shape parameter $b = 3$ and scale parameter $T = 50{,}000$ h. Here, a replacement interval of $T_{PM} = 29{,}000$ h is limiting the failure rate up to $2 \cdot 10^{-5}$ 1/h.

5.2.2 *Limiting the failure probability*

The replacement interval can be determined in order to keep the failure probability within a specific limit. This strategy is shown in Figure 11 for a component with a Weibull distributed failure behaviour with shape parameter $b = 3$ and scale parameter $T = 50{,}000$ h. Here, a replacement interval of $T_{PM} = 16{,}667$ h is limiting the failure probability to 20% within the intended operation time of 100,000 h.

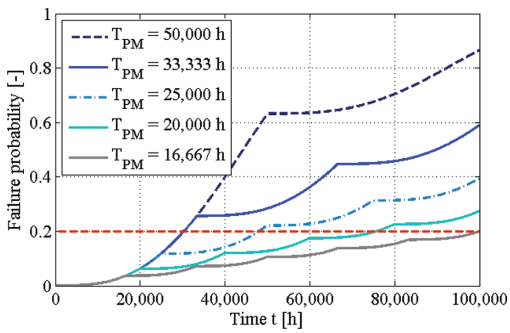


Figure 11. Limiting the failure probability by preventive maintenance.

5.3 *Influence on functional safety*

The standards for functional safety (e.g. ISO 26262 2011) define a maximum level of unsafety, so-called Safety Integrity Levels (SIL), which is tolerated for a specific level of danger. As the malfunction of electronic components can also contribute to the level of unsafety, an increasing failure rate would lead to an exceeding of the SIL over life time. This situation is illustrated in Figure 12. A component with constant failure rate is constantly within the SIL, whereas the increasing failure rate leads to an exceeding of this limit.

Here, two countermeasures should be considered in the specification. The specification of a maximum component failure rate (according to section 5.1.2) in order to fulfil the SIL within the intended product life time might be necessary.

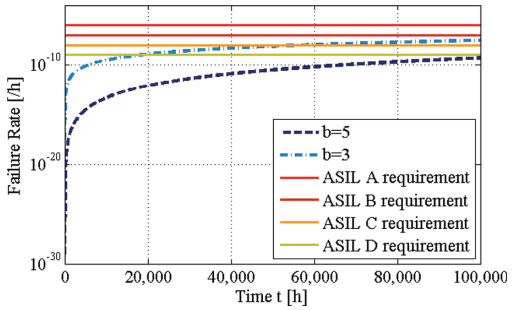


Figure 12. Influence of shape parameter b on functional safety (T = 1,000,000 h); Requirements from ISO 26262.

Alternatively, the specification of preventive maintenance in order to keep the failure rate within the necessary level might be considered (according to section 5.2.1).

5.4 *Influence on procedure to calculate the component availability*

Taking reparable systems into account, where a failed component is repaired and then set into operation again, the availability is used as the relevant parameter.

Assuming constant rates for failure and repair behaviour, the availability can be specified based on the Markov process. Often the calculation is based on an analytical solution.

If time-dependent failure and repair rates need to be considered, the Markov process is no longer applicable. Then, other methods like renewal process (Fritz et al. 2000) or even Petri nets (Zeiler & Bertsche 2013) need to be used. These methods are typically analysed by numerical or simulation based procedures.

6 CONCLUSIONS

For reliability calculation of electronic components, handbooks are typically used. The calculation shows a high level of uncertainty and usually has no direct relationship to a physical damage mechanism. Moreover, the calculation procedure assumes constant failure rates.

A power module (integrated in electric and hybrid vehicles) and an electrolytic capacitor were used to examine whether this assumption is universally valid. The physics of failure of both exemplary electronic components showed that the dominant failure mode had a significantly increasing failure rate. Even though these are electronic components it was explained that finally cyclic mechanical stresses prevail which lead to fatigue or ageing of the component material or the packaging. Crack formation or wear-out is then the typical failure mode which can be observed.

This demonstrates that the general assumption of constant failure rate for electronic components is not permissible. Moreover, beside the failure modes based on electronic physics of failure the failure modes based on mechanical physics of failure needs to be considered.

Several consequences of a time-dependent failure rate were presented. The commonly used specification parameters for electronic components—the failure rate or the *MTTF* value—are no longer applicable or provide dramatically misleading specifications. This was shown by investigating the influence of different increasing failure rates on the reliability and safety characteristics. A more appropriate specification parameter for components with time-dependent failure rates was defined. Specifying preventive maintenance is able to limit the increasing failure rate or to guarantee a maximum failure probability. For functional safety, an increasing failure rate can lead to an exceeding of the safety integrity level. This can be avoided by either appropriate component specification or by applying preventive maintenance. The specification of the component availability requires different methods compared to them applicable for constant failure rates. Based on these specifications a correct and safe application of electronic components can be ensured.

REFERENCES

Bertsche, B. 2008. *Reliability in Automotive and Mechanical Engineering*. Berlin Heidelberg: Springer.

Denson, W. (2006). *Reliability Modeling: The RIAC Guide to Reliability Prediction, Assessment and Estimation*. RIAC, Department of Defence, ISBN 1933904178, 9781933904177.

Fritz, A.; Pozsgai, P. & Bertsche, B. 2000. Notes on the Analytic Description and Numerical Calculation of the Time Dependent Availability. In Nikulin, M.; Limnios, N. (eds.): *Proc. International Conference on Mathematical Methods in Reliability (MMR 2000)*, July 4–7 2000, Bordeaux, France, pp. 413–416.

Gerling 2011. *Reliability of Power Electronic Systems: Securing the reliability of power electronic systems during design*, ECPE Tutorial, Bordeaux.

Hensler, A. 2012. *Lastwechselfestigkeit der Leistungselektronik bei Sperrschichttemperaturen bis zu 200°C für den Einsatz in Hybridfahrzeugen (Power cycling capability of power electronics for junction-temperatures up to 200°C for use in hybrid vehicles)*, Dissertation, Technische Universität Chemnitz.

IEEE-Guide 2003. *IEEE Guide for selecting and using reliability prediction based on IEEE 1413*.

ISO 26262 2011. International standard ISO 26262: Road vehicles—Functional Safety. International Organisation for Standardization.

Jensen, F 1995. *Electronic Component Reliability*. Chichester: Wiley.

Koller, O.; Jazdi, N.; Göhner, P.; Hipp, U.; Liedtke, T. & Mayer, A. 2011. *Ausfallraten unter Feldbedingungen berechnen—Ein Werkzeug auf Basis des Part-Stress-Modells (Calculation of failure rates under field conditions—a tool based on the Part-stress model)*, atp-edition 10/2011. pp. 36–43.

Lutz, J.; Schlangenotto H.; Scheuermann, U. & De Doncker, R. 2011. *Semiconductor Power Devices: Physics, Characteristics, Reliability*. Heidelberg Dordrecht, London, New York: Springer.

MIL-HDBK-217F Notice2 1991. *Military Handbook—Reliability Prediction of Electronic Equipment*, United States of America—Department of Defence.

Perisse, F.; Venet P. & Rojat G. 2004. *Reliability determination of aluminium electrolytic capacitors by the mean of various methods*. Application to the protection systems of the LHC., Microelectronics Reliability 44 (2004) pp. 1757–1762.

Poech, M. 2010. *Test und Zuverlässigkeit von Leistungsmodulen: Belastungsanalyse und Lebensdauerprognose (Testing and reliability of power modules: stress analysis and life time prediction)*, Kompetenzzentrum Leistungselektronik Schleswig-Holstein, Fraunhofer ISIT.

Zeiler, P. & Bertsche. B. 2013. Performance and Risk Based Service Development by means of RAMS+C Modelling and Analysis. In: *Proceedings of European Safety and Reliability Conference (ESREL) 2013*, 29th September–2nd October 2013, Amsterdam, The Netherlands.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Availability and reliability evaluation of systems periodically maintained

N. Hu, J. Huang, Ch. Yang, Y. Zheng & O. Dong
China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou, China

ABSTRACT: Availability and reliability evaluation of redundant systems under periodic maintenance is one of the difficulties in the field of reliability engineering. In order to overcome the disadvantages of existing evaluation methods, an instantaneous availability analytic approach for such systems is deduced, considering fault detection rate, fault isolation rate and repair rate. Limitations of this approach are discussed. Furthermore, a simulation model is devised to accomplish the evaluation of instantaneous availability and MTBCF. The validity of this simulation method is proved. And a simulation tool for availability and reliability evaluation of redundant systems periodically maintained is developed with MATLAB. At last, a case is studied.

1 INTRODUCTION

Redundancy design is an effective method to improve system availability and reliability, which is always used in the design of large and complex equipment. Redundancy is designed to enhance systems' ability to complete required functions, and to satisfy the demands of availability and mission reliability. However, maintenance is an important and essential guarantee for the long-running operation of redundant systems. As time goes by, the full potential on availability and reliability of such systems can only be reached through multiple maintenance and repair. Otherwise, the availability and reliability will both degrade ceaselessly; afterwards the systems will develop into non-redundancy, and finally breakdown.

For some large and redundant systems, such as space stations and unattended radars on islands, the most popular and appropriate maintenance policy is periodic maintenance. For the demonstration and design of these systems, availability and reliability evaluation under periodic maintenance needs to be solved first.

So far, studies related to availability and reliability evaluation of redundant systems with repairs are mostly aimed at on-condition maintenance (RADC-TR-77-287 1977, Chen 2007, Liu & Song 2010, and some of the references therein). In especial, Markov chains (Liang & Zhang 2011), Petri nets (Yuan 2011) and their extended models are widely used. Semi-Markov chains (Li 2013) and DSPNs (Deterministic and Stochastic Petri Nets, Yuan 2011) provide feasible ideas for the modeling of systems periodically maintained. But there are still some problems remain to be solved when evaluating system availability and reliability with them, for examples, the mathematical description of waiting time form failure occurrence to the next maintenance, and the algorithms for instantaneous availability and system MTBCF (mean time between critical failures).

Concerning the evaluation of systems periodically maintained there are only a few papers. Chen (1997) built the evaluation model for both availability and MTBCF of systems under periodic maintenance. Zhao et al. (2004) studied the approximation algorithm for MTBCF, based on the assumption that reliability function of systems periodically maintained could be regarded as exponential distribution with constant failure rate and reasonable error. Nicholls (2005) deduced the accurate algorithm for MTBCF of systems periodically maintained. However, these studies are all based on the assumption that all faults could be repaired successfully within a period of time. The fact is that any fault in complex systems needs to be detected, isolated, and then fixed. Each of the three steps is with a probability of success rather than inevitable event. The probabilities, namely FDR (Fault Detection Rate), FIR (fault isolation rate) and RR (repair rate), are all between 0 and 1 in engineering practice. In this case the above research findings will be not applicable any more.

The propose of this paper is to build the availability and reliability evaluation model of systems periodically maintained, concerning FDR, FIR and RR. The limitations of analytical algorithm are discussed, and a simulation model is devised to accomplish the availability and reliability evaluation of redundant systems under periodic maintenance. The validity of this simulation method is proved. Then, a simulation tool for the evaluation is developed with MATLAB.

2 AVAILABILITY MODELING OF SYSTEMS PERIODICALLY MAINTAINED

2.1 *System model and assumptions*

Systems definition: It is supposed that a redundant system contains n units. The instantaneous availability of which are independent but follow the same exponential distribution ($A(t) = e^{-\lambda t}$, where t = the failure rate of each unit. Note that the probability that a unit or system without maintenance is able to perform its mission at time t equals to the probability that it is able to perform its mission for a stated period of time [0, t]—that is the instantaneous availability equals to the reliability). The system is workable when at least k units are in operation without failures. Maintenance interval is constant T_0. And fault detection rate is supposed to be *FDR*; fault isolation rate equals *FIR*; repair rate equals *RR*. Maintenance time is negligible.

Without regard to maintenance, the instantaneous availability model of redundant systems could be easily obtained according to system reliability algorithm. For example, the instantaneous availability function of k/n(G) voting systems composed of n same units is

$$A_S(t) = \sum_{i=k}^{n} C_n^i (A(t))^i (1 - A(t))^{n-i} \quad (1)$$

where $A(t)$ = instantaneous availability of a unit; and $A_S(t)$ = instantaneous availability of the system.

In accordance with equation (1), if we can get the instantaneous availability $A^*(t)$ of a unit periodically maintained, then instantaneous availability of the system $A_S^*(t)$ could also be calculated.

2.2 *Availability modeling of units under periodic maintenance*

Under the condition of periodic maintenance, the states of a unit may develop as Figure 1. The availability of a unit in each maintenance period could be calculated according to the developing path.

Maintenance is generally divided into three steps: fault detection, fault isolation and repair. In order to simplify the calculation, the probability of a unit to be repaired well could be expressed as the product of the probabilities of success of each step:

$$P = FDR * FIR * RR \quad (2)$$

In the first maintenance period, $t \in [0, T_0)$; maintenance is not yet involved, and the instantaneous availability of the unit equals to

$$A^*(t) = e^{-\lambda t} \quad (3)$$

In the second maintenance period, $t \in [T_0, 2T_0)$; there are two available paths leading the unit state to be workable: (1) the unit worked until time t without failures; (2) the unit failed in the first maintenance period, and repaired (at T_0) to work

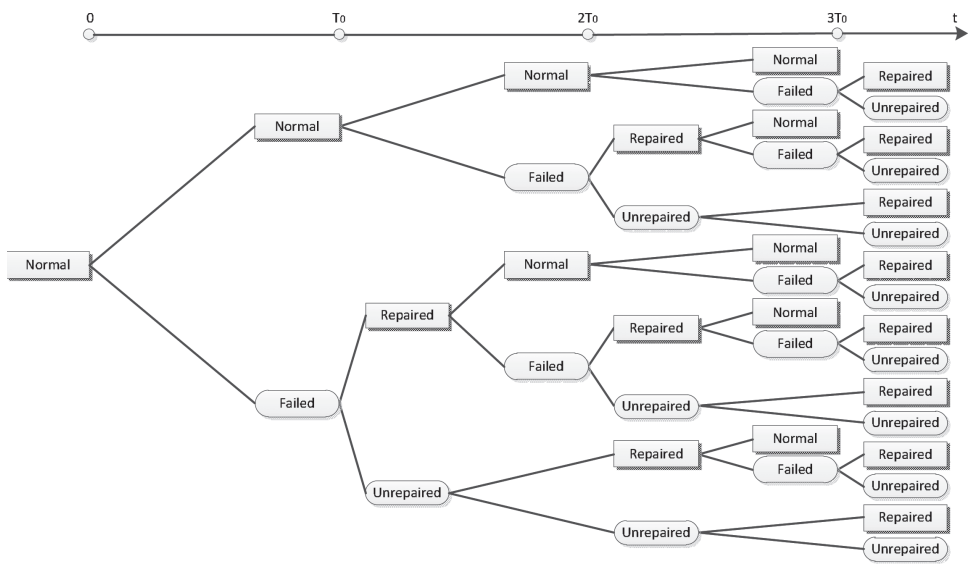


Figure 1. States developing paths of a unit under periodic maintenance.

until time t. So the instantaneous availability of the unit equals to

$$A^*(t) = e^{-\lambda t} + (1 - e^{-\lambda T_0}) * P * e^{-\lambda(t-T_0)} = e^{-\lambda t}[1 + P(e^{\lambda T_0} - 1)] \quad (4)$$

In the third maintenance period, $t \in [2T_0, 3T_0)$; there are five available paths leading the unit state to be workable: (1) the unit worked until time t without failures; (2) the unit failed in the second maintenance period, and repaired (at $2T_0$) to work until time t; (3) the unit failed in the first maintenance period, and repaired (at T_0) to work until time t; (4) the unit failed in the first maintenance period, and repaired (at T_0) to fail in the second maintenance period, and repaired (at $2T_0$) to work until time t; (5) the unit failed in the first maintenance period, but repaired in the second maintenance period (at $2T_0$), and worked until time t. So the instantaneous availability of the unit equals to

$$A^*(t) = e^{-\lambda t}\{[1 + P(e^{\lambda T_0} - 1)]^2 + P(1-P)e^{\lambda T_0}(e^{\lambda T_0} - 1)\} \quad (5)$$

Analogously, in the fourth maintenance period, $t \in [3T_0, 4T_0)$; there are thirteen available paths leading the unit state to be workable. And the instantaneous availability of the unit equals to

$$A^*(t) = e^{-\lambda t}\{[1 + P(e^{\lambda T_0} - 1)]^3 + P(1-P)e^{\lambda T_0}(e^{\lambda T_0} - 1)(1 - P + 2e^{\lambda T_0})\} \quad (6)$$

This can be proved that the number of workable states of a unit under periodic maintenance will increase following exponential distribution with time, and the instantaneous availability of a unit approximately appears as periodic changes. As a result, it is not practical to calculate the instantaneous availability of a unit in each maintenance period, but when $t \in [4T_0, +\infty)$, the instantaneous availability of a unit in each maintenance period could be regard approximately as the same distribution within the maintenance period $t \in [3T_0, 4T_0)$.

2.3 *Availability modeling of systems periodically maintained and its limitations*

The unit states developing paths under periodic maintenance have been described in the above chapter, and the piecewise function of instantaneous availability of a unit has been built. Combine the piecewise function with equation (1), the instantaneous availability of redundant systems could be obtained as follows:

$$A_S^*(t) = \sum_{i=k}^{n} C_n^i (A^*(t))^i (1 - A^*(t))^{n-i} \quad (7)$$

However, besides the deviation introduced by approximate treatment, the above calculating method also bears the following weaknesses:

1. The calculating method could only calculate instantaneous availability of the system, but not MTBCF.
2. When the number of redundant units is too large, the combinatorial number in equation (7) could easily become too large to calculate. For example, a phased array radar may contains tens of thousands of components, and less than 10% of component failures are permitted for the radar working state. Using MATLAB (R2012a), we can obtain that $C_{10000}^{9866} \approx 2.0501 \times 10^{307}$, but larger combinatorial number would become incomputable.

Calculating methods has been greatly limited in practical applications because of its weaknesses analyzed above. A simulation method will be devised to accomplish the availability and reliability evaluation of redundant systems periodically maintained.

3 AVAILABILITY AND RELIABILITY SIMULATIONS OF SYSTEMS PERIODICALLY MAINTAINED

3.1 *Simulation inputs*

The inputs of this simulation model contain information on three aspects:

1. System information: *n* represents the number of units; *MTBF* (mean time between failures) represents the mean lifetime of units; *k* represents the number of essential working units for the redundant system.
2. Maintenance policy: T_0 represents repair interval; *FDR* represents fault detection rate; *FIR* represents fault isolation rate; *RR* represents repair rate.
3. Simulation set-up: *TT* represents task time; *m* represents the number of simulation.

3.2 *Simulation outputs*

The outputs of this simulation model mainly contain instantaneous availability of the system and MTBCF, which are defined as follows:

1. Instantaneous availability of the system $A_S^*(t)$: the probability that redundant system is in workable state at time *TT*, namely the probability that the number of workable units is not smaller than *k* at time *TT*.
2. MTBCF: the mean task time between critical failures (the number of workable units is smaller than *k*) of the redundant system.

3.3 *Simulation process*

A simulation method will be introduced in this passage to generate the state sequence of the redundant system in the mission time. In the sequence, 1 represents that redundant system is in workable state; 0 represents that system is in failed state. The time intervals among system failures could be obtained through the state sequence, and the mean of such time intervals could be regarded as MTBCF if the sequence is long enough. Through large amount of simulations, the frequency ratio of the redundant system in workable state at each moment could be regard as instantaneous availability of the system. The simulation process is depicted in Figure 2, and the main procedures are as follows:

1. Generate a random number according to exponential distribution the mean of which is MTBF as a lifetime of the unit.
2. Remark the unit state as 1 within the life cycle; remark the unit state as 0 till the next repair cycle.
3. At the beginning of the next repair period, generate a random number between 0 and 1, remarked as pp.
4. If pp ≤ P (P = FDR * FIR * RR), the unit is successfully repaired, and return to (1).
5. If pp > P, the unit is not successfully repaired this time. Remark the unit state as 0 till the next repair cycle, and return to (3) until the full state sequence of the unit in mission time has been generated.
6. Repeat (1)~(5) until the state sequence of n units have all been generated.
7. According to k and the state sequences of n units, generate the state sequence of redundant system; calculate MTBCF.
8. Repeat (1)~(7) until m groups of simulations have been done. Calculate instantaneous availability of the system according to the frequency ratio of the redundant system in workable state at each moment.

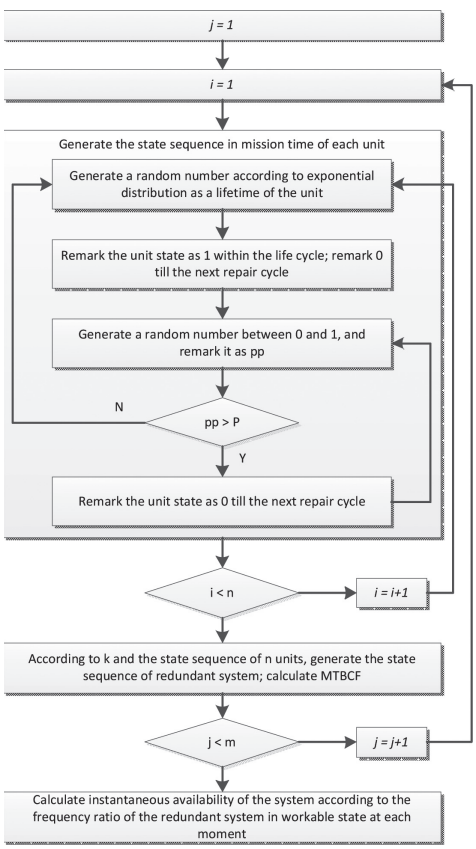


Figure 2. Availability and reliability simulation process of systems periodically maintained.

3.4 *Proving of simulation model*

As for small-scale redundant systems, the instantaneous availability under periodic maintenance could be obtained by calculating method introduced before. An 11/12(G) voting system is to be discussed. Through comparing simulation results with computing results, the validity of this simulation method could be proved.

Model parameters are set up as follows:

$n = 12$, $MTBF = 80{,}000$ h,
$k = 11$, $T_T = 20{,}000$ h,
$T_0 = 2160$ h, $FDR = 0.98$,
$FIR = 1$, $RR = 0.97$,
$m = 10{,}000$.

The results of system reliability obtained from the two methods are depicted in Figure 3. The red curve repeats system reliability using the calculating method introduced before, and the blue one repeats system reliability obtained from simulation method. These two curves basically coincide

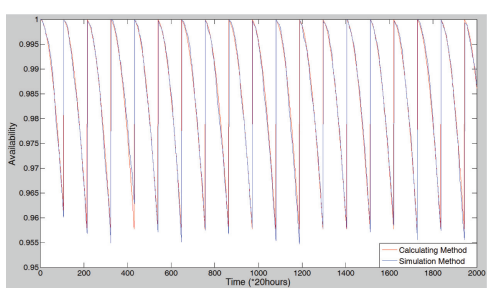


Figure 3. Instantaneous availability of a system obtained from calculating and simulation methods.

with each other. This illustrates the consistency of the two methods. Through further analysis, the maximum relative error between the results is calculated to be 1.6055%. Thus, the simulation model is proved to be correct and applicative.

4 CASE STUDY

Towed array sonar is a system of hydrophones towed behind a submarine or a surface ship on a cable. It mainly consists of a source array and a receiver array. In order to ensure its detection range and positioning accuracy, the source array is always hundreds of meters long and contains thousands of similar components.

Supposing that a source array of sonar contains 1000 components, and 10% component failures are allowable. The lifetime of each component follows a same exponential distribution, the mean of which is 20,000 hours. The source array works 24 hours a day without closing down. MTBCF of the source array is demanded to be 35,000 hours in the contract. If maintenance personnel repair the source array every three months; *FDR*, *FIR* and *RR* are all supposed to be 0.98, does the source array satisfy its demand on MTBCF?

Applying the availability and reliability simulation approach for redundant systems periodically maintained, a simulation tool is developed, the interface of which is depicted in Figure 4. Set 1000 times of simulation, the instantaneous availability distribution of the source array is obtained, as shown in Figure 5, and the MTBCF equals to

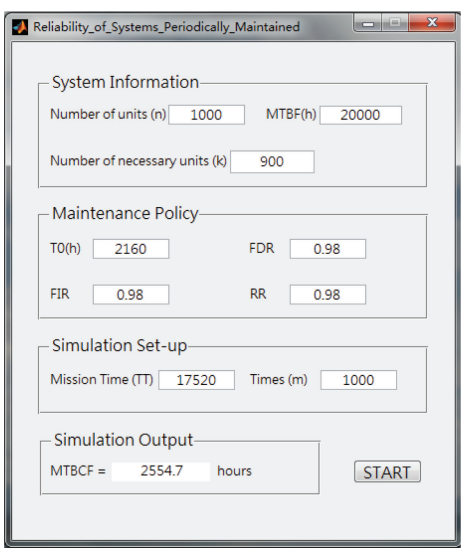


Figure 4. Simulation interface.

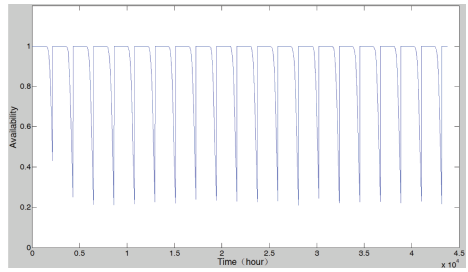


Figure 5. The instantaneous availability distribution of the source array in the first five years.

Table 1. MTBCF of the source array with different periodic maintenance interval (T_0).

Periodic maintenance interval (day)	MTBCF (hour)
90	2554.7
85	3388.6
80	5573
75	12,289
70	39,105
65	181,580

2554.7 hours. Apparently, this does not satisfy the demand of design.

In order to increase MTBCF of the source array to satisfy its designing demand, system design and/or maintenance policy need to be modified. Generally there are four doable solutions: (1) design or purchase components with higher reliability (to get larger unit *MTBF*); (2) increase the number of redundant components (to get larger n); (3) improve maintenance level (to get larger *FDR*, *FIR* and/or *RR*); (4) shorten periodic maintenance interval (to get smaller T_0).

At a later developmental stage, changing system design is always difficult and costly; the aim of specified MTBCF could be achieved through shortening periodic maintenance interval without any other changes. Using the simulation tool (Fig. 4) MTBCF of the source array with different periodic maintenance interval (T_0) could be easily obtained, as depicted in Table 1.

As shown in Table 1, it could be concluded that when the repair cycle is short than 70 days, the MTBCF of the source array will be larger than 35,000 hours, and there are still a tolerance of 11.73%. In this way, the designing demand will be satisfied properly.

$$\frac{39{,}105-35{,}000}{35{,}000}\times 100\% \approx 11.73 \tag{8}$$

5 CONCLUSION

An analytic and a simulation approaches are presented in this paper. Both of the approaches are aimed at solving the problem of availability and reliability evaluation of redundant systems under periodic maintenance, considering fault detection rate, fault isolation rate and repair rate. Using the simulation tool we have developed, instantaneous availability and MTBCF of the system could be easily obtained, which are of great significance for designers to make and optimize the maintenance policy. The simulation efficiency would be raised in further application to shorten the simulation time.

REFERENCES

Chen, H.C., 1997. The reliability calculation of complex electronic systems under periodic maintenance. *Electronic product reliability and environmental test*, 4: 2–5.

Chen, L., 2007. Research on the reliability model of repairable redundant systems. Lanzhou University of Technology, Lanzhou.

Li, J., 2013. Bearing performance degradation assessment based on continuous hidden semi-Markov model. South China University of Technology, Guangzhou.

Liang, L.D. & Zhang, M.Y., 2011. Reliability analysis of four-component cold maintainable Markov system with priority. Journal of Sichuan University of Science & Engineering (Natural Science Edition), 24(3): 292–295.

Liu, Q.H. & Song, N.Z., 2010. Reliability, Maintainability and logistic support—Life cycle methods. Beijing: Electronic industry press.

Nicholls, D., 2005. System Reliability Toolkit. Reliability Information Analysis Center.

RADC-TR-77-287, 1977. A Redundancy Notebook, Rome Laboratory.

Yuan, J.M., 2011. Reliability modeling and intelligent analysis methods of complex systems with Petri nets. Beijing: National defense industry press.

Zhao, J.C. et al., 2004. The estimate error of periodically maintained systems. *Modern electronic engineering*, 2: 89–92.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability and safety based design of lifesaving appliances systems

Z. Burciu
Gdynia Maritime University, Poland

ABSTRACT: Life boats and liferafts are the lifesaving appliances used on all types of vessels. Liferafts are the most popular due to their low weight and low space demands. However they are used for the dozens of years their operational characteristics did not change a lot. The main improvements are the lighter materials and better constructions of boarding platform for easier entry of survivors from the water. The paper presents a new approach to design of the elements of liferaft system based on the liferaft reliability and safety functions developed on the basis of model and real scale investigations.

1 INTRODUCTION

1.1 *Backgound*

The liferafts are the most popular lifesaving appliances used on board all types of floating units—from the largest offshore installations and merchant vessels to the sport yachts and leisure boats. They are used in advanced Maritime Evacuation Systems on passenger ships with thousands people on board.

The serious accidents at sea are always related to the necessity of making decision to abandon ship, taking into consideration the real chances of survivors (Burciu, 2011; Gerigk, 2004; Gerigk, 2005; Gerigk, 2006; Gerigk, 2008; Gerigk 2012). Even in calm weather and in coastal or harbour waters the accidents can happen (Abramowicz-Gerigk, 2005; Abramowicz-Gerigk, 2006; Abramowicz-Gerigk, 2008; Abramowicz-Gerigk & Burciu, 2013), in case of extensive fire or hull damage due to collision the people on board have to leave the vessel.

In cases of sudden disasters, when there is no time to launch any lifesaving appliances the only available means of protection for the survivors are the liferafts, which can be launched automatically from 4–8 m depth, by the hydrostatic release system.

There are several problems with liferafts operation, which can be solved changing the recently used traditional approach to the design into the reliability and safety based approach (Abramowicz-Gerigk & Burciu, 2012).

1.2 *General requirements*

The liferafts are used for the dozens of years however their operational characteristics did not change a lot. The main improvements allowed decreasing their weight and increasing insulation to give better thermal protection of the survivors on board.

This situation is mainly caused by the general assumption that liferaft should be not expensive and commonly available, meeting the rules of the International Life Saving Appliances Code (LSA), Convention for Safety of Life at Sea (SOLAS, 2008; IMO Resolution MSC. 48(66), 1996) and European Union standards (EU Directive of Marine Equipment 96/98/EC, 1996).

The practical result is that the survivors in real sea conditions have serious problems to get into the liferaft from the water, liferafts lose their stability in wind and waves (Hervey & Jordan, 1990, www.surviteczodiak, 2013; Standards for Life Rafts and Inflatable Rescue Platforms, 1992) and it is not possible to predict their leeway due to their shape and flexible construction of the canopy.

The general requirements for liferafts comprise:

– design and construction of buoyancy part,
– canopy,
– canopy supports,
– capacity and mass.

All materials and components used in the construction and repair of liferafts shall be weather resistant. A liferaft shall withstanding exposure for 30 days afloat in all sea conditions and shall be able to withstand 15 months on board ship with a minimum of protection. It should withstand dropping into the water from a height of 18 m. A floating liferaft shall be capable of withstanding jumps onto it from a height of at least 4 m above its floor and towing at a speed of 3 knots in calm water when is fully loaded.

Every liferaft shall have a canopy. The canopy should be automatically set in place when the liferaft is launched. The canopy shall provide:

– insulation against heat and cold;

– one entrance for a liferafts designed to accommodate eight or less persons and two diametrically opposed entrances for the others;
– entrance shall be clearly indicated and be provided with a closing arrangement;
– sufficient ventilation inside;
– viewing port;
– means for collecting rain water;
– headroom under all parts of the canopy for occupants to sit comfortably upright on the floor.

Canopies should have supports; they are mainly the inflatable arches. Capacity and mass of an approved liferaft shall have a carrying capacity of six or more persons but no more than fifty persons, except in special cases.

The total mass of a liferaft, not designed to be launched, its container and its equipment shall not be greater than 185 kg.

There are no remarks with respect to the stability and motion characteristics, which have the biggest influence on the success of Search and Rescue Action at sea.

2 PERFORMANCE OF LIFESAVING APPLIANCES DURING SEARCH AND RESCUE ACTION AT SEA

2.1 *Reliability of liferaft*

The success of search and rescue action at sea is dependent on the time to rescue the survivors and on the type and condition of lifesaving appliances available to be used by survivors.

Search and rescue action at sea can be carried out during the day and at night. Time of search action is the basic reliability parameter, describing possibility to rescue survivors.

The reliability of *SAR* system is defined as follows:

$$R_{SAR} = P\left(S_p \geq T_D\right) \tag{1}$$

where R_{SAR} = reliability of *SAR* system; T_D = time of rescue action; and S_p = time to survive for the search object.

With respect to the International Life-Saving Appliances Code, Chapter IV (SOLAS, 1980) every liferaft should be constructed in the way it can withstand 30 days in all sea conditions.

$$R_{tr}(30) = P\left(t_p \geq 30\right) \tag{2}$$

where $R_{tr}(30)$ = reliability of liferaft; t_p = time of operation without failure.

The operational reliability of a liferaft can be defined as a characteristic informing whether it fulfils live saving functions in the given hydrometeorological conditions.

To define the reliability function for the liferaft a random variable Z denoting limit wind velocity for the liferaft have been introduced (Burciu & Grabski, 2011). The value of the liferaft reliability function for wind speed x is given by the formula:

$$R(x) = P\left(Z > x\right) \tag{3}$$

where $R(x)$ = is the liferaft reliability; Z = is the maximum wind velocity with respect to liferaft safety, x = is the wind velocity.

Applying the relation of functions gamma and beta we can obtain:

$$f_Z(x) = \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}}{3^{\alpha_1}2^{\alpha_2}B(\alpha_1,\alpha_2)} \frac{x^{\alpha_2-1}}{\left(\frac{\lambda_1}{3}+\frac{\lambda_2}{2}x\right)^{\alpha_1+\alpha_2}}, \quad x>0 \tag{4}$$

Density of distribution of the random variable Z, which can be interpreted as 'limiting safe' wind velocity for the liferaft can be formulated. Function $R(x)$:

$$R(x) = P\left(Z > x\right) = 1 - \int_0^x f_z(z)dz$$
$$= 1 - \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}}{3^{\alpha_1}2^{\alpha_2}B(\alpha_1,\alpha_2)} \int_0^x \frac{z^{\alpha_2-1}}{\left(\frac{\lambda_1}{3}+\frac{\lambda_2}{2}z\right)^{\alpha_1+\alpha_2}}dz \quad z>0$$

is the reliability function of the liferaft.

Values of reliability function for 6, 10 and 20 person's liferafts without sea anchor (drogue) (Burciu & Grabski, 2011, Burciu Z. 2012) are presented in Table 1.

2.2 *Design parameters and elements influencing liferaft safety and reliability*

The basic elements influencing liferaft reliability and safety of the survivors on board are:

– construction parameters: size—dimension and capacity, shape of underwater part and canopy, ballast system, shape and position of canopy supports,
– operational parameters:
  • trim of the liferaft,
  • non-linearity of the wind coefficients,
  • air pressure in buoyancy chambers,
  • number and position of the occupants.

The lack of the significant changes in the construction of liferafts is mainly caused by the limited

Table 1. Values of reliability function for 6, 10 and 20 persons liferafts without drogue.

Wind speed x [knots]	Liferaft 6-1 $R(x)$	Liferaft 6-6 $R(x)$	Liferaft 10-1 $R(x)$
40	0.999996	0.9999999	0.9999999
44	0.9991	0.9999997	0.999997
48	0.9712	0.99992	0.99957
52	0.7785	0.9962	0.9864
56	0.3895	0.9474	0.8774
60	0.1046	0.7405	0.5742
64	0.0151	0.3945	0.2342
Wind speed x [knots]	Liferaft 10-10 $R(x)$	Liferaft 20-2 $R(x)$	Liferaft 20-20 $R(x)$
40	0.99999999	0.9957	0.9993
44	0.99999991	0.9012	0.9688
48	0.99997	0.5234	0.7368
52	0.9980	0.1417	0.3092
56	0.9673	0.0170	0.0611
60	0.8073	0.0009	0.0058
64	0.4824	0.00003	0.0003



Figure 1. Trials of the liferaft leeway conduced in real working conditions.

requirements and satisfactory results of the trials performed only in calm sea conditions.

Figure 1 presents the field investigations on the liferaft leeway—trials carried out in real sea conditions.

The results of the field experiments carried out at Gdynia Maritime University in real sea conditions showed that search and detection of liferafts are very difficult. The reasons of the obstructions are liferaft construction, shape, construction materials, equipment and colour of the canopy.

A. Construction characteristics

All the currently produced and purchased liferafts are diverse with respect to their size, shape, construction solutions, including:

– entrance openings,
– landing platforms,
– ladders,
– ballast systems—ballast chambers or pockets.

The basic elements of a liferaft are presented in Figure 2.

The elements of a liferaft influencing leeway and reliability of a liferaft are presented in Figure 3.

B. Material characteristics

The traditional liferaft is made of rubber and impregnated fabric, which are very good dielectrics. This is the reason they are almost invisible on the screen of the navigational radar.

There are several types of passive radars reflectors used to increase the reflective characteristics of a liferaft. The folded reflectors can be unfolded automatically or manually (Polish liferafts) and installed on the canopy, after the liferaft is launched.

This means that the possibility of liferaft detection is dependent mainly on the applied or not radar reflector, its technical parameters—mainly the effective reflection area and its proper installation on the liferaft canopy.



Figure 2. A liferaft with a canopy, drogue and ballast system.

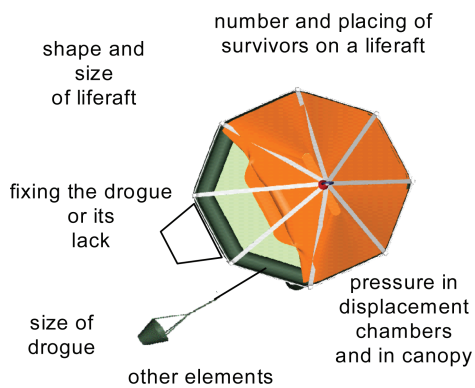


Figure 3. Elements influencing leeway/reliability of a liferaft.

The liferaft echo and disturbances from waves visible in the navigational radar display, on board a ship is presented in Figure 4.

The maximum range of liferaft detection very seldom exceeds the distance of 0.5 ÷ 0.6 Nm (Nautical mile). At the sea state 8 due to the intensive disturbances from the waves they are not visible.

The diagram in Figure 5 presents the trim of 6 persons liferaft with 10% of occupants.

Trim of the liferaft is defined as the list angle measured between the liferaft axis on the direction of liferaft motion and line perpendicular to the water surface.

The lack of the stiffened floor, drop of the pressure inside the liferaft causes the change of liferaft floor shape, trim to the leeward side and in case the liferaft sea anchor is not deployed or has broken off—loss of stability and keel of.

The shape and size of liferaft are the reasons of non-linearity of aerodynamic coefficients, causing the unpredictable leeway divergent from wind direction.

The non-linear aerodynamic coefficients in the stream layout, influencing the errors of leeway direction determined in wind tunnel for 6—persons liferaft at wind speed 10 m/s (20 knots) is presented in Figure 6.

The flexible inflatable liferaft construction and material characteristics are the main reasons of serious difficulties in liferaft operation by survivors. The operational obstructions for the survivors can be classified as follows:

– constructional: difficulties to get into the liferaft from the water, insufficient thermal protection, difficulties with bailing out the water from the liferaft,
– applied materials: difficult or even impossible radar detection,
– outfitting in radar reflector: the existed radar reflectors have to small effective reflecting surface, decreasing the probability of search object detection.

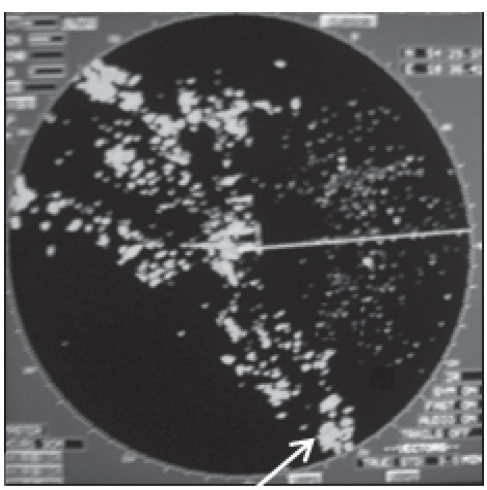


Figure 4. Radiolocation signal—radar echo of a liferaft and disturbances from waves presented in the navigational radar display on board ship.

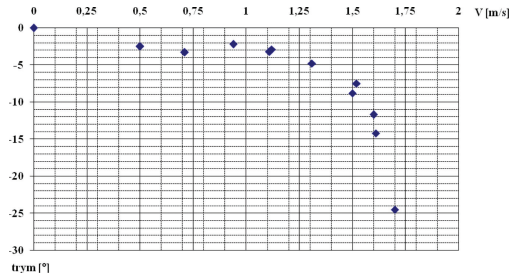


Figure 5. Trim of 6—persons liferaft with 10% occupancy.

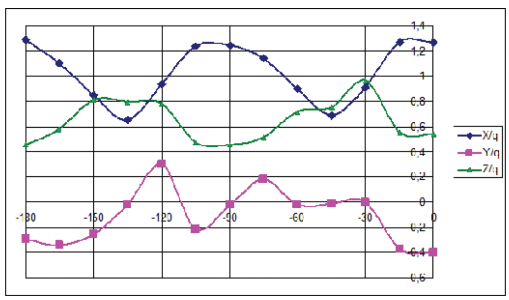


Figure 6. Diagram of non-linear aerodynamic coefficients in the stream layout, influencing the errors of leeway direction determined in wind tunnel for 6—persons liferaft at wind speed 10 m/s (20 knots).

The described elements and characteristics of the liferaft decrease the reliability function of the liferaft. Safety and reliability enhancement should be obtained using safety and reliability based approach in liferaft design.

3 DESIGN SOLUTIONS INCREASING SAFETY AND RELIABILITY OF LIFERAFT

The proposed design solutions increasing liferaft detection and operational standards are as follows:

– equipment increasing liferaft signature in all ranges of detection: NIR, VIS, LIR and radar, with use of the most advanced materials and technologies,

– application of coatings with high reflection characteristics influencing visual detection,
– elimination of disturbances in the wind leeway by the new design of liferaft shape, decreasing the aerodynamic resistance,
– drainage system allowing to keep dry floor inside the liferaft,
– entrance lock,
– efficient ballast system,
– new solution of marine anchor—construction and fastening to the liferaft,
– new solution of non flexible liferaft floor for better stability and thermal protection of survivors.

4 CONCLUSIONS

The results of the research conducted are as follows:

– lack of the canopy and not full (not sufficient) internal pressure result in an increase of trim of the liferaft in the downwind direction,
– flooding of the liferaft occurs at a 6 person liferaft occupied by 3 up to 6 persons, when the pressure is lower than the operational value,
– the liferaft trim increases with an increase of the number of persons onboard the liferaft,
– low pressure in the liferaft floor increases the angle of flooding of the liferaft.

The proposed solutions will increase the safety of survivors using the liferaft and increase liferaft reliability:

– decrease of hydrodynamic resistance,
– reduction of non-linearity of aero dynamical coefficient in stream layout influencing the errors of leeway direction,
– easier entrance to the liferaft—elastic lock,
– decrease of survivor contact with water and influence of low temperature—inflatable floor,
– increase of range of detection with different types of detectors:
  • radiolocation means,
  • infra-red cameras,
  • optical day light cameras.

REFERENCES

Abramowicz-Gerigk T., 2005. Investigation on Standards for Ship Manoeuvring Performance at Slow Speed in Constrained Space. in C. Guedes Soares, Y. Garbatow & N. Fonesca (eds.), Maritime Transportation and Exploitation of Ocean and Coastal Resources. Vessels for Maritime Transportation. Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean (IMAM'2005), Lizbona, Portugalia, Vol. 1: 3–8. London, Balkema.

Abramowicz-Gerigk T., 2006. Determination of Safety Factors for Ship Berthing Operations. in C. Guedes Soares & E. Zio (eds.), Safety and Reliability for Managing Risk. Proceedings of the European Safety and Reliability Conference 2006 (ESREL'2006), Estoril, Vol. 3: 2737–2742. London, Balkema.

Abramowicz-Gerigk T., 2008. The risk analysis of harbour operations. in S. Martorell, C. Guedes Soares & Julie Barnet (eds.) Safety Reliability and Risk Analysis: Theory, Methods and Applications. Proceedings of the ESREL 2008 and 17th SRA-Europe Conference, Valencia, Vol. 4: 33343–3350, London: Balkema.

Abramowicz-Gerigk T. & Burciu Z., 2012. Analysis of Safety Requirements for Large Offshore Units Evacuation Systems. LSA safety function. Archives of Transport VOL. XXIV NO 4.

Abramowicz-Gerigk T. & Burciu Z., 2013. Safety assessment of maritime transport—Bayesian risk-based approach in different fields of maritime transport. in C. Guedes Soares, & F. Lopez Pena (eds.) Developments in Maritime Transportation and Exploitation of Sea Resources. Proc. 15th Int. Congress of the International Maritime Association of the Mediterranean (IMAM'2013), A Coruna, Vol. 2: 699–704, London: Balkema.

Burciu Z., 2003 Modelowanie obszarów poszukiwania w aspekcie bezpieczeństwa transport ludzi na morzu, ISSN 1230-9265, Oficyna Wydawnicza Politechniki Warszawskiej. p. 128.

Burciu Z., 2012. Niezawodność akcji ratowniczej w transporcie morskim. ISBN 978-83-7207-994-7. Oficyna Wydawnicza Politechniki Warszawskiej. p. 284 J.

Burciu Z. & Grabski F., 2011. The experimental and theoretical study on the reliability of the life rafts. Reliability Engineering and System Safety, 96(2011), s. 1456–146.

EU Directive of Marine Equipment 96/98/EC, 1996.

Gerigk M., 2004. On a risk-based method for safety assessment of a ship in critical conditions at the preliminary design stage. *Polish Maritime Research*, No. 1 (39), Vol. 11, 8–13.

Gerigk M., 2005. Challenges of modern assessment of safety of ships in critical conditions. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the 12th International Congress of the International Maritime Association of the Mediterranean IMAM 2005,* Volume 2, Lisboa, Portugal, 26–30 September 2005, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 1529–1536.

Gerigk M., 2006. A method for assessing hazards, risks and safety of damaged ships at sea. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006),* Volume 3, Estoril, Portugal, 18–22 September 2006, Published by Taylor & Francis/Balkema, London/Leiden/New York/Philadelphia/Singapore, 2783–2790.

Gerigk M., 2008. Modeling of hazards, consequences and risk for safety assessment of ships in damaged conditions in operation. *Proceedings and Monographs in Engineering, Water and Earth Sciences. Proceedings of the European Safety and Reliability Conference, ESREL 2008 and 17th SRA-Europe,* Volume 4, Valencia, Spain, 22–25 September 2008, Published by CRC Press, Taylor & Francis Group, Balkema, Boca Raton/London/New York/Leiden, 3303–3310.

Gerigk M., 2012. Assessment of safety of ships after the collision and during the ship salvage using the matrix type risk model and uncertainties. in *Sustainable Maritime Transportation and Exploitation of Sea Resources. Proceedings of the 14th International Congress of the International Maritime Association of the Mediterranean (IMAM)*, Volume 2: 715–719, London: Balkema.

Hervey C.L. & Jordan D.J., 1990. Model tests of inflatable life rafts in breaking waves. *Final Report for U.S. Coast Guard. U.S. Department of Transportation, United States Coast Guard, Office of Engineering, Logistics, and Development,* Washington.

IMO Resolution MSC., 48(66). 1996. LifeSaving Applianced Code.

SOLAS'74, 1980. International Convention of Safety of Life at Sea. *International Maritime Organisation*.

Standards for Life Rafts and Inflatable Rescue Platforms, 1992. Marine Safety Directorate Transport Canada, Ottawa. www.surviteczodiac.com. 2013.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Nuclear power plant safety improvement with new system for safety injection

B. Gjorgiev & A. Volkanovski
Reactor Engineering Division, Jožef Stefan Institute, Ljubljana, Slovenia

ABSTRACT: Nuclear power plant safety depends on the actions taken to prevent nuclear and radiation accidents or to limit their consequences. This paper proposes improvements of nuclear power plants safety with consideration of a new system for safety injection. The system consists of water source, pipes, valves and portable fossil-fuel driven pump. Similar mitigation concept is the diverse and flexible coping capability strategy, or shortly known as FLEX, proposed by the US industry. The paper investigates the system capability to cope with the station blackout event and the large loss of coolant accident. Analyses are done with probabilistic safety assessment. The reference probabilistic safety assessment model of a nuclear power plant is modified in order to take into account additional system. The core damage frequency of the nuclear power plant probabilistic safety model is used as a risk measure. The new system is modelled using the fault tree approach with a top event defined as a possible failure to deliver water to the nuclear power plant. The obtained results show decrease of core damage frequency with the introduction of the proposed system. This finding indicates improvement of nuclear power plant safety.

1 INTRODUCTION

Nuclear Power Plant (NPP) safety depends on the actions taken to prevent nuclear and radiation accidents or to limit their consequences. The Probabilistic Safety Assessment (PSA) results show that the Station Blackout (SBO) event, implicated by complete loss of Alternate Current (AC) power in the NPP, is important for NPP safety (Volkanovski and Prošek, 2013). When SBO occurs one of the main challenges is to maintain effective decay heat removal. Another important safety event is the large loss of coolant accident (Large LOCA). The pressure and water in the primary loop are lost in few seconds in case of Large LOCA event. If no coolant is injected in the reactor core and no decay heat removal is established core damage is eminent.

A connection between NPP and different types of hydro power plant is proposed for NPP safety improvements (Gjorgiev et al., 2012, Gjorgiev et al., 2014). The hydro power plants are used as alternative AC power sources. The main objective of such source is the SBO event mitigation, i.e. provide cooling of the reactor core using electrical energy from alternative power supply. The results show significant decrease of the station blackout core damage frequency and significant decrease in total core damage frequency. For the performed analyses (Gjorgiev et al., 2012, Gjorgiev et al., 2014) the standard PSA methodology was used on systems which are non-safety classified and not located at the NPP site.

The US Nuclear Regulatory Commission (NRC) issued order EA-12-049 (U.S.NRC, 2012a) requiring nuclear power plants to develop mitigation strategies for beyond-design-basis external events, shortly known as FLEX. The nuclear industry in US, through the Nuclear Energy Institute (NEI), developed a generic framework for response to this order that is documented in the NEI FLEX Implementation Guide (NEI 12-06) (NEI, 2012). The FLEX represents an approach to develop flexible and diverse strategies for increased defense-in-depth by providing multiple, diverse methods to supply power and water to support key safety functions.

A new system for nuclear power plant safety improvement which consists of water source (off-site or on-site) and components for establishing connection with a nuclear power plant is proposed in this paper. For the connection a pipe under pressure is considered. To establish the required pressure both a portable gas-fired motor driven pump and gravity are used. Water reservoir or the nearest river can be considered as a source of water. In this paper for demonstrative purposes a water reservoir was selected as a source of water. The reservoir may be placed on-site or offsite as a part of on-river accumulation, i.e. hydro power plant reservoir or any other natural or manmade accumulation. Since the system has passive component

for water injection, it can be considered as partially passive system for injection of water in the primary or secondary reactor coolant side. The system is utilized in at least two scenarios. One is the loss of all offsite and onsite alternating current power supply, which is known as station blackout event. The other is the large loss of coolant accident (Large LOCA).

The main objective of this paper is to investigate the safety implications of the proposed system on a NPP. Probabilistic Safety Assessment (PSA) is used as tool for risk assessment. A PSA model of generation two NPP is used as a case study. The reference PSA model is modified in order to consider the proposed system. The change in core damage frequency is used as risk measure. The proposed system is modelled using the fault tree approach with a top event defined as a possible failure to deliver water to the nuclear power plant.

The changes of the NPP core damage frequency and the shares of the SBO and Large LOCA events are quantified. The effects of the proposed system on NPP safety are analyzed and discussed. The results show that the introduction of the new system in the NPP-PSA model improves NPP safety.

2 DESCRIPTION OF THE PROPOSED SYSTEM

2.1 *System configuration*

The proposed system for water injection in both the primary and secondary loop is presented with the schematic shown on Figure 1. The system as shown on Figure 1 is consisting of water source, pipes, portable fossil-fuel powered pump and valves. In order to satisfy the required conditions for work additional elements are considered as well. In this study water reservoir is considered as a source of water. The valves 1, 2, 3, 4 and 5 are identical. Valve 1 is continuously open, valves 2 and 3 are opened when the pump is used for water injection in the Steam Generators (SG), and valves 4 and 5 are opened when the water has to be injected in the primary coolant loop. The basic principle of the system shown in Figure 1 is that both, pump or gravity can be used as necessary force that drives the water from the reservoir towards nuclear power plant cooling systems. It is assumed that the portable pump is protected from the severe internal external events.

In this study the application of the proposed system for mitigation of two initiating events, SBO and Large LOCA, is analyzed. Figure 1 shows that two connections to the NPP systems are provided. Line 1 is used for the SBO event mitigation, while Line 2 is used for the Large LOCA mitigation.

When SBO occurs the cooling of the reactor core must continue in order to remove the decay heat. The proposed system is connected to the secondary loop, i.e. the steam generators through the same connection used by the Auxiliary Feedwater (AFW) system. After SBO occurs, valves that provide the connection with the secondary loop and the proposed system are opened. The system delivers cold water to the secondary side of the steam generators, this way allowing heat to be dissipated through the secondary side safety valves. In this scenario a certain pressure in the range of 80 bars (Volkanovski and Prošek, 2013) is required. This is the main reason for the application of the portable pump shown on Figure 1.

For Large LOCA mitigation, the proposed system is connected to the primary loop through the same connection used by the low pressure injection system. Water is directly injected in the primary coolant loop vessel by gravity.

2.2 *Potential issues and solutions*

During Large LOCA fresh non-borated water can cause increased reactivity when injected in

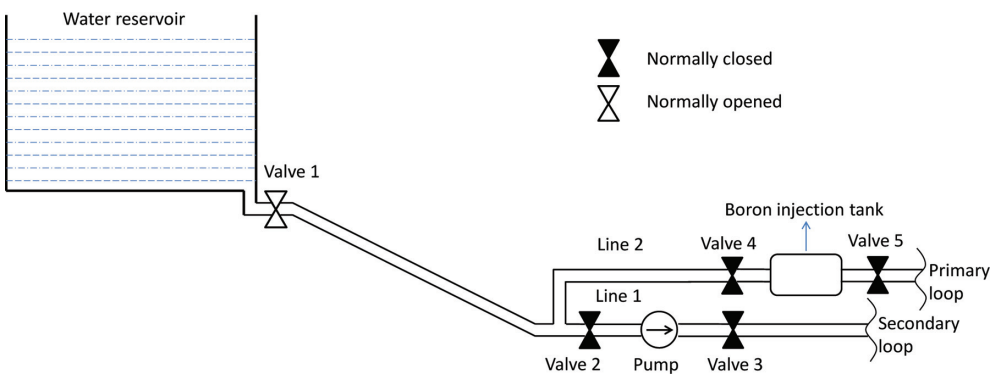


Figure 1. Schematic of the passive system and NPP connection.

the reactor core (U.S.NRC, 2012b). Therefore, the water from the system is borated before it is injected in the primary loop. One way to provide boron in the water is using tank as shown on Figure 1. The boron is directly diluted, i.e. carried by the water when it passes through the tank. This tank can be positioned near the joint were the connection between the proposed system and the installation of the low pressure injection system is established. It is assumed that the water temperature never falls beneath the minimal allowed temperature according to technical specifications (U.S.NRC, 2012b).

The uncontrolled water injection during SBO in a steam generator may result with overfill, which in turn may result in jeopardizing of steam generator integrity (U.S.NRC, 2012b). This issue also applies to any other system (e.g. FLEX) that can be used for residual heat removal through the steam generators when no power is available to monitor their water level. In this study is assumed that the amount of water and the time intervals in which the water is injected in the steam generators is known.

3 PROBABILISTIC SAFETY ASSESSMENT MODEL

PSA is a standard method for assessing, maintaining, assuring and improving the nuclear power plant safety (U.S.NRC, 1982, Roberts et al., 1981). It is generally used to find the weak points of a plant and to make recommendations for possible changes in design (Čepin, 2002). The traditional application of PSA for NPP safety evaluation in general considers only safety related systems which are located at the NPP site. In this paper The PSA model takes into consideration systems that are classified as non-safety systems. This modification allows PSA evaluation of changes in core damage frequency of an NPP when new systems that can be used in emergency scenarios such as SBO and Large LOCA are introduced.

3.1 *Reference nuclear power plant model*

The PSA model of a generation 2 Pressurized Water Reactors (PWR) was used in the analyses (Bertucio et al., 1990). The NPP model has two emergency diesel generators. The model considers only the internal initiating events. Figure 2 shows the share of the most dominant initiating events in the total CDF.

The first ten basic events identified with largest Fussell–Vesely (FV) importance measure in the reference PSA model are given in Table 1. The second column in Table 1 contains basic events with description given in third, unavailability in fourth column and FV importance measure given in fifth column.

Table 1 shows that the basic events FE-NRAC-HALFHR and FE-NRAC-7HR, both related to AC power restoration, are dominant contributors in the reference PSA model.

3.1.1 *Station blackout event tree*

The station blackout event tree is given on Figure 3. The SBO event tree contains all functional events of a representative SBO event tree for Westinghouse pressurized water reactors (Volkanovski and Prošek, 2013, Bertucio et al., 1990, U.S.NRC, 2005). Due to the phenomenology and possible special events that can occur, the station blackout is evaluated in separate event tree. Those special events include preservation of coolant inventory, controlled supply of feed water to

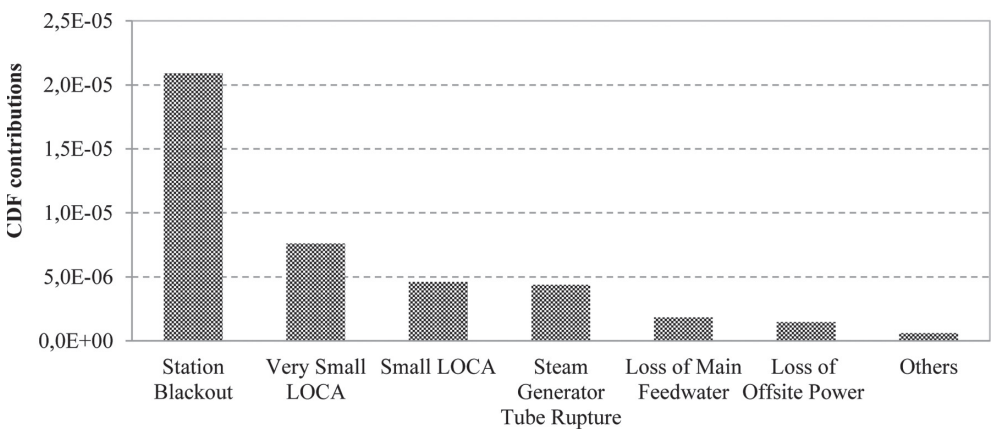


Figure 2. Schematic of the proposed system for safety injection.

Table 1. Basic events with largest FV in the reference PSA model.

No.	ID	Description	Nom. val	FV
1	FE-NRAC-HALFHR	Failure to recover AC power within 30 minutes	6.00E-01	2.90E-01
2	FE-NRAC-7HR	Failure to recover AC power within 7 hr	5.00E-02	2.82E-01
3	AFW-TDP-FR-2P6HR	AFW turbine-driven pump fails to run for 6 hr	3.00E-02	1.30E-01
4	HPI-XHE-FO-FDBLD	Operator failure to establish feed and bleed	7.10E-02	8.44E-02
5	SLOCA90MIN	Seal LOCA	3.50E-01	1.25E-01
6	FE-QS-SGTR	Failure of SG safety relive valves to reseat during SBO transient	2.70E-01	7.06E-02
7	AFW-CCF-LK-STMBD	Undetected leakage	1.00E-04	6.73E-02
8	HPI-CCF-FT-867CD	CCF of motor operated valves	2.60E-04	6.08E-02
9	HPI-CCF-FT-115BD	CCF of motor operated valves	2.60E-04	6.08E-02
10	AFW-TDP-FS-FW2	AFW turbine-driven pump fails to start	1.10E-02	5.53E-02

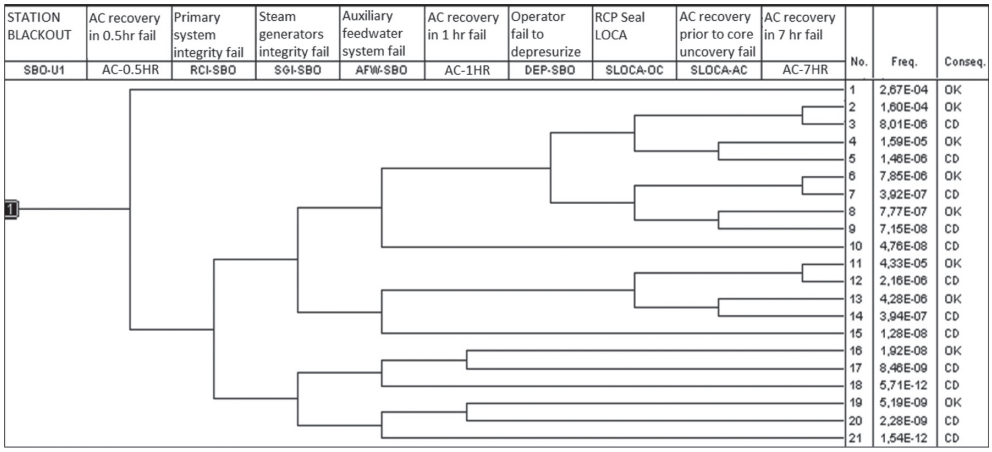


Figure 3. The SBO event tree for the reference PSA model.

the steam generators and extension of battery life (Volkanovski and Prošek, 2013, Bertucio et al., 1990). Successful reactor scram is being presumed when entering into the SBO event tree. Additionally, separate event tree considers the anticipated transients without scram.

The second functional event AC-0.5HR in the station blackout event tree is related to the restoration of electrical power to the plant safety buses before the dryout of the coolant on the secondary side of the steam generator, assessed from the wide range level, and start of the core heat up. Period of 30 min is assumed to be available for restoration of power in the PSA model for this functional event (Volkanovski and Prošek, 2013, Bertucio et al., 1990). The successful mitigation of the transient is related with power restoration within first 30 min results in successful mitigation of the transient, regardless of other failures, except criticality, in that time period.

The preservation of the reactor coolant system inventory until power is restored is related with the third functional event RCI-SBO. Loss Of Coolant Accident (LOCA) is being implicated by the failure to reclose the power operated relief valves. The importance of this functional demand is related with the failure probability of the power operated relief valves during SBO.

The fourth functional event SGI-SBO represents the secondary side integrity functional event. The reference PSA model (Bertucio et al., 1990) assumes inoperability of the atmospheric relief valves during station blackout due to the unavailability of control power. It is assumed that the safety valves will conduct the steam relief. Uncontrolled depressurization is implicated by the safety valves failure to reclose. This jeopardizes the steam generators integrity.

The probability of the auxiliary feedwater system failure during SBO, calculated with a

corresponding fault tree, is related with the fifth functional event AFW-SBO. The auxiliary feedwater fault tree comprises multiple failures of the auxiliary feedwater system during SBO including turbine-driven pump failure to start and operate, check valves failures, air operated valves failures and undetected leakage. The fault tree does not consider the motor operated pumps and their equipment since these pumps are not available during SBO.

The sixth functional event AC-1HR corresponds to the restoration of power to the plant safety busses and isolation by the pressurizer block valve before core uncover starts. In the reference PSA model, period of 1 h is taken (Volkanovski and Prošek, 2013, Bertucio et al., 1990) as an available time for power restoration.

The cooling and depressurization of the reactor coolant system during a long term station blackout is represented with the seventh functional event DEP-SBO. The goal of the depressurization is to reduce pressure and consequential reactor coolant system leak rate, in case any leak develops. Reactor coolant system pressure reduction as well as Seal LOCA risk decrease is achieved by depressurization. However, this reduction of Seal LOCA risk is not considered in the model.

The eighth functional event SLOCA-OC corresponds to the reactor coolant pumps Seal LOCA. While the ninth functional event, SLOCA-AC, corresponds to the Seal LOCA with failure to recover electrical power prior to core uncover.

The tenth functional events AC-7HR is related to the power restoration to the plant safety busses before core damage starts. In the reference PSA model, a period of 7 h is taken (Volkanovski and Prošek, 2013, Bertucio et al., 1990) as an available time for power restoration before core damage starts.

3.1.2 *Large LOCA event tree*

The Large LOCA event tree is given on Figure 4. The Large LOCA contains all functional events of a representative Large LOCA event tree for Westinghouse pressurized water reactors (Bertucio et al., 1990).

The second functional event D5 in the Large LOCA event tree is related to the injection of water from the accumulators in the primary loop. The water is injected immediately as the pressure in the reactor coolant system drops as a result of the large brake in the cooling system pressure boundary.

The third functional event D6 in the Large LOCA event tree is related to the capability of the Emergency Core Cooling Systems (ECCS) to respond early after the Large LOCA event occur, thus providing high volume, low pressure injection flow needed to cool the reactor core (Bertucio et al., 1990).

The forth functional event CS corresponds to the containment integrity, i.e. capability of the containment heat removal system to successfully maintain containment pressure and temperature at acceptable levels. While the fifth functional FE-CV event is related to the functionality of the emergency core cooling systems due to containment failure.

The sixth functional event H1-LH is related to the low pressure recalculation cooling. This system has to provide the volume of flow needed under large LOCA condition.

3.2 *PSA model with the proposed system*

As shown on Figure 1, there are two modes for operation of the proposed system. First mode is when the system is used for SBO mitigation. Second mode is when the system is used for Large LOCA mitigation. Two fault threes were created for modeling of the system failure in each mode of operation.

3.3 *Proposed system—NPP connection modelling*

3.3.1 *The SBO event tree modification*

The SBO event tree from Figure 3 was modified in order to consider the proposed system. The functional event ADD-SYS.SG was added between AFW-SBO and AC-1HR functional events as shown in Figure 5. The ADD-SYS.SG functional event corresponds to the delivery of water by the proposed system to at least one of the three steam generator during SBO.

The system is considered to be capable to deliver water to at least one steam generator for 72 hours. A new functional event AC-72 HR which corresponds to recovery of AC power in 72 hours is added as the last functional event in the SBO event tree. The failure of both, the AFW and the proposed system, results with core damage.

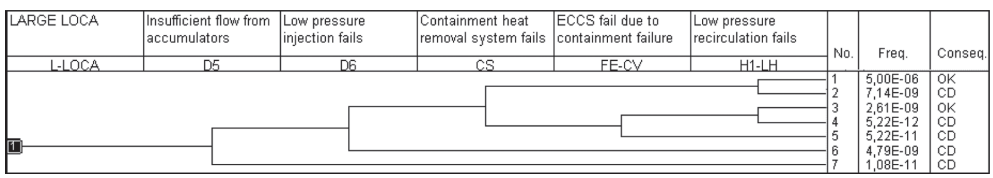


Figure 4. The Large LOCA event tree for the reference PSA model.

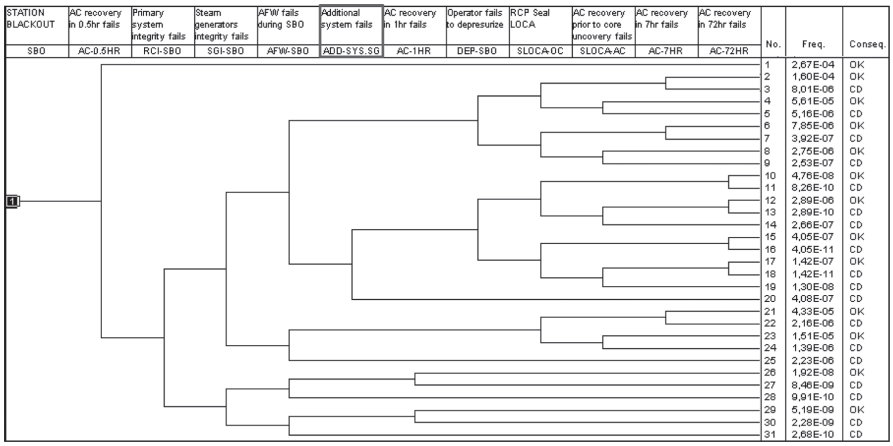


Figure 5. The SBO event tree, comprising the proposed system.

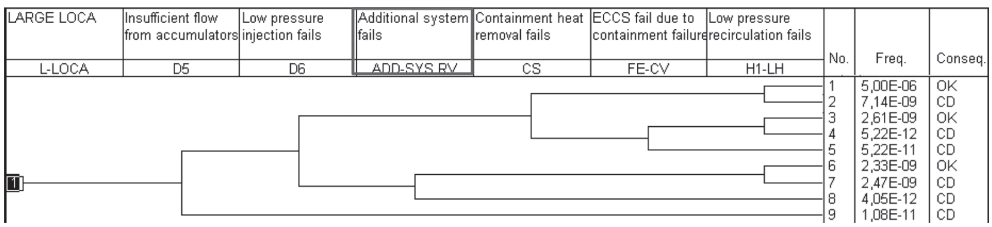


Figure 6. The Large LOCA event tree, comprising the proposed system.

Table 2. Reliability parameters of components used in the fault tree analysis.

Component failure mode	Unavailability [/]	Source
Pump failure to start	4.82E-2	(IAEA, 1988)
Pump failure to run	3.00E-5	(IAEA, 1988)
Pump operator failure	1.00E-3	(Bertucio et al., 1990)
Valve failure to stay open	6.18E-5	(IEEE, 1983)
Valve failure to close	4.24E-6	(IEEE, 1983)
Boron tank failure	6.43E-4	(IAEA, 1988)
Reservoir failure	1.00E-5	(Yan and Lan, 2013)
Pipe failure	1.00E-4	(Fleming and Lydell, 2004)

3.3.2 *The Large LOCA event tree modification*
The Large LOCA event tree (Fig. 4) was modified with the introduction of the ADD-SYS.RV functional event. As shown on Figure 6 the ADD-SYS. RV functional event was positioned between the D6 and CS functional events. The ADD-SYS.RV functional event corresponds to the delivery of water by the proposed system to the primary coolant system.

3.3.3 *Proposed system input data*
For the unavailability of the components of the proposed system two failure modes were considered: failure to remain in position and failure to change position. For the failure to remain in position mode the repairable parametric reliability model was used. For the failure to change position mode the per-demand reliability model was used. The reliability parameters are presented in Table 2.

4 ANALYSIS AND RESULTS

The results from the proposed system fault tree quantification analysis are shown in Table 3, where $Q_{ADS\text{-}SG}$ denotes the unavailability of the system used for SBO mitigation, while $Q_{ADS\text{-}RV}$ denotes the unavailability of the system used for Large LOCA mitigation.

The results from the CDF quantification are shown in Table 4. Table 4 shows that the Total CDF

Table 3. Top event probability.

	Top event unavailability
Fault tree for SBO mitigation (Q_{ADS-SG})	4.94E-02
Fault tree for Large LOCA mitigation (Q_{ADS-RV})	8.44E-04

Table 4. NPP–CDF quantification.

	Reference PSA model	PSA model with additional system	Relative difference [%]
Total CDF [/ry]	4.14E-05	3.61E-05	13
CDF (SBO) [/ry]	2.09E-05	1.55E-05	26
CDF (Large LOCA) [/ry]	1.19E-08	9.16E-09	23

Table 5. Basic events with largest FV in the PSA model with the additional system included.

No.	ID	Description	Nom. val.	FV
1	FE-NRAC-HALFHR	Failure to recover AC power within 30 minutes	6.00E-01	4.32E-01
2	FE-NRAC-7HR	Failure to recover AC power within 7 hours	5.00E-02	2.22E-01
3	FE-SLOCA-NRACSL-LT	Conditional probability of core uncover during SBO due to seal LOCA and no AC power	9.20E-02	1.43E-01
4	SLOCA90MIN	Seal LOCA	3.50E-01	1.43E-01
5	FE-QS-SGTR	Failure of SG safety relive valves to reseat during SBO transient	2.70E-01	8.11E-02
6	AFW-CCF-LK-STMBD	Undetected leakage	1.00E-04	7.70E-02
7	HPI-CCF-FT-867CD	CCF of motor operated valves	2.60E-04	6.98E-02
8	HPI-CCF-FT-115BD	CCF of motor operated valves	2.60E-04	6.98E-02
9	FE-QS-SBO	Failure of SG safety relive valves to reseat during SBO transient	2.70E-01	6.26E-02
10	AFW-TDP-FR-2P6HR	AFW turbine-driven pump fails to run for 6 hr	3.00E-02	5.91E-02

is reduced for 13% compared to the base model. Table 3 also shows that both the CDF (SBO) and CDF (Large LOCA) are reduced for 26% and 23% respectively with the introduction of the proposed system.

The identified first ten basic events with largest FV importance measure in the modified PSA model with the proposed system considered is given in Table 5.

Table 5 shows that the basic events FE-NRAC-HALFHR and FE-NRAC-7HR, both related to AC power restoration, remain dominant when the proposed system is introduced in the reference PSA model. The basic event FE-SLOCA-NRACSL-LT, related to core uncover during SBO due to seal LOCA, is becoming the third most dominant basic event according to FV importance measure as shown in Table 5. This event is not among the ten most important basic events in the reference PSA model as shown in Table 1. Table 5 shows the basic event AFW-TDP-FR-2P6HR, related to the AFW turbine-driven pump capability to run for 6 hr, has decreased importance when the new system is considered for coolant injection.

5 DISCUSSION

As observed from the obtained results when the new system for water injection is introduced in the PSA model of an NPP, the shares of the SBO and Large LOCA events in CDF are significantly reduced. The introduction of this system can be especially beneficial for NPPs that have large share of these two events in the total CDF.

6 CONCLUSIONS

New system for nuclear power plant safety improvement has been proposed. The system is consisted of water reservoir, pipes, portable fossil-fuel powered

pump and valves. It uses both, pump and gravity to inject the water in the nuclear power plant cooling systems.

The proposed system is connected with the primary coolant loop through the connection for low pressure injection systems and with the steam generator through the connection for the auxiliary feedwater system. In this study the proposed system is used for mitigation of SBO and Large LOCA initiating events. The core damage frequency of a nuclear power plant is used as a risk measure.

Probabilistic safety assessment model of a nuclear power plant was used for the analyses. The model is limited to the internal initiating events only. Fault tree models of the proposed system are made. The SBO and the Large LOCA event trees in the reference nuclear power plant model are modified with the introduction of the new system.

The results show decrease of the SBO and Large LOCA core damage frequencies. Subsequently this resulted with reduction of the total core damage frequency. The results show that the introduction of the new system contributes to improvement of nuclear power plant safety.

ACKNOWLEDGMENTS

This research was partly supported by the Slovenian Research Agency (research program P2-0026) and partly by the European Atomic Energy Community's (Euratom) Seventh Framework Programme FP7/2007–2011 under grant agreement No. 605001.

REFERENCES

Bertucio, R.C., Julius, J.A. & Cramond, W.R., 1990. Analysis of core damage frequency, *Surry, Unit 1 internal events appendices, NUREG/CR-4550*. pages 703.

Čepin, M., 2002. Optimization of safety equipment outages improves safety. *Reliability Engineering & System Safety,* 77(1): 71–80.

Fleming, K.N. & Lydell, B.O.Y., 2004. Database development and uncertainty treatment for estimating pipe failure rates and rupture frequencies. *Reliability Engineering & System Safety,* 86(3): 227–246.

Gjorgiev, B., Kančev, D. & Čepin, M., 2012. *A new perspective in nuclear power plant safety considering pumped-storage hydro plant.* 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, 5): 3705–3713.

Gjorgiev, B., Volkanovski, A., Kančev, D. & Čepin, M., 2014. Alternative off-site power supply improves nuclear power plant safety. *Annals of Nuclear Energy,* 71(0): 304–312.

IAEA (1988). *TECDOC-478, Component Reliability Data for Use in PSA.* Vienna.

IEEE (1983). *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*. IEEE Std 500-1984: 17–18.

NEI (2012). *Diverse and Flexible Coping Strategies (FLEX) Implementation Guide.* WASHINGTON, D.C.

Roberts, N.H., Vesely, W.E., Haasle, D.F. & Goldberg, F.F., 1981. *Fault Tree Handbook*, NUREG-0492, Washington.

U.S.NRC (1982). NUREG/CR-2300, *PRA Procedures Guide*. Washington.

U.S.NRC (2005). *Reevaluation of Station Blackout Risk at Nuclear Power Plants*, NUREG/CR 6890. Washington.

U.S.NRC (2012a). *Issuance of order to modify licences with regard to requirements for mitigation strategies for beyond-design-basis external events*. WASHINGTON, D.C.

U.S.NRC (2012b). *Standard Technical Specifications* Westinghouse Plants. Washington.

Volkanovski, A. & Prošek, A., 2013. *Extension of station blackout coping capability and implications on nuclear safety*. Nuclear Engineering and Design, 255(0): 16–27.

Yan, F. & Lan, Y. 2013. Probabilistic Slope Stability Analysis: The Case Study of a Deposit Slope in Hydropower Reservoir. *In: Digital Manufacturing and Automation* (ICDMA), 2013 Fourth International Conference on, 29–30 June 2013 2013. 948–951.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A systematic approach for defense against transient failures

H. Schäbe
TÜV Rheinland InterTraffic, Cologne, Germany

I. Shubinski
IBTrans., Moscow, Russia

ABSTRACT: Transient failures become more and more important because computer systems become smaller and it can be expected that a growing number of charged electric particles are able to penetrate Earth's weakening magnetic field. Charged particles cause transient failures in computer systems. A transient failure does not persist in the hardware but, however, can influence data and program flow. We describe the mechanisms that lead to transient failures. There exist many measures to protect safe computers from these influences. We provide a systematic method of defense against transient failures. The method is based on the idea to express the computing system as a Markov automate. Then, the method consists of two steps. In the first step, the system is expressed as a Markov automate and a method is applied to ensure that the present state cannot be changed by transient failures. For this purpose, checksums, self-correcting codes or saving redundant copies of the data can be used. In the second step, the transition between states is secured against transient failures. For this sake, repeated computing and protection of the software executing code against transient failures is applied. We demonstrate the approach with the help of an example. The approach helps to give a systematic approach to construct a system that is stable against transient failures. It needs to be noted, that the methods applied do not fully protect against systematic or persisting faults.

1 INTRODUCTION

Usually in the theory of reliability and safety of a lot of attention is dedicated to failures, especially to dangerous ones. However, apart from them, there are other events that seem to be much less important at first sight. These are transient failures (faults), see Shubinski (2012), Qi et al. (2008) and the references cited in Shubinski (2012). Transient failures are defined as follows. A functional transient failure is an event consisting of a unique distortion of information that is either processed or stored in an information processing and transmitting system under the influence of interior or exterior destabilizing influences (e.g. noise) Shubinski (2012).

Current standards on railway safety as EN 50128 or IEEE 1483 name them or require some countermeasures which do not necessarily cover transient failures completely. ISO 26262-109 names transient faults and describes, how they should be accounted for in reliability and safety calculations. But the standards do not give a systematic approach against transient failures or provide a deeper discussion on the causes and nature of transient faults.

Research has been carried out on many specific problems connected with transient faults. We cite here only the dissertations by Xiaobin (2005) and Gfeller (2009). These studies are focused on specific problems as e.g. transient faults in networks or specific processors.

The subject has become relevant for two reasons. Firstly, the miniaturization of computer technology leads to increasing sensitivity of hardware to exterior influences. Secondly, the weakening of the magnetic field of the earth is accompanied with an increasing number of charged cosmic particles arriving at the earth's surface. As a result, occurrence rate of transient failures can be greater than the failure rate of hardware failures by three or more orders of magnitude Shubinski (2012).

This paper presents a systematic method of developing a system that is stable with respect to transient failures.

In the second chapter, it is discussed how transient failures arise and to which consequences they lead. The third chapter is devoted to methods of detection of transient failures. The fourth chapter is dedicated to protection methods against transient failures gives a systematic approach for protection against transient failures. Principle is explained, which basic properties a system must have to be stable against transient failures. In the

fifth chapter an example is given. The conclusion is contained in the last chapter.

2 TRANSIENT FAILURES

In Information Systems (IS), transient failures and intermittent failures have no significant effect on the reliability of the IS. This is explained by the following reasons:

- Many ISs are classified as mission-critical systems. Therefore, when designing the information system special measures to stabilize the system are taken regarding acceptable limits of temperature and humidity, climatization, careful design of electrical schemes, excluding events as races between and competing signals etc.
- Many information systems work in real time. They perform well-defined informational tasks according to a given schedule. For these systems, transient failures mainly influence the function of these system. These are such failures that, under certain circumstances, can lead to control failures under certain conditions and have serious consequences for the entire system, and even for the environment.
- Transient failures exist only for very short time. They occur in hardware and are vanishing themselves, i.e. the hardware returns to its original physical condition, but not necessarily to the original functional state.

Hardware failures can be caused by:

2.1 *Noise acting on inputs and power supply*

The actual transfer function of a circuit can be approximated by a piecewise linear function. Figure 1 provides an example of the transfer function. It is characterized by the parameters a_i ($i = 1,0$)—the output voltage level of a logic one or zero, b_i—input level for a switching from $1 \rightarrow 0$ ($i = 1$) or from $0 \rightarrow I$ ($i = 0$). The switching band is given by $\Delta b = |b_1 - b_0|$. For a typical transfer characteristic, there are three areas, corresponding to the different states of the circuit. Area I—closed contacts, area III—open contacts, and an intermediate area II—switching between the states. Under the influence of influences the system can move from area I to area III, i.e. a malicious output code "I" is produced instead of the "0" (transient failure $1 \rightarrow 0$). Under the influence of interference also a failure with a $0 \rightarrow 1$ transition can occur.

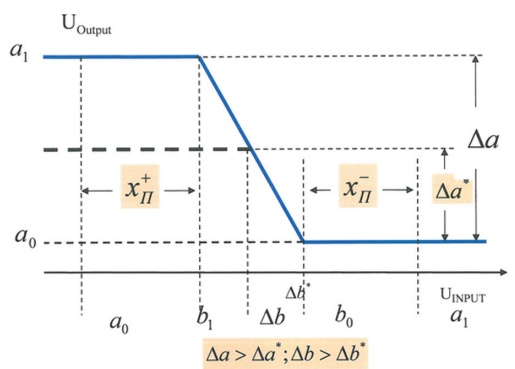


Figure 1. Typical transfer characteristics of a digital integrated circuit.

From Figure 1 its can be seen that for a given threshold Δa, a larger differences between b_0 and b_1 leads to smaller admissible amplitudes of input noises x_π^+ and x_π^-. This causes a reduction of the stability of the system with respect to noise. An analogous result is caused by a reduction of the difference of logical levels Δa. Note that, Δa is especially small for fast integrated circuits, since a reduction of the switching time Δb^* requires a reduction of Δa^*.

Systematic experimental data on transient failures of integrated circuits are not available. In order to derive the characteristics of transient failures it is convenient to use experimental data on the input signal and noise and the transmission characteristics in the amplitude-frequency range of the integrated circuits and to apply computational models. By this approach, first a range of possible probabilities of transient failures of trigger components at the inputs are obtained. From them, the characteristics of transient failures of the integrated circuit are derived.

2.2 *Electromagnetic interference*

If the noise can affect the system through inputs, power and weight, then the system can also be exposed to electromagnetic radiation. Consequently, a current can be induced, an interference occurs which impacts the components. This signal acts in the same method on the contacts of IP as an obstacle to coming right contacts and wires and as described top.

2.3 *Influence of radioactive particles*

The third mechanism is the impact of radioactive particles. Usually, in a first step gamma quants pass close to the IC. This can likely be radiation produced as a result of radioactive decay. Gamma radiation has the property that it passes through the material quite well and it is difficult to protect against it. A Gamma quantum can yield emission

of an alpha particle by an excited nucleus. An alpha particle is a charged particle that can affect the inputs and outputs of the integrated circuits or the registers and the memory. Due to this impact, a bit might switch.

The consequences of transient failure can be the following:

- Distortion of stored data
  In this case, the system continues to function on the basis of incorrect information. Then, even correctly executed functions provide a false result. If the data are no corrected this process continues. In particular, a transient failure can influence the output of the integrated circuit and cause a dangerous command.
- Changing the program sequence
  This means that the system does not perform a function at all, performs another function instead, performs the function early, late or in a wrong order, which can lead to a dangerous system failure.

3 DETECTION OF TRANSIENT FAILURES AND PROTECTION FROM THEIR DANGEROUS CONSEQUENCES

There are a number of well-known methods of protection from the effects of transient failures [1]. First of all, methods for the detection of transient failures are needed. The following well-known methods of detection exist:

- Cross comparison in multi-channeled systems
  In this approach, the results of two or more channels of a system are compared. If they results differ, a failure or a transient failure is assumed.
- Use of checksums
  Besides the data themselves, checksum is saved. Changes of the data changes will lead to a situation, where the checksum and the data do not match any more. By this means, many faults can be detected, but not all.
- Algorithms
  Algorithms are used for calculation or for the determination of the reaction system that are tolerant with regard to transient failures.
- Multi-version programming
  Two or more versions of the software are created, which are based on the same algorithm. The results are compared. Since the impact of a transient failure is supposed to be different on both versions of the software, faults would be detected by comparison.

These are the well-known, classic methods of protection, which are suitable for a wide class of faults and failures.

After having detected a transient failure, a reaction of the system is required, which should be implemented in another part of the system than that one, in which the fault has occurred. However, also the equipment used for fault detection and reaction is susceptible to transient failures and, therefore, also these devices must be protected against transient failures.

4 A SYSTEMATIC APPROACH

In this section we construct a systematic method for protection from transient failures.

A system failure caused by a transient failure arises due to a deviation, which is kept in the system either directly or indirectly. Indirectly saving to memory a transient fault is more dangerous, as it is more difficult to detect.

An example of a direct saving to memory incorrect data is the distortion of saved data, such as system parameters. Indirect saving to memory occurs, for example, if the system performs an incorrect operation that will lead to distortion of data, which are then saved to the memory.

Software can be imagined as a finite automate. The status of the automate is the entirety of all of the data recorded in the memory and that either came from the outside (sensor data, the status of external devices etc.) or that were derived as a result of the software processes themselves (calculation results, commands that were derived by the software and have been directed to external devices, the point at which the software has arrived in the program sequence). All information is discrete and depends only on the entire history of the system, but not on its future.

Now, the software will be expressed as a Markov system (described by a Markov chain or a Markov process, see Feller (1968)): That means, the next step depends only on the current state, but not on the history.

This is described in the sequel. The state of the system at a given moment in time is described as vector in the state space of the system, which contains all necessary information for an unambiguous description of all data, code, registers, etc. This state vector can have a very large size, but it is finite. Then the software and the computing system a digital system can be represented as a Markov chain.

The task of protection from transient failures is thus reduced to two sub-problems:

1. Protection of the system state as stored in the memory from distortion by transient failures,
2. Protecting of the transition to the next state (i.e. computing) from distortion caused by transient faults.

In order to solve both these subtasks, for each of these tasks the following measures can e applied:

1. Use of checksums, redundant storage
   With these methods it is possible to detect corruption of data characterizing the system state. If the method of information storage includes redundant information, it is even possible to recover distorted information. This might happen if one uses error-correcting codes, as e.g. applied on CDs, or the information is stored twice with separate checksums for each version.
   In order to have a safe working system, one can introduce a state machine, which reflects all important aspects of the information processing process, especially the distinction between hazardous and safe conditions. It is important to a state machine, which is as simple as possible.
   In the standard EN 50128 (2011), Annex D.24 Finite State Machines are required as a possible measure. This measure is just motivated by protection against transient faults.
2 Multi-version programming
   If the software is programmed in various versions carrying out calculations using different methods, transient failures cannot distort the data processing in both versions of the software in such a manner, that the results are the same. It is also possible to apply the same code on different computers with different compilers so that different executable software results.

If a state machine is used, before a state transition is initiated the conditions and the next state can be obtained using different algorithms.

5 EXAMPLE

This section an example of a system is described that uses a systematic approach for protection against transient faults presented above. For the example we assume that a safe computer is required for calculations. In addition, these computations have to be carried out cyclically. For example, the braking distance is computed every 100 milliseconds in order to verify that the train will be able to stop before the next red sign.

In the first step those data set needs to be determined, which clearly describes the state of the system. In this example, these are the position, the speed, the deceleration and the braking curve, which describes the braking ability of the train. Further, the actual time is important, alternatively the cycle number. Obviously, these data should be written into memory together with a checksum. Then it is possible to detect data corruption caused by malfunctioning. If, however, it is important not only to detect but also restore the correct data, i.e. restoring the correct state, it is necessary to either store data redundant or to use error-correcting codes. In the first case, the data is stored twice with a hash code. Then it is easy to determine which version of the data has been damaged. In the second case, one needs to pay attention to the fact that with a large number of transient failures a recovery of a wrong state would become probable.

Anyway, calculations need to prove that the measures implemented against transient failures detect errors with sufficiently high probability, so that the probability of undetected distortions is sufficiently low.

In the second step, the system needs to be protected from the consequences of transient failures when transition from one state to another occurs. The easiest option is the determination of the next state several times. Calculations are carried out twice, so that possible errors can be detected. If in case of failure, the calculation is repeated for the third time, so the error can be corrected by switching to that state, which has been determined by the majority of calculations.

In this example, same calculations are repeated on the same processor and with the same software version. This is possible because the transient failure does not lead to a permanent fault. It should be noted that the described measures do not protect from permanent or systematic failures.

In connection with the transition of the system to the next state, however, one needs to consider the software module that carries out the calculations to determine the subsequent state. If a transient failure distorts the software, then the software remains in a distorted form in the memory, although the memory would store the software correctly at the next occasion of software upload to the system. Therefore, the software must be written into memory together with a checksum. Moreover, for each application of this software, i.e. also when recomputing the transition to the next system state it is necessary to check the integrity of the software (or portions thereof) with the checksum.

6 CONCLUSION

In this paper, we studied transient failures. We have described the causes of transient failures and protection methods against them. The description given in chapter 2 can be seen as an illustration, where transient failure come from. Also, the description of detection mechanisms in chapter 3 is a list of known mechanisms. In the fourth section we have derived a systematic approach, which consists in two steps. At the first step, the system is represented as a Markov automate, the state of which is stored using protection methods, for

example using a checksum. In the second step, a reliable method of transition between states is constructed, e.g. using redundant calculations. The systematic approach has not been derived using cause and effect analysis by just combining causes of transient failures with detection mechanisms, because both lists can be incomplete. Instead, we consider the system as a system with discrete and countable system states with the Markov property. Such an approach is new. From this model, the two step approach is derived.

The approach is illustrated by an example.

REFERENCES

EN 50128, 2011 *Railway applications—Communication, signaling and processing systems—Software for railway control and protection systems*.

Feller, W. An Introduction to Probability Theory and Its applications, J. Wiley & Sons, New York, London, Sydney, 1968.

Gfeller, B., 2009, *Algorithmic Solutions for Transient Faults, in Communication Networks, On Swap Edges and Local Algorithms*, Diss ETH Zurich.

IEEE 1483,1999, *Standard for the Verification of Safety for Processor-based Systems Used in Rail Transit Control*.

ISO 26262-10, 2012 *Road vehicles—Functional safety—Part 10: Guideline on ISO26262*.

Qi, H., Ganesan, S. Pecht, M., 2008 No-fault-found and intermittent failures in electronic products, *Microelectronics Reliability* 48: 663–674.

Shubinsky, I.B. 2012, *Functional reliability of information systems*, Nadyozhnost, Moscow, 2012.

Xiaobin L., 2005, *Tolerating Radiation-Induced Transient Faults in Modern Processors*, Diss. Univ. of California, Irvine.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability allocation for a system with complex redundancy

Z. Vintr & T. Vintr
University of Defence, Brno, Czech Republic

ABSTRACT: The paper deals with the possibilities of allocating reliability requirements for a system using complex redundancy. It means system consists of a few identical subsystems and for its common function it is quite enough if only certain part of these subsystems operates. The subsystems not operating at a certain moment serve as redundancy in case that the subsystems which are operating fail. All the system, however, is not a trivial parallel structure, because if the system is to work properly, always more than one subsystem should operate and the subsystems can operate only in configurations set in advance. Practical application of the suggested method of reliability allocation is demonstrated for a pantograph system of a high-speed train. In order to provide the proper function of the system, the minimum number of operating pantographs in pre-set configurations providing safe current collection has to be always available. Using some pantograph configurations (e.g. two pantographs being one after another very closely) is in fact not possible for safety reasons. The article presents the procedure of reliability allocation for this specific system. Suggested method is based on a truth table and Boolean algebra application.

1 INTRODUCTION

At present it is common that when placing an order for developing and designing complex technical systems, it is essential to include both quantitative and qualitative reliability requirements for a specific system (IEC 2007).

Quantitative requirements are usually put in the form of the numerical values of selected reliability measures which are supposed to be met by a suggested system as a whole. It is then necessary to divide these global requirements properly into single parts of a system. This process is called the allocation of reliability requirements.

The aim of the process is to determine the reliability requirements of single parts of the system so that the system as a whole could satisfy the set requirement while meeting the partial ones. This process should be understood at the same time as essential part of the allocation of requirements for other system properties related to its dependability (Bartak et al. 2006).

It is always necessary to consider the fact that the decisions made in terms of reliability requirements allocation affect significantly system life cycle cost (Balik at al. 2005). In technical literature we can find a great deal of different procedures and methods of allocating reliability requirements (Kuo & Zhu 2012, Stapelberg 2009, Wessels 2010). They are, however, mostly restricted only to the systems of simple series or a parallel structure, or the system having simple ways of redundancy.

If the system structure is more complex, all the allocation process will be a lot more complicated and it is necessary then to combine single procedures and methods, or find new ones (Vintr & Vintr 2012, Vintr & Holub 2001, Wang et al. 2001, Furch 2012, Valis 2014, Maga 2006).

In the article we have introduced a possible procedure for allocating system reliability requirements. The system consists of a few identical subsystems and for its common function it is quite enough if only certain part of these subsystems operates. The subsystems not operating at a certain moment serve as redundancy in case that the subsystems which are operating fail.

All the system, however, is not a trivial parallel structure, because if the system is to work properly, always more than one subsystem should operate and the subsystems can operate only in configurations set in advance.

A high-speed train pantograph system which is introduced in this article can serve as an example of such system. When allocating reliability requirements for this system, a method using a truth table and Boolean algebra has been used.

2 RELIABILITY ALLOCATION PRINCIPLES

When considering complex technical systems, usually it is not possible to quantify reliability requirements for single items directly, but it is necessary to perform the gradual decomposition of the

requirements depending on the complexity and functional structure of the system. The starting point is to define single levels of system complexity characterized by items which are considered to be inseparable at a certain level. The example of such system division is shown in Figure 1.

The allocation of reliability requirements is then performed gradually following single selected levels of system complexity. Requirements for all the system are first redistributed throughout single subsystems, afterwards, when made for single subsystems, the requirements are distributed to subsystem assemblies, and the process will continue throughout all selected levels of system complexity up to individual components.

The process should be performed so that the set requirements for individual elements reliability would provide that the requirements for the system as a whole will be satisfied (Birolini 2004). Then it should be provided that:

$$R_S \geq R_S^*, \tag{1}$$

where: R_S-system reliability given by the reliability of single system items specified during allocation along with considering the system structure, R_S^*-required system reliability.

Allocation process can be relatively simple if the system has no redundancy. Should the system contain redundancy, allocation of reliability goals for individual components is more difficult.

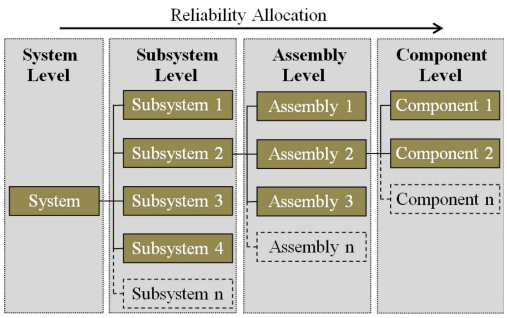


Figure 1. Reliability allocation concept.

In addition to above, complexity of individual components, costs, technology risks and failure effects should also be considered. In other words the allocation must be done in such a way that other design constrains are not violate. A case-by-case optimization is often possible (Birolini 2006).

3 TRAIN PANTOGRAPH SYSTEM

The suggested method, dealing with the allocation of reliability requirements, will be shown with the example of the pantograph system of a high-speed train with two engines placed at the beginning and at the end of the train (see Fig. 2). Either of these engines is equipped with pantographs designed the same way, but only one pantograph can operate on each engine. In order to assure right in-service operation, it is necessary to keep a certain minimum distance between single pantographs which operate (collect power) simultaneously. This is provided only in certain operating pantograph configurations shown in Table 1 (a cross in the table represents pantograph in operation).

When pantographs move along the overhead line, the line starts vibrating and if the specified minimum distance between pantographs were not kept, it could result in damaging the pantographs or the overhead line. Moreover, the train is required to be constantly powered by both engines. The train operator is permitted to use during the operation any of the allowed pantograph configurations.

The technical specification states that the reliability of a pantograph system as a whole cannot be lower than a required value R_S^*, and then the requirement expressed by the Equation 1 should be met. The aim of the allocation in this case is to determine the requirement for single pantograph reliability.

Further solution is based on a simplified assumption that a train set moves in one direction during all its life time. It is also presumed that all pantographs are designed identically and are of the same reliability. Basically, it is about a uniform distribution of reliability requirements.

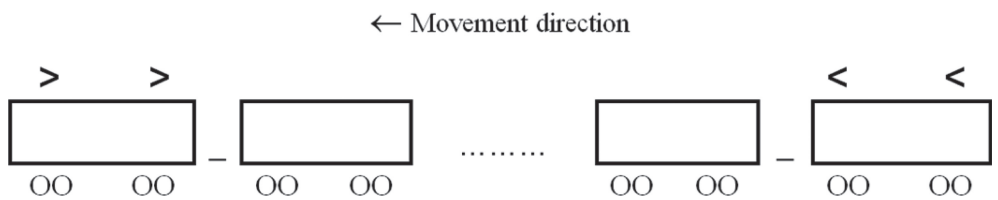


Figure 2. Pantograph system configuration.

Table 1. Allowed operational configuration of the pantograph system.

Allowed operational configuration	Ordinal number of pantograph (from the front of the train set)			
	1	2	3	4
I	X		X	
II	X			X
III		X		X

4 PROCESS OF RELIABILITY ALLOCATION USING THE TRUTH TABLE

The indicated task may be solved in different manners, but in view of its character applying a truth table seems to be the most convenient (IEC 2006). All possible combinations of faults and up states of single pantographs are going to be put in the table and each combination will be matched with all the system state with respect to allowed pantograph operational configurations.

Possible system states are put in Table 2 where value "0" means fault, whereas value "1" means up state. In the last column of the table there is for each combination an expression showing the probability that the combination will occur.

The symbols used in the Table 2 have the following meaning R_i—up state probability of *i*-th pantograph and Q_i—fault probability of *i*-th pantograph. Mutual relationship of these quantities can be expressed by the following formula:

$$Q_i = 1 - R_i \tag{2}$$

The probability that during assumed operating time all system will be in the up state might be, when applying the truth table, set as the sum of probabilities put in these lines which express some of the system up states:

$$\begin{aligned} R_S = {} & R_1R_2R_3R_4 + R_1R_2R_3Q_4 + R_1R_2Q_3R_4 \\ & + R_1Q_2R_3R_4 + Q_1R_2R_3R_4 + R_1Q_2Q_3R_4 \\ & + R_1Q_2R_3Q_4 + Q_1R_2Q_3R_4 \end{aligned} \tag{3}$$

Further solution is based on the assumption that the reliability level of all used pantographs is the same and the following equations apply:

$$\begin{aligned} R_1 = R_2 = R_3 = R_4 = R_p \\ Q_1 = Q_2 = Q_3 = Q_4 = Q_p \end{aligned} \tag{4}$$

Then, the Equation 3 might be put in the form below:

$$R_S = R_p^4 + 4R_p^3Q_p + 3R_p^2Q_p^2 \tag{5}$$

Table 2. Possible states of the pantograph system.

No.	Ordinal number of pantograph: 1	2	3	4	System state	Probability of relevant state occurrence
	State of pantographs					
1	1	1	1	1	1	$R_1R_2R_3R_4$
2	1	1	1	0	1	$R_1R_2R_3Q_4$
3	1	1	0	1	1	$R_1R_2Q_3R_4$
4	1	0	1	1	1	$R_1Q_2R_3R_4$
5	0	1	1	1	1	$Q_1R_2R_3R_4$
6	1	1	0	0	0	$R_1R_2Q_3Q_4$
7	1	0	0	1	1	$R_1Q_2Q_3R_4$
8	0	0	1	1	0	$Q_1Q_2R_3R_4$
9	0	1	1	0	0	$Q_1R_2R_3Q_4$
10	1	0	1	0	1	$R_1Q_2R_3Q_4$
11	0	1	0	1	1	$Q_1R_2Q_3R_4$
12	1	0	0	0	0	$R_1Q_2Q_3Q_4$
13	0	1	0	0	0	$Q_1R_2Q_3Q_4$
14	0	0	1	0	0	$Q_1Q_2R_3Q_4$
15	0	0	0	1	0	$Q_1Q_2Q_3R_4$
16	0	0	0	0	0	$Q_1Q_2Q_3Q_4$

and after replacing Q_p according to the Equation 2 and proper modifications we get the following equation:

$$R_S = 3R_p^2 - 2R_p^3 \tag{6}$$

After solving this equation, we get the requirement for pantograph up state probability.

5 PROCESS OF RELIABILITY ALLOCATION USING THE BOOLEAN ALGEBRA

Application of Boolean algebra is the second way haw to solve the presented problem. According to Table 1 the conditions for the pantograph system up state can be described by the following equation:

$$S = (S_1 \cap S_3) \cup (S_1 \cap S_4) \cup (S_2 \cap S_4) \tag{7}$$

where: S = the symbol indicates that the pantograph system is in up state, S_i = the symbol indicates that the *i*-th pantograph is in up state.

However, the Boolean terms S_1, S_2, S_3, and S_4 cannot be directly replaced by the corresponding probabilities in order to obtain a value for system reliability. This is because Equation 7 is in effect a set of "overlapping" (not "disjoint") terms. For these reason Equation 7 should by modified to non-overlapping terms using the methods for disjointing Boolean expressions (IEC 2006).

Application of these methods the following equation can be received:

$$S = (S_1 \cap S_3) \cup (\bar{S}_1 \cap S_2 \cap S_4) \cup (S_1 \cap \bar{S}_3 \cap S_4) \quad (8)$$

where: $\bar{S}_i$—the symbol indicates that the *i*-th pantograph is in down state.

In purely Boolean terms, Equation 7 and Equation 8 are equivalent. In Equation 9 each literal can be replaced by the corresponding probability:

$$P(S) = P(S_1)P(S_3) + P(\bar{S}_1)P(S_2)P(S_4) + P(S_1)P(\bar{S}_3)P(S_4) \quad (9)$$

where $P(S) = R_s$ = probability of the pantograph system up state (pantograph system reliability), $P(S_i) = R_i$ = probability of the *i*-th pantograph up state (*i*-th pantograph reliability), $P(\bar{S}_i) = Q_i$ = probability of the *i*-th pantograph down state (*i*-th pantograph unreliability).

After replacing individual probabilities corresponding reliability/unreliability term the following equation can be received:

$$R_S = R_1R_3 + Q_1R_2R_4 + R_1Q_3R_4 \quad (10)$$

Further solution is based on the assumption that the reliability level of all used pantographs is the same (see Equation 4):

$$R_S = R_p^2 + 2Q_pR_p^2 \quad (11)$$

After replacing Q_p according to the Equation 2 and proper modifications we can get the same formula as it has been already presented (see Equation 6). A practical solution of the Equation 6 is not presented there, since it is not the area of our interest in the article and it is purely mathematical.

6 CONCLUSION

The article introduces a possible procedure for allocating reliability requirements for a system consisting of a few identical subsystems. For a common system operation it is quite sufficient if only a certain part of these subsystems works. It applies that these systems can operate only in the configurations set in advance. A possible representative of a system of this kind is the pantograph system of a high speed train.

While allocating reliability requirements for this system, it is impossible to use standard methods and allocation procedures. That is the reason why we introduced a relatively simple procedure using a truth table which solves the problem effectively. The truth table can be used also for other types of systems where conventional methods of reliability requirements fail.

ACKNOWLEDGMENT

The work presented in this paper was supported by the Ministry of Defence of the Czech Republic (PRO K-202, University of Defence).

REFERENCES

Balik, R., Bartak, J., Cornak, S. & Furch, J., 2005. A Relation between Dependability Specific Aspects and Vehicles LCC in Operation and Maintenance. In *Proceedings of 9-th International Conference Transport Means*. Kaunas: Kaunas University of Technology, pp. 62–65.

Bartak, J., Cornak, S. & Balik, R., 2006. Perspective methods of vehicles maintenance. In *Transport Means 2006—Proceedings of the International Conference*. Kaunas: Kaunas University of Technology Kaunas, pp. 183–186.

Birolini, A., 2004. *Reliability Engineering—Theory and Practice*. New York: Springer—Verlag.

Furch, J., 2010. Determination of Vehicle Durability Based on Life Cycle Costs and Failure Intensity. In *Intelligent Technologies in Logistics and Mechatronics Systems ITELMS'2010*. Kaunas: Kaunas University of Technology, pp. 23–26.

IEC 60300–3–4, 2007. *Dependability management—Part 3–4: Application guide—Guide to the specification of dependability requirements.* Geneva: IEC.

IEC 61078, 2006. *Analysis techniques for dependability—Reliability block diagram and boolean methods.* Geneva: IEC.

Kuo, W. & Zhu, X., 2012. *Importance Measure in Reliability, Risk, and Optimization.* Chichester: John Wiley & Sons.

Maga, D., Hartansky, R. & Manas, P., 2006. The Examples of Numerical Solutions in the Field of Military Technology. *Advances in Military Technology,* 1(2): 53–66.

Stapelberg, R.F., 2009. *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design.* London: Springer.

Valis, D., Zak, L., Walek. A. & Pietrucha-Urbanik, K., 2014. Selected mathematical functions used for operation data information. In *Safety, Reliability and Risk Analysis: Beyond the Horizon*. London: Taylor & Francis Group, pp. 1303–1308.

Vintr, T. & Vintr, M., 2012. Reliability Allocation of a Vehicle With Regard to Warranty Costs. In 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012). Red Hook: Curran Associates, pp. 4612–4620.

Vintr, Z. & Holub, R., 2001. R&M Requirements Allocation in Upgrading a System. In *Proceedings of Annual Reliability and Maintainability Symposium*, New York: IEEE, pp. 258–263.

Wang, Y., Yam, R.C.M., Zuo, M.J. & Tse, P., 2001. A comprehensive reliability allocation method for design of CNC lathes. *Reliability Engineering & System Safety,* 72(3): 247–252.

Wessels, W.R., 2010. *Practical reliability engineering and analysis for system design and life-cycle sustainment.* Boca Raton: CRC Press.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Effective searching process used in obtaining Pareto solutions of two-objective network design problem

N. Takahashi & H. Yamamoto
Tokyo Metropolitan University, Tokyo, Japan

T. Akiba
Chiba Institute of Technology, Chiba, Japan

K. Shingyochi
Jumonji University, Saitama, Japan

ABSTRACT: There are many network systems in the world, for example, Internet, electricity network and traffic network, etc. In this study, we consider two-objective network design problem with all-terminal reliability and construction cost. In the general, it is a rare case that a solution makes both of all-terminal reliability and construction cost optimum simultaneously. Therefore we consider an algorithm for obtaining Pareto solutions. However, existing algorithms for Pareto solutions are inefficient as we must calculate all-terminal reliabilities of all sub-networks. So, it takes much time to obtain Pareto solutions when the number of nodes and edges is large. For an efficient algorithm, we research the difference between the Pareto solutions and the other networks. By using such properties, we constitute the searching space in which sub-networks take close values to Pareto solutions, and propose new algorithm for obtaining Pareto solutions. Finally, we evaluate our proposed algorithm by numerical experiments.

1 INTRODUCTION

There are many network systems in the world, for example, Internet, electricity network and traffic network, etc. These systems forms basis of society, so stabilizing operation of systems and designing systems to operate effectively are important problems. The evaluation of network systems considers various measures, for example, reliability, distances, flow and time. To optimize these measures, the problems are formulated as shortest path problem, maximum flow problem and so on.

Making a decision reasonably needs to consider plural measures when we evaluate these network systems. In our study, we consider all-terminal reliability and construction cost for network as important measures for evaluation. However, there exists a trade-off between reliability and construction cost, so it is a rare case that a solution (network system) makes all-terminal reliability and construction cost optimum simultaneously. Therefore we consider an algorithm for obtaining Pareto solutions of a two-objective network with all-terminal reliability and construction cost. The reliability and cost problems for the network systems have been studied in a long period. Specially calculating reliability is known to be more difficult than other measures, and the numerous papers have been published. As to calculation of reliability, many papers have appeared over the years dealing with the network reliability theory. These studies were reported by Boesch et al. (1988, 2009). Koide (2002) proposed efficient algorithm for calculating reliabilities of all sub-network. Akiba et al. (2007) improved Koide's algorithm and applied its improved algorithm to obtaining Pareto solutions with all-terminal reliability and construction cost. Though, this algorithm also needs to calculate all-terminal reliabilities and costs for all sub-networks. So, taking much time to obtain Pareto solutions is problem, as the number of nodes and edges in the all-terminal network is large.

In order to construct an efficient algorithm, we researched differences between the optimum networks, which become Pareto solutions, and the other networks. Based on these obtained properties, we reduce the number of networks whose reliability and cost must be calculated, and propose a new algorithm for obtaining the subset of Pareto solutions. And we evaluate the efficiency and accuracy of a proposed algorithm by numerical experiments.

2 DEFINITION OF PROBLEM

2.1 *Network model*

In this study, we consider networks with undirected edges, that is, networks have not directed flow for constructing networks. Let $g = (V, E)$ be a given network with the set $V = \{v_1, v_2, \ldots, v_n\}$ of nodes and the set $E = \{e_1, \ldots, e_m\}$ of edges. $X_g = (x_1, x_2, \ldots, x_m)$ also signifies a given network g, where x_i is a binary variable which takes 1 if edge e_i exists or else takes 0. Furthermore, we define some notations as follows.

n, m: The number of nodes and edges in V and E, respectively
G_n: The set of network with all n nodes connected.
For $i = 1, 2, \ldots, m$,
e_i: i-th edge
p_i, c_i: Reliability and construction cost of edge e_i, respectively
$R(g)$, $C(g)$: All-terminal reliability and total cost for network g, respectively.

The following assumptions are considered throughout this paper.

A. All terminal nodes do not fail.
B. Connections for all edges are mutually statistically independent.
C. All edges have reliability and construction cost.

2.2 *Definition of problem*

In this study, we consider network design problem with all-terminal reliability and construction cost. The problem can be expressed as follows.

$$R(g) \rightarrow \max$$

$$C(g) \rightarrow \min$$

$$s.t.\ g \in G_n$$

It is a rare case that a network makes all-terminal reliability and construction cost optimal simultaneously. For solving this problem, we search for Pareto solutions. Let G be the set of feasible solutions. For g, $g' \in G$, g becomes Pareto solutions if there are no other feasible solution g' which satisfies either 3 conditions as follows:

1. $R(g) < R(g')$ and $C(g) > C(g')$
2. $R(g) = R(g')$ and $C(g) > C(g')$
3. $R(g) < R(g')$ and $C(g) = C(g')$

That is, our considered optimal network design problem means obtaining Pareto solutions from all the sub-networks g', where $g' = (V, E')$ is all the sub-networks of g for $g = (V, E)$, $E' \subseteq E$.

2.3 *Existing algorithm*

We introduce existing algorithm by Koide (2002), which calculate all-terminal reliabilities for all sub-networks of complete graph. This algorithm divides edge sates into two conditions as follows.

a. "Deleting" means an operation of removing edge e_i from the network g, that is, edge e_i fails.
b. "Contracting" means an operation of unification for both end nodes of edge e_i, that is, edge e_i works completely.

Let $g - e_i$ be the network g with edge e_i deleted, and g/e_i represent the network g with edge e_i contracted, respectively. Then, all-terminal reliability $R(g)$ can be expressed as the following equation.

$$R(g) = (1 - p_i)R(g - e_i) + p_i R(g / e_i) \quad (1)$$

When equation (1) is applied to all sub-networks of complete graph, same form sub-networks appear plural times in recursive process. Koide (2002) proposed the efficient algorithm in which calculated reliabilities were memorized and referred. He called it "factmem method".

Furthermore, Akiba et al. expanded "factmem method" and proposed advanced algorithm, "improved factmem method" (Akiba et al. 2007). The following properties are considered in Akiba et al.'s algorithm.

1. If sub-network with n nodes and less than $n - 1$ edges is conducted by factmem method, it is not necessary to calculate its all reliability.
2. If the number of nodes comes to one in contracting process, it is not necessary to operate anymore for its network.

Moreover, Akiba et al. apply "improved factmem method" to two-objective network design problem with all-terminal reliability and construction cost.

3 PROPERTIES OF NETWORKS

3.1 *Outline of our proposed algorithm*

We consider network design problem with all-terminal reliability and construction cost. For this problem, proposed algorithm by Akiba et al. (2007) can reduce computing time for all-terminal reliability. However, their algorithm doesn't consider the relation between reliability and cost, and must calculate reliabilities and costs for all sub-networks. This process expands search space for Pareto solutions and makes computing time increase.

This section describes outline of our proposed algorithm. For explanation, the following nota-

tions are defined. For $k = n - 1, n, \ldots, n(n-1)/2$, let us define notations blow.

g_k: The network with n nodes connected by k edges
G_n^k: The set of g_k
$pareto(G)$: The set of network $g \in G$ which satisfies the definition of Pareto solutions.
gp_k: The network which satisfies definition of Pareto solutions in G_n^k
GP_n^k: The set of g_k. That is, $GP_n^k = pareto(G_n^k)$.

Figure 1 shows the outline of algorithm. Our proposed algorithm does not consider all sub-networks. We assume networks G_n^k are constructed. When $k = n - 1$, the set G_n^k has all networks which connect all nodes. Among G_n^k, a part of networks are selected as the candidate networks for construction of network set G_n^{k+1}. And an element of G_n^{k+1} is constructed by adding one edge to selected networks from G_n^k. For G_n^{k+1}, a part of G_n^{k+1} are selected, and an edge is added. This operation is repeated until $k = n(n-1)/2$.

The following sections explain the range of selected networks and criteria for added edge.

3.2 *Range for considered networks*

3.2.1 *Classifying Pareto solutions*

We consider selecting networks for adding edges. We divided G_n^k into the following two kinds of networks. One is $gp_k (\in GP_n^k)$ obtained as Pareto solutions and the other is $g_k (\in G_n^k \backslash GP_n^k)$. We researched which of the following two cases was efficient. One is the case that an edge is added to gp_k and $g_{k+1} (\in G_n^{k+1})$ are constructed. Another is the case that an edge is added to g_k. When g_k has much lower reliability and higher cost than gp_k, g_{k+1} constructed from g_k can hardly become Pareto solutions GP_n^{k+1}. Based on the above property, we define rank of Pareto solution and suppose the following property in order to select networks to add an edge.

Definition 1: Let $GP_n^{k,j}$ be Pareto solutions in rank j ($j = 1, 2, \ldots, R$), and defined as following formula.

$$GP_n^{k,j} = pareto(G_n^k \backslash \bigcup_{i=1}^{j-1} GP_n^{k,i}) \quad (2)$$

where $GP_n^{k,1}$ is the same as GP_n^k.

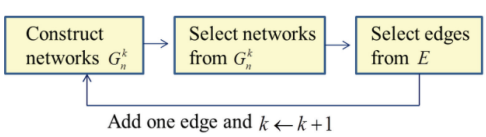


Figure 1. The outline of our algorithm.

Property 1: g_{k+1} constructed from $gp_k (\in \cup_{i=1}^{R} GP_n^{k,i})$ is likely to be Pareto solutions GP_n^{k+1}.

Property 1 means networks close to each Pareto solutions $GP_n^{k,1}$ are likely to be candidate networks for construction of G_n^{k+1}. R is lower boundary of considered rank as candidate. In an experiment with networks of 5 nodes, all Pareto solutions GP_n^{k+1} could be constructed by $gp_k \in GP_n^{k,1}$, $GP_n^{k,2}$.

3.2.2 *The slope of Pareto solutions*

Next, we take notice of the shape of Pareto front and propose restricting the range by the slope of Pareto solutions. This restriction adopts the straight line connecting origin point and one of Pareto solutions. Two properties are assumed below.

Property 2–1: For $gp_{k-1}^* = \arg \max_{gp_{k-1} \in GP_n^{k-1}} R(gp_{k-1})$, g_k which satisfies $R(gp_{k-1}^*) < R(g_k)$ can construct $gp_{k+1} \in GP_n^{k+1}$ by adding an edge.

Property 2–2: For $gp_k'' = \arg \min_{gp_k \in GP_n^k} (R(gp_k)/C(gp_k))$, g_k which satisfies $R(gp_k'')/C(gp_k'') < R(g_k)/C(g_k)$ can construct $gp_{k+1} \in GP_n^{k+1}$ by adding an edge.

By the above two properties, we consider two lines as shown in Figure 2. First line is L_1 which is parallel to abscissa axis and passes through gp_{k-1}^*. Property 2–1 means the region above L_1. Second line L_2 is connecting gp_k'' and origin point. Property 2–2 signifies the region above L_2. In Figure 2, the region surrounded by two lines, L_1 and L_2, is made the range of network selection.

3.2.3 *Network topology*

We consider characteristic of network topology. For network with all nodes included cycle structure, its all-terminal reliability is known to be higher than other topologies' all-terminal reliabilities (Jan 1993). Comparing networks (a) and (b) in

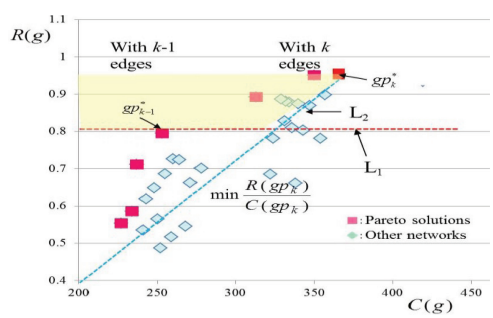


Figure 2. The image of restricted space by two straight lines.

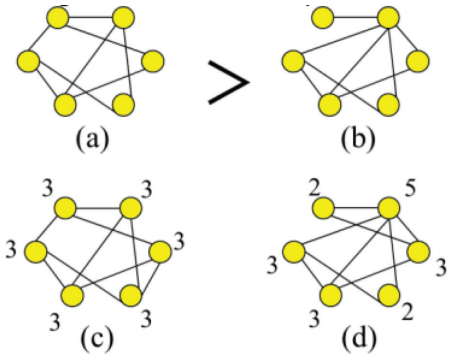


Figure 3. The influence of network topologies.

Figure 3, all-terminal reliability of network (a) is superior to that of network (b).

In addition, we researched Pareto solutions in terms of the degree of node. Networks like (c) in Figure 3 were more found in Pareto solutions as compared with networks like (d). Networks (c) and (d) are different in the number of edges connected to some node. The number of edges is called the degree of node. In network (c), degree of each node takes similar value. On the other hands, network (d)'s degrees vary widely. Using binary variable x_i which takes 1 if edge e_i exists or else takes 0, we assume the property about the degree of node below.

For node v_j, let d_j be the degree of node v_j as follows.

$$d_j = \sum_{i=1}^{n} x_i \tag{3}$$

where x_i are summed up on i such as $s(e_i) = v_j$ or $e(e_i) = v_j$, and $s(e_i)$ and $e(e_i)$ are nodes at both ends of edge e_i.

Property 3: Pareto solutions include networks as the degree of node satisfies following equation.

$$\left| D_1 + D_2 \right| = n \tag{4}$$

where $D_1 = \{d_j \mid 1 \le j \le n, d_j$ is the sum of 1 and quotient of 2 $k/n\}$, and $D_2 = \{d_j \mid 1 \le j \le n, d_j$ is equal to the quotient of $2k/n\}$.

3.3 *Criteria for adding edges*

3.3.1 *Efficiency of edges*

Next, we consider adding edge to selected networks. Pareto solutions depend on two objective functions, reliability and cost of each edge. Therefore this section mentions how two values of edge give influence on Pareto solutions. For e_i, we define following index.

Definition 2: $f_i = p_i/c_i$ denotes efficiency of edge e_i.

Figure 4 shows the following two cases. One is the case of adding the edge e_1 with minimum f_i. Another is the case of adding the edge e_2 with maximum f_i. In both cases, e_1 or e_2 is added to the network g_k. In light of this result, we assume the property as follows.

Property 4: If f_i is larger than other edge's, network $g_{k+1} = (V, E' \cup \{e_i\})$ is likely to be Pareto solution $gp_{k+1} \in GP_n^{k+1}$, where $g_k = (V, E')$.

3.3.2 *Validity of edge*

Next, our study focuses on the number of times that each edge is contained in Pareto solutions. To look for influences other than the value of reliability and cost, we researched Pareto solutions with small number of edges. The edges included in many Pareto solutions GP_n^k were also included considerably in Pareto solutions with more than k+1 edges. In addition, the many included edges don't necessarily match edges with high efficiency f_i. Whether a network becomes Pareto solution will depend on the way of edge link in addition to the value of reliability and cost on edge. Therefore, considering the number of times allows us to construct dominant networks effectively.

For obtained Pareto solutions GP_n^k, we sum up included times for each edge and this measure is applied to select edge. Using binary variable x_i which takes 1 if edge e_i exists or else takes 0, we define the following index.

Definition 3: Total value as satisfying following equation (5) is defined as validity x_i^k of edge e_i.

$$x_i^k = \sum_{\{gp_r \in GP_n^r\}} x_i \tag{5}$$

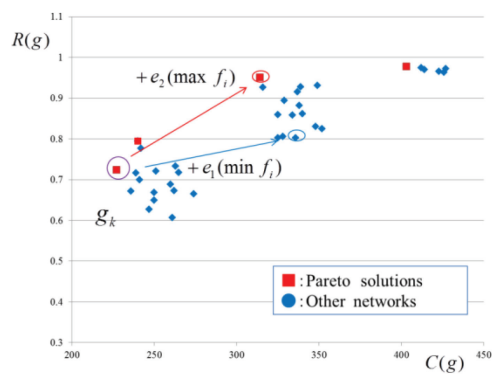


Figure 4. The influence of efficiency of edges for networks.

4 PROPOSED ALGORITHM

Combining the above-mentioned criteria of edge and range of considered networks, we construct algorithms which reduce the number of considered networks. However, reduction of considered networks influences obtaining Pareto solutions, and causes us subset of Pareto solutions. Computing time and accuracy of search vary according to considered lower boundary rank R and the number of edges ec added to candidate networks.

Numerical experiments were given by using a network with 6 nodes and 15 edges. Cost c_i and reliability p_i of each edge were prepared in a following pattern. p_i was given by random number uniformly between 0.50 and 0.99. c_i was set for $c_i = 100 * p_i + a$, where a was given by random number uniformly between 5 and 10. Calculating reliabilities and costs for all sub-networks took around 10 seconds.

Table 1 shows some algorithms which are different in combination of range for considered networks and criteria of edge. For example, $AL_{SD,V}$ adopts the slope of Pareto solutions and the degree of nodes as range for considered networks, and adds edges according to validity of edge. The following sections compare these algorithms.

4.1 *Comparison of ranges of considered networks*

In the following explanation, we describe $AL_{SD,V}$ of Table 1. ${G_{n,1}}^k$ and ${GP_{n,1}}^k$ signify considered networks by the slope of Pareto solutions, and ${G_{n,2}}^k$ and ${GP_{n,2}}^k$ by the degree of nodes. Among ${G_{n,1}}^k$, networks which satisfy the range for considered networks are set in ${GP_{n,1}}^{k,2}$, where $pareto({G_{n,s}}^k)$ is set in ${GP_{n,1}}^{k,1}$.

[Algorithm $AL_{SD,V}$]

STEP 1: Set lower boundary rank R and ec.
$k \leftarrow n-1$, $r \leftarrow 1$ and $s \leftarrow 1$.

Table 1. Combination of ideas in evaluated algorithms.

	Range of networks			Criteria of edge	
	Rank	Slope	Degree	Efficiency	Validity
$AL_{SD,V}$		Used	Used		Used
$AL_{S,V}$		Used			Used
$AL_{RD,V}$	Used		Used		Used
$AL_{R,V}$	Used				Used
$AL_{RSD,V}$	Used ($k \geq K1$)	Used ($k < K1$)	Used		Used
$AL_{RSD,E}$	Used ($k \geq K1$)	Used ($k < K1$)	Used	Used	

STEP 2:
STEP 2–1: If $s = 2$, for all $g_k \in {G_{n,s}}^k$ calculate d_j ($j = 1, 2, \ldots, n$).
If $|D_1 + D_2| \neq n$, ${G_{n,s}}^k \leftarrow {G_{n,s}}^k \backslash \{g_k\}$.
STEP 2–2: For all $g_k \in {G_{n,s}}^k$, calculate $R(g)$ and $C(g)$.

STEP 3:
STEP 3–1: If $s = 2$ and $k = n(n+1)/2$, calculate $pareto\{\cup_{i=n-1}^{k}({G_{n,1}}^i + {G_{n,2}}^i)\}$ and end algorithm. Else go to STEP 3–2.
STEP 3–2: For $gp_{k-1}^* = \arg \max_{gp_{k-1} \in GP_{n,s}^{k-1}} R(gp_{k-1})$,
if any $g_k \in {G_{n,s}}^k$ satisfies $R(gp_{k-1}^*) > R(g_k)$, ${G_{n,s}}^k \leftarrow {G_{n,s}}^k \backslash \{g_k\}$.
STEP 3–3: ${GP_{n,s}}^{k,1} \leftarrow pareto({G_{n,s}}^k)$.
For $gp_k'' = \arg \min_{gp_k \in GP_{n,s}^k} (R(gp_k)/C(gp_k))$,
if any $g_k \in ({G_{n,s}}^k \backslash {GP_{n,s}}^{k,1})$ satisfies $R(gp_k'')/C(gp_k'') < R(g_k)/C(g_k)$, ${GP_{n,s}}^{k,2} \leftarrow {GP_{n,s}}^{k,2} \backslash \{g_k\}$.

STEP 4:
STEP 4–1: If $k = n-1$ or n, $x_i^k \leftarrow f_i$. Else if $k = n+1$, calculate x_i^k and $x_i^k \leftarrow f_i + x_i^k$.
STEP 4–2: Select $gp_k \in (\cup_{r=1}^{R} {GP_{n,s}}^{k,r})$.
$l \leftarrow ec$.
STEP 4–3: Select $e_i \in (E \backslash E')$ which satisfies max x_i^k, and construct g_{k+1} and ${G_n}^{k+1} \leftarrow {G_n}^{k+1} \cup \{g_{k+1}\}$. $E' \leftarrow E' \cup \{e_i\}$, $l \leftarrow l-1$. Repeat up to $l = 0$.
STEP 4–4: If select all $gp_k \in (\cup_{r=1}^{R} {GP_{n,s}}^{k,r})$, go to STEP 4–5. Else go to STEP 4–2.
STEP 4–5: If $k = n-1$, construct sub-networks GC with cycle topology independently from x_i^k, and ${G_n}^{k+1} \leftarrow {G_n}^{k+1} \cup GC$.
STEP 4–6: $k \leftarrow k+1$, $r \leftarrow 1$ and go to STEP 2–2.
STEP 4–7: $k \leftarrow n$, $s \leftarrow 2$ and ${G_{n,s}}^k \leftarrow GC$. Go to STEP 2.

Moreover, changing combination of network properties constructs three other algorithms which are $AL_{S,V}$, $AL_{RD,V}$ and $AL_{R,V}$ of Table 1. $AL_{S,V}$ (Takahashi et al. 2013) excludes STEPs on the node degree from $AL_{SD,V}$. $AL_{RD,V}$ and $AL_{R,V}$ substitute rank of Pareto solution for STEPs on slope of Pareto solution of $AL_{SD,V}$ and $AL_{S,V}$, respectively. Varying parameters R and ec as shown in Table 2, numerical experiments are conducted. For example, $AL_{RD,V}$ takes values of 3 patterns on R and 10 patterns on ec, so 30 experiment patterns are conducted. Table 1 also indicates where the result

Table 2. Parameters on each algorithm.

	$AL_{SD,V}$	$AL_{RD,V}$	$AL_{S,V}$	$AL_{R,V}$
R		1 to 3		1 to 3
ec	1 to 10	1 to 10	1 to 10	1 to 10
Result	Figure 4	Figure 4	Figure 5	Figure 5

of each algorithm is shown. Figure 4 and Figure 5 compare the above four algorithm on influence by R and ec. Figures 4 and 5 show change of obtained rate and computing time in each algorithm. Obtained rate means the percentage of obtained Pareto solutions by our algorithm to real Pareto solutions. In Figure 4, items of "rank1, rank2 and rank3" are results of $AL_{RD,V}$, and "slope" corresponds to $AL_{SD,V}$. Similarly, items of "rank1, rank2 and rank3" and "slope" are results of $AL_{R,V}$ and $AL_{S,V}$, respectively in Figure 5.

Comparing both figures, using the slope of Pareto solutions is efficient. Although more computing time is taken, using the rank of Pareto solutions can obtain real Pareto solutions more. In terms of node degree, the pattern number that obtained rate is over 90% is 7 in Figure 5. In Figure 4 this number is 13. However increasing computing time is problem.

4.2 *Combination of ranges for considered networks*

Next, we construct algorithm $AL_{RSD,V}$ of Table 1, which changes the range for considered networks at some number of edges. K_1 is the parameter.

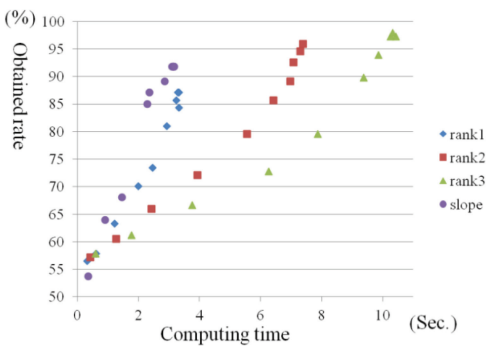


Figure 4. The comparison of $AL_{SD,V}$ and $AL_{RD,V}$.

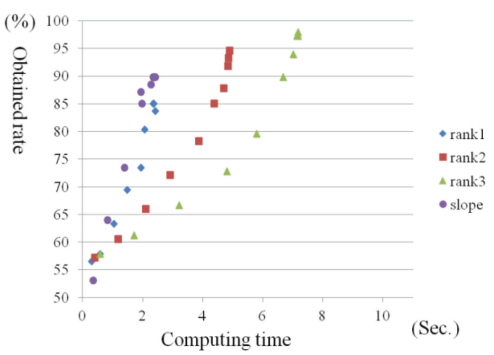


Figure 5. The comparison of $AL_{S,V}$ and $AL_{R,V}$.

[Algorithm $AL_{RSD,V}$]

Substitute following STEP 3 for STEP 3 of $AL_{SD,V}$.

STEP 3:

STEP 3–0: If $k < K_1$, Go to STEP 3–1–1. Else go to STEP 3–2–1.

STEP 3–1–1: For $gp_{k-1}^{*} = \arg \max_{gp_{k-1} \in GP_{n,s}^{k-1}} R(gp_{k-1})$, if any $g_k \in G_{n,s}^{k}$ satisfies $R(gp_{k-1}^{*}) > R(g_k)$, $G_{n,s}^{k} \leftarrow G_{n,s}^{k} \backslash \{g_k\}$.

STEP 3–1–2: $GP_{n,s}^{k,1} \leftarrow pareto(G_{n,s}^{k})$. For $gp_k'' = \arg \min_{gp_k \in GP_{n,s}^{k}} (R(gp_k)/C(gp_k))$, if any $g_k \in (G_{n,s}^{k} \backslash GP_{n,s}^{k,1})$ satisfies $R(gp_k'')/C(gp_k'') < R(g_k)/C(g_k)$, $GP_{n,s}^{k,2} \leftarrow GP_{n,s}^{k,2} \backslash \{g_k\}$. Go to STEP 4–1.

STEP 3–2–1: If $k = n(n+1)/2$, obtain $pareto\{\cup_{i=n-1}^{k} G_{n,1}^{i}\}$ and end of algorithm. Else, $GP_{n,s}^{k,r} \leftarrow pareto(G_n^{k} \backslash \cup_{j=1}^{r-1} GP_{n,1}^{k,j})$.

STEP 3–2–2: If $r = R$, go to STEP 4–1. Else, $r \leftarrow r+1$ and go to STEP 3–2–1.

In $AL_{RSD,V}$, slope of Pareto solutions is used as the range for considered networks when $k < K_1$. In the case of $k \geq K_1$, rank of Pareto solutions is applied to the range for considered networks.

Setting patterns of parameters R, ec and K_1 as shown in Table 3, numerical experiments are conducted. Figure 6 shows comparison of $AL_{RSD,V}$ and $AL_{SD,V}$. In this figure, the items of "rank1, rank2 and rank3" mean results of $AL_{RSD,V}$. The item of "slope" is the same as "slope" of $AL_{SD,V}$ in Figure 5, where Figure 6 is different in the scale of abscissa axis. From this result, using rank of Pareto solutions becomes more efficient in some patterns than using the slope of Pareto solutions. In addition, from an accurate point of view, the number of patterns that obtained rate is over 90% is 18 in Figure 6.

4.3 *Comparison of criteria of edge*

In order to research the influence of efficiency and validity of edges, we describe $AL_{RSD,E}$ and compare $AL_{RSD,E}$ with $AL_{RSD,V}$ of Table 1.

[Algorithm $AL_{RSD,E}$]

Substitute following STEP 4 for STEP 4 of $AL_{RSD,V}$.

Table 3. Parameters on $AL_{SD,V}$ and $AL_{RSD,V}$.

	$AL_{SD,V}$	$AL_{RSD,V}$
$R(k \geq K_1)$		1 to 3
ec	1 to 10	1 to 10
K_1		9

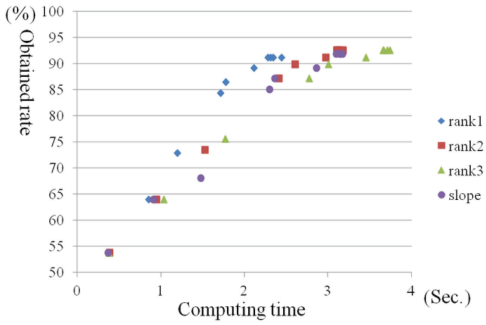


Figure 6. The comparison of $AL_{SD,V}$ and $AL_{RSD,V}$.

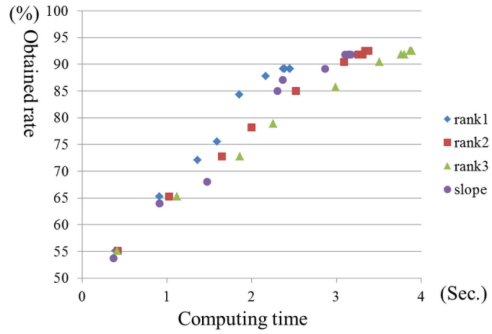


Figure 7. The comparison of $AL_{RSD,V}$ and $AL_{RSD,E}$.

Table 4. Parameters on $AL_{RSD,V}$ and $AL_{RSD,E}$.

	$AL_{RSD,V}$	$AL_{RSD,E}$
$R(k \geq K_1)$	1 to 3	1 to 3
ec	1 to 10	1 to 10
K_1	9	9
Result	Figure 6 & Figure 8	Figure 7 & Figure 9

STEP 4:

STEP 4–1: If $k = n - 1$, calculate f_i.

STEP 4–2: Select $gp_k \in (\cup_{r=1}{}^{R} GP^{k,r}{}_{n,s})$. $l \leftarrow ec$.

STEP 4–3: Select $e_i \in (E \backslash E')$ which satisfies max f_i, and construct g_{k+1} and $G_n{}^{k+1} \leftarrow G_n{}^{k+1} \cup \{g_{k+1}\}$. $E' \leftarrow E' \leftarrow \{e_i\}$, $l \leftarrow l - 1$. Repeat up to $l = 0$.

STEP 4–4: If select all $gp_k \in (\cup_{r=1}{}^{R} GP_{n,s}{}^{k,r})$, go to STEP 4–5. Else go to STEP 4–2.

STEP 4–5: If $k = n - 1$, construct sub-networks GC with cycle topology independently from f_i and $G_n{}^{k+1} \leftarrow G_n{}^{k+1} \cup GC$.

STEP 4–6: $k \leftarrow k + 1$, $r \leftarrow 1$ and go to STEP 2–2.

STEP 4–7: $k \leftarrow n$, $s \leftarrow 2$ and $G_{n,s}{}^{k} \leftarrow GC$. Go to STEP 2.

Setting patterns of parameters R, ec and K_1 as shown in Table 4, numerical experiments are conducted. In Figure 7, the items of "rank1, rank2 and rank3" show results of $AL_{RSD,E}$. The item of "slope" is the same as "slope" of $AL_{SD,V}$ in Figure 6. "Slope" is plotted as a measure for comparison with $AL_{RSD,V}$ of Figure 6. As the result, $AL_{RSD,E}$, which used efficiency as criteria of edge, made efficiency of search decrease a little.

We take notice of error rate of both algorithms. Our algorithms output some non-Pareto solutions as optimum solutions. Error rate means the percentage of these non-Pareto solutions by our algorithm to real Pareto solutions. Figure 8 and Figure 9 compared error rate when ec varied as shown in Table 4. Comparing two figures, $AL_{RSD,E}$ is likely to obtain non-Pareto solutions. When $ec = 2,3,4$, the error rate increased.

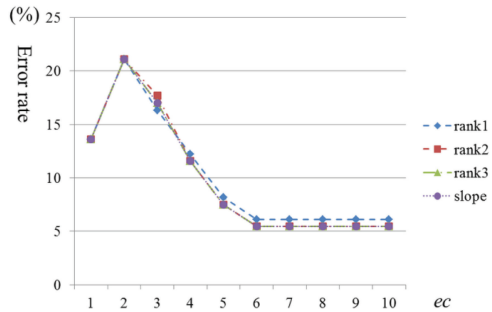


Figure 8. The influence of validity of edges for networks.

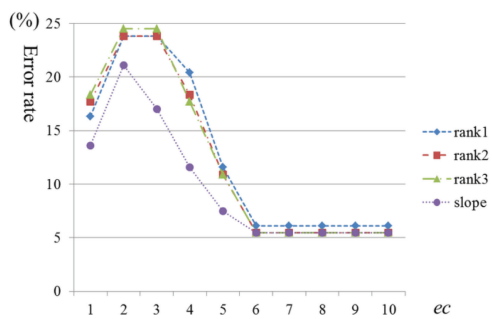


Figure 9. The influence of efficiency of edges for networks.

5 CONCLUSION

In our study, we focused on optimum network design problem with two-objective network with

all-terminal reliability and construction cost. Our study introduces criteria for added edges and range of considered networks. Combining these properties, we proposed the algorithm restricting the number of networks that must be calculated. With regard to the range for considered networks, numerical experiment suggested combining slope and rank of Pareto solutions was effective. As criterion of edge, using validity of edge wasn't greatly different from using edge efficiency in obtained rate, but validity was superior in error rate. Therefore $AL_{RSD,V}$ could obtain the subset of Pareto solutions more accurately and efficiently among algorithms which we constructed in this study. The future work is to consider combination of network properties which we haven't used, and to adapt these network properties to algorithm process effectively.

ACKNOWLEDGEMENTS

This work was partially supported by Grant #25350456, Grant-in-Aid for Scientific Research (c) from JSPS(2013-). The authors thank the JSPS for their support.

REFERENCES

Akiba, T., Asukagawa, H., Yamamoto, H. & Nagatsuka, H. 2007. An efficient algorithm for Pareto-solutions of a network with the all-terminal reliability and construction cost. In Proc. I*nt. Conf. on Mathematical Methods in Reliability,* CD-ROM.

Boesch, F.T. 1988. A Survey and Introduction to Network Reliability Theory, *IEEE International Conference on Communications* 2: 99–107.

Boesch, F.T., Satyanarayana, A. & Suffel, C.L. 2009. A Survey of Some Network Reliability Analysis and Synthesis Results. *Networks* 54(2): 678–682.

Jan, R.H. 1993. Design of Reliability Network, *Computers & Operations Research* 20: 25–34.

Koide, T., Shinmori, S. & Ishii, H. 2002. An Efficient Complete Enumeration Method for Network Design Problems and Its Applications, *Journal of the Operations Research Society of Japan* 45(3): 299–316.

Takahashi, N., Akiba, T., Yamamoto, H. & Shingyochi, K. 2013. The effective measures of network for optimizing two-objective network. *In Proc 15th Asia Pacific Industrial Engineering and Management Systems Conf.*, CD-ROM.

Reliability and safety data collection and analysis

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

SYMBAD—Artificial Neural Networks in furtherance of managing aircraft testing

W. Kosiński, J. Wójcik & M. Zieja
Air Force Institute of Technology, Warsaw, Poland

ABSTRACT: SYMBAD is the structure of Artificial Neural Network (ANN) developed on the basis of experimentally gained data from the military aircraft testing. These tests were done in Air Force Institute of Technology for many years and for the different types of aircraft. Potential usage of this programme for the managing of aircraft prototypes testing has been formulated as well. This case is presented in this article. The presented program will be improved based on the knowledge of researchers.

The SYMBAD program has been developed under the Borland C++ Builder programming environment. It uses an innovative approach to any issues of the aeronautical testing.

The SYMBAD's structure can be easily adjusted depending on the type of test equipment, eg. for unmanned air systems, helicopters and combat aircrafts. Moreover, programme modification can include type of research being conducted: for a new-designed and -developed aircraft as well as for an upgraded one, for those in production, and for the aircraft equipment/systems built in the aircraft.

Input programme data take into consideration requirements listed in technical specifications, rules and regulations of aircraft building, standards, and Customer's requirements.

Paper presented programme uses neutral network to optimize the flight test programme as well, according to the Customer's requirements, at a proposed cost, with safety of both the staff and the aircraft provided.

1 INTRODUCTION

In-flight aircraft testing is conducted according to Flight Test (FT) programme which is already prepared and approved (MoD 2010). Creating FT Programme requires enormous experience of researchers as well as knowledge of requirements listed in technical specifications, rules and regulations on aircraft building, standards, and Customer's requirements. The FT schedule which is a plan of flight trials execution over a specific period of time is an integral part of the FT programme. Account is taken of the availability of labour and resources, climatic conditions and other factors that may affect the execution of the trials, such as predispositions of flight test team members, their proficiency, etc., with flight test safety taken into consideration.

Taking into consideration all conditions mentioned above, which FT programme should fulfill, a tool, which allows to streamline FT programme development basing on AFIT experience, was presented.

Neural networks (Tadeusiewicz R. 1993, Rutkowski L. 2005), were used ex. for optimization of municipal transport vehicles usage (Świderski A, 2006) or for risk areas determination in aircraft renovation conduction (Jasińska J, 2010).

Presented programme has to be adjusted to match specified time and expenses. Tool used for FT programme time optimization is SYMBAD, software developed by Air Force Institute of Technology (AFIT).

2 FLIGHT TEST TIME SIMULATION SOFTWARE SYMBAD 2012/2013

The SYMBAD 2012/2013 software has been developed under the Borland C++ Builder programming environment. It uses an innovative approach to any issues of the aeronautical testing. The software can be used to estimate time consumed by specified tests on particular date and in particular place. Software uses following information as input data:

- reliability of individual aircraft tests,
- flyable days in particular months,
- flyable hours in particular months
- availability of the pilots
- the pilot data,

The software may also deliver a printout with the set of tests and predictions on time needed to accomplish them.

Interface of SYMBAD software and its modules have been expanded on in articles (Wójcik, J, & Zieja, M. 2012, Wójcik, J, & Kosiński, W. & Zieja, M. 2013).

Below, as a remainder, two example software windows are presented. (Fig. 1 and Fig. 2).

When analysing aircraft testing data, firstly, identification of threats that can influence programme is done and risk of occurrence of such events is estimated. Secondly, results of these analysis are imported directly to SYMBAD software.

An example of flyable hours in function of test conducting date analysis is presented below Depending on date specified by costumer, amount of flyable hours in the day varies (Fig. 3).

Another analytical example is the dependence of the number of days suitable for aircraft flight testing on the Customer-indicated test site (Fig. 4).

Data presented above is obtained from annual analysis performed during flight tests. The problem of analysis conduction and identification of threats has been expanded on in article (Hass A.M.J.: 2003, Jasińska, J. & Wójcik, J. & Kosiński, & W. Krupnik, D, 2011, Jasińska, J. & Wójcik, J. & Kosiński, W. 2012, Kosiński, W. & Pokora, W. 2012, Kosiński, W. & Wójcik, J, & Warchulski, J. & Zieja, M. 2012).

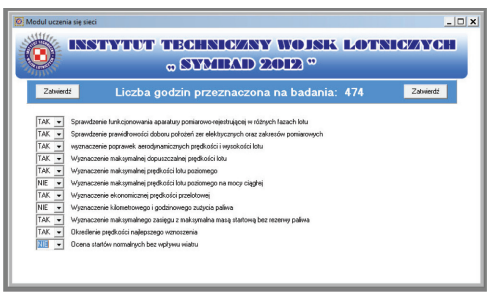


Figure 1. Network learning module in SYMBAD software.

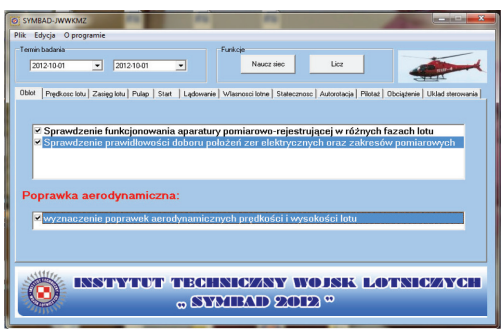


Figure 2. SYMBAD software interface.

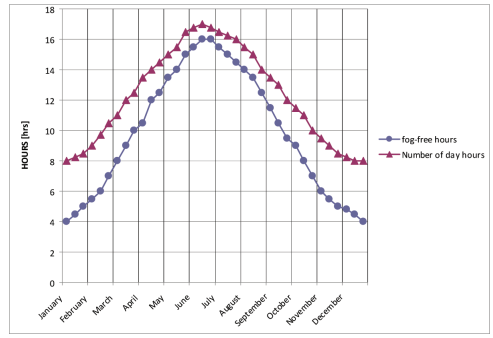


Figure 3. Distribution of flying hours in the daytime in particular months.

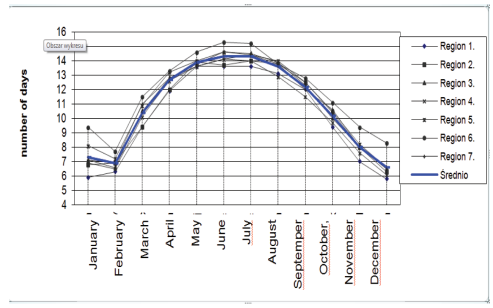


Figure 4. The average number of days with the following weather conditions: cloud cover ≤ 6/10; visibility ≥ 6 km on military airfields in various regions of Poland.

2.1 *Formal structure of aircraft testing model implemented in SYMBAD software*

For the need of flight tests optimization, flight test programme model (MBL) has been defined as ordered three:

$$MBL = < S_o, S_t, S_i > \quad (1)$$

where: S_o—organization structure of flight test programme, S_t—technical structure of flight test programme, S_i—information structure of flight test programme.

2.1.1 *Organization structure of flight test programme*

Within the concept of organization FT programme the following ordered pair is defined:

$$S_o = <B, R_o> \quad (2)$$

where: B—set of tests, R_o—relation defining organization of FT programme.

The initial assumption is $B \neq \phi$, which means that set of flight tests cannot be empty because:

$$B = \left\{ b_i; i = \overline{1,I} \right\} \neq \phi$$

where: b_i—pointer (np. number) of flight test, I—cardinality of set B.

Reliances and dependencies direction between two flight tests in given FT programme are described by relations. Hence, relation R_o takes the following form:

$$R_0 \subseteq B \times B = \left\{ < b_i, b_j >; i \neq j; ij = \overline{1,I} \right\} \quad (3)$$

Relation R_o, which is transformation of flight test research set B into itself, defines organizational-dependency reliances between each flight test in FT programme. Mainly they are limited to Figure 5.

$$R_0 = \left\{ R_0^1, R_0^2, R_0^3 \right\}$$

where: R_0^1—relation of organizational dependency (test subordination), R_0^2—relation of organizational priority (prioritized test), R_0^3—relation of organizational equivalence (independent tests).

Formally, dependency (or priority) can be specified by order relations ($\prec$) described on two elements b_i,b_j

$$< b_i, b_j > \in R_0^1 \Rightarrow b_i \prec b_j \quad (4)$$

Relation (4) describes organizational dependency between test, that is, if test b_j is to be done, test b_i has to be completed prior to it. This means that test b_j cannot be carried out without completing test b_i, while equivalence relation (R_0^3) marks possibility of simultaneous test conduction.

2.1.2 *Technical structure of flight test programme*

Concept of technical flight test structure S_t is referred to total personnel and aircraft readiness concerning specified flight test $b_i \in B$.

Formally, technical flight test structure S_t is defined in the form of ordered three:

$$S_t = <P, SP, R_t> \quad (5)$$

where: $P = \{pk; k = \overline{1,K}\}$—personel set, $SP = \{sp_l; l = \overline{1,L}\}$—aircraft set, R_t—relations of aircraft personnel assigning them to specified aircrafts and FT programmes.

Set of personnel P and aircraft set SP is synonymous with sets of technical readiness $\{dgt\}$ which are describing readiness to carry out given test set, that is:

$$P \equiv \left\{ dgt_i; i = \overline{1,I} \right\} \wedge SP \equiv \left\{ dgt_j; j = \overline{1,J} \right\} \quad (6)$$

By the relation R_t elements of personnel set P and aircraft set SP are assigned to specified flight tests (or FT sets) $b_i \in B$, that is:

$$R_t = \subseteq B \times P \times SP = \left\{ < b_i, p_{ik}, sp_{il} >; i = \overline{1,I}, k = \overline{1,K}, l = \overline{1,L} \right\} \quad (7)$$

Ordered threes $<b_i, p_{ik}, sp_{il}>$ defined in that way consist of personnel and aircraft readiness to carry out any given FT sets. Hence, relation R_t defines subsets of personel and aircraft for each and every fight test:

$$R : B \times P \times SP \rightarrow \left\{ DGT_i; i = \overline{1,I} \right\} = \left\{ P_i \subseteq P; SP_i \subseteq SP; i = \overline{1,I} \right\} \quad (8)$$

where: DGT_i—set of personnel and aircraft assigned to specified flight test set.

2.1.3 *Information structure of flight test programme*

Within the concept of informational structure S_i of MBL model, data analysis and threats identification system is defined. Mainly it consist of:

$$S_i = <A, O> \quad (9)$$

where: A—data analysis and threats identification system, O—planned optimization and applied prevention system.

Main task of data analysis and threats identification system A is determining:

- faulty elements of FT system,
- flyable days in particular months,
- flyable hours in particular month days,
- the necessity to repeat the test because of either weather conditions or a failure to carry out the test,
- unreliability of measuring equipment,
- susceptibility of the aircraft to failure, necessity of fault clearing,
- unforeseen events,

In turn, tasks of planned optimization and applied prevention system include:

- determining time of carrying out single flight test, $b_i \in B$,
- introducing correspondent prevention $\beta_i \in \beta$,
- determining personnel work time,
- determining aircraft work time.

Information structure S_i supplies SYMBAD software with relevant input data, that is, having

specified time period $T_i \in T$ available (counted in days N, where $i = \overline{1,N}$) which is spent on carrying out FT, calculating pointer of FT intensification α is possible. Thanks to this pointer, real time of carrying out the FT (αt), measured in hours, can be estimated.

Hence

$$\alpha t = \sum_{i=1}^{i=N} \alpha_i t_i, \tag{10}$$

where: $t_i = t_m^d$—flyable days in particular day (d—day, m—month), $\alpha_i = k_i l_i$—k_i marks number of personnel (crew) while l_i is the pointer of flyable hours t_i usage.

For the need of article case with using one aircraft in FT was considered. If more aircraft is available for FT, their readiness and amount has to be included in calculations, which makes problem more complicated.

3 ADAPTATION OF ANN ALGORITHM IN MBL STRUCTURE OF SYMBAD SOFTWARE

According to the article (Wójcik, J, Kosiński, W. Zieja, M. 2013) expected value of uncompleted FT in amount of time takes the following form:

$$B(t) = \frac{\lambda}{\beta} \ln(1 + \beta\alpha t) \quad for\ \beta \geq 1, \tag{11}$$

where: α—flight tests (flights) intensity, t—time planned for competing the tests, λ—pointer of uncompleted tests, β—pointer of learning, effectiveness of prevention applied during tests.

In turn, general model of artificial neuron network takes Figure 5.

Problem of ANN neuron network functioning and creating as well as activation function alone has been covered in article (Wójcik, J, & Zieja, M. 2012, Kosiński, W. Wójcik, J, Warchulski, J. Zieja, M. 2012).

It is worth to remark that information structure S_i of model MBL determines time of FT $T_i \in T$ while organization structure S_o as well as technical structure S_t is responsible for pointer of FT completion failure and activation function. In addition, organization structure determines way of neuron construction in ANN. In turn, pointer $\beta_i \in \beta$ is determined in process of network learning.

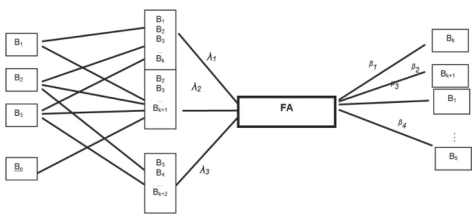


Figure 5. ANN Model.

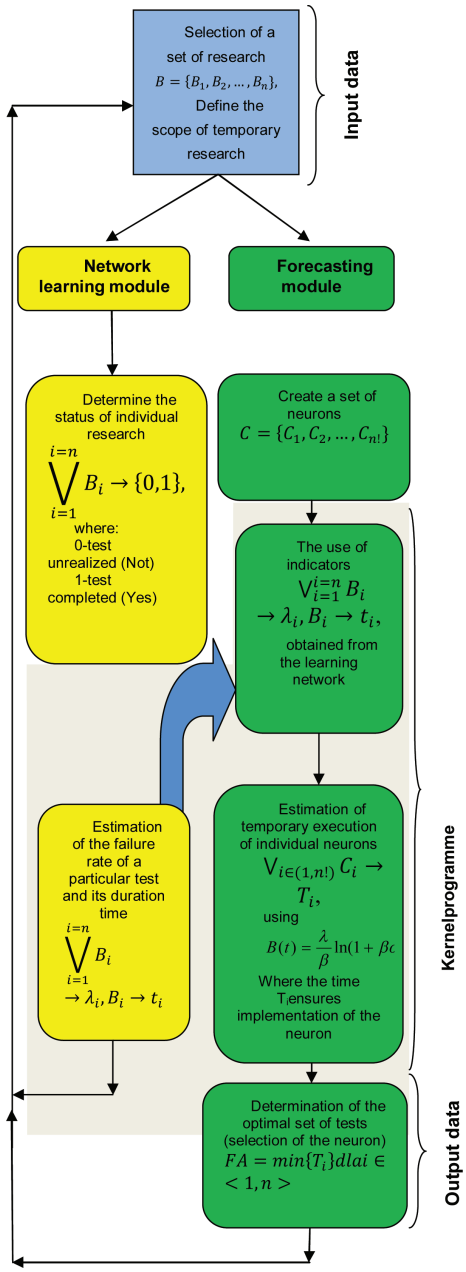


Figure 6. SYMBAD software algorithm.

4 GRAPHICAL INTERPRETATION OF THE MODEL

At the end, an example of MBL model usage for graphical imagining of processes occurring in SYMBAD software is presented. Algorithm presented below is described with details in article (Wójcik, J, Kosiński, W. Zieja, M. 2013).

5 CONCLUSION

Analysis of developed tests programmes and FT carried out according to them shows, that not always FT programme is completed totally according to assumptions. FT specification, complexity of test subject, participation of many teams, great variability of logistic insurance concepts and third conditions cause that big experience of project manager and collaborating teams as well as ability to foresee and estimate possible threats is required to estimate FT programme completion times.

Therefore, risk management in FT planning relies in great part on FT completion experience database. To meet requirements listed above, FT model (MBL) which corresponds with risk management in FT planning was presented in this article. MBL model enables to:

- identificate threats (S_i),
- estimate FT programme failure rate (S_l),
- develop FT programme (S_o),
- propose action that influence FT reliability (S_t),
- estimate time of FT programme completion (S_t,S_o),
- estimate place and year season influence on FT completion time (S_i).

As the next step ANN algorithm was adapted to MBL model (chapter 4,5). That enabled to extract in most transparent way each and every step of network's actions. Only ANN defined in that way was implemented in SYMBAD software. ANN is computing kernel of the software. Thanks to usage of MBL model and ANN, SYMBAD software has become tool that enforce FT developing.

Considering complexity of FT development and conduction process it is correct to make a statement that SYMBAD software alone will not exchange project manager (his rational way of thinking), however, it can be valuable assistance for him, foreseeing and estimating relevant pointers.

Model approach to problem of FT, adapted by MBL, enabled additional systemizing of FT completion experience database.

Further work on usage of ANN in MBL model will concentrate on detailed analysis of activation function which will be presented in next articles.

Developed programme is transparent and functional. It can be supporting tool not only for aircraft test planning but also for various technical objects tests planning, based on test conduction experience database.

REFERENCES

Hass, A.M.J., 2003. *Configuration Management Principles and Practice.* Addision, Wesley.

Instrukcja organizacji lotów próbnych w lotnictwie sił zbrojnych Rzeczypospolitej Polskiej, ILOP-2010, załącznik do *decyzji nr 476/MON Ministra Obrony Narodowej z dnia 17.12.2010 r*.

Jasińska, J. & Wójcik, J. & Kosiński, W. & Krupnik, D, 2011. Model procesowy szacowania ryzyka badań statków powietrznych, *Logistyka*, nr 4, poz. 357 płyta CD.

Jasińska, J. & Wójcik, J. & Kosiński, W., 2012. Metodyka oceny ryzyka w badaniach statków powietrznych, *Logistyka*, nr 4, poz.305 płyta CD.

Jasińska, J. 2010. Innowacyjne metody oceny ryzyka w procesach realizacji wyrobu, *Konferencja międzynarodowa, ZSJZ*.

Kosiński, W. & Pokora, W., 2012. The change control in aircraft testing, *KONES'12*.

Kosiński, W. & Wójcik, J. & Warchulski, J. & Zieja, M., 2012. Risk management in the course of aircraft flight test planning and the flight test programme optimization ESREL'12.

Rutkowski, L., 2005. *Metody i techniki sztucznej inteligencji,* PWN.

Świderski, A., 2006. Koncepcja wspomagania procesu decyzyjnego w certyfikacji systemów zarządzania z wykorzystaniem sztucznych sieci neuronowych, *Problemy Jakości, nr 6*.

Tadeusiewicz, R., 1993. *Sieci neuronowe*, Akademicka Oficyna Wydawnicza, Kraków.

Wójcik, J., & Zieja, M., 2012. Artificial neural networks as applied to aircraft flight test planning, *Journal of KONBIN* 1(21)2012 (ISSN 1895-8281).

Wójcik, J. & Kosiński, W. & Zieja, M., 2013, SYMBAD—instrument in the course of aircraft flight test planning, *Journal of KONES. Powertrain and Transport*, 4(20).

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Accelerated Life Test method for satellite electronic instrument

D. Shu, Z. Liang, Z. Zhiteng & M. Haibo
China Academy of Aerospace Standardization and Product Assurance, Beijing, China

ABSTRACT: This paper described the general process of Accelerated Life Test and its limits in use of satellite electronic instrument briefly; analysis several accelerated life test methods based on failure rate, empirical formula, accelerated degradation and transformation; proposes accelerated life test method based on activation energy estimate forecast, provided a new way for ALT of satellite electronic Instrument, and validated its applicability. Subject results promote the use of other satellite electronic instrument.

1 INTRODUCTION

For a spacecraft with high reliability and long life, electronic products reliability directly determines the life and reliability of the system. As the increase of satellite life and reliability index, higher requirements of life and reliability of satellite electronic products on project is also put forward. So how to evaluate and verify the life and reliability index is a problem that must be solved, and Accelerated Life Test (ALT) method can well solve the problem. The ALT method and assessment theory for electronic products on parts and subassembly level are relatively mature now and widely applied in engineering. But for an electronic unit, the ALT method and evaluation theory are not yet mature due to its complex in structure, diversity of failure mechanism and failure mode. Generally, only 1:1 life validation test or baseline test under accelerated stress is carried out. The role of accelerated life test on single devices cannot be replaced by the test on parts and subassembly, which is a new research direction of the accelerated life test technology. The study and application of the technology will be able to save a lot of research time, funds, manpower and material resources, having important engineering significance.

2 TRADITIONAL PROCESS OF ALT DESIGN AND EVALUATION AND ITS LIMITATIONS

2.1 *Traditional process of ALT design and evaluation*

According to the traditional design and evaluation process of ALT, the stress that affects the trial product most should be selected as accelerated stress. Then the acceleration model, product life distribution on this stress level, the accelerated stress level and distribution of tested samples can be determined and the test can be carried out. So product life data can be evaluated and product life can be obtained eventually. The details of traditional design and evaluation process of ALT are described in the following sections.

2.2 *The limitations of traditional methods in ALT design assessment of satellite unit*

The ALT experimental design mentioned in section 2.1 of traditional process is not applicable to satellite unit due to its characteristics which mainly include the following aspects:

1. The sample size is small
   The manufacturing process is complex and the cost is higher for satellite products, so the life test sample size is unlikely to be too large, especially for satellite unit. Sometimes only one product can be used for the life test. So it's hard to get the acceleration coefficient of products by the method of assessment.
2. Failure modes are diverse and failure mechanisms are complex
   The structure satellite unit is complex and its failure modes are diverse, and the corresponding failure reason is more complex. One of the premises of ALT is to ensure that the failure mechanism doesn't change and the accelerating model used for extrapolation is established based on the failure mechanism analysis. So the complexity of failure mechanism limits the application of ALT on satellite unit.
3. Failure data is difficult to obtain
   With continuous increase of satellite life, the designed life of the satellite products is also greatly increased. The time and money required to obtain failure data are very high, sometimes it is very difficult to accept even on the project. In traditional method, there must be sufficient

failure data for statistical analysis. So the obstacle for obtaining failure data is also one of the difficult points of ALT for satellite unit.

3 THE IDEA FOR ALT OF SATELLITE UNIT

There are several ideas in the study of ALT of satellite unit. The ideas are introduced here and their advantages and disadvantages are briefly analyzed.

3.1 *Failure rate ratio method*

According to GJB/Z299c-2006 "Electronic Equipment Reliability Prediction Handbook" and MIL-HDBK-217-F "Electronic Equipment Reliability Prediction", it can be seen that failure rate of components under different temperature is different. Through statistical calculations of all components failure rate, we can get product failure rate λ under different temperature T, also known as reliability prediction with stress method. With the increase of temperature, the product failure rate also will increase. As for the electronic products obeying index distribution, life characteristic (the reciprocal of failure rate, also known as average life) will be reduced accordingly.

The assumption is that the expected value of instrument failure rate is λ_0 under the using stress S_0 and the expected value of instrument failure rate is λ_i under the accelerated stress S_i. According to the characteristics of exponential distribution, the acceleration coefficient can be defined as:

$$A_i = \frac{L_0}{L_i} = \frac{\lambda_i}{\lambda_0} \tag{1}$$

where A_i is the acceleration coefficient, L_i the life characteristic under accelerated temperature stress, L_0 is the life characteristic under normal temperature stress, λ_i is the working failure rate under accelerated temperature stress; λ_0 is the working failure rate under normal temperature stress.

According to the above method, we can estimate the acceleration coefficient and carry out experiment design and evaluation. We should note that this method is based on the stress reliability prediction method. If the expected value cannot fully reflect the accelerated stress, the use of this method is restricted, such as multiple stress accelerated life test, etc. And for satellite unit, due to the complexity of its failure mechanism, failure rate ratio can only be as a reliability characterization of the product in different conditions but not as an accurate measure of life characteristic value, and there is no accurate theoretical basis.

3.2 *Empirical formula method*

This method is based on the empirical formula for the research of electronic products in USA. Namely the temperature raises every 10 °C, the double failure rate rises:

$$A_i = \frac{\lambda_i}{\lambda_0} = 2^{\left(\frac{T_i - T_0}{10}\right)} \tag{2}$$

where A_0 is the acceleration coefficient, T_i the acceleration temperature, T_0 is the normal temperature, λ_i is the working failure rate under accelerated temperature stress, λ_0 is the working failure rate under normal temperature stress.

This method can be used to estimate the acceleration coefficient and carry out experiment design and evaluation. Similar with failure rate ratio method, the theory of this method is not accurate, only as an experimental design reference value of the acceleration coefficient, and can only be used when the temperature is a single accelerated stress.

3.3 *Degradation fitting method*

For space instruments, the accelerated degradation test method is good ways to solve the difficulty of obtain the failure data. There are many literatures about accelerated degradation test and there are two problems we should pay attention to:

1. The degradation trends must be accurately obtained. This method can be only used for space instrument that its key performance parameters is obtained conveniently and has obvious degradation trends. The performance degradation of life for the instruments commonly used on the satellite at present, such as interfering closed loop fiber optic gyro, secondary power, PVC and PCU, cannot be measured generally because of closed loop feedback. So degradation test method is not suitable for these products.
2. The performance degradation component caused by accelerated stress must be decoupled from the measured data. The key performance parameters of instrument are often affected by many factors because of the complexity of its failure mechanism. How to decouple and fit the performance degradation caused by accelerated stress is one of the guarantees for implementing accelerated degradation test successfully.

3.4 *Transformation method*

The basic idea of transformation method is according to the principle of bucket. The life of any kind of product depends on the life of its component that easily becomes invalid. No matter how

superior the performance of important parts and design on the product is, if the failure of any spare parts or components that affect product performance occurs, the product's life comes to an end. So the product life depends on the reliable life of its weak parts. Therefore, the ALT of the product is converted into ALT of its parts or components after the weak points are found out.

Usually, the methods to find out the weak points of the instrument are as follows:

- Similar products analysis
- Statistical analysis to determine weak points from the using information
- Pareto diagram method
- Failure tree analysis method
- Failure Mode, Effects and Criticality Analysis (FMECA) method.

It is worth to notice that the weakness of satellite unit is often affected by the complex natural and induced environment. Because of the complexity of electrical and thermal stress, it's a large risk to replace the unit's ALT with weak components' ALT.

3.5 *Summary*

Four kinds of ALT methods of instrument are introduced in this section and have their own advantages and disadvantages. A new ALT design method based on reverse deduction of activation energy will be put forward in the following representation. Then combined with a certain type satellite control system PVC, the design and evaluation methods are introduced.

4 ALT DESIGN AND EVALUATION METHODS BASED ON THE ESTIMATION OF ACTIVATION ENERGY

The core of ALT is to find the life characteristic relationship of products between normal and accelerated stress. That is to describe the relationship between the two life characteristics with acceleration model and obtain the estimating parameters of the model through the evaluation data. In this chapter, the acceleration coefficient under different stress is got through analysis of product weaknesses and estimation of activation energy, as the basis of experiment design and data extrapolation.

4.1 *Establishment of model*

According to different stress, the acceleration model should be different. For electronic products, generally high temperature is chosen as the accelerated stress and Arrhenius model is selected as the acceleration model. Arrhenius model expression as follows:

$$L(T) = Be^{\frac{E_a}{KT}} \tag{3}$$

where L is the life characteristics, T is the absolute temperature; K is the Boltzmann constant, E_a is the activation energy, B is the undetermined coefficient.

Then the acceleration coefficient under the using temperature T_i as opposed to temperature T_0 is:

$$A_i = e^{\frac{E_a}{K}\left[\frac{1}{T_0}-\frac{1}{T_i}\right]} \tag{4}$$

where T_0 is the using environment temperature, T_i is the acceleration temperature, A_i is the acceleration coefficient.

4.2 *Activation energy determination of key components*

The unknown parameter E_a in formula 4.1 is activation energy that an atom on the crystal lattice to move to another lattice or clearance position need. For products, there is barrier in the process of transformation from normal state to failure state. The barrier is just the activation energy. The smaller the activation energy is, the easier the physical failure process becomes. If the activation energy is large, the acceleration coefficient becomes larger, then the failure speed is accelerated and failure happens. For certain types of products, activation energy is the physical significance of a fixed value. The activation reference value of main failure mechanism for some components is given by standard of the USA and Europe Aviation Bureau, and listed in Table 1.

Table 1. The typical activation energy given by ECS-Q-30-1 (2002).

Products	Type	Activation energy (eV)
Semiconductor	Gallium arsenide	1.4
	Silicon	1.1
Resistance	Metal film resistor	1.35
	Carbon resistor	1
	Winding resistor	1
Capacitor	Ceramic capacitor	1.67
	Glass film, mica capacitor	1.1
	Plastic film capacitor	3.4
	Tantalum capacitor	0.34

*In addition to the above table, activation energy of failure mechanism for silicon semiconductor is given by MIL-HDBK-338.

The activation energy in the table above is obtained from statistical analysis of test data after a large number of samples. But for aerospace electronic products, because of the lack of history test information, the unknown parameters in the acceleration model is often difficult to obtain by assessment especially for the lack of 1:1 life test failure data, making it difficult to obtain aerospace electronics acceleration life. The following methods can solve this problem to some extent.

4.3 *Solving the acceleration coefficient*

When estimating acceleration coefficient, failure rate ratio method tends to be more conservative and the computing process is also more complex because of the inclusion of all components' failure rate. According to formula (4), acceleration factor can be determined if the acceleration energy of the product is known. In the case of difficult to get the activation energy of the product, the activation energy of key or weak components can be used to replace it. The experimental design can be done after the calculation of acceleration coefficient. Then combined with the test results, the test can be evaluated and the effectiveness of the test can be verified.

The selection of activation energy should be determined comprehensively by FMEA, thermal analysis and reliability prediction of the product. Generally the largest inherent failure rate activation energy of the component is the priority. And the activation energy of key or weak components can be used to replace the product activation energy according to the engineering experience.

4.4 *Reverse deduction of test time*

To meet the needs of product reliability test, the accumulative test time which is used to check the reliability index R_L can be deduced:

$$R_L = \exp\left\{-\frac{t\chi_\gamma^2(2r+2)}{2T^*}\right\} \tag{5}$$

where R_L is the reliability lower limit, the equivalent accumulative test time, r is the correlation failure number, γ is the confidence, according to the requirement of the reliability of the product, t is the life index requirements.

If the T^* is got, then the experimental time can be deduced under the accelerated stress through the acceleration factor obtained above, and the test should be designed.

$$T^* = \sum_i t_i n_i A_i + \sum_j t_j n_j k_j \tag{6}$$

where T^* is the accumulative test time, t_i is the accelerated life test time, n_i is the sample size of accelerated life test, A_i is the acceleration coefficient, t_j is the on-orbit and history test time, n_j is the sample size of on-orbit and history test, k_j is the environmental factors.

4.5 *ALT of a certain electronic satellite unit*

PVC product is a voltage conversion component specially developed for control and propulsion system. It supplies power for the control and propulsion systems, such as the central control unite, gyro, momentum wheel, SADA, earth sensor, sun sensor, promoting power amplifier, etc. It is a certain type of key instrument directly related to the normal working of a certain satellite platform. Because of its high life and reliability requirement, the conventional test methods are not suitable for it. ALT of the PVC mainly including the following several aspects:

(1) Determine key and weak points of the product and estimate the activation energy of the machine, according to which to conclude the acceleration coefficient under different stress; (2) Estimate the test time required for verifying the life and reliability index. Then through analysis with the conventional life test and on-orbit data, the validity of the test and the correctness of the method can be verified; (3) Through estimated test time and combined with the engineering practice, the stress level and the cut-off time of the experiment can be finally determined; (4) Implement the test. Then process the test data to judge whether there are degradation trends and combine with other data to do the assessment; (5) Determine the activation energy by the test results, and the validity of the test results can be verified by the reverse deduction of the activation energy.

The life index of the product is verified by experiment. Reliability index under different working mode is presented by assessment, providing the basis for subsequent products. The good results are recognized by the product development personnel and experts in the industry.

5 CONCLUSIONS

The conclusions of this paper are as follows:

1. When the sample size, test time and many other conditions are limited, using the activation energy of key components to replace the one of electronic instruments to design and evaluate the test is feasible.
2. Because the determination of experimental time is very sensitive to the choosing of activation energy in the design of experiment, how to reasonably determine the activation energy

is the key part in the process of experimental design.

3. In this paper, the ALT methods of instruments satisfy the long life and high reliability requirement of aerospace electronic product assessment project in a certain extent, and can be applied in other aerospace electronic, electromechanical and photoelectric products.

At present, the above method has been applied to a variety of accelerated life tests on electronic product design, implementation and data assessment, having excellent application prospect.

ACKNOWLEDGMENT

The research described in this paper was carried out by the China Academy of Aerospace Standardization and Product Assurance.

What is need to be emphasized is that the accelerated life test method discussed in this paper has got good achievement in a certain type of satellite device developed by China Academy of Space Technology. For security reasons, public discussion of test data is prohibited here.

REFERENCES

Dong Shu, Zhang Yunzhong, ZhuWei, 2009, A method for ALT Data Process based on compete-failure-model, China Space Reliability Conference, Beijing.

Dong Shu, Li Shuzhen, 2012, ALT design and evaluation for Space FOG [J]. Equipment quality, Beijing.

Elsayed E.A, Zhang Hao. Design of PH-based accelerated life testing plans under multiple-stress-type [J] Reliability Engineering and System Safety, 2006.

Loon-Ching Tang, Kai Xu. A Multiple Objective Framework for Planning Accelerated Life Tests[C] IEEE Transaction on Reliability, 2005, 54(1): 58–63.

Mohammed Al Haj Ebrahem, James J. Higgins. 2006, Non-parametric analysis of a proportional wearout model for accelerated degradation data[J]. Aliped Mathematics and Computation, 174:365–373.

Mohammed Al Haj Ebrahem, James J. Higgins. Non-parametric analysis of a proportional wearout model for accelerated degradation data [J]. Aliped Mathematics and Computation, 2006, V174:365–373.

Nelson W.B. A Bibliography of Accelerated Test Plans [J]. IEEE Trans. Reliab, 2005, 54(2): 194–197.

Tian Z., 2007 Multi-state system reliability analysis and optimization [D]. Alberta: University of Alberta.

Won Young Yun, Eun Suk Kim, Ji Hwan Cha. Accelerated life test data analysis for repairable systems [J]. Communications in Statistics-Theory and Methods, 2006, V35(10):1803–1814.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability of the airlines operations system

A. Słodownik & J. Żurek
Air Force Institute of Technology, OH, USA

ABSTRACT: Liberalization of European air transportation market resulted in more competitive airlines business environment and intensified airlines efforts to improve effectiveness of schedule performance. The problem of effectiveness of flights schedule performance has become more important in light of introduction of limits on free of charge aviation emissions and announced introduction of airlines financial responsibility to passengers for flights delays.

Airlines perform flights within the frame of their operational systems in close cooperation with air traffic management system. The key factor influencing effectiveness of performing flights is access to air space in accordance with offered schedule timing and possibility of flights realization at minimum fuel cost. In real conditions of constrained capacity and disturbed air space it is not possible to provide optimum access to air space for all space users what results in flights delays and higher fuel consumption, what in turn negatively impacts airlines profitability. In order to objectively assess the quality of access to air space one should compare total costs of flight realization incurred by airlines against optimum flight realization cost. This kind of analysis lays the ground for valuation of air traffic management system performance. In general the value of air traffic management system performance is manifested in its relationship to the airlines main product—the flight schedule. Measuring the value of air traffic management system performance should therefore be related to how the air traffic management system impacts the airlines' ability to plan and operate their schedules. This is the issue of reliability cost of the airlines operational system. To be competitive the airlines should maintain equilibrium of operational reliability and cost. In general airlines calculate their flight operations cost as a sum of direct operation cost and cost of delays. Direct operating cost is the sum of fuel cost and time related cost and is dependent on quality of access to air space managed by air traffic management system. Delay cost in turn is the sum of additional direct operation cost and market cost calculated as potentially lost revenue. The analysis of potentially lost revenue can be based on the models of decision choice, where schedule unreliability is modeled as a loss of utility of the airlines product. For the purpose of airlines schedule reliability cost analysis the problem should be analyzed as total cost of access to air space including additional costs of adjustment of the flight timing imposed by air traffic control. Currently applied measures are based on high level Key Performance Indicators (KPI) and their application for more detailed analysis is limited. In this paper authors propose more specific category of schedule reliability cost measure based on the concept of division of reliability states space into four categories of states depending on cost effectiveness of punctual (against flight plan) flight realization. The measure of cost effectiveness of reliable flight realization is based on the known concept of cost index but interpreted as a function of marginal cost of aircraft ground speed. Proposed measure of reliability cost is also the measure of such categories of flight operations reliability measures like equity of airlines access to the air space and effectiveness of flight planning.

1 CURRENT STATE OF TAXONOMY OF FLIGHT OPERATIONS PERFORMANCE METRICS

Under general concept of System Effectiveness (SE), the System Effectiveness is defined as:

$$\mathrm{SE} = O_R * R_M * D_A \tag{1}$$

In equation (1) operational readiness, O_R is the probability that the system is either available at beginning of the mission or can be brought to an operationally ready state by the beginning of the mission within a prescribed period of time. The probability that having started the mission successfully, system will complete the mission without failure is mission reliability, R_M. The probability that having completed the mission the system has performed successfully all of its required mission objectives and required end results is design adequacy, D_A. Following definition of System Effectiveness (SE), the effectiveness of flight realization can be modeled as a realization of transportation cycles. Operational readiness O_R of the

transportation cycle is the probability of the completion of the aircraft ground service cycle until scheduled time of departure. Mission reliability is the probability of punctual realization of scheduled flight, but design adequacy is the probability of the assignment of the aircraft of sufficient capacity (sufficient number of passenger seats) to accommodate demand for the flight.

Under current taxonomy of reliability of flight operations metrics, the following basic measures are in use by airlines: distribution of arrival delays, distribution of departure delays, distribution of block times (from departure from airport departure gate to time of arrival at arrival airport gate), distribution of load factors (percentage of used passenger seats). Airports monitor following productivity measures: departing and arriving passenger and cargo traffic by time of the day, day of the week, months and calendar year, departing and arriving aircraft by aircraft type and time of operations (departure, arrival, ramp handling timing). With known distribution of the flight operations times, the reliability of realization of transportation cycle can be modeled as a consecutive realization of basic transportation cycles composed of two phases of the cycle, the ground service phase followed by flight realization phase. Reliability of realization of the phase of transportation cycle is defined as:

$$R = P[X'' \le t'' \mid X' \le t'] \tag{2}$$

$$R = \frac{1}{H(t)} \int_{-\infty}^{t''} F(t'' - s, s) * \quad h(s) ds \tag{3}$$

where: X''—random moment of the completion of realization of the phase; t''—scheduled time of the completion of realization of the phase; X'—random moment of the beginning of realization of the phase; t'—scheduled time of the beginning of realization of the phase; $H(t)$ id the CDF of the random moment of beginning of the phase; $h(s)$ is the PDF of random moment of beginning of the phase; $F(\cdot)$ is the CDF of the time of realization of the phase. The model of airline operation cycle is being applied for stochastic optimization of time buffers in airline schedules for improvement of robustness of planned schedules. Reliability of realization of transportation tasks can be analyzed from different perspectives, the airlines perspective, the Air Traffic Control (ATC) system perspective, the airports perspective and passengers and air cargo markets perspectives.

Taking into consideration the dependence of airline flight operation on air traffic management system the Air Traffic Services Performance Focus Group of FAA identified the following attributes of flight operations performance: Capacity—potential throughput that can be achieved under a given set of conditions; Delay—difference between actual flight time and baselined optimum times; Access—users ability to utilize system resources and services; Predictability—ability to forecast system behavior and to meet a commitment; Flexibility—ability of the system to permit users to adapt their operations to changing conditions; Efficiency—a percent measure of how close an operational parameter is close to a given "optimal" value (System Efficiency, User Efficiency, Resource Efficiency). With reference to given attributes of system performance, several detailed measures have been identified: Capacity—System Level Capacity, Airport Level Capacity, Airspace Volume Capacity, Diversions by Course; Delay—Delay by Phase of Flight, General Delay, Delay by Course; Access—Approvals, % of requests approved for user preferred flight plan by Communication, Navigation, Surveillance Services; Predictability—Variability of delay (for delays by phase of flight), Standard Deviation of absolute difference between forecast and actual delay; Flexibility—Alternatives—an average number of alternative flight plans offered in response to flight plan request; Approvals for deviations (% of approvals related to flight plan changes; max. allowable deviation from approved flight plan); total number of restrictions in route, altitude, speed, heading per volume of aerospace); Efficiency—Time (% of departure within x minutes of standard departure time); Altitude (% of difference between user requested (optimal) and system imposed changes); Speed (% of difference between user requested (optimal) and system imposed changes); Distance (% of difference between user requested (optimal) and system imposed changes.

According to Eurocontrol rules, the performance of European air traffic control system is monitored by following performance/safety categories: Traffic, Safety, Capacity, Environment and Cost. The key performance indicators per performance category are defined as following: Traffic: Number of IFR flights in European airspace per year; Safety: Number of accidence including accidences with Air Navigation System (ANS) contribution; Capacity: Average en-route Air Traffic Flow Management (ATFM) delays per flight; Environment: Horizontal en-route flight efficiency measured by percentage of trajectories flown not in conformance with planned trajectories;

From system effectiveness perspective, the reliability of the timely schedule realization represents only one dimension of the system effectiveness. The second dimension is economy of realization of air transportation tasks. Both dimensions are interdependent. Currently, the flight operation costs are measured at high level of aggregation. Air Traffic

Management System costs are measured as an en-route real cost per Service Unit (SU*); Service unit is related to Maximum Take-Off Weight of the aircraft (MTOW) and is defined as:

$$\text{Weight Coefficient} = (\text{MTOW})^{0,7} \tag{4}$$

$$\text{TSU} = \sum_{\text{Number of flights}} (\text{Weight Coefficient}) \tag{5}$$

where TSU is total service units. Current system of charges for ATC services in based on the concept of service units SU (charges for overflying of the airspace) and terminal service units TSU for services provided in the terminal airspace.

Airlines calculate aggregated direct operation cost per unit of aircraft productivity (one passenger seat flown per distance of 1 mile (or 1 kilometer). For each flight airlines forecast direct operating cost based on statistic weather forecast data and related statistic optimum flight levels (tables of statistic of available loads).

In general, the contemporary level of measurement of flight operation performance can be described as a statistical description of the air traffic and timing of flights realizations. There are no in-depth absolute measures of flight operations reliability costs. The problem lies in high level of complex interactions between all factors involved in flights realizations and random nature of operations environment. Therefore in search for industry accepted metrics of flight reliability and related costs, the contemporary research is oriented on comparative analysis of performance trends. Based on such analysis the industry is developing methods of compensation for air traffic management system related inefficiencies. It seems to be the only way to improve the methodology of calculation of charges for air space usage based on real airlines flight operations costs.

2 PROPOSED APPROACH TO RELIABILITY COSTS

In the controlled airspace, aircraft perform flights on the basis of optimal flight plans filled before the flight and corrected according to changes in the air traffic. Flights are performed along available optimum trajectories and at the speed resulting from the timing of flight realization imposed by air traffic control. At every moment of cruising phase, the state of the flight is defined as a vector $s(t)$:

$$\overline{s(t)} = \left\{ \begin{matrix} GW(t), \overline{k(t)}, P(t), H(t), T(t), \\ M(t), W_f(t), \overline{V_{GR}}(t) \end{matrix} \right\} \tag{6}$$

where: $GW(t)$—aircraft weight; $\overline{k(t)}$—coordinates of the aircraft position; $H(t)$—altitude; $T(t)$—air temperature; $M(t)$—Mach number; W_f—fuel flow; $\overline{V_{GR}}$—ground speed. For each aircraft type and each state of the flight the corresponding fuel efficiency performance of the aircraft is defined as a specific range S_R defined as a distance flown by the aircraft from one unit of consumed (burned) fuel:

$$S_{R(CORR)} = \frac{V_{GR}}{W_f} \tag{7}$$

where $S_{R(CORR)}$ is specific range corrected for wind (in still air $S_{R(CORR)} = S_R$). Given the term (definition) of the scheduled flight time cost (c_t), the direct operating cost of the scheduled flight (sdoc) of the flight lasted T time units is defined as:

$$\text{sdoc} = c_t * T + c_f * F \tag{8}$$

where: c_t—cost of the unit of the flight time; c_f—cost of the unit of the fuel; T—flight time; F—total fuel used.

$$\text{sdoc} = c_t * T + c_f * F = c_t * \left(\frac{R}{V_{gr}} \right) + c_f * \left(\frac{R}{S_{R(CORR)}} \right) = c_t * \left(\frac{R}{a \times M + V_w} \right) + c_f * \left(\frac{R}{S_{R(CORR)}} \right) \tag{9}$$

where: R—range (distance flown); a—speed of sound; M—Mach number; V_w—wind speed. Given the definition of the Operation Reliability Cost Function (ORCF) as a direct operating cost (doc) of scheduled (punctual) realization of the flight per unit of distance flown and definition of the Reliability Cost Index (RCI) as a ratio of the time cost (c_t) to fuel cost (c_f), the RCI and ORCFCF are defined as:

$$\text{RCI} = \frac{c_t}{c_f} \tag{10}$$

$$\text{ORCF} = \frac{doc}{R} = c_t \left(\text{RCI} \frac{1}{a \times M + V_w} \right) + c_f \left(\frac{1}{S_{R(CORR)}} \right) \tag{11}$$

For the given state of the flight realization $s(t)$, parameterized by gross weight of the aircraft, altitude and atmospheric conditions there is Mach number corresponding to maximum range of aircraft—the maximum distance flown from the unit of fuel. This Mach number is defined as M_{LRC} and corresponds to long range cruise state of the flight. From perspective of flight economy, the realization of the flight at the M_{LRC} Mach number,

is the most fuel cost effective (fuel efficient) flight realization. However the possibility of the flight realization at M_{LRC} is dependent on approval by Air Traffic Control (ATC) of the availability of optimal access to airspace at the flight timing corresponding to flying at M_{LRC} Mach number. In general the ATC system imposed speed (and resulting flight timing) is the result of the analysis of availability of the airspace capacity at forecasted time of arrival at arrival airport terminal zone. The cost of fuel required to increase speed from maximum range cruise Mach number (M_{LRC}) to ATC system imposed speed is equal to the cost of flight time reduction resulting from increasing speed from maximum range cruise speed to required speed. This cost can be interpreted as a marginal cost of the cruising speed (MC) and are defined as:

$$\mathrm{MC} = \frac{\partial ORCF}{\partial M} \tag{12}$$

The minimum of the Operation Reliability Cost Function (ORCF) and related Mach number can be computed from the following equation:

$$\frac{\partial ORCF}{\partial M} = 0 \tag{13}$$

The Operation Reliability Cost Function (ORCF) is the sum of flight time cost and fuel cost. Based on definition of Reliability Cost Index, the flight time cost can be interpreted as additional fuel cost to complete the cruising phase of the flight within time T. If the flight realization at M_{LRC} Mach number corresponds to ATC approved flight timing, the time cost and RCI are equal to zero. Therefore the time cost can be interpreted as an additional cost expressed in cost of the additional fuel required to complete the flight in conformance with the ATC requested flight timing. So the RCI is the indicator of the marginal cost of the cruise speed. For each moment of the realization of the flight at system's imposed speed and for the known cost of the fuel there is corresponding Reliability Cost Index RCI (t) which can be interpreted as an indicator of current reliability cost of flight realization. The indicator of reliability cost of the whole flight, the Flight Reliability Cost Index (FRCI) is defined as:

$$\mathrm{FRCI} = \frac{1}{t''_{crs} - t'_{crs}} \int_{t'_{crs}}^{t''_{crs}} \mathrm{RCI}(t)dt \tag{14}$$

where t'_{crs}—moment of the beginning of the cruise phase of the flight; t''_{crs}—moment of the completion of the cruise phase of the flight. Based on the definition of FRCI, one can propose the measure of effectiveness of the ATC system as two parametric Key Performance Indicator (KPI) of the effectiveness of flight realization. Let's define two random variables X and Y corresponding to different categories of the effectiveness of flight realization as following:

$$X = \begin{cases} 1 & \text{for } FRCI_R \le FRCI_P \\ 0 & \text{for } FRCI_R > FRCI_P \end{cases}$$
$$Y = \begin{cases} 1 & \text{for } T'' \le t'' \\ 0 & \text{for } T'' > t'' \end{cases} \tag{15}$$

where: T''—actual time of arrival; t''—planned time of arrival. Let's define four sets of states S_{11}, S_{10}, S_{01}, S_{00} corresponding to different categories of effectiveness of flight realization:

$$\begin{aligned} &S_{11}\text{—}\textit{Set of Intentional Stated};\ P_{11} = P\{X = 1, Y = 1\} \\ &S_{10}\text{—}\textit{Set of Disturbed States};\ P_{10} = P\{X = 1, Y = 0\} \\ &S_{01}\text{—}\textit{Set of Disturbed States};\ P_{01} = P\{X = 0, Y = 1\} \\ &S_{00}\text{—}\textit{Set of Disturbed States};\ P_{00} = P\{X = 0, Y = 0\} \end{aligned} \tag{16}$$

where, P_{11}, P_{10}, P_{01}, P_{00} are probabilities of the defined states. State S_{11} is intentional state or state of intentional flight realization. State S_{10} is the state of delayed flight realization but without additional fuel cost. State S_{01} is the state of punctual flight realization (against flight plan timing) but at additional fuel cost. State S_{00} is the state of total inefficiency characterized by delayed flight realization and higher (against flight plan) fuel consumption at cruising phase of the flight. Probabilities of defined states are proposed Key Performance Indicators of the effectiveness of airline's realization of the scheduled flights in controlled airspace. They are also measures of the quality of the information provided by Air Traffic Control system (ATC). The advantage of the proposed methodology of measurement of airlines operation reliability over current statistical measures is in assumption of the aircraft performance characteristic as a reference base for assessment of quality of flight planning and air traffic management services manifested in adjustment of flight plan during the flight realization according to current flights movements in controlled airspace. Under this methodology one can take into account fuel cost used for adjustment of aircraft movement to ATC system's requirements. This assumption allows for better assessment of the results of the complex interdependencies of the airline, Air Traffic Control (ATC) system and airports (as points in the process of schedule realization).

REFERENCES

Ahmed Abdelgany and Khaled Abdelgany 2009. *Modeling Applications in the Airline Industry.*

Air Traffic Services Performance Focus Group (ATSP FG) of CNS/ATM Focused Team of the Federal Aviation Administration (FAA) 1999. *Airline Metric Concepts for Evaluating Air Traffic Service Performance.*

Cheng-Lung Wu 2010. *Airline Operation and Delay Management.*

David Allen Manager CNS/ATM Projects Boeing Commercial Airplane Group. *The Business Side of CNS/ATM.*

Massoud Bazagran 2010. *Airline Operations and Scheduling 2nd edition.*

2nd USA/Europe Air Traffic Management R&D Seminar December 1998. *Impact of Air Traffic Management on Air Space User Economic Performance.*

5th USA/Europe Air Traffic Management R&D Seminar June 2003. *Standardizing Performance Metrics.*

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantitative evaluation on storage reliability of pyrotechnics based on thermodynamic characteristic of dynamite and performance degradation data

Zhao Wan, Wu Hang & Cheng Hai Long
China Academy of Aerospace Standardization and Product Assurance, Beijing, China

ABSTRACT: Aiming at the deficiency of the traditional storage reliability evaluation method in dealing with zero-failure data, a method was proposed based on the performance degradation data. By analyzing the thermodynamic characteristic of dynamite and the failure physical model of pyrotechnics, the relationship of reliability and the performance degradation quantity was established, and then the storage reliability evaluation for pyrotechnics could be evaluated. An example was given about how to practice finally. The validity and applicability was validated. This method puts forward a new idea for storage reliability evaluation of pyrotechnics and other analogous products.

1 INTRODUCTION

Pyrotechnics is widely used in kinds of spacecraft, and it is a kind of high reliability and long storage life of one-shot product. It is difficult to obtain the storage failure data in a short term, traditional method based on failure data can't meet the requirements of its storage reliability evaluation.

The storage failure of pyrotechnics is often caused by several kinds of failure mechanisms, and multiple degradation processes occurs at the same time. The degradation reaction rate depends on the fastest process. Generally speaking, Storage reliability of pyrotechnics depends on three aspects:

1. The storage properties of pyrotechnics, such as thermal stability, hygroscopicity;
2. The structure of pyrotechnics, such as airproof quality;
3. The external environment, such as temperature, humidity conditions.

It has been shown that among the above three aspects, the thermodynamic characteristics of pyrotechnics is the immanent cause that determines the storage reliability, and environmental temperature and humidity are important external factors influencing storage reliability. At present, humidity is controlled strictly during the design, production, storage period, and the structure has a good airproof performance. In this case, the change of environmental temperature is the main factor which can cause the gradual degradation of thermodynamic characteristic of dynamite. Final failure occurs when the degradation develops to a certain extent.

According to the engineering experience, the sensitive parameters of pyrotechnics are the most critical parameters which can reflects its performance change. The poor sensitive parameter expresses the poor performance of pyrotechnics. Therefore, the relationship between reliability and storage time can be established through the analysis of the trend of sensitive parameters change. Accelerated storage life test is a way to get storage performance degradation data. This paper presents a method to establish the quantitative relationship between reliability and storage time by analyzing the temperature stress accelerated storage life test data for example. This method puts forward a new idea for storage reliability evaluation of pyrotechnics and other analogous products.

2 CHOOSING THE SENSITIVE PARAMETERS OF PYROTECHNICS

In order to determine the failure degradation of pyrotechnics in the storage process, the sensitive parameters is chosen as degradation parameters. A certain pyrotechnics has two sensitive parameters at most, usually one. When the sensitive parameters can't meet the design requirement, the degradation failure occurs. Thus the sensitive parameters must have following properties:

1. They can be precisely defined and monitored;
2. They have significant time-degradation trend in long-time work or test.

For example, the average ignition sensitivity, reaction time of electric detonator, the ignition

pressure of igniter and the separation impulse of explosive bolt.

These parameters objectively reflect the working status of pyrotechnics.

3 DEMONSTRATION OF QUANTITATIVE EVALUATION METHOD

Assuming that a certain explosive bolts conducted accelerated storage life test under three temperature stress as 60°C, 71°C, 80°C, and Arrhenius model was chosen as the accelerated model. Samples and detecting time in the test process was shown in Table 1.

Assuming that its reliability requirements was $R_L = 0.99$ ($r = 0.95$), and its sensitive parameter was separation impulse ($m_L v$, the impulse generated by bolt body when separated). Zero-failure data was achieved in three stress level. It was difficult to solve the storage reliability evaluation problem by traditional method based on failure data analysis. If the separation impulse test data appeared obvious degradation trend along with prolonged test time, then it was able to assess the storage reliability by analysis on the degradation trend of its separation impulse.

3.1 *Reliability model*

Explosive bolt achieves the separation function mainly by using the force of the explosion which can make the bolt body to break off. When the explosion pressure is increased to certain strength, explosive bolt is divided into two bodies. Assumed that the explosion force of dynamite and bearing capacity of structure are two random variables, the product separation reliability can be expressed as the probability of explosion force exceeds bearing capacity of structure, and the expression is:

$$R = P(E_{explosion} > E_{bearing}) \tag{1}$$

Reference to the stress-strength model in mechanical field, the reliability model of explosive bolt can be established as follows:

$$R = \Phi\left(\frac{K-1}{\sqrt{C_{VL}^2 \cdot K^2 + C_{VS}^2}}\right) \tag{2}$$

where:

C_{VL}—variation coefficient of explosion force;
C_{VS}—variation coefficient of bearing capacity;
K—Margin, $K=E_{\text{explosion}}/E_{\text{bearing}}$

Table 1. Sample size and time for explosive blot accelerated storage life test.

T/°C	No. of explosive bolts	Group	No. of experiment	Detecting time/d
60	30	1	10	36
		2	10	57
		3	10	71
		4	8	85
71	30	1	10	14
		2	10	22
		3	10	28
		4	8	35
80	24	1	10	13
		2	10	15
		3	10	20

3.2 *Determination of the model parameters*

3.2.1 *Determination of K*

Assumed that the dynamite combustion product obey the ideal gas equation:

$$pV = m_D f \tag{3}$$

where:

p—Pressure generated by combustion or explosion of dynamite, $N \cdot m^{-2}$
V—capacity of vessel, m^3
m_D—main charge mass of explosive bolts, mg
f—dynamite characteristics, energy produced by per unit mass of dynamite, $N \cdot m \cdot kg^{-1}$

When the structure design is finalized and the dynamite is selected, the explosion force is proportional to the dynamite mass. As the working time is nearly instantaneous, this research ignored the heat loss and the tiny change of the chamber volume as working, which means that the explosion energy has been used in two aspects; one is to separate the bolt body, the other is to produce kinetic energy when bolt body flies out.

Assuming that

- m_M is the critical dynamite charge mass, mg, the charge mass which just makes the explosive bolt to separate;
- m_L is the mass of the bolt head, mg
- v is the average speed of the bolt head flying out when the explosive bolt separates, m/s

Then, according to the working principle of the explosive bolt, its output energy meets the relationship below:

$$m_D RT = E_{explosion} = \frac{1}{2} m_L v^2 + E_{bearing} = \frac{1}{2} m_L v^2 + m_M RT \tag{4}$$

That is:

$$K = \frac{E_{explosion}}{E_{bearing}} = \frac{m_D f}{m_M f} = \frac{m_D}{m_M} = \frac{\frac{1}{2} m_L v^2}{E_{bearing}} + 1 \qquad (5)$$

After storage, the dynamite characteristics f changed, then induced the explosive force changed. According to the formula (7), as the bearing capacity unchanged, the dynamite characteristics change inevitably caused the speed change of the bolt head flying out. That's to say, the separation impulse changed. Kinetic energy 1/2 $m_L v^2$ can be calculated by detect the separation impulse $m_L v$. Then the margin K can be achieved.

3.2.2 *Determination of variation coefficient*

According to the above analysis, variation coefficient of explosion force C_{VL} can be expressed by the variation coefficient of Kinetic energy. The tensile strength of the material and the section diameter of the bolt body are the main factors which can influence the bearing capacity. But the design of these factors is aiming to meet the connection function, and it has been determined before the separation reliability design, and these factors change so little in the process of storage that can be neglected. Then the variation coefficient of bearing capacity C_{VS} can be considered constant and it can be calculated by the acceptance test data.

3.3 *Reliability calculation based on performance degradation data*

Assuming that $f = 11.63 \times 10^5 N \cdot m/kg$, $m_D = 480$ mg, m_M = 255 mg, then margin before storage is K = 1.8824 and the variation coefficient C_{VS} = 0.1149. According to calculation method above C_{VL}, K and R before and after storage can be calculated under the triple temperature levels.

According to the design requirements of this explosive bolt reliability and the above calculated results, the time when the reliability down to less than 0.999 marked the failure time under each temperature level with the analysis tool MATLAB. The results are as follows:

$T_1 = 60°C$, $t_{failure} = 80d$;
$T_1 = 71°C$, $t_{failure} = 31d$;
$T_1 = 80°C$, $t_{failure} = 15d$;

According to the acceleration model, it can be obtained:

$E_a = 81.77124\ kj \cdot mol^{-1}$
$t = 4013.804\ d \approx 10$a

The explosive bolt approximately has 10 years storage life in which it can meet the reliability requirement of 0.999. According to Table 2 and computing results above, two parameter exponential fitting curve (R^2 = 0.9708) of relationship between the reliability and storage time at normal temperature can be achieved as shown in Figure 1.

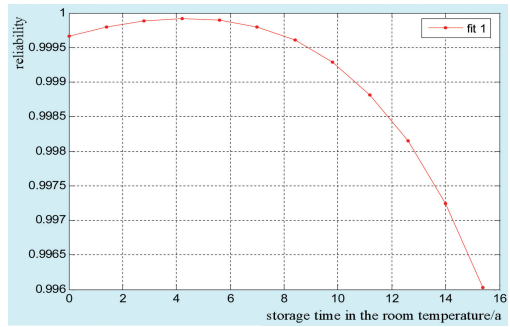


Figure 1. Reliability curve of explosive blot at normal temperature.

4 ANALYSIS AND CONCLUSIONS

Through the above research and analysis, this paper draws the following conclusions and suggestions:

1. As for the pyrotechnics sensitive to temperature, the quantitative relationship between reliability and storage life can be established. This paper presented the method and demonstrated it by a specific example.
2. The earlier storage period is a gradual mixing, homogeneous process for dynamite, and its performances won't appear obvious degradation within a short period of time (such as less than 4 years) usually but a certain improvement. However, with increasing of storage temperature and prolonged storage time, the molecules number and its vibration amplitude and frequency continually increase, which can increase the fracture probability of the weakest pharmaceutical molecules, then the dynamite chemical decomposition gradually accelerate which can cause the obvious degradation of sensitive parameters.
3. The more samples and detection points, the higher credible degrees of the calculation results. All the dear readers are advised to perform further application verification and improvement to this method in the follow-up test and study.

REFERENCES

AIAA S-113-2005 Criteria for Explosive Systems and Devices Used on Launch and Space Vehicles (DRAFT).

AIAA 2004-3419. Uses and Abuses of Accelerated Age Testing of Pyrotechnic Devices. 40th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit.

AIAA 2000-3646 Accelerated Aging Testing of Energetic Components—A current Assessment of Methodology. 36th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit.

Dong-yang Li, Zhi-ling Liu Analysis on the long storage invalidation [J]. Initiates & Pyrotechnics. 1996. (2):28~30.

MIL-HDBK-83578 (USAF) criteria for explosive systems and devices used on space vehicles, 1 January 1999.

Zhang YA, An Xiao hong. The Evaluation Method Study on the Storage Life of Initiating Explosive Device [J]. Journal of projectiles, rockets, missile and guidance, 2006(2):74~76.

Zhao Wan, Research on the Step Stress Accelerated Storage Life Test Method of Space Pyrotechnic Devices [J]. 2008(3):20~23.

Zhao Wan, Tian-long HAN. Optimum Design Method of the Accelerated Storage Life Test for Pyrotechnics Based on Activation Energy [J]. Chinese journal of energetic materials, 2009(4):475~477.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Telematics used in the campaigns machinery safety management systems

J. Napiórkowski, P. Szczyglak & K. Kołakowski
University of Warmia and Mazury, Olsztyn, Poland

ABSTRACT: The manuscript used in the campaigns machines management supporting systems analyzed. The types of demonstrated systems in the direction of productivity and quality of worker process growth, and service maintenance supporting are developed. Despite the many advantages they support user safety in a small extent. For this reason, the authors, four concepts of existing supervising work processes extensions present. These include: the concept of the machine exploitation permissions and the operator daily work time supervising system, the field emergency call system, the agricultural machinery rotating components limited access, and field collision courses correction system.

1 INTRODUCTION

The main technical objects used in the campaigns are the agricultural machineries. The reliability and safety of these machines evolution takes place at the all stages of its existence, instead especially during their exploitation. This type of machines are characterized by a short period of use in relation to the storage period, and the work processes execution under varying field and weather conditions, biological materials with variable, dependent from time, physical and chemical properties, and persons do not have a proper general education accessibility. Therefore, they have to fuel feel the strict of realized quality and safety process requirements.

There are many emergency in the agricultural sector every year. In Poland, only in 2013, the number of 23 374 emergency to the Regional Offices and Local Insurance Institutions were reported. 11.8% of all cases were accidents which by the hit or grab by the moving machinery elements occurred. In Poland, in 2013, the number of 77 fatal accidents were reported (OPR. 2013). In many cases, in addition to bodily injury or death during an accident, related to the machinery and the plantation destruction considerable material losses occurs. The main reasons of the accidents with the agricultural machines are: the inadequate machine technical condition, not in accordance with applicable regulations maintenance performing, unauthorized and noncompliance with the operator work time. For this reasons it is very important to emergency risk and its effects minimizing technologies develop. The main objective of machinery safety models developing is to identify the potential hazards, and terms of the reliability and safety critical machines elements, and the intended emergency due to the function implementation analysis, and operators injury risk (Wenlong & Wentao 2012, Griepentrog, Andersen, Andersen, Blanke, Heinemann, Madsen, Nielsen, Pedersen, Ravn & Wulfsohn 2009).

Mostly, the machinery safety analysis is carried out using models:

- cause-and-effect relationships—emergency effects in terms of their appearance reasons analysis;
- sequential—chains of emergency analysis, the tree of fault and accidents method;
- biotechnical—the human-machine relations disturbance analysis;
- energy transfer—the destructive energy transfer analysis;
- deviations analysis—the deviations from the normal, containing human, techniques and the environment influence identification;
- holistic—takes into account the organizational, environmental, technical and technological functions.

For campaigns machinery use, the holistic models are of particular significance. The appearance of the accident which can be regarded as a systemic approach is a dynamic change of energy, matter, and information. Each process of this machines can be in the system terms described, which take into account:

- organizational functions—safety, training, and control procedures; personnel education and training; management procedures, unauthorized persons access; work procedures; process implementation parameters.

– environmental functions—formation, soil type and moisture, machinery movement system, weather conditions, working elements physicochemical characteristics and parameters variability, communication system.
– technical and technological functions—safety provide technical systems, functional process solutions, machine constructional parameters, the process realization ergonomics, machine preparation for the campaign,the machine maintainability.

Safety system modeling can be carried out using two research methods:

– constructional and functional structure of the machine in terms of the relevant legislation requirements analysis;
– constructional and functional solutions adaptation in the risk analysis aspect.

The crisis situations dynamic, the need of fast analysis and interactive decisions makes implies. It can occur that the incoming information analysis exceeds the capabilities of the operator. At this point the specialized decision support systems lend a hand.

The aim of this paper is to develop the original solutions for decision in crisis situations in the operating, multi-functional, telematics, used in the campaigns, agricultural machinery systems supporting.

2 AGRICULTURAL MACHINERY MANAGEMENT SYSTEMS ANALYSIS

The dynamic growth of digital technology characterized past years. It has been a significant development of the agricultural machinery used in the campaigns management supporting systems. They mainly focused on an efficiency and quality of work improvement and service performed operations supporting. For these type of agriculture telematics, based on GPS technology systems belongs:

– John Deere FarmSight (John Deere 2014).
– Efficient Agriculture Systems (Claas 2014).
– Advanced Farming System (Case IH 2014).
– The Precision Land Management (New Holland in 2014).
– Agrosky + iMonitor (Same 2014, Deutz-Fahr 2014 Lamborghini 2014).
– Fendt Variotronic (Fendt 2014).

These systems have a similar functional structure and allow for (Doruchowski 2009, DomiScore 2010, John Deere 2014, Claas 2014):

– Stress-free operator's work, supported by precision GPS positioning system with an accuracy at the operating time to a few centimeters.
– Field machine automatic steering.
– The fuel costs, work time, pesticides, fertilizers, seeds grains, etc., by the working width utilization factor and the effective efficiency improving reduction.
– Work at night in limited visibility conditions, while maintaining the highest quality of working process.
– The functioning machinery and transport objects automatic synchronization.
– Work time control (operating time, stop time, transport time).
– The machine position localization using the Google Earth (the ability to machine during the night parking monitoring, in this time when machine will change its position, the system generates an unauthorized use alarm signal).
– Selected machine settings from the stationary fleet management equipment supervision.
– Remote data acquisition in order to use them to the worker process functional optimization.
– Remote diagnostics and maintenance scheduling with the immediate service notification possibility.

Despite of many advantages of applied, agricultural machinery used in the campaigns management supports systems, they slightly enhance the safety of their use and mainly limited to:

– The cutting Header disconnection after the harvester operator seat will be left for longer than 5 seconds,
– The cutting Header disconnection and the grain harvester on a circular trajectory set, after the 20 minutes of steering wheel extortion disappearance.
– Stop the engine in case of the ladder for access to engine compartment lowering.
– Prevent to control the position of a sloped conveyor in transport mode.
– Field mode restriction of maximum speed 19 km/h.
– Blockage the harvester engine start in the case of the threshing, header or the harvest drive is switched on.

In terms of the safety of use the agriculture machinery in campaign conditions, there is no operator daily work time permissions supervising systems. There are also no field emergency call rapid solutions. Another solution that should be used is to supervise the machinery rotating components access, as well as the other machines online positioning data exchange to correct field collision courses.

3 THE CONCEPT OF THE MACHINE EXPLOITATION PERMISSIONS AND THE OPERATOR DAILY WORK TIME SUPERVISING SYSTEM

The agricultural machines unauthorized exploitation belong to a frequent abuses. The accidents perpetrators are people do often not have the relevant qualifications. In this group there are persons which do not have an authorized permissions from the producer to operate and service the machine. Unfortunately, many of these people are irresponsible parents and permitted to operate the machines by children. To prevent this type of incidents, the operate permissions verification, machine producer supervised system is proposed. The necessary thing in the system is to online permissions verification, divided to utilities (working process control) and maintenance permissions (service and re abbreviated pair operations). For this reason, the producer, after having been conducting appropriate training, should give registered, individual, personal chip cards. Their task is to limit the access to the machines exploitation of unauthorized persons. Each mobile machine should be equipped with card reader. Starting the machine requires activation using the chip card. After reading the data from the card, the onboard mounted GSM/GPRS module will transmit to the machine producer monitoring server the identification data. Identification data will be compared with a stored on the server database. In case of identified data with stored in the server data compatibility, the machine will sent an information to deactivate the security system. After the verification, the user will be able to start the machine. While machine is running (only in the field), the permissions will be checked at the defined time interval. This solution will allow to stop the machine in case of the chip card from the reader in order to use it to activate other machines removal. In the case of assemblage of machines, composed of tractor and accompanying machine, the system will gave the possibility to the producer and type of accompanying machine by ISOBUS module check. In this case, the system may generate for both, the tractor and the accompanying machine the independent activation messages. Starting the assemblage of machines will be possible in the case of more than one producer permissions authorization. In the assumption of personal card is to give the possibility to store the necessary information, to run a group of machines that are in a one farm and which were manufactured by different producers. In the system, as was earlier mentioned, will functioning cards with a different permissions range. The user card will have permissions to the machine work process. This will be the basic functional range. The service card provides access to, related to the exploitation, more than standard options (e.g. the service technician will have permission to start machine working components while the rotating elements cover panel is removed, in order to carry out the measurements of vibration and rotation speed).

In such a way functioning system will allow to monitoring the operator daily work time. At the time the user logs in the system, (insert personal chip card) at the card will be the activation recorded. From this moment, the units of time, from the daily work time resource, until they are run out, the system will be subtracted. Additionally, after the allowable time, the operator, to complete the technological process, will be able to extend the work time of a maximum 30 minutes. After this time, the

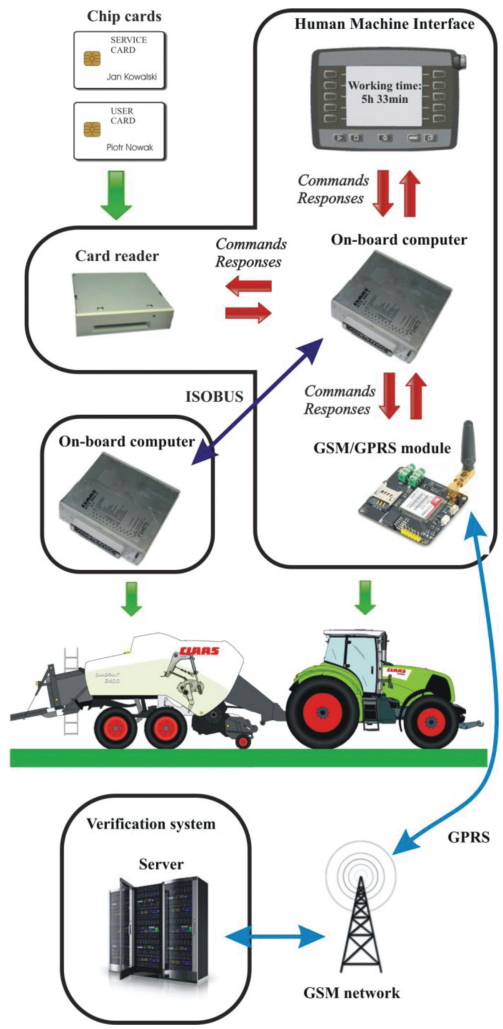


Figure 1. Structural diagram of the machines exploitation and operators daily work time permissions supervision system.

engine stop and the machine will start only in the transport mode. Thanks to the possibility of stored on the card daily work resource time, the proposed monitoring subsystem, after the time limit is run out, prevent to continue the work with this card at the other machines. The time limit will be renewed every 24 hours by the system. Operator during operation of the machine will be able to, using the display board system, the available daily work time control. Figure 1 shows a structural diagram of the machines exploitation and operators daily work time permissions supervision system. The presented system implementation standardization of the shared by the various machines producers chip card recording data requires. Operator monitoring time will be only in the field mode by the onboard machine control system realized. Stopping the machine in the transport mode caused by work time resource exhaustion could have finish in collision.

4 THE CONCEPT OF THE FIELD EMERGENCY CALL SYSTEM

The accidents during agricultural machinery exploitation occur frequently. The major safety approach objective is to prevent them. In the case of an accident, through the systemic solutions, the associated with its losses should be minimize. This type of systems are being developed in a many research centers in the world. The most advanced, that automatically call emergency services in the case of an road accident is eCall system (Emergency Call). It is under the European program in the field of road safety implemented. The studies, conducted using eCall has shown that its use can response time from the emergency calls by 40–50% reduce and the accident losses reduce by 15%. According to the EU directive, the all new vehicles sold in the EU after 1 October 2015 should be provided with an IVS (In Vehicle System). In option for an additional charge, this type of devices, by producers of vehicles are already offered (Friday 2009, Bronk, Lipka, Low & Zurek 2011).

From the information transfer aspect, the eCall is an extension of the functioning 112 emergency call system number, of the E112 position location. In this system the telecommunication operators commit themselves to the vehicle location to the PSAP rescue center (Public Safety Answering Point) by MNO (Mobile Network Operator) free information transfer. In the case of an accident, the vehicle sensors (e.g. temperature, acceleration, airbags initiation) generate signals that will be by the IVS module analyzed. This module receives information about the current position of the vehicle from the GPS. In the next step, the IVS, in the form of a data block MSD (Minimum Set of Data) normalized message generate. This is the minimum set of data that is necessary to locate the vehicle. The MSD data structure describes the European EN15722 standard. MSD dataset contains information about: signal control (if the IVS system generated the MSD automatically or was by the driver initiated), the Vehicle Identification Number (VIN according to ISO 3779), UTC timestamp, location data (geographic longitude and latitude, travel direction), the energy carrier placed in the vehicle characterization (e.g. petrol, diesel, CNG, LPG, hydrogen) and other data from the IVS module board. In addition to the MSD messages, simultaneously in the eCall system, using the in-band techniques, the transmission of the voice is realized. Voice transmission allow to complete the transferring information to the PSAP in the case of the accident victims the consciousness keeping

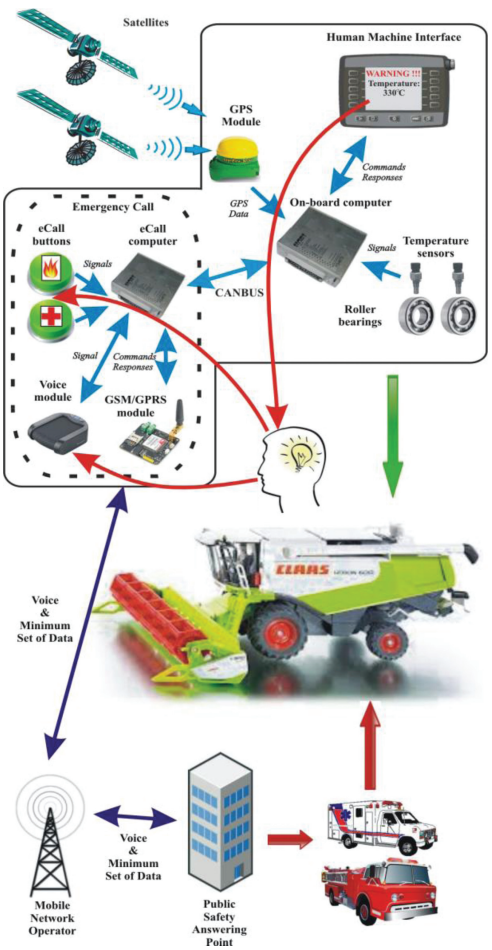


Figure 2. Structural diagram of modeled on the eCall, original field emergency call system.

(Bronk, Lipka, Low & Zurek 2011, Nowacki & Kaminski 2011, Botezatu & Barca 2008, Żardecki & Pijanowski 2012). Figure 2 shows a structural diagram of the proposed, modeled on the eCall, original field emergency call system.

To the necessary changes, aiming at the adaptation to agricultural machineries the eCall system are:

- Resignation of MSD automatic message transmission. MSD message should be initialized only by the operator. During the agricultural machinery work, there are big vibrations and dust, which the correct work of the standard diagnostic sensors disabling (such as acceleration sensors). This could bring the fake alarms.
- The operator should has a possibility to the MSD message with the needed assistance type data generate (in the case of fire—the fire department, in the case of injury—the ambulance service is called). For this reason it is necessary to respectively a MSD message sending buttons secured and tagged. The message after several seconds of delay time should be sent. At the time, when only one button is pressed, the MSD sent message contains information about the need for intervention only one of the emergency services (fire department or ambulance). However, if two buttons at the delay time will be pressed, the message will contain MSD about the need for the intervention of two emergency services. This solution will reduce the number of generated MSD messages and will eliminate the useless emergency call. It should be noted that the system in this form will be used for emergency calls that have also with other, combined machines occurred.
- On-board information systems, in which modern agriculture machinery are equipped, should be with a selected working groups temperature monitoring subsystem, with an alerts generating possibility equipped. This subsystem will the operator in the early detection of the fire risk support. Machines used in the harvest season are to the invitation of fire particularly hard working environment exposed (dust, low humidity and flammability of material). Machines elements of that the greatest risk generate are the engine and high loaded bearings that require the grease with abnormal characteristic use (e.g. the straw chopper bearing mounted in the grain harvester). In the case of fatigue wear of this bearings, they produce large amounts of energy. Their temperature monitoring could the occurrence of fire eliminate and in the case of fire, the time to call the appropriate emergency services through the field emergency call system shorten. The selected working groups temperature monitoring subsystem would the improper grease for high loaded bearings use make difficult. The agricultural machinery users, often to minimizing the cost of exploitation, the cheap substitutes of recommended grease use. In the case of high loaded bearings, cause they fast fatigue wear and as a consequence of this it may bring out the fire. In the case of permanently ignoring of selected working groups too high temperature alerts, subsystem will stop the machine (only in the field mode). Reactivation of the machine would need the service intervention. This solution allowed to reduce the risk of the fire.

5 THE CONCEPT OF THE AGRICULTURAL MACHINERY ROTATING COMPONENTS LIMITED ACCESS SYSTEM

In the case of agricultural machinery technical unfitness, the unauthorized persons (not having theoretical and practical knowledge) attempt to repair the damaged components and the current procedures are breaking. During this type of repairs, often comes to emergency, of which the clothes grab by rotating parts mostly occur. The consequence of this are extensive injuries, bones fractures and even death. Agricultural machinery producers warns the users against the cover panel during the components work opening by appropriate signs at the machine placing.

In order to limiting the access to the working, rotating machine components, the modification of the on-board information system to control possibility of the cover opening is need. While running the engine, the locks that allow to open the machine covers must be locked by the driver. Locking should be initiated by a sent from the machine driver via CANBUS module the coded signal. In the case of using the analog signal lock control (voltage application) machine users could bypass the security by get the voltage from an external source. This system would prevent also the start of the engine when the cover opening was diagnosed. During the machine qualified service technician repair, there is a need to perform confirmatory tests. These include for example the acceptable level of vibrations measurements. This required to run the machine while the covers are open. To verify the permissions of the service technician, the chip card reader can be used. After a chip card in the on-board information system chip card reader is placed, the service employees would obtain the special access to more than standard permissions, that allow the machine with open covers start. Figure 3 shows a structural diagram of the proposed, agricultural machinery rotating components limited access system.

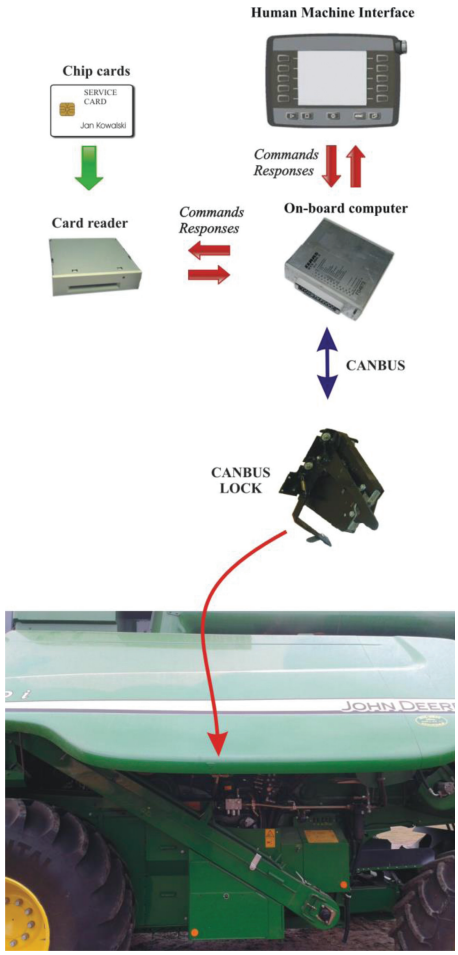


Figure 3. Structural diagram of the proposed, agricultural machinery rotating components limited access system.

6 THE CONCEPT OF THE FIELD COLLISION COURSES CORRECTION SYSTEM

In order to reduce the field collision probability, it is desirable to collision courses monitoring. The system concept is on the V2V (Vehicle to Vehicle) technology modeled. From the second half of 2012 in Ann Arbor, Michigan, USA, the researches with the participation of 3000 vehicles of V2V system were conducted. V2V system assumes the traffic movement vehicles data exchange. Each of the equipped with V2V driver vehicles, exchange data (vehicle location, speed, etc.) with other vehicles by radio. The frequency of data exchange is set at 10 Hz. The V2V functioning systems assumes: fuel consumption and exhaust emissions, and the number of accidents and unwanted crashes reduction (e.g. reckless driving), and the traffic movement improve (Siva & Narla 2013).

The concept of the proposed field collision courses correction system is on machines necessary information radio transfer to enable their position prognoses focused (location coordinates, direction and speed of the movement). In the case of two machines movement trajectory intersection, the system prevent the collision by immobilized them. Once they stop, it will be necessary to switch the machines in safe mode and maintaining, with extreme caution, move the machine to a safe distance. Then the operator will be able to restart the system. The machines used in the campaign season conditions (vibrations and huge dust) making impossible the distance ultrasonic sensors use (a solution for many years in the cars to supporting the driver during parking used). For this reason, mutual positioning and track prediction, only on the basis of onboard GPS module data, in which modern precision agricultural machines are equipped as standard, will be performed. Another problem to be solved is to determine the position of the cooperating machines (e.g. tractor and trailer). In this case, two solutions are proposed. The first one is dedicated to modern machines with on-board controller equipped. The memory controller will the necessary parameters needed to determine their location saved (dimensions and turning radius). After connected the machine to the tractor, the data will be to the mounted on the tractor controller via ISOBUS sent. During the location data analysis, the controller will determine the whole machine movement trajectories. Another solution would through the operator panel to the mounted on the tractor memory controller, the relevant data of connected machine introducing. The data will be entered once, and on further machine uses it will be from the controller memory loaded. This solution is dedicated for machines that are not in the board driver equipped. In addition, the system will be able to field obstacles data (e.g. trees, energy poles) and the machines operation field range enter. This information will, to the system from the stationary, equipped with a specially software, computer management position introduced. After draw up the machine areas maps range, with added obstacles, these data via a telematics system will be to the on-board machine controller transferred. It is very important in the case of operator unconsciousness, when the machine try to leave the defined area of its operation, the system will disable the engine itself and switch off its working components (optional dedicated to grain harvesters). It should be noted that each machine in the system will be able to the system deactivation.

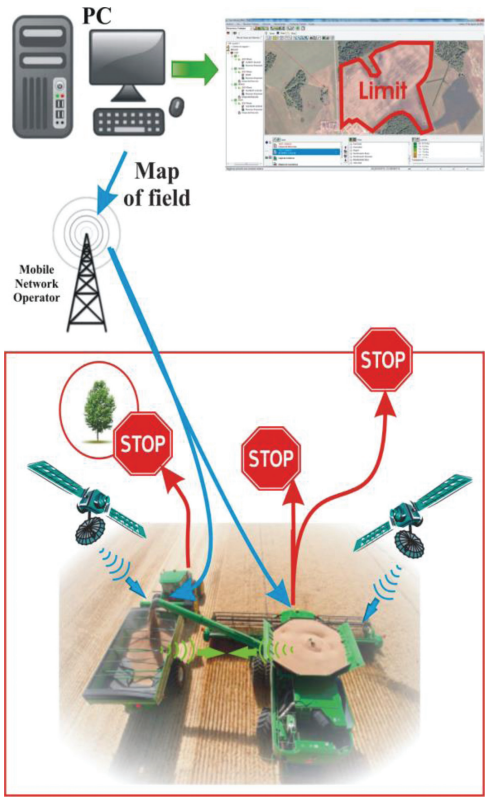


Figure 4. Structural diagram of the proposed field collision courses correction system.

Figure 4 shows a structural diagram of the proposed field collision courses correction system.

7 SUMMARY

Many agricultural machinery producers the management process support systems for used in campaigns agricultural machinery offer. They are mainly targeted to the performance and quality of working process and service maintenance supporting improve. Despite many advantages, unfortunately, they support their use and service safety to a small extent. Presented concepts of extension of existing machines working processes supervising systems can reduce the risk of: field conditions collision, the unauthorized persons exploitation and emergency occurrence at the maintenance and repair time access. In case of field emergency call system, there is a possibility of the emergency services arrival time by 40–50%, and emergency losses by 15% reducing. The system checked solutions, upon the agreed in the EU eCall system that will be in new cars sold from the October 1, 2015 installed is using. This will the conceptual field call system implementation process shorten and also will on its reliability and functionality affect.

REFERENCES

Botezatu, C. & Barca, C. 2008. Intelligent vehicle safety systems—eCall. *Journal of Information Systems & Operations Management*. Volume 2, Issue 2. 487–494.

Bronk, K., Lipka, A., Low, R. & Zurek, J. 2011. The concept of implementation modems IVS and PSAP eCall technology SDRs. Scientific Papers of Gdynia Maritime University, No. 70 Selected aspects of telecommunications. Gdynia. 19–31.

Dominik, A. 2010. Farming Systems. Agricultural Advisory Centre in Brwinów. Branch in Radom. Radom. ISBN: 978-83-60185-71-1.

Doruchowski, G. 2008. Progress and new concepts in precision agriculture. Agricultural Engineering 9 (107). 19–31.

EN15722: 2011. Intelligent transportation systems. eSafety. eCall Minimum Set of Data (MSD).

Friday, S. 2009. Regulatory aspects of the notification of road accidents—eCall. *Telecommunications and information technology* 1–2/2009. 57–65.

Griepentrog, H.W., Andersen, N.A., Andersen, J.C., Blanke, M., Heinemann O., Madsen, T. E., Nielsen, J., Pedersen, S.M., Ravn, O. & Wulfsohn, D. 2009. Safe and reliable: further development of a field robot. Precision agriculture '09. 857–866.

http://www.caseih.com.

http://www.claas.de.

http://www.deere.co.uk.

http://www.deutz-fahr.com/en-GB/.

http://www.fendt.com.

http://www.komputerswiat.pl/artykuly/redakcyjne/2014/02/ecall-w-kazdym-aucie.aspx.

http://www.lamborghini-tractors.com/en- GB/.

http://www.same-tractors.com/en-GB/.

Materials published by New Holland, http://agriculture.newholland.com.

Nowacki, G. & Kaminski, T. 2011. Problems interoperability ITS—based on the design implications KSAPO and eCall. Scientific Papers of the University of Warsaw. Transport. Issue 80 Warsaw. 95–116.

Office of Prevention and Rehabilitation. 28/01/2014. Emergency cases at work and occupational farmers diseases. Warsaw.

Siva, R.K. Narla 2013. The Evolution of the Connected Vehicle Technology: From Smart Drivers to Smart Cars to … Self—Driving Cars. *ITE Journal*/July of 2013. 22–26.

Wenlong, C. & Wentao, H. 2012. Research of the Assessment for Agricultural Machinery Driving Safety Based on AHP-Fuzzy Method. Proceedings of the 2012 International Conference on Automobile and Traffic Sciences, Materials, Metallurgy Engineering. MMAT. 49–54.

Żardecki, D. & Pijanowski, B. 2012. Information in car safety system with the "e—Call". *The Archive of Automotive* 4/2012.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Collection and analysis of failure data for pressure equipment

P.A. Bragatto, S. Ansaldi, C. Delle Site & P. Agnello
Inail Settore Ricerca Certificazione e Verifica, Rome, Italy

ABSTRACT: Failure rates of pressure equipment are essential for plant operators to plan risk based inspection as well as for Authorities to make decisions on land use planning. Detailed failure records have been gathered for a decade in a couple of industrial districts, with a significant number of installed equipment. Documents have been analyzed by means classical statistical method to get failure rates and compared with the values used in European countries for decision making. In order to understand how failure modes are affected by the types of equipment, construction material, industry and management model gathered documents have been organized by means of advanced semantic methods. A number of "frequent accident" has been singled out, to be proposed to inspectors and industrial practitioners.

1 INTRODUCTION

Pressure equipment is essential in many industries, including oil, chemical, textile food, waste and healthcare industry. In high risk industries, furthermore, pressure systems are critical also for major accident prevention. Thus in all involved industries, it is essential to assure pressure equipment reliability and safety. In this framework the knowledge about the pressure equipment failures is essential to drive inspection and maintenance activities. In particular the failure rates FR and failure mode FM, associate with a type of equipment, are the basic parameters. FRs, in particular, are essential for the risk assessment and FMs for the risk management.

In the Seventies huge efforts have been made to provide the nuclear and chemical engineers with a credible set of data on pressure vessels failure frequencies and modes. In an article by Bush (1988), the historical studies, conducted in previous decades at three major industrial countries, USA, UK and Germany, are reviewed and compared in a critical way. In the review eight national studies on pressure vessels are reported in detail. In each study, 10.000 to 100.000 pieces of equipment were observed for ten years and more. Those studies consider, as a whole, 3 million years-vessel (both fired and unfired) with some 8.600 minor faults and 155 major events. In following decades the world of pressure equipment changed dramatically, because the new steels alloys introduced in the years, the new certification rules introduced by the PED Directive in 1998, the new design and production techniques, the new inspection and maintenance methods; but, at now, the study of the Seventies are still unparalleled.

2 FAILURE RATE AND RISK MANAGEMENT

The importance of FM and FR for risk management are briefly discussed, as well as the information sources available in the public domain and the research needs.

2.1 *Failure rates and modes for risk based inspection and maintenance*

The pressure equipment risk management is aimed to control uncertainties that could jeopardize in the objectives of these systems, which are basically a profitable and safe production and a continuous and regular service. Equipment failure is still a major uncertainty in a process plant and consequently efforts to develop knowledge about the frequency and the mode of failures are worthwhile indeed. For that reason a credible set of general failure rates is essential to promote an efficient management of hazardous equipment. A particular application of risk management is the Risk Based Inspection RBI program, which optimizes inspection at process plants and other facilities. In RBI, times and types of inspection are driven, inter alia, by FMs and by FRs. American Petroleum Institute provides, in the recourses basis for RBI implementation, general failure rates and modes for many type of systems, including pressurized ones (API 2008). RBI details, benefits and compatibility with European and national

legislations on pressure equipment verification has been discussed by Bragatto & al. (2012) and by Pittiglio & al. (2014).

2.2 *Process equipment failure rates for risk based decisions in land use planning*

FRs affect also a few essential decisions by competent Authorities in the framework of the "Seveso" Directive. According to the art. 10 of the Directive 2012/18/EU Seveso III (replacing art. 9 in Seveso II Directive), establishments' operators must provide the authority with a detailed "Safety Report", which must include a probabilistic evaluation of the accident scenarios connected to the top events, as derived by hazard identification. The event probabilities are, in turn, derived from the FRs of the preventive and protective systems, by means of Fault Tree and Event Tree Analysis. The FRs of pressure equipment contribute to the computation with other mechanical, hydraulic, electrical, electronic and possibly human and organizational systems. The probabilistic evaluations coupled with consequence modeling and potential impact area computation are essential for Authorities to make vital decisions about new plants approval, emergency planning and land use planning LUP. Even decision making models for LUP are very different in different countries, FRs play always an essential role, as discussed by Bragatto & al. (2013).

2.3 *Trustable sources for pressure equipment failure rates*

The scientific weakness of the generic failure frequencies have been discussed by a historical review of Fragola (1996). Authorities must anyway accept a trade-off to make standardized and uniform decisions. An inadequate value of a single FR value in a fault tree is able to affect vital decisions. For that reason, in order to harmonize LUP decisions in the framework of Seveso Legislation, in a few countries set of "official" FRs was published by competent authorities. The main sources are the following:

i. PURPLE BOOK (1997) is a study of the TNO for the Dutch Competent Authority.
ii. FRED (2012) is managed by the British Competent Authority, HSE.
iii. AMINAL (2009) is the study of the Flanders Regional Authority in Belgium.

FRED is more conservative than PURPLE BOOK and AMINAL, but the approach is basically the same: data are derived from scientific literature and processed considering the advices of a number of experts (Pasman 2011). Thus for pressure equipment the historical studies of the Seventies, even though in new guise, are still alive. The criticality of the general frequency of has been recognized by British and Dutch Authorities, which has promoted, in the framework of "Seveso" activities. a feasibility study to improve the level of trust of FRs, gathering new data on the "field". In this study (Bellamy & al. 2012) accident national and European databases have been exploited. According to Manuel & al. (2012), the two found limits are: i) it is difficult evaluate the actual reference equipment population, because there are no data on the total number of pipes and pressure vessels at the Seveso establishments; ii) failures without severe consequences for humans or environment are not reported in the open sources.

Multinational chemical and oil corporations, which control directly hundreds of plants, are able to gather detailed and complete information on both equipment failures (even without consequences) and equipment population, but results, as proprietary, cannot be found in the public domain and, consequently, they cannot be accessed neither by Authorities or minor companies.

2.4 *Knowledge management techniques*

Even more important than establishing shared FRs is to understand of the types of failure depend on the type of equipment, as well as on the operating condition and on the industrial sector. The collection of data on failures should serve primarily to develop and share this knowledge. The information, however, is fragmentary and not homogeneous at all, thus it is important to have appropriate tools peer knowledge management.

In order to extract knowledge from heterogeneous sources and to support semantic search "ontology" has been widely used for a decade. It is, basically, a way to put together concurrent taxonomies, adding a number of relationships. It has been demonstrated adequate to support pressure equipment certification by Camossi & al. (2008) and Ansaldi & al. (2006).

3 OBJECTIVES

The present study focuses just the pressure equipment, for which data in the public domain are quite older, even though essential in many industries. As in a few countries, including Italy, all phases of pressure systems life-cycle are driven by national regulations a valuable source of knowledge could be provided by the competent authorities. The control bodies' experience has been exploited both to update pressure equipment FRs and to improve and share knowledge about the types and causes of the failures in pressure equipment.

3.1 *Update failure rates*

The first objective is to have updated pressure equipment FRs, suitable for risk management in Italian industries, as well as to make equitable decisions on Seveso plants and LUP. For those purposes it is necessary to gather data on pressure equipment failures in a few sample area, where equipment population is known, to derive failure rates and to compare them with the values adopted by other competent authorities in Europe.

3.2 *Improve knowledge about failure mode*

The second and more important objective is to provide the Italian industries with a trustable basis of knowledge on pressure equipment FMs. The types of failure are expected to depend on the types of industry, of equipment, of management system and of material. Furthermore types of inspection and repair may be suggested, based on the collected experience. The knowledge must be accessible and usable for all industries.

4 MATERIAL AND METHODS

4.1 *Pressure equipment verification*

In Italy the mandatory periodical verifications on pressure equipment, are in charge of the local control agencies (ASL), whilst INAIL is in charge of the first verifications. Thus the two bodies, working together, may have a clear picture of pressure equipment on the territory and gather detailed information on incidents and failures that occur in their territory. Together with the ASL of Varese, a systematic information collection about pressure equipment failures was experimented. Varese province is featuring a large number of small and medium sized manufacturers, in particular in textile and allied industries. The observation time was 11 years, until 2013. The equipment population is 6000 items in service, including some 400 steam generators. This data has been assumed almost constant in the observation time. In the observation period there are 53 recorded event. The recorded events include both major failures with severe consequences (e.g. loss of the equipment, injuries or death, environmental damage) and minor fixable failures. For each event has been produced a detailed sheet, describing type of failure, type of equipment, type of material, type of consequences, type of causes, type of certifications and lifetime. Further details and photographs, as relevant, have been enclose too. The industries are classified according to the NACE scheme.

For the purpose of comparison was analyzed also a collection of recorded faults present in the public domain (Frabetti & al. 2006). It contains 53 events collected in 7 years (1995–2001) in a highly industrialized Italian area (Emilia-Romagna), with a population of about 46,000 in equipment pressure. The study did not provide frequencies.

In Emilia data collection, steam generators were considered separately, as failures of boilers were recognized much more frequent and less severe than other type of equipment. To keep consistency with Emilia data, also in our study steam generators has been definitely discriminated from other type of equipment.

A number of failures, recorded by others regions, have been included into the study. Namely there are 5 records coming from other districts and 4 documents on failure much more detailed, coming from testing laboratories. Furthermore a dozen of accident records, coming from national and international databases have been included as relevant to the pressure equipment. They have not been useful for the FRs as data on the reference population are lacking, but they have been valuable for investigating the FMs.

4.2 *Statistical analysis*

The FR calculation needs just the number of occurrences and the number of items in the reference population. The number of events is relatively low, but the information collected for each event is very detailed. As a large diversity of equipment is involved, with many types of fault; the statistical analysis of the documents had to balance two conflicting needs: the different classes of membership (e.g. types of activities, types of equipment, types of damage, class of age) should be discriminated to have interesting and detailed results; but the sample cannot be fragmented too much, to avoid a loss of statistical significance. For this reason, before numerical processing, has been investigated the different taxonomies to be used to organize the study. A too articulate taxonomy cannot lead to significant statistical results, but a flat classification leads just to generic results. The strategy then is to obtain classifications with two or a maximum three levels.

The first level of the taxonomies will drive the numerical calculations, to have failure rates, while the second level, not suitable to produce "numbers", will be used to synthesize the documents in order to facilitate the search for recurring events. In Table 1 the list of the used taxonomies are shown.

4.3 *Frequent accident*

Starting from the taxonomies mentioned in § 4.1 a complete "ontology" of the matter "pressure equipment failure" have been built. To have the ontology of the pressure equipment failure a number of relationships between concurrent classification have been added.

Table 1. The basic taxonomies used to organize the matter. Just the very first level is shown.

Equipment	Steam generator, sterilizer, LPG tank, vessel, piping, heat exchangers, chemical oven, cylinders, tanks
Consequences	Production, asset, workers, environment
Part	Shells, ends, openings, nozzles, manifolds, supports, valves, tube plate, tube, furnace
Industry	According to NACE code
Fluid	Liquid, gas vapour; non hazardous, hazardous, corrosive
Repair	Restoration, replacement, surface treatment, non repairable
Failure/defect	Crack, crack through/hole, surface deterioration, deformation, occlusion, explosion/fire, rupture
Cause	Welding, human factor, maintenance, process, fatigue/corrosion, age

For instance a few parts are present just in a few types of equipment; a few type of equipment are present just in a few industry, a few damage occur just in a few types of equipment; a few types of repair are just for a type of failure and so on. The resulting ontology has been used to drive both basic failure statistics and knowledge organization. By exploiting the developed ontology, it is possible to have a sort of "intelligent search". Instead of looking for a string as in usual search engine, it is possible to look for a complete sentence that must put together a few types or "categories" present in the taxonomies included in the ontology. For instance it is possible to find in the stored documents a sentence where a particular type of damage occurs in a certain type of equipment in a certain type of industry. A free text search is even possible, as the pre-defined taxonomies cannot cover such a complex matter. The search is highly facilitate by the use of IBM® OmniFind™, a special engine, which recognize synonyms, even in different languages. The engine is also able to summarize automatically the resulting document, according to the key words used in the free text input and the categories as defined in the taxonomies. As the search is based on both the taxonomies and free text, the "logical proximity" definition adopted to find out "similar" events, combines both hierarchical distances coming from taxonomies and distance coming from text comparison according to MinHash algoritm:

$$P_{a-b} = \frac{\left(\Sigma_i^N \left(1 - \frac{h_i^{a-b}}{R_i} \right) + \frac{K^a \cap K^b}{K^a \cup K^b} \right)}{N+1}. \quad (1)$$

where p_{a-b} = proximity of event records a and b; h_i^{a-b} = hierarchical distance of event records a and b, according to the ith taxonomy; r_i = rank of ith taxonomy; N = number of taxonomies; K^a and K^b sentences singled out respectively in the event records a and b by the free search.

The index p^{a-b} ranges from 0 to 1. By means of the proximity metrics it is possible to build a set of similar events, which may be considered "frequent failures". Two event records have been considered "similar" if proximity $p^{a-b} \geq 0{,}67$. Similar events have been clustered in order to have a "frequent failure". A cluster of failures has been eligible as "frequent failure" if the number of events is ≥3 and all proximity are above "similarity" condition.

5 RESULTS

5.1 *Failure rates*

FRs have been derived separately for the new data of Varese and for the older data from Emilia. Steam generators have been discriminated. Resulting failure rates have been compared with the value suggested by the National Competent Authorities and by API. Furthermore the failure rate derived from Bush's review has been included. Table 2 summarizes the results.

The rate of failure for steam is very high, even though there are no major failures. It has to be stressed that, a number of major defects, resulting after periodical inspections have been accounted as "failures", because the significant consequences on repair costs or plant availability. As in other studies "major defects" are not included, the rate is not so worrying. Furthermore the age of failed equipment end the type of industry are essential for understanding the data.

As shown in Table 3 the steam boilers in Varese are quite older and, obviously, that affects the failure rates. The types of industry are shown in Figure 1.

Table 2. Comparison of failure rates.

	Minor/ repairable	Non repairable	Major
Bush 1970*	3.9E-04	1.3E-04	2.6E-05
TNO 1999	9.6E-06	9.6E-07	5.0E-07
API 2008	1.0E-04	1.0E-05	6.0E-06
AMINAL 2009	1.2E-05	2.2E-06	3.2E-07
HSE 2012	4.0E-05	1.0E-05	6.0E-06
Other Emilia*	6.6E-05	3.8E-05	6.9E-06
Steam Emilia*	4.7E-04	2.5E-04	3.1E-05
Other Varese**	8.9E-05	5.4E-05	1.8E-05
Steam Varese**	9.0E-03	1.3E-03	–

*Reworked from literature data; **Original data.

Table 3. Age and failure.

	Steam Varese	Other Varese	Steam Emilia	Other Emilia
Average	23.4	14.5	14.2	15.0
Max	54.0	36.0	37.0	41.0
75° percentile	31.0	19.0	20.0	22.0

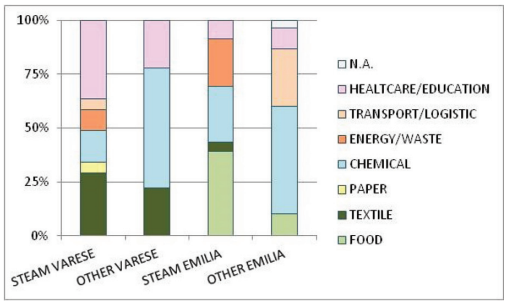


Figure 1. Failures and type of industry.

For Varese, there is a predominance of failures in textile and healthcare, whilst in Emilia food industry is peculiar. For the other equipment (non steam boiler), results for Varese are not so far from FRED (2012) and API (2008) suggestions, and lower than historical rates by Bush (1988). In the rates derived from the literature rates, healthcare facilities are not included, whilst are present in Emilia and in Varese studies and, contribute to increase the rates.

5.2 *Failure types*

As shown in Figure 2 failures have been classified as blast, fire, deformation, total and partial ruptures, as well as a number of degradation (peeling, occlusion, fouling, extended surface corrosion, multiple cracks, hole and crack through).

The assumed causes range from environment, inadequate repair or maintenance, inadequate design, process, human error, inadequate welding, stress and chemical corrosion, obsolescence (Fig. 3).

As shown in Figure 4, repairs after failure techniques include surface treatment, NDC programs, equipment modification, restoration (filling and grinding), and replacement of the damaged part.

The types of failure, the damaged part and the types of repair depend on the process and on the fluid, which in turn depend on type of industry. A more depth statistical study could need a fragmentation of the sample with loss of significance. Thus the further investigation are to find "frequent failures", as discussed in § 4.3.

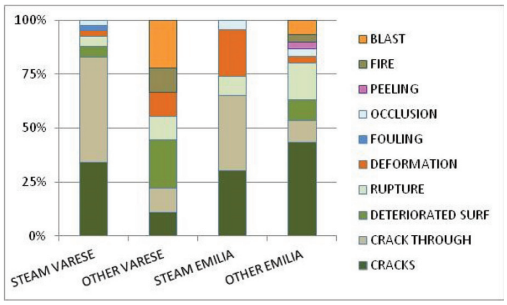


Figure 2. Failures and types of damage.

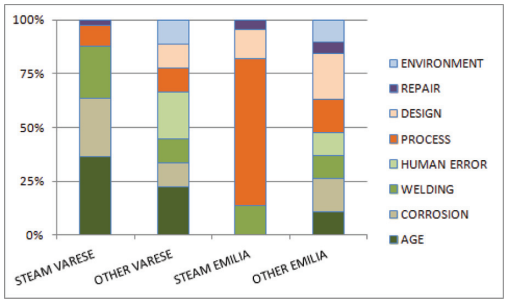


Figure 3. The types of assumed cause.

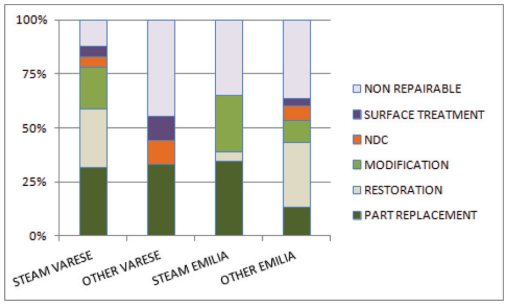


Figure 4. The types of repair.

5.3 *Frequent failures*

Table 4 show an example of the identification of a "frequent failure".

It is known that the chemical characteristics of the water supply is a source of troubles for thermal systems, including steam generators, health exchanger and sterilizer autoclaves. The problem is recorded in 6 documents, as shown in Table 4. Items matched in the defined categories are highlighted in different colour and searched free text is underlined. The first two records are very close indeed and the four following ones are less and less

Table 4. A set of "similar" incidents. The keywords, as given to the search engine are highlighted.

1	**Steam Generators** cracks in the weld between the tube shell and tube plate caused by corrosion due to incorrect treatment of water. Demolition
2	**Steam Generators** cracks in the weld between the tube shell and tube plate caused by corrosion and caustic fragility due to incorrect treatment of water Demolition
3	**Steam Generator** Following internal visit is detected widespread fouling of all parts side H_2O. Causes: the water supply to the **Steam Generator** without or insufficient treatment of water due to the softener device out of order. Repair: Chemical washing
4	**Heat Exchanger** corrosion of all parts on the water side Cause the sulfite concentration was less than that recommended by the manufacturer. This have resulted in the presence of a non-negligible amount of dissolved O_2 in water that has given rise to the widespread pitting. Repair: Chemical washing
5	**Autoclave Sterilizer** Steam formed by water from the ion exchange resin softener. Safety valve abnormality blocked by fouling. Absence of the condensate drain hole and the use of water with features not appropriate are the causes. Repair: Valve replacement and modification of the vent line.
6	**Autoclave Sterilizer** tearing of the shell due to a weakening of the intergranular material stainless steel triggered by chlorinated compounds as was used sea water. Demolition

Table 5. A further set of "similar" incidents. The keywords, are highlighted.

1	Food industry **Steam Generator** deformation in the central area of the rear tube plate deformation caused by pressure of the furnace probably due to stress … resulting in **excessive heat load** on the furnace …
2	Food Industry **Steam generator** some deformation of the tubes of the combustion chamber … with bulges result in **overheating** bubble
3	Food industry **Steam Generator** … ***Intermittent operation with alternating cycles very frequent***. three crack though in the back of the shell … It is assumed that the **continuous thermal stress** and the resulting deformation of the tube plate has caused the cracks …
4	Textile Industry **Steam Generator** plastic deformation due to the operation of the furnace in the **absence of water supply** as shown in photographic surveys the fault was caused by the **failure of the supply of water** to the generator for about 3 hours

"similar", according to the adopted metric. In the set the average mutual proximity is 0.73, with a standard deviation 0.08.

A further example of frequent failure identification is in Table 5. The problem is the thermal stress and the consequent deformation of some parts. The four case are pretty close each other. The average mutual proximity is 0.91 with a standard deviation 0.04.

Two further significant clusters have been found:

– reactors in chemical industry with corrosion phenomena due to aggressive compounds, such as chlorides (3 records; 0.8 average proximity);
– boilers switching from oil-fired to natural gas-fired, with consequent thermal stress, due to the higher calorific value of the natural gas (3 records; 0.75 average proximity).

A few documents contain also photos and evidences from metallurgical studies. Thus, for described "frequent failures" it is possible to add also imagine, in order to have more effective alert sheets for the industrial practitioners.

6 CONCLUSIONS

General pressure equipment failure frequencies, as proposed by FRED or API are basically confirmed by the filed experience of the Italian control bodies; but for steam boilers, which should be considered apart.

Types of equipment, damage mechanisms, materials, industries, processes are very different and available data are few. For this reason, the "frequent failures" found by means of the semantic search, are more interesting. In the future the metric will be improved, in order to include the experts' judgment and have more focused sets. Also taxonomies need to be improved, in order to include the user experience. A further develop line is to extend the document collection, including also national and international open data and proprietary sources.

ACKNOWLEDGEMENTS

The authors are particularly in debt to Mr. Sergio Barassi of ASL/Varese, for his valuable contribution to the present research.

REFERENCES

Aminal 2009 *Handbook failure frequencies for drawing up a safety report Flemish Government LNE Department BE* http://www.lne.be/en/safety-reporting/downloads.

Ansaldi, S., Bragatto, P., Camossi, E., Giannini, F., Monti, M., Pittiglio, P. 2006 A knowledge-based tool for risk prevention on pressure equipments, *Computer-Aided Design and Applications*, 3 (1–4): 99–10.

API Risk-Based Inspection Base Resource Document RP581, 2008 American Petroleum Institute, Washington USA.

Bellamy, L.J. Lisbona, D. Johnson, M. Kooi, E.S. Manuel, H.J. 2012 The major accident failure rates project HSE/RR915.

Bragatto, P.A. Ansaldi, S. Delle Site, C. 2013 A Pooled Knowledge Basis on Pressure Equipment Failures to Improve Risk Management in Italy. *Chemical Engineering Transactions*; 33: 433–438.

Bragatto, PA, Delle Site, C, Faragnoli, A 2012 Opportunities and threats of risk based inspections: The new Italian legislation on pressure equipment inspection. *Chemical Engineering Transactions*; 26:177–182.

Bush, SH Statistic of Pressure Vessel and Piping Failures. 1988 *J. of Pressure Vessel Technology*; 110: 225–233.

Camossi, E., Giannini, F., Monti, M., Bragatto, P., Pittiglio, P., Ansaldi, S. 2008 Ontology driven certification of pressure equipments, *Process Safety Progress*, 27(4): 313–322.

Frabetti, M. Pallavicini, L. Notari, V. 2006 La sicurezza delle attrezzature in pressione Arpa Rivista n.3 http://www.arpa.emr.it/documenti/arparivista/pdf2006n3/frabettiAR3_06.pdf. *in italian*.

Fragola, J.R. 1996 Reliability and risk Analysis data base development: an historical perspective *Reliability Engineering & System Safety; 51*:125–136.

FRED 2012 Failure Rate and Event Data for use within Land Use Planning Risk Assessments updated 28-6-2012 http://www.hse.gov.uk/landuseplanning/failure-rates.pdf.

Manuel, H.J. Kooi, E.S. Bellamy, L.J. Mud, M.L. Oh, J.I.H. 2012 Deriving major accident failure frequencies with a story builder analysis of reportable accidents. *Process Safety Progress*; 31(4): 381–389.

Pasman, H.J. 2011 History of Dutch process equipment failure frequencies and the Purple Book. *J. of Loss Prevention*; 24: 208–213.

Pittiglio, P. Bragatto, P. Delle Site, C. 2014 Updated failure rates and risk management in process industries Energy Procedia 45: 1364–1371.

Purple book 1997 Guideline for quantitative risk assessment http://www.publicatiereeksgevaarlijkestoffen.nl/publicaties/pgs3.html.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability analysis of prototypes based on small and heterogeneous test data volumes. Case study: Organic fibre prototype analysis

A. Lücker, M. Hinz & S. Bracke
University of Wuppertal, Germany

G. Knübel
Henkel, Germany

ABSTRACT: The analysis of failure behaviour and reliability parameters concerning the product's life cycle is fundamental within the early product development phases. Initial measurements regarding the product reliability analysis are based on prototypes. Especially in chemical process engineering, which deals with organic materials (e.g. fibre technologies), the scattering of the product characteristics (e.g. fibre strength or geometry), treatments and load profiles is significant. The challenge regarding the further processing during the prospective product life cycle is the quantitative, statistical risk and reliability estimation, which is primarily caused by the small prototype test data in combination with heterogeneous distributions of fibre characteristics. In this paper, an approach for the analysis procedure of prototype test results, based on heterogeneous prototype characteristics and small data volumes (e.g. sample size 15–25), is shown. The approach is explained within a case study out of the chemical process industry with the focus on the analysis of reliability parameters of fibre samples.

1 INTRODUCTION

The analysis of product failure behaviour and reliability parameters concerning the products life cycle is fundamental within the early product development phases. Initial measurements regarding the analysis of product reliability characteristics are based on prototypes. The challenge is the comprehensive analysis regarding the detection and mapping of expected failure modes and failure behaviour. Based on this analysis, product and manufacturing process optimisation is feasible.

Especially in the chemical process engineering, which deals with organic materials (e.g. fibre technologies), the scattering of the product characteristics (e.g. fibre strength or fibre geometry) is significant. Furthermore, the influences of product treatment (e.g. stress, side load, chemical treatment) have to be analysed. In this paper, the statistically reliability and risk analysis of organic fibre material within in the early phase of the product development is shown.

The challenge regarding the further processing and the usage during the prospective product life cycle is the quantitative risk and reliability estimation, which is primarily caused by the small prototype test data in combination with the heterogeneous distributions of the fibre and treatment characteristics.

From a statistical point of view, the validity of the test results based on a low test data volume and the distribution heterogeneities is considerable. For example parametrical distribution models are unverifiable; therefore parametric significance tests are not applicable.

This paper shows results of research collaboration between University of Wuppertal and Henkel, Düsseldorf, with regard to the development of an approach for the analysis procedure of prototype test results, based on heterogeneous prototype characteristics and small data volumes.

2 GOALS OF RESEARCH WORK

The goals of the development of an approach for the analysis procedure of organic fibre test results, based on heterogeneous prototype characteristics and small data volumes, are as follows:

1. Detection of significant impacts with regard to fibre strength and fibre geometry,
2. Analysis of significant impacts of the stress, side load and chemical treatment regarding the test cycle,
3. Determination of reliability characteristics of organic fibre materials based on heterogeneous prototypes,

4. Determination of facility adjustment for the maximal differentiability based on an analysis of variance and optimisation of accelerating testing method for further prototype tests (e.g. pre-damaged organic fibres).

The approach is explained with the help of a case study "Organic fibre prototype analysis" out of the chemical process industry with the focus on the analysis of reliability parameters of fibre samples. With the use of nonparametric as well as parametric statistical methods, fibre characteristics (e.g. centre, dispersion, trends) and interdependences are analysed with regard to material, geometry and origin aspects.

3 3 BACKGROUND: PROTOTYPE TESTING STRATEGIES

This chapter focuses on theoretical principals and application areas of accelerated testing procedures. Based on these theoretical aspects the analysis of the main characteristics regarding the test cycle within the case study "Organic fibre prototype analysis" is performed (Hinz 2014).

According to (Escobar 2006), "Accelerated Tests" (ATs) is a term used for two completely different kinds of tests with different purposes, "qualitative ATs" and "quantitative ATs". The key differences are presented briefly in Figure 1.

Qualitative ATs are used to identify product weaknesses caused by flaws in the product's design or manufacturing process. This is done by gradually increasing stresses until the product fails. The aim is to improve the product reliability in a very short period of time, usually hours or days. Common names for this type of tests are HALT (Highly Accelerated Life Test), STRIFE (Stress-Life) and EST (Environmental Stress Testing) (Chan 2001). Tests of this type do not involve any statistical or mathematical methods. The only target of these methods is the increase of the robustness of the product. The knowledge about the product lifetime or the degradation process over time is not in demand.

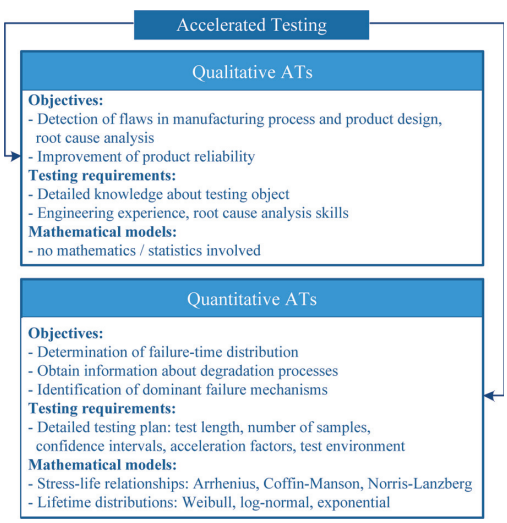


Figure 1. Test strategies of accelerated testing.

Quantitative ATs are used to obtain information about the failure-time distribution and degradation in a relatively short period of time (usually weeks or months) by accelerating the use environment. In most cases a model to describe the relationship between failure mechanism and accelerating variables already exists. They are also well-suited for finding dominant failure mechanisms and are usually performed on individual assemblies rather than full systems. In order to set up a quantitative AT, several different parameters must be known, for example test length, number of samples, desired confidence intervals, field and test environment, stress-life relationship and distribution model.

3.1 *Acceleration models*

One key factor is to determine the acceleration factor. It can be obtained by two different methods, either by using existing physical/chemical acceleration models or by determining empirical acceleration models by experimentation.

Various physical/chemical models for well-understood failure mechanisms are already available. They describe the failure-causing process and allow extrapolation to use conditions for specific environment variables.

If there are no chemical/physical models to describe the failure-causing processes adequately it may be necessary to develop an own empirical model by experimentation. An empirical model usually provides an excellent fit to the available data, but still can provide false extrapolations for working conditions.

3.2 *Acceleration methods*

Products, which are not in continuous use, can be accelerated by the increase of the usage rate. This means that the time between the load phases is reduced. It has to be considered whether the increased use rate changes the cycles to failure distribution. A toaster for example could heat up increasingly cycle after cycle until it reaches temperatures which would not appear under normal use conditions. A case study for this purpose was performed by (Guangbin 2006).

By increasing experimental variables like temperature, humidity or radiation, chemical processes that lead to certain failure modes can be accelerated (e.g. the chemical degradation of a photovoltaic module can be accelerated by inducing an electric potential).

If the environmental stress exceeds the strength of the testing object, the unit (prototype) will fail. This means that a unit operating at higher stress levels will generally fail after a shorter period of time than a unit at lower stress levels (e.g. amplitude in temperature cycling, voltage, or pressure).

The test strategy used in the case study "organic fibre prototype analysis" is a quantitative accelerated test with the need of the development of own empirical model by experiments. Though, the usage rate of the fibres is increased. The response type of the test used in the case study relates to the accelerated life test which is neither right nor interval censored.

Detailed information about response types of accelerated tests can be found in (Escobar 2006), (Nelson 1990), (Escobar 2003) and (Hinz 2014).

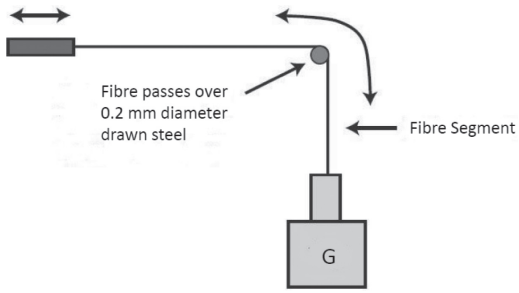


Figure 2. Schematic visualisation of test facility (Swift 2001).

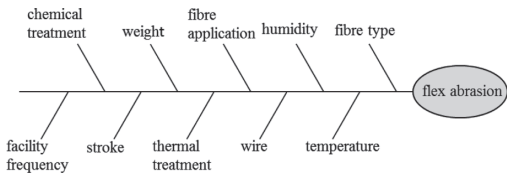


Figure 3. Main influence variables regarding the test procedure of flex abrasion.

4 ORGANIC FIBRE PROTOTYPE ANALYSIS

In this chapter, organic fibre prototype analysis including test facility is discussed. Subsequently, organic fibre data such as thickness or heterogeneity is explained. Furthermore the main influences on the fibres and the test plan is presented. However, various works on flex abrasion resistance investigations with the focus on chemical treatments of organic fibres were performed by (Yang 2001), (Yang 2003), (Dusenbury 1954), (Choi 1992) and (Pyket 1998).

The prototype analysis is the base of operations for present and future work on reliability analysis of organic fibre prototypes after chemical or thermal treatment.

4.1 *Test facility*

Reliability of organic fibres, such as cotton, depends on various influences, e.g. mechanical stress, different types and applications, external treatments or environmental conditions. Main influence variables regarding the test procedure are shown in the Figure 3. In order to simulate the most important impacts, a flex abrasion test facility, shown in Figure 2, was used. Detailed information about the testing machine can be found in (Swift 2001).

Fibres are placed in a plastic tab on the one side over 0.2 mm diameter steel wire and a weight on the other side. The plastic tab is connected to a drive unit, which induces a constant, linear, reciprocating motion. The flex abrasion machine provides the opportunity of variation of three parameters: stroke and frequency of the motion as well as the weight placed at the end of the fibre. Every measurement consists of 24 fibres.

Measured reliability information is the number of cycles of passes of the fibre, whereby back and forth motion is counted as one cycle.

Every parameter of the machine can be varied discretely within given ranges.

In order to avoid a high number of experiments, the number of every parameter will be limited to two adjustments:

- stroke—4 and 10 millimetre
- frequency—1 and 2 Hertz
- weight—10 and 20 gram

4.2 *Organic fibre*

Different types of organic fibres can be found in many branches of the industry (chemical, textile, cosmetics) and products (also of everyday use, like clothes, ropes, bags).

High number of applications corresponds to the number of fibre types. Within the case study "Organic fibre prototype analysis" three different types of fibres have been tested. For the sake of convenience they are renamed to type A, type B and type C and are representative for a wide range of products.

Heterogeneity of organic fibres plays a certain role due to the variance of material properties and

Table 1. Excerpt of the test plan.

No.	Fibre type	Stroke [mm]	Frequency [Hz]	Weight [g]
1	Fibre type A	10	2	20
…	…	…	…	…
5	Fibre type A	10	1	10
6	Fibre type A	10	1	20
7	Fibre type A	10	2	10
8	Fibre type A	10	2	20
9	Fibre type A	4	1	10
10	Fibre type A	4	1	20
11	Fibre type A	4	2	10
12	Fibre type A	4	2	20
…	…	…	…	…
19	Fibre type B	4	2	10
20	Fibre type B	4	2	20
…	…	…	…	…
28	Fibre type C	4	2	20

physical dimensions. Previous to the flex abrasion tests, the thickness in form of the cross section of the fibres has been measured and varies between 1695 μm^2 and 7016 μm^2 with the mean value of 3446 μm^2.

4.3 *Test plan*

A two-stage test plan for the flex abrasion experiments of the organic fibres was developed. The first stage investigates the influence of mechanical parameters and heterogeneity of organic fibres. Second stage deals with thermal and chemical treatment, which is not part of the current case study, and is planned to be examined in the further research work.

An excerpt of the first stage of the test plan is shown in the Table 1. The first four measurements (no. 1–no. 4) are of the same type of fibres and have the same adjustment of the parameters. The aim of these measures was the determination of the homogeneity of the samples. The next measurements contain all possible permutations of three fibre types, two strokes, two frequencies and two weights. This leads to eight (number of permutations for stroke, weight and frequency) measurements for every fibre type and 28 measurements (24 with parameter variation and four for the homogeneity of the samples) all in all.

5 STATISTICAL ANALYSIS AND RESULTS

The applied parametric and nonparametric statistical methods with their advantages and disadvantages shall be discussed in this chapter.

In the first instance, goodness of fit test will be performed in order to choose the proper statistical methods in the subsequent steps. Afterwards, the correlation analysis shall be undertaken in order to detect the linear dependencies between the single samples as well as between the number of cycles and the diameter of the fibres within every single sample. The homogeneity of the fibres is to be investigated with the help of significance tests with regard to the focus and the variances of the samples.

Lastly, the results of the measurements in form of plotted cumulative probabilities will be discussed.

5.1 *Goodness of fit tests*

In order to choose the eligible strategy for the correlation analysis as well as significance tests, the distribution of all samples has to be examined. Therefore, the goodness of fit tests with the null (and alternative) hypothesis:

$$H_0 : F = F_0 \text{ (and } H_1 : F \neq F_0) \quad (1)$$

that the sample data is distributed in a certain way (either normally or Weibull) has to be proven. Thus, for the normal distribution Kolmogorov-Smirnov and Shapiro-Wilk (Sachs 2009) tests are available. Accordingly Anderson-Darling, Kolmogorov-Smirnov and Chi-squared (Sachs 2009) tests can be applied for the Weibull distribution (Table 2).

In case of both distributions the applied Kolmogorov-Smirnov test doesn't provide results for all samples (sample size to small). Therefore, the results of this test will not be analysed.

The hypothesis that the sample data are Weibull distributed by a significance level of $\alpha = 5\%$ can't be rejected in case of 79% (for Anderson-Darling) and 93% (for Chi-squared) of the samples. Nevertheless it's important to note, that the amount of data within a sample stays at a low level. An example of Weibull distributed fibres (Table 1, fibre no. 1) is shown in Figure 4.

The hypothesis that the sample data are normally distributed by the same significance level as

Table 2. Goodness of fit tests—results.

	Normal distribution	Weibull distribution
Anderson-Darling	–	79%
Kolmogorov-Smirnov	No results	No results
Pearson χ^2	–	93%
Shapiro-Wilk	50%	–

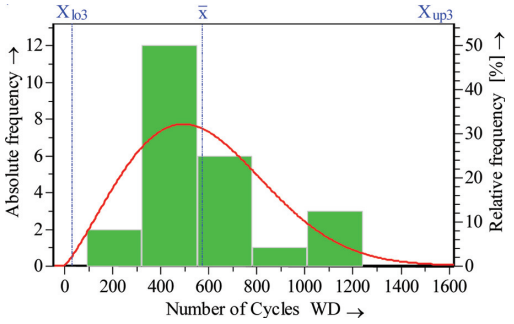


Figure 4. Density function of fibre no. 1 (Table 1).

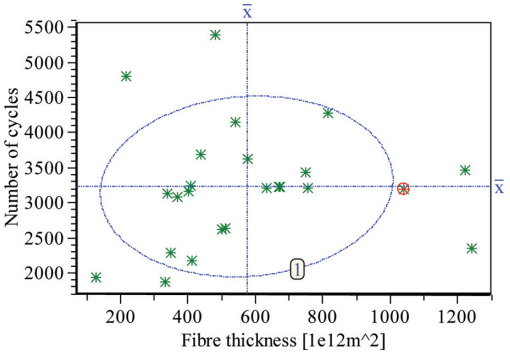


Figure 5. Scatter plot of fibre no. 1.

in case of Weibull distribution can't be rejected in case of 50% of the samples by an application of the Shapiro-Wilk test.

For the reason, that the null hypothesis of normally distributed samples can't be rejected only by the half of the measurements, the use of parametric tests is not possible. Therefore, nonparametric tests such as Mann-Whitney U or Levene's (Hartung 1998) for the comparison of the samples shall be applied. Also the Pearson product-moment correlation assumes the normal distribution of the samples. Hence, the use of Spearman's rank correlation, which is independent on the distribution model, is more adequate.

5.2 *Correlation analysis*

This part of the research work focuses on the impact of the fibre thickness on the durability of the fibres. Durability is represented quantitatively by the number of cycles of the flex abrasion test. The impact is presented in form of the Spearman's rank correlation coefficient. The correlation coefficient gives a value between –1 and 1 inclusively, where –1 is total negative, 1 is total positive and 0 is no correlation. Spearman's rank correlation is a nonparametric tool which describes the linear dependency between two variables, and can be defined as:

$$r_S = \frac{\sum_{i=1}^{n}(R(x_i)-\overline{R(x)})(R(y_i)-\overline{R(y)})}{\sqrt{\sum_{i=1}^{n}(R(x_i)-\overline{R(x)})^2 \sum_{i=1}^{n}(R(y_i)-\overline{R(y)})^2}} \quad (2)$$

where r_s is the rank correlation coefficient; $R(x_i)$, $R(y_i)$ are the ranked variables and, $\overline{R(x)}$, $\overline{R(y)}$ are the ranked arithmetic means.

A representative example of a distribution of the measured quantities in form of a scatter plot of fibre no. 1 is shown in the Figure 5. In this case the rank correlation coefficient equals $r_s = 0.31$.

The correlation analysis has been performed in case of all samples. Therefore, 28 coefficients are available. The mean value of the coefficients is $\overline{r_{mean}} = 0.23$, whereupon the maximum value equals to $r_{max} = 0.58$. This result provides very weak linear dependency of fibre thickness on the fibre durability. This means, that the fibre durability is independent of the fibre thickness.

5.3 *Significance tests*

For the comparison of samples, various significance tests according to different applications are available. Nonparametric significance tests do not require dependences on specific distributions. In comparison to similar application cases of parametric significance tests, further application cases and benefits such as simple calculation and detection of randomness of failure data are available.

The main focus of these tests is the comparison of the first four samples (fibre no. 1—no. 4) in order to prove their homogeneity. For this purpose two nonparametric statistical tests were performed.

Mann-Whitney U test with the null (and alternative) hypothesis:

$$H_0 : F(z) = G(z) \text{ (and } H_1 : F(z) \neq G(z-\Theta)) \quad (3)$$

that the samples have the same focus, and

Levene's test with the null (and alternative) hypothesis:

$$H_0 : F(z) = G(z) \text{ (and } H_1 : F(z) \neq G(\Theta z)) \quad (4)$$

that the variances of the samples are equal.

A visual example of the comparison of fibre no. 1 and no. 2 in form of a boxplot is shown in Figure 6. It can be observed, that no significant difference with regard to the focus (horizontal, black line in the middle of coloured rectangles) as well as variances (bold, vertical, black lines) between both samples occurs. This qualitative analysis can be

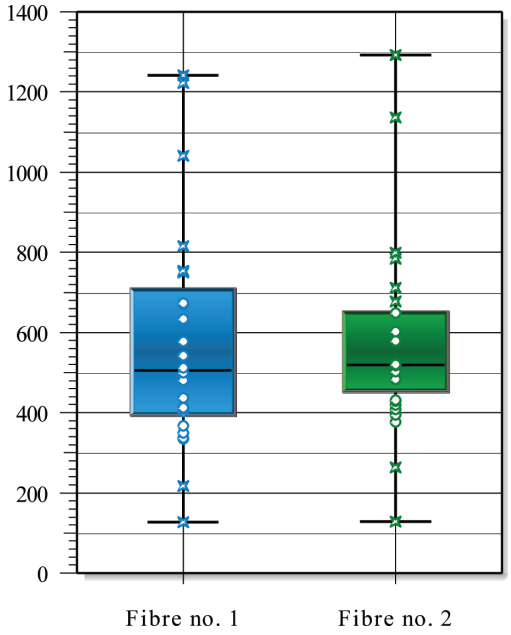


Figure 6. Boxplot—comparison of the samples.

confirmed by the quantitative study of all samples. Null hypothesis of both tests couldn't be rejected in all cases (comparison of every single sample with all the others). This means, that the samples (not the single fibres!) are homogeneous. Therefore, every single measured sample is representative for the rest of the result analysis.

5.4 *Discussion of test results*

In this chapter, results of the measurements of flex abrasion test procedure shall be discussed. The results in form of plots of cumulative probability are shown in Figures 7–9. All three figures are build-up in the same way: Number of cycles is plotted on the abscissa and cumulative probability on the ordinate. The scaling of the abscissa varies in different figures.

In Figure 7 measurements (no. 5–no. 12) of fibre type A are presented in order to discuss the influence of all parameters of the tests.

At first, the influence of the frequency shall be discussed. For this purpose, four pairs of measurements with constant stroke and weight and varying frequency, are available in Figure 7. The red and blue curve (fibre no. 5 & 7) or the dashed green and dashed black curve (fibre no. 10 & 12) serve as an example for the characteristics of the frequency influence of all measurements. It can be observed that the variation of the frequency between one and two Hertz has no influence on the trend of

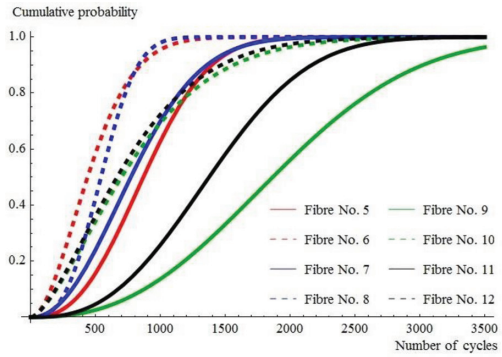


Figure 7. Results of flex abrasion test of all measurements of fibre type A.

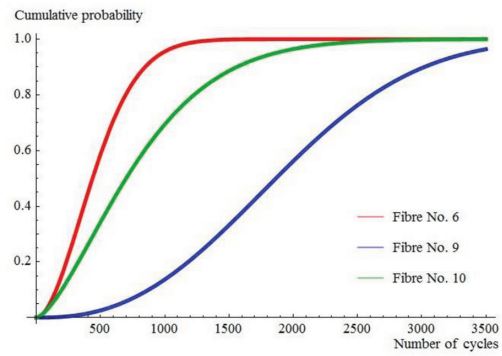


Figure 8. Influence of the weight and stroke on the measurements.

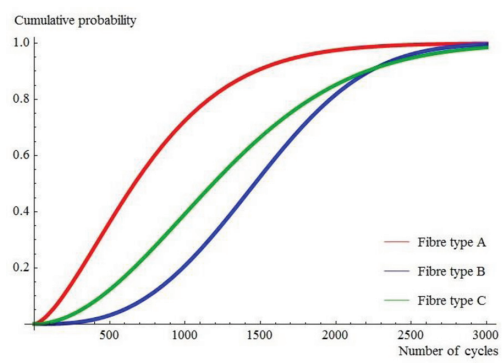


Figure 9. Influence of different types of fibres.

the curves (curve pairs mentioned above are nearly congruent). To confirm this statement, an analytical calculation with assumption of linearity of the movement acceleration has been performed. The result was considered in form of rate of the origin

Table 2. Impact of weight and stroke—setup and results.

No.	Stroke [mm]	Weight [g]	x_{min}	x_{av}	x_{max}	s_{min}	s_{av}	s_{max}
6	10	20	355	474	593	219	281	395
9	4	10	1553	1909	2266	657	845	1185
10	4	20	559	803	1046	447	576	808

force acting on the fibre by a weight of 20 grams to the force caused by the acceleration. The increase of the frequency from one to two Hertz causes a force change of about 2%.

For a remarkable difference of the results, the frequency would have to be increased into a level which is already out of the specification range of the test facility.

Figure 8 shows the impact of the stroke and the weight on the reliability of the fibres. For the comparison of the parameters adjustment and results Table 2. The presented results are in form of the arithmetic mean (x_{av}) with its confidence interval consisting of lower and upper confidence bounds (x_{min} & x_{max}) as well as the variance (s_{av}) with the confidence interval (s_{min} & s_{max}).

By the systematic analysis of the curves in Figure 8 and numerical results in Table 2, it can be observed that fibre no. 6 reached the lowest and fibre no. 10 the highest number of cycles. Therefore, the corresponding weight and stroke setup of fibre no. 6 causes the highest loss of reliability. Furthermore, the increase of the weight causes remarkable higher difference in the results than the increase of the stroke. In spite of the increase of the stroke, the upper bound of the confidence interval of fibre no. 6 is still higher than the lower bound of fibre no. 10. As a consequence, the visualisation of the distribution models is different, but statistically not significant. The influence of the fibre type on the reliability is shown in the Figure 9. It can be noticed that the fibre type A reaches the lowest and the fibre type C the highest number of cycles. All the fibres were tested by the same setup of the testing parameters.

6 SUMMARY AND OUTLOOK

This paper shows results of a research work with regard to an approach for the analysis procedure of prototype test results, based on heterogeneous prototype characteristics and small data volumes within the early phase of product development. The research activities were applied within a case study "Organic fibre prototype analysis" out of the chemical process industry. The goal is the analysis of reliability parameters of heterogeneous fibre samples. The analysis of fibre characteristics (e.g. centre, dispersion, trends) and interdependences were done with the use of nonparametric as well as parametric statistical methods. Main results are:

1. 93% of the fibre samples can be fitted by using Weibull distribution models in a sound way.
2. Thickness of fibres has no impact regarding to the reliability parameters within the analysed range of number of load cycles.
3. Variation of frequency within the range of 1 Hz–2 Hz has no impact regarding the reliability parameters.
4. The length of stroke has a significant impact in comparison to the weight load.
5. The arithmetical differentiation of reliability parameters between fibre types A to C is feasible in spite of small sample sizes and heterogeneous data.
6. The facility adjustment for the maximal differentiability for further prototype tests.

The used approach shows that the structured combined application of nonparametric as well as parametric statistical methods is successful. The transfer of the approach to similar technical problems is feasible. Next steps of research work will be the analysis of chemical treatment and their impact on fibre reliability parameters.

ACKNOWLEDGEMENTS

The author thanks Doris Oberkobusch, Detlef Fischer and Andreas Kirch (all Henkel AG & Co. KGaA) for their support with regard to fibre information and support of test procedure as a basis for our research work.

REFERENCES

Chan, H. & Englert, H. 2001. *Accelerated stress testing handbook: Guide for achieving quality products.* New York: IEEE Press.

Choi, H.Y. 1992. Nonformaldehyde Polymerization-Crosslinking Treatment of Cotton Fabrics for Improved Strength Retention. *Textile Research Journal* 62 (10): 614–618.

Dusenbury, J.H. & Mercer, E.H. & Wakelin, J.H. 1954. The Influence of Chemical Treatment on the Properties of Wool—I. Alkali Solubility as a Measure of Sulfuric Acid Degradation. *Textile Research Journal*: 890–899.

Escobar, L. & Meeker, W. 2003. Accelerated destructive degradation tests: Data, models and analysis. *Mathematical and Statistical Methods in Reliability*, World Scientific, River Edge, pp. 319–337.

Escobar, L. & Meeker, W. 2006. A Review of Accelerated Test Models. *Statistical Science* 21(4): 552–577.

Guangbin, Y. & Zaghati, Z. 2006. Accelerated life tests at higher usage rates: a case study. *Annual Reliability and Maintainability Symposium (RAMS)*: 313–317.

Hartung, J. & Elpelt, B. 1998. *Lehr- und Handbuch der angewandten Statistik; mit zahlreichen, vollständig durchgerechneten Beispielen.* 11. Edition. München, Wien: Oldenbourg.

Hinz, M., Temminghoff, P. & Bracke, S. 2014. Beitrag zur multivariaten Analyse von Qualitäts- und Zuverlässigkeitsdaten in der Produkt-Erprobungsphase am Beispiel der Fahrzeugtechnik. *Berichte zum Qualitätsmanagement* 16: 93–114.

Nelson, W. 1990. *Accelerated testing: Statistical models, test plans and data analyses.* New York: Wiley.

Pykett, M.A. & Swift, J.A. 1998. Schutz vor Haarbruch nachweisen. *Parfümerie und Kosmetik 79. Jahrgang* (10): 38–40.

Sachs, L. & Hedderich, J. 2009. *Angewandte Statistik Methodensammlung mit R.* (13). Berlin: Springer.

Swift, J.A. et al. 2001. Flexabrasion: A Method for Evaluating Hair Strength. *Cosmetics & Toiletries magazine* 116 (12): 53–60.

Yang, C.Q. & Quian, L. & Lickfield, G.C. 2001. Mechanical Strength of Durable Press Finished Cotton Fabric—Part IV: Abrasion Resistance. *Textile Research Journal* 71 (6): 543–548.

Yang, C.Q. & Zhou, W. & Lickfield, G.C. & Parachura, K. 2003. Cellulase Treatment of Durable Press Finished Cotton Fabric: Effects on Fabric Strength, Abrasion Resistance, and Handle. *Textile Research Journal* 73 (12): 1057–1062.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

How to present and understand uncertainty of production assurance analyses with respect to data quality

C. Persskog-Lundtofte, S. Isaksen & L.M. Pedersen
Safetec Nordic AS, Oslo, Norway

ABSTRACT: Production assurance analyses of production systems include reliability data such as failure rates and repair data. Often the available data from reliability data sources are poor with respect to population or not existing when searching for reliability data of a specific component of the production system. As a consequence, a more generic data set is applied, which might not be relevant for the component since the data set might contain data from components that are constructed differently or operate differently. These two issues are typically conflicting and the challenge is to find a proper balance. Results commonly produced from Production assurance analyses, like system production availability and component criticality, depend heavily on the reliability data which have been used as input. Reliability data used in such studies are typically listed in a report, but without further discussion or evaluation of data quality. This paper proposes a simple and practical method of understanding and presenting the uncertainty related to these quality aspects, which involves evaluating and ranking components with respect to data quality. This paper also discusses how to analyse the effect of reliability data quality on the production assurance analysis results.

1 INTRODUCTION

In production assurance analyses, also called Reliability, Availability and Maintainability (RAM) analyses, the performance of a production system can be measured and form a basis for decisions that can increase profit through reduced downtime and reduced operations and maintenance cost.

Typically, a flow network as a representation of the production system and its components combined with Monte Carlo simulation utilizing the discrete event simulation technique is used to generate the results of a RAM analysis.

These analyses have been performed for production systems in the oil and gas sector for about 30 years and an industry standard, ISO 20815, describing the methodology has been established. Even though this standard gives the industry the clarity and precision required to be able to carry out high quality analyses, some have pointed out (e.g. Aven & Pedersen (2014)) that there still is confusion in the industry concerning how to represent and treat uncertainties with respect to production assurance analyses. Aven & Pedersen further present a framework on how to understand and present these uncertainties in practical production assurance analyses.

This paper follows the lead of this framework but focuses in detail on uncertainty factors related to quality in reliability data. Results commonly produced from production assurance analyses, like system production availability and component criticality, depend heavily on the reliability data which have been used as input. Reliability data used in such studies are typically listed in a report, but without further discussion or evaluation of data quality. The purpose of this paper is to propose a simple and practical method of understanding, presenting and treating the uncertainty related to quality of reliability data.

Section 2 presents and discusses quality aspects of reliability data. Section 3 discusses the effect of data quality on the results of a production assurance analysis. In Section 4, a case study is introduced which presents an example of how to understand and present the uncertainty related to data quality aspects in a simple and practical way.

2 DATA QUALITY

2.1 *Definition of high-quality data*

In ISO 14224 high-quality data are defined to be characterized by the following:

1. Completeness of data in relation to specification;
2. Compliance with definitions of reliability parameters, data types and formats;
3. Accurate input, transfer, handling and storage of data (manually or electronic);
4. Sufficient population and adequate surveillance period to give statistical confidence;
5. Relevance to the data user's need.

In ISO 20815 it is stated that selection of data should be based on the following principles:

1. Data should originate from the same type of equipment and, if possible, originate from identical equipment models.
2. Data should originate from equipment using similar technology.
3. Data should originate from periods of stable operation, although early-life or start-up problems should be given due consideration.
4. Data should, if possible, originate from equipment that has been exposed to comparable operating and maintenance conditions.
5. The basis for the data used should be sufficiently extensive.
6. The amount of inventories and failure events used to estimate or predict reliability parameters should be sufficiently large to avoid bias resulting from "outliers".
7. The repair and downtime data should reflect site specific conditions.
8. The equipment boundary for the originating data source and analysis element should match as far as possible (study assumptions should otherwise be given).
9. Population data (e.g. operating time, observation period) should be indicated to reflect the statistical significance (uncertainty related to estimates and predictions) and the "technology window".
10. Data sources should be quoted.

Based on these definitions of high-quality data and statements of what principles selection of data should be based on, the need for a practical method to evaluate quality of reliability data has been identified.

2.2 *Data quality aspects*

When choosing reliability data for a component one often needs to compromise between two aspects of data quality; relevance and population, see Point 4) and 5) of the ISO 14224 definition of high-quality data. A more generic data set has a larger population but is less specific and the data set might contain data from components that are constructed differently or operate differently and therefore are less representative.

The authors of this paper are not aware of any standard which classifies relevance and population of reliability data. There may be many opinions about e.g. which factors are important when defining relevance of data and what a large data set is. The examples in the next subsections are merely suggestions.

2.2.1 *Relevance*

One can set up a scale of relevance with grades of Low, Medium and High with respect to the principles from ISO 20815 stated in chapter 2.1. This classification of relevance is a difficult exercise and must be done by people who understand both the equipment in the system to be analyzed and the equipment from which historical data is obtained. It is not feasible to come up with general criteria for classification into e.g. High, Medium and Low relevance of reliability data which is valid for all industries and equipment. For instance, the first principle for selection of data in ISO 20815 is about the "same" type of equipment, but this is not clearly defined. In ISO 14224, "equipment type" is defined for many equipment classes, but it is difficult to generally classify data from the same equipment type with certain relevance. For instance, pump types include centrifugal, reciprocating and rotary. But one can still argue that data for small centrifugal pumps in a chemical injection system are not very representative for large crude oil export centrifugal pumps.

There are other factors than the general design which should determine if equipment is of the same 'type' or not. Which factors are the most relevant may vary from one equipment class and industry to another. Manufacturer, size, design power, design pressure, design temperature, etc may have different significance and uniqueness in different cases and it is up to experts to use their knowledge of these factors to classify the relevance of the available data.

Other criteria related to relevance like operating and maintenance conditions must also be taken into account. The first principle of data selection in ISO20815 also mentions identical equipment models. If this is the case and operating and maintenance conditions also are the same, the relevance is obviously high. However, usually the data source contains a mix of many different equipment manufacturers and models which are unknown. It is rather the exception that the analyst has access to much data for the one particular equipment model of interest. If this condition is not fulfilled, it can be argued that relevance may still be high if equipment can be defined as similar based on other factors.

When only low relevance data (or no data) are available, it is recommended to perform an Failure Mode, Effect and Criticality Analysis (FMECA) to identify possible failure modes and have experts giving their views on the likelihood of these failures occurring.

2.2.2 *Population*

In order to calculate the reliability of equipment, information regarding the number of failures, the surveillance (or operational) time and the age of the equipment at the time of failure is required. The latter is only relevant if another lifetime model than the exponential is used. In order to have a solid basis for calculating the failure rate, there

should be a lot of failures. This is the paradox of reliability data; the analyst wants failures whereas the operator does not.

There may be large differences in the failure rate for different equipment classes. If a certain number of failures is required before the data quality in terms of population can be graded with 'high', the surveillance time of reliable equipment must generally be longer than the surveillance time of unreliable equipment. Perhaps data collection on non-pressurized tanks would require thousands of equipment years in surveillance to give an amount of failures to establish high quality data, while data collected for only one large compressor over a few years would give the same quality.

For the non-pressurized tank, the total surveillance time would be a better indicator of data quality. If this is large and the failures few, it only means that reliability is high. For the compressor, failures are more frequent, and a sufficiently high amount may be reached long before surveillance time equals that of the tanks. 'Sufficient' in this case expresses the amount which gives the analyst confidence that the lifetime distribution derived from the data is suitable and accurate for predicting the reliability of similar equipment. Hence, depending on the equipment class, there should be a balance between total surveillance time and amount of failures.

In case of no observed failures there are several Bayesian methods to estimate the failure rate, for instance using a non-informative prior.

Grading into e.g. high, medium and low may in this case be purely quantitative. The following scale is suggested:

- High quality: Total surveillance time > 100 years OR Total number of failures > 20
- Medium quality: Total surveillance time > 30 years OR Number of failures > 6
- Low quality: None of the conditions above are met.

Dependent and cascading failures should not be counted when comparing the amount with the criteria.

It should be noted that the classification above is merely a suggestion. When grading reliability data from high to low quality with respect to population, it is suggested to apply a scale which is relative to the amount of data that is generally available in the industry. This scale is suggested based on experience and available data in the Norwegian oil and gas industry.

When speaking about data population, one would perhaps think of the amount of components, rather than the amount of failures or surveillance time. The total surveillance time is calculated as the number of equipment units multiplied by their average surveillance time. So when the criterion for high quality is more than 100 years, it refers to so-called equipment-years. The amount of equipment units is not included in the suggested grading, since the difference in quality of data based on e.g. 10 equipment units observed for 10 years each or 50 equipment units observed for 2 years each depends on the context.

When the purpose is to undertake lifetime analyses, a longer surveillance time per equipment unit may be preferred. In other circumstances, a higher amount of equipment units may be preferred. For instance with a dataset containing little information, it is not known to what degree it is homogeneous. In that case, as many different equipment units as possible may be preferred to cover the variety and not have biases in one direction or the other. If a non-homogeneous data set is the only data available, the variance in the empirical data is used in the predictions to express uncertainty of the time to failure due to low quality data as described in Section 3.3.

2.2.3 *Availability of information*

Point 1), 2) and 3) of the ISO 14224 definition of high-quality data relates mainly to quality properties to be ensured in the data collection process, rather than relevance or population. Even though ISO 14224 is a standard which is written to ensure these properties when followed, mistakes can be made during the data collection process. It can therefore be beneficial for data quality improvement to assess the basis of the reliability data at hand, such as the registered failure events and make adjustments if needed.

Another aspect is the availability of this information regarding boundaries, definitions of failure, etc. Many data collection projects do not follow ISO 14224. They may or may not make accurate definitions and guidelines for data collectors to follow and if they do, these may not be transparent in a data handbook with "processed" reliability data in the form of e.g. failure rates.

If failure rates on e.g. gas turbines are used as input in a study, are the definitions associated with the data source clear? What are the defined boundaries of the gas turbine? Are failures on the Waste Heat Recovery Unit (WHRU) included in the failure rate? Are trips due to excess of specified operational parameters defined as gas turbine failures and included? Obviously, the answers to these questions influence the failure rate. Unfortunately, several data sources are not clear on these points and rely on the analysts to define gas turbines and gas turbine failures the same way as the data collectors.

The result of lack of information of this kind does not reduce the relevance of data, but the *uncertainty* about the relevance of data. Hence, the amount of information regarding definitions associated with the data becomes an important quality

aspect as well. Again it may be difficult to establish general criteria to classify the amount of information as high, medium or low. However, relevance of data cannot be classified as high, if there are large uncertainties about the data set, and many of the factors defining high relevance are unknown.

The whole process of data collection involves several steps, where each can lead to loss of information. This is illustrated in Figure 1. The information loss can be due to limitations in information systems or wrong interpretations, errors when recording information, etc. Normally the information about equipment attributes or failure events is not recorded for the purpose of reliability analyses in the first place. People recording this information do not have that objective in mind and often little knowledge about reliability data and analyses in general. This will often result in manual work by the data collector to covert information into a reliability data format like e.g. ISO 14224. Spelling mistakes and similar can always be identified and corrected with proper quality assurance at several stages in the process, but established formats is more difficult to change.

Also, it is quite common that the interpretation and analysis of raw data is not done by the person applying the data for a reliability study. In many cases, access to the database itself is restricted, and analysis, handling and organising of data are done for publishing in a reliability data handbook, which is the only access the analyst has. Such a handbook of processed data will typically lack a lot of the information available in the raw data.

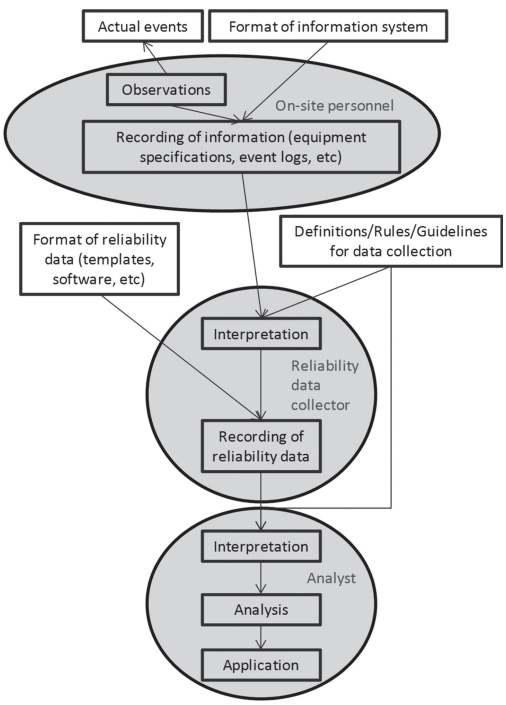


Figure 1. Illustration of data collection process.

2.2.4 *Maintenance data*

As reliability data is discussed and evaluated in terms of quality, it is important not to forget maintenance data, since availability depends on both. Maintenance data or downtimes tend to get less attention because it is often excluded from reliability data handbooks or other sources. This exclusion is justified by the argument that generic data are not useful since the downtimes are plant-specific and dependent on different maintenance strategies, as stated in data quality principle 7 in ISO 20815.

The quality of these data, however, is just as important. To evaluate the quality, however, may be more difficult since they are often given as expert judgment. Also, the downtimes may consist of several factors such as run-down, diagnosing, mobilization, active repair and ramp-up. Each of these factors may be of various quality even though they are given by the same expert, since some downtime-related activity may be harder to predict than others.

3 EFFECT OF DATA QUALITY ON RESULTS

In almost every reliability analysis, the reliability data are one of the main uncertainty factors due to lack of quality. This results in a certain lack of confidence in the prediction which has been made. This section discusses how to possibly manage such uncertainties. There are different topics to discuss as there is not one solution. In general, the best way to handle uncertainties related to lack of quality reliability data depends on the purpose of the analysis. When the goal is to prove that the production availability reaches a certain target, it may be useful to reverse the traditional analysis and investigate what reliability parameter values are required to reach it. Then, by comparing those with the actual data at hand, one may evaluate the degree of confidence in those values representing good predictions.

If the purpose is to compare different designs solutions, perhaps the main focus should be on the components which are different from one design to another, and especially those with low quality reliability data. By e.g. sensitivity analyses as described later in this Section, the influence of different parameter values can be evaluated and compared for different concepts.

Knowing that the results are heavily influenced by the reliability data which are used in the study, it

would be useful to obtain more detailed knowledge about this effect. New and improved information about reliability would change the results, but the question is if that change can be quantified. If so, it would help the analyst to know which data are more crucial to improve.

In any case it is important to address and not avoid the problem. It may be tempting to leave the result without highlighting the data quality issues. It is better, however, to evaluate the effect of low quality data on the results and identify the components where data quality improvement is the most crucial.

3.1 *Importance measures*

Component importance measures are commonly used to quantify the impact of one component on the system availability. Applying importance measures would thus seem the appropriate solution to the problem of evaluating the impact of low quality data on the results. Unfortunately, things are a bit more complicated than that. There are many component importance measures, but they are all functions of both the component's structural position in the system and its availability. When there is large uncertainty associated with the component's availability due to low quality data, there will also be large uncertainties in the component importance results. In other words, when the availability changes, the importance of the component also changes.

A possibility could be to temporarily ignore the availability and only consider the criticality given the structural position in the system. This can be found by e.g. assigning equal availabilities to all components and then apply an importance measure. No component can be more critical than the ones which are in series with the rest of the system. These are often present in production systems and will thus always end up with the highest criticality when differences in availability are ignored. In that case it is easy to determine which components should be prioritized when it comes to obtaining improved reliability data.

There are several challenges still. Sometimes, the only way to obtain better data is to start a new data collection campaign. This may take time, and perhaps decisions which the analysis influences need to be taken quickly. Also, by ignoring the availability to obtain component importance results one may get a wrong impression of the priorities. Even though there is uncertainty about the lifetime distribution of a component, one would usually have an idea about which components are more reliable and which are less reliable. For instance, one may have a system with a storage tank in series with the system and connected with two redundant offloading pumps, all with low quality reliability data. When availability is not considered, the tank is much more critical for production, but even with low quality data, most analysts would agree that it also is much more reliable than the pumps. So it cannot easily be concluded that obtaining high quality data for the tank is more crucial. Hence, applying importance measures for this purpose should always be accompanied by sound judgment.

3.2 *Sensitivity analysis*

Sensitivity analyses can be performed on parameters in a lifetime distribution, and will in that case be related to the component importance measures as they in essence evaluate the effect of changes in the component availability. The advantage of sensitivity analyses is that they provide more flexibility where the analyst can experiment with different specific parameter values. These may for instance represent failure rates from different data sources. Or one may define a range covering what is perceived as the most realistic values and plot a graph showing the system availability as a function of component availability within that range.

Sensitivity analyses are very simple. As long as a model is established, the calculations or simulations are just repeated over again for different parameter values. As new results are produced, one can observe the effect of the change in the parameter value. Whenever Monte Carlo simulation is used as the calculation method, a possible disadvantage with sensitivity analysis is the additional simulation time. Depending on the duration of the initial base case simulation, the extra time required for sensitivity analyses may be an issue, because one parameter change requires one additional full simulation.

3.3 *Lifetime distributions*

There are many methods to fit empirical failure data to a probability distribution function. That distribution is typically also used in the predictions, i.e. the variation in empirical data represents the uncertainty in the prediction. However, with little data, the exercise of fitting them to a distribution is difficult. With e.g. only two failure records at times t_1 and t_2, there can be no good fit. For equipment in the oil and gas industry with regular preventive maintenance, it is common to assume that the time until a failure follows the simple one-parameter exponential distribution. That way, all which is needed is finding the λ parameter by dividing the number of failures by total surveillance time.

If data quality is low, one may want to reflect the high uncertainty in the predictions with high variance. For a given mean, the variance in the exponential distribution is also given. Hence, another distribution with higher variance might be appropriate. However, sometimes the analyst

may be convinced that the exponential model is suitable without having good quality reliability data, just because e.g. similar type equipment with more data shows this trend. The dilemma is then what failure rate, λ to use. If the data consist of only one component observed for 5 years with two failures, the assumption of an exponential distribution yields $\lambda = (5/2 = 2.5)$. A confidence interval for λ is given by the Chi square distribution (See Ross 2009). A 90% confidence interval gives $[1.1 < 1/\lambda = MTTF < 14.1]$.

There is obviously a very large difference between a failure every year and every 14 years. The large spread in the confidence interval makes it difficult to be confident about 2.5 being a good predictor for the future failure rate, when only based on these data. One possibility is to perform sensitivity analyses as discussed, where a best case and worst case is calculated in addition to the base case, and where certain percentiles of λ are used. But if there are many components with low quality data, there may be too many sensitivities to keep the overview of all the results.

Another possibility is to express the parameter(s) with a distribution function. In the exponential case, the λ can first be generated from a Chi square distribution and then the failure time generated from the exponential distribution based on this λ. This is a quite common approach but one needs to be careful with the interpretation as it is important to understand the difference between the history (empirical data) and the future (predictions). The traditional interpretation of this distribution is that it represents the uncertainty of λ, as if there were a true or correct value. Aven (2009), however, emphasises the subjective nature of predictions and advocates the interpretation of λ as the analyst's degree of confidence in λ being a good predictor for the failure time. The outcome of this model is therefore nothing but a representation of the analyst's uncertainty regarding the time of failure due to low quality in historical data.

4 A CASE STUDY

4.1 *General information*

The case study is based on a production assurance analysis of an offshore oil production system in the Norwegian oil industry. The production system is considered to be representative for a typical topside oil production system with regards to design, production critical subsystems and components. One of the objectives and focus in this case is to provide decision support for several power generation/supply alternatives:

1. Two turbine driven generators
2. One larger turbine driven generator
3. As case 2 but with additional combustion chamber, HRSG and steam turbine
4. Power from shore.

A number of components modeled in the analysis have been selected to be assessed with regards to the quality of their reliability data as described in section 2 of this paper.

4.2 *Reliability data*

Part of the data dossier of the components in the study is presented in Table 1. The data in the case study are comparable with data from typical reliability data sources in the oil and gas industry which follows ISO 14224 during the data collection process.

4.3 *Data quality assessment*

A data quality assessment was carried out and each component's data source was graded with High (H), Medium (M) or Low (L) with respect to relevance and population. The result of the data quality assessment is presented in Table 2.

The scale presented in Section 2.2.2 has been used to score the data sources with respect to population. Relevance has been scored with respect to the author's knowledge of the data sources and the analyst's knowledge of the components in the system which has been communicated to the analyst through meetings and technical documentation.

A more graphical representation of the data quality result, which shows the distribution between population and relevance with reference to the component IDs is presented in Table 3.

Table 3 shows that the most critical components with respect to data quality are components with ID: 3, 4, 5, 7 and 10.

As shown, a large generic data set of centrifugal pumps has been chosen to represent specific groups of components due to lack of more relevant data.

Further, a more specific data set with low population has been chosen for the heating medium circulation pumps.

There were no specific Waste Heat Recovery Unit (WHRU) data found, only Heat Recovery Steam Generator (HRSG) which is a type of WHRU generating steam and is present for one of the power alternatives. However, two of the other alternatives include one or two WHRUs which are made for water heating and therefore a different type. Hence WHRU data have low relevance.

The submarine power cable data (12) are highly relevant as the source contains the exact same cable type and the population is barely on the "medium" level. Normally, the argument would be that there is enough evidence of a high reliability with only two failures in 35 years. However, since the downtime is expected to be very high compared to other equipment on the platform, a change in the data may have

Table 1. Case study reliability data.

Component	Nr. of failures	Surv. time (years)	Data source categorisation
Inlet heater	12	111,5	Heat exchangers—shell and tube
1st stage separator	59	535,8	Vessels—separator
Gas injection discharge cooler	11	55,1	Heat exchangers—plate conventional
Heating medium circulation pumps	1	12,0	Pumps—centrifugal—cooling systems
Produced water recycle pump	210	370,0	Pumps—centrifugal
Foam inhibitor pump motor	2	50,0	Electric equipment—electric motors—pump-chemical injection
Seawater lift pump	210	370,0	Pumps—centrifugal
Gas turbine	175	43	Gas turbines—10–50 MW
Electric generator	12	34	Electric generator—turbine driven
Waste Heat Recovery Unit (WHRU)	287	784	HRSG—combined cycle plants
Heat Recovery Steam Generator (HRSG)	287	784	HRSG—combined cycle plants
Submarine power cable	2	35	Submarine power cables-AC—XLPE type—60–219 kV

Table 2. Result of data quality assessment.

		Data quality	
ID	Component	Relevance	Population
1	Inlet heater	M	H
2	1st stage separator	M	H
3	Gas injection discharge cooler	L	M
4	Heating medium circulation pumps	M	L
5	Produced water recycle pump	L	H
6	Foam inhibitor pump motor	H	M
7	Seawater lift pump	L	H
8	Gas turbine	M	H
9	Electric generator	M	H
10	WHRU	L	H
11	HRSG	M	H
12	Submarine power cable	H	M

Table 3. Graphical representation of data quality assessment.

	Relevance		
Population	Low	Medium	High
High	**5, 7, 10**	1, 2, 8, 9, 11	
Medium	**3**		6, 12
Low		**4**	

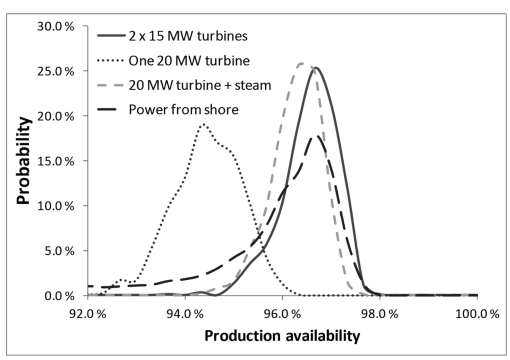


Figure 2. Production availability results.

high impact on the results. Because of this expected high sensitivity and the fact that the population is close to fall in the "low" category, the power cable should be subject to extra attention as well.

If it is desired to improve the data quality of the data dossier of this production assurance analysis, one should focus on these components and data sources.

4.4 *Effect of data quality on results*

The production availability results for the four power alternatives are given in Figure 2. Since we know that these results in part are based on low quality reliability data, it seems appropriate to evaluate the effects of this uncertainty factor.

Many of the components in Table 3 with low relevance or population are common for all 4 power alternative cases. Instead, the study focused on the components with low quality data which were not common for all 4 cases, namely the Waste Heat Recovery Unit (WHRU) and the submarine power cable. The power cable is only included in Case 4 and the WHRU in Cases 1 and 2 as listed in Section 4.1.

Component importance results were already present as part of the output from the initial calculations. The submarine power cable was the most important of all components in the system, according to the applied measure. The WHRU had little importance in Case 1 (2×15 MW turbines) due to redundancy but somewhat higher importance in Case 2 (single 20 MW turbine). It was then decided to run sensitivities on WHRUs as well as submarine power cables to evaluate the effect of different parameter values for the time to failure.

Experts were brought in who agreed that the WHRU generally should be more reliable than the HRSG. Hence, the data assigned to the WHRU could be regarded as "worst case". Improving WHRU reliability could only benefit Case 2, but running sensitivities for higher WHRU Mean Time To Failure (MTTF) values only yields a very marginal improvement.

It was more difficult for experts to agree on the reliability for submarine power cables. Hence it was decided to look at chi square quantiles as discussed in Section 3.3. Instead of generating chi square distributed lambdas in the simulation, sensitivities were run for different quantiles, where the lowest and highest values used were the 5% and 95% quantiles, respectively.

Figure 3 plots the mean system availability as a function of submarine power cable MTTF.

It seems from the graph that the system is quite sensitive to changes in the submarine power cable MTTF. Using the base case value for MTTF of power cable, Case 4 results are quite similar to Case 1 and Case 3 in terms of mean system availability. But varying the power cable MTTF, Case 4 may also be significantly better or worse. Due to this and the already existing heavy left tail seen in Figure 2 due to the long downtime, Case 4 (power from shore) represents a more risky alternative for better or for worse. This is important information for a stakeholder and would not have been highlighted in a more traditional approach without data quality assessments and sensitivity analyses.

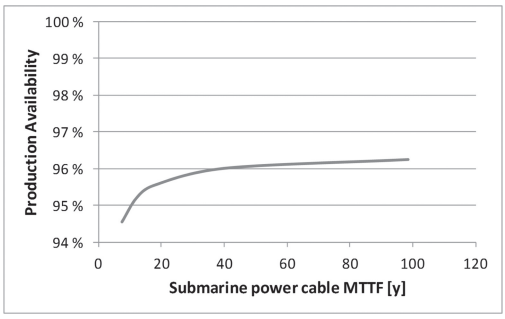


Figure 3. Case 4: System availability as a function of submarine power cable MTTF.

5 CONCLUSION

Results commonly produced from Production assurance analyses, like system production availability and component criticality, depend heavily on the reliability data which have been used as input. Reliability data used in such studies are typically listed in a report, but without further discussion or evaluation of data quality. This paper has proposed a simple and practical method of understanding and presenting the uncertainty related to data quality aspects, which involves evaluating and ranking components with respect to the population and relevance of their data source. This paper has also discussed how to analyze the effect of reliability data quality on the production assurance analysis results.

The case study has demonstrated how evaluating quality and performing additional analyses give a broader picture of the expected system performance. It is by no means giving definite or simple answers which give the stakeholders obvious choices as this is impossible with low quality data. Hence, presenting results as one correct answer obscures inevitable uncertainties and may lead to bad decisions because they are based on less information than they could have been. By evaluating the quality of the data and the impact on the results, uncertainties, which should be an important part of the decision making, become more visible.

REFERENCES

Aven, T., 2009. *Foundations of risk analysis,* second edition. Wiley.

Aven, T. & Pedersen, L.M., 2014. On how to understand and present the uncertainties in production assurance analyses, with a case study related to a subsea production system. Reliability Engineering and System Safety 124(2014): 165–170.

International Organization for Standardization (ISO) 2006, *Petroleum, petrochemical and natural gas industries—Collection and exchange of reliability and maintenance data for equipment*, International Standard ISO 14224, second edition, 2006-12-15.

International Organization for Standardization (ISO) 2008. *Petroleum, petrochemical and natural gas industries—Production assurance and reliability management,* International Standard ISO 20815, first edition, 2008-06-01.

Ross, S.M., 2009. *Introduction to probability and statistics for engineers and scientists*. Fourth edition. Associated press: 267.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Universal method of battery life prediction

Y. Hanyu, T. Yamamoto, T. Ezawa & A. Itakura
Systems Engineering Laboratory, Toshiba Research and Development Center, Japan

ABSTRACT: Grid-connected Lithium-ion Battery based Energy Storage Systems (LiB-ESS's) must maintain strict safety and reliability standards for more than 15 years. However, predicting the lifespan of LiB-ESS's has been a difficult task, since the cells inside usually contain battery cells supplied by third-party manufacturers. Especially, the lack of detailed information on chemical composition and aging behavior of such battery cells pose a problem in quantifying reliability and establishing maintenance schemes. Therefore, a universally applicable cell diagnostic and life prediction method is highly desirable.

1 INTRODUCTION

The utility-scale Energy Storage Systems (ESS's) market is set to expand to more than 6 GW in 2017 to accommodate more intermittent power sources such as wind and solar. Among such ESS's, on lithium-ion secondary battery (LiB) based systems are expected to play a key role. This is because high capacity and voltage (hence, high energy density) and versatility in scales and layouts makes LiB-ESS's an attractive option for integration in existing facilities. In the meantime, the system requirements span safety, reliability, long mean-time-before-failure and system life for building-integrated systems. For the system life, technical recommendations issued by Electric Power Research Institute gives a typical figure of 10 years or longer (Rastler 2010).

To date, correctly predicting the lifespan of LiB-ESS's, or even estimating the remaining battery lifetime has been a formidable task, since the component cells often come from third party sources and information on chemical composition and aging behavior is not always available. This is because such data is often directly linked to manufacturer's market competitiveness, but at the same time, the unavailability of data would pose a problem in quantifying reliability, predicting battery life and establishing maintenance schemes. Ideally, we must have a universal method that does not rely on classified information. Therefore, we have developed a universal method of LiB life prediction based on differential capacity versus potential (dQdV) profiles that are obtainable from routine charging. Since the method does not use any classified information, it can be applied to any LiB-ESS systems.

The peaks on dQdV profiles are usually associated with certain chemical or physical processes. These peaks are known to exhibit high sensitivity toward slightest changes in the chemical state of battery electrodes, and any associated changes to the internal resistance upon aging (Wang 2010). The dQdV profiles are effective for fingerprinting batteries, but the same methodology can be applied to identify battery aging. In essence, our "universal method of battery life prediction" is fingerprinting of battery aging.

The method has three stages: initial battery aging experiment on the specimen cells to construct a database, then formulation of aging behavior, and then the actual evaluation and life prediction. Once the battery database is built by the end of second stage, the target battery model of any conditions—new or used, can be evaluated at will in the third stage, possibly as a commercial service.

2 METHOD

The charge-discharge (C/D) experiments were conducted in a MP-01 programmable temperature-controlled galvanostat/potentiostat (Fujitsu Telecom Network). Data analysis was conducted by Matlab software. Eight 30 Ah electric vehicle battery specimen cells were used for the experiment. 2 cells were tested for long-term storage test under increased temperatures. 6 cells were tested for continuous C/D cycling under different temperatures and current rates. The temperature levels were 35 degrees and 45 degrees, the C/D cycling depths were 50–90 and 10–90, and the electric current levels were 30 A and 90 A. The combination of these levels generated 8 combinations, but cycling experiment for SoC 10–90% at 30 A current was omitted due to logistical constraints. The experimental conditions are summarized on Figure 1 (Left). The current, voltage, temperature and cumulative charge in Ah were recorded at 1 s interval, which typically gave a potential profile consisting of ~3600 data points

Ch.	Temp.	Current	SoC Range
1	35°C	0 A	100%
2	45°C	0 A	100%
3	35°C	90 A	10-90%
4	45°C	90 A	10-90%
5	35°C	30 A	50-90%
6	45°C	30 A	50-90%
7	35°C	90 A	50-90%
8	45°C	90 A	50-90%

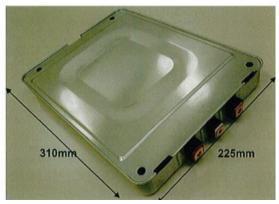


Figure 1. Experimental conditions of cells (left) and the photograph of a specimen EV cell used in the experiment (right)—The capacity was 30 Ah.

for one charge or discharge. The potential profiles were smoothed by taking a simple moving average over 20 points and dQdV profiles were derived. The dQdV parameters were found by fitting 5th-order polynomials to segments of dQdV profiles. Once the peaks were identified, other parameters such as peak height ratio, peak width, peak area and inflection points were calculated.

3 RESULTS AND DISCUSSION

Battery aging is a complex phenomenon with numerous inputs and outputs. However, there are essentially only two key performance indexes—capacity and power. Our method aims to predict the two key performance indexes.

The method starts with prior construction of a database for target battery model. The database contains a list of selected dQdV parameters sorted according to aging time and conditions. This puts a limitation that only commercially available mass-produced cells on the market can be evaluated by this method. On the contrary, the method is not limited to certain battery types or brands. Although the method's primary target is LiB's, it is potentially applicable to other batteries including Ni-H_2 and Na/NiCl.

3.1 *Parameterization of differential potential (dQdV) profiles*

In the first stage, a cell's aging behavior is parameterized by obtaining the time series of a changing dQdV parameter. This is achieved by subjecting multiple specimen cells to different aging conditions and periodically measuring the potential profile at different stages of aging. In our experiment, 2 cells were tested for long-term storage at 35 and 45 degrees. 6 other cells were tested for continuous charge-discharge (C/D) cycles under different controlled conditions. The variables were temperature, current rate, and the state of charge (SoC). Each had two variations as shown on Figure 1.

The collected potential profiles were re-drawn into dQdV profiles by plotting $(Q_n - Q_{n-1})/(V_n - V_{n-1})$ against V (Fig. 2). In general, dQdV profiles are highly sensitive. For example, any small changes to the voltage plateau in charge profiles appear as noticeable peak shift in the corresponding dQdV profiles.

On this plot, the highest peak near 4.13 V and peaks between 3.80 V and 4.05 V are thought to have their origins in Lithium Manganese Oxide (LMO) and Nickel-Cobalt-Aluminium oxide (NCA) cathode materials, which were also confirmed by spectroscopic methods (X-ray photoelectron spectroscopy and energy dispersive x-ray spectroscopy). The LMO peak near 4.13 V was virtually constant regardless of the state of aging, but the NCA peaks between 3.80~4.05 V exhibited a rapid decay over time. The assignment of peaks was confirmed by measuring the dQdV profiles of pure LMO-based cells and NCA-based cells.

In addition to peak heights and positions, inflection point, area, width and depth were parameterized, too. The inflection point $V_{MAX/5}$ was approximated as the point where the profile rises above 1/5 of the LMO peak height. In our specimen cells, the inflection point near 3.8 V ($V_{MAX/5}$) shifted to higher voltage in pace with aging. In addition, while the area (Q_{LMO}) on the right of LMO peak remained constant, area on the left (Q_{NCA}) has decreased (Fig. 2).

The fact that LMO is unmoving implied that V_{LMO} can be used as a point of reference. By taking the distance between peaks and features, one may take potential biases and electrical resistance out of the equation. In our example, this was achieved by measuring V_{rel} ($V_{LMO} - V_{MAX/5}$) instead of V_{LMO} and $V_{MAX/5}$. Another possible use of V_{LMO} is to determine if the cell is not fatally damaged. If V_{LMO} is found outside certain "normal" range (in this case, 4.11 V ~ 4.16 V), one may detect an abnormality for the cell and may halt its use for safety reasons.

Another notable finding was that changes in dQdV parameters often preceded capacity loss.

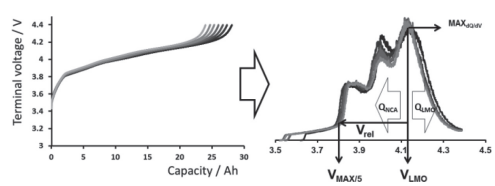


Figure 2. Conversion of charge profiles (left) into dQdV profiles obtained by plotting $(Q_n - Q_{n-1})/V_n - V_{n-1}$ against V. The peak heights, peak area and such are extracted as dQdV parameters (right).

A common practice is monitoring of battery capacity alone, but this may overlook the preliminary signs appearing in dQdV profiles regarding future capacity loss.

Many more parameters can be extracted from a dQdV profile, but choosing parameters showing good correlation to battery performance is crucially important. In our example, V_{rel} and Q_{NCA} were found to have strong correlation to capacity and internal resistance respectively (Fig. 3C and D). Polynomial fitting can be performed to parameters other than what is shown on Figure 3, but the criteria and methods for choosing the correct dQdV parameters is an ongoing work.

To establish a quantitative relation between dQdV parameters and battery performance, polynomials were fitted to the correlations. These polynomials have dQdV parameters as the input, and battery performance as the output. Once the polynomials are in place, it sometimes becomes possible to find the parameters from mere segments of a dQdV profile. For example, charging from SoC = 0% 15% would probably be enough to deduce V_{rel}, from which the cell capacity can be estimated.

It is a typical occurrence that two cells with the same charging capacity age at different rates in the future. Such difference is caused by difference in the battery's internal state, but they are not detectable by conventional method that measures capacity alone. For example, if two cells have 96% retention of the original capacity, but one cell's V_{rel} is found 10% lower than the other, we can conclude that the cell is about to start losing its capacity very soon. This has been otherwise indistinguishable.

3.2 *Formulation of battery aging in terms of dQdV parameters*

The second stage focuses on establishing an equation that has aging conditions and time as the input, and dQdV parameters as the output. Battery aging is a complex phenomenon involving electrolyte decomposition, formation of solid electrolyte interface, degradation of cathode materials and many other causes. Nevertheless, the complex phenomenon roughly divided into two large categories: aging due to time and aging due to current load. We hypothesized changes in dQdV parameters also consist of time contribution and load contribution. (Fig. 4) The aging conditions investigated in this study included temperature, State of Charge (SoC) and current rate, as their link to battery aging has been discussed many times in literature.

We have assumed a model shown on Figure 4A to describe the changes in dQdV parameters. The equation calculates the change for certain duration of time, and by recursively solving the equation and summing all results, the total change over a prolonged period of time can be found. The change due to time was labelled "CAL" and the change due to load was labelled "CYC". In this scheme, battery aging occurring under long-term storage condition would consist of only CAL element, and a under load would have both CAL and CYC element.

In our model, the CAL element consists of two functions, $F_{cal}(SoC_i)$ and $\exp(\alpha/T_i)$. The former depends on the SoC, and the latter depends on the temperature. The CYC element consists of three parts: The SoC-dependent $F_{cyc}(SoC_i)$, the temperature dependent $\exp(\beta/T_i)$, and the current-

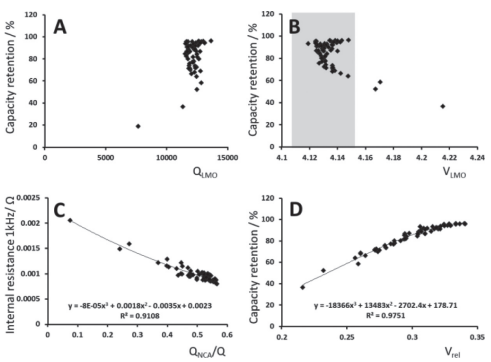


Figure 3. Correlation of dQdV parameters to battery performance—(A) The correlation between Q_{LMO} and capacity, (B) V_{LMO} (LMO peak position) as a diagnostic tool, with the green band showing the "healthy" or "safe" zone. (C) The correlation between Q_{NCA}/Q vs. internal resistance and (D) the correlation between V_{rel} and capacity.

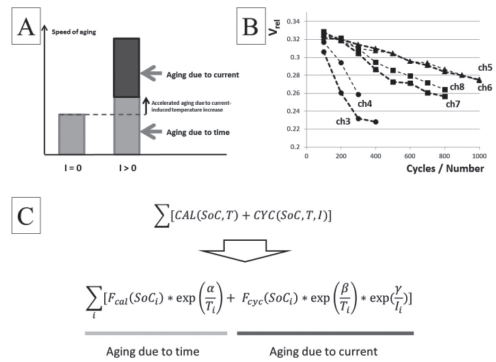


Figure 4. (A) The aging behavior of cells in ch 3–8, (B) the aging phenomenon divided into CAL and CYC, each corresponding to "Aging due to time" and "aging due to current". Each has different input variables. (C) The overall equation that estimates the progress of aging over a certain interval. In our case, the interval was set as 1 min.

dependent exp(γ/I_i). We have applied this model to explain two selected dQdV parameters—Q_{NCA} and V_{rel}, and found all coefficients by comparing the slopes between channels shown on Figure 4B.

The coefficients of CAL were found by first comparing ch-1 and ch-2, which had CYC = 0, for having zero applied current. First, coefficient α was found by dividing CAL of ch-1 by CAL of ch-2. Subsequently, the value of $F_{cal}(SoC_i)$ was found. The CAL contributions were calculated for ch3~8 and subtracted to single out CYC contributions for these channels. The CAL element found from this experiment appeared rather large, or in other words, aging due to time is grossly overestimated. This is an ongoing work.

First, the calculated CAL elements were subtracted from the graphs of ch3~ch8 of Figure 4(B) to highlight the CYC element and generate calibrated graphs for ch3~ch8. Then, γ was found first by dividing the calibrated slope of ch-7 by ch-5. Likewise, β was found from ch-7 and ch-8. Finally, $F_{cyc}(SoC_i)$ was found by dividing ch-3 with ch-7. Here, γ < 0, and Ii = "very small" when there was no current, so that CYC tended to zero when there was no current. Conversely, rapid aging was expected if I was large. The worked coefficients are shown on Figure 5. The equations deduced here are used in the third stage to predict Q_{NCA} and V_{rel}, and further, the battery performance.

Due to limited number of experiments, $F_{cal}(SoC_i)$ and $F_{cyc}(SoC_i)$ were assumed as stepped functions, but in reality, they are probably curved functions. More accurate functions can be found by performing aging experiments with a higher resolution of SoC, i.e., conducting long-term storage experiment at SoC = 10, SoC = 20, SoC = 30 and so on.

3.3 *Estimation of expected battery life*

The third stage is the operational phase. In this stage, cells of unknown state, whether new or old, are evaluated. The equations deduced in the first and second stages are used and future battery performance is predicted for evaluation. However, assumption of future battery usage and settings of the threshold of decision is at operator's discretion.

Figure 6 (left) represents one possible implementation format. In this implementation, the axes of this XY plane are capacity and internal resistance. The error margin is represented in terms of data point dispersion, and we can see that the result becomes less certain toward "2nd year." When a cell's capacity drops or internal resistance increases to a certain level, one may declare that the cell must be renewed. A typical threshold is 70% for electric vehicle batteries. In this example, we have assumed a typical commuter use of an EV—one round of charging and discharging every day.

Figure 6 (right) is the second form of implementation. This time, the axes are capacity and power. The "Power" here is defined as the cell capacity measured at high current rate. In this example, a cell enters the "red zone" (end of life or unsafe for use) if either the capacity drops below 10 Ah, or fast discharge capacity drops to below 10 Ah. Either case, one may decide to renew the cell.

The procedure for the third stage starts with acquiring the dQdV profile for the target cell. Then, the dQdV parameters are extracted and compared against the database. In our example, if V_{LMO} lay outside 4.11~4.15 V range, we can conclude that either the cell is unusable, or the measurement is incorrectly set up (Fig. 3). If the latter is unlikely, we can reject the cell as "not safe for use" or "end of battery life reached".

By setting the future battery usage conditions such as temperature of operation and charge-discharge patterns, the equations obtained in the second stage can be used to approximate how current dQdV parameters change into the future. Once the future parameters are estimated, the polynomials from the first stage (Fig. 3) are used to deduce the future cell performance.

In the first form of implementation, we made an assumption that probability distribution of battery performance expands according to a "Brownian motion". This expansion can be refined by increasing the number of experiments

$$\sum_i [F_{cal}(SoC_i) * \exp\left(\frac{\alpha}{T_i}\right) + F_{cyc}(SoC_i) * \exp\left(\frac{\beta}{T_i}\right) * \exp(\frac{\gamma}{I_i})]$$

Q_{NCA}		V_{rel}	
α	-4675.43	α	-5582.55
β	2009.426034	β	808.2075908
γ	-3.199074273	γ	-3.449673721
F_{cal}(SoC=90)	3.433095	F_{cal}(SoC=90)	17.00965
F_{cyc}(SoC=70)	2.32044E-07	F_{cyc}(SoC=70)	1.6305E-06
F_{cyc}(SoC=30)	9.4E-07	F_{cyc}(SoC=30)	4.5E-06

Figure 5. The deduced coefficients for each dQdV parameters.

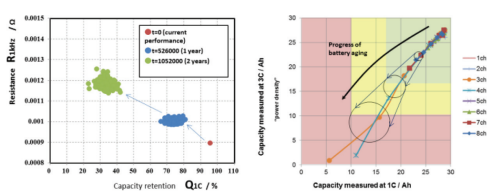


Figure 6. Examples of implementation—(left) visualization of aging in terms of probability distribution on capacity-resistance plane (right) and a representation of the aging curve on a Ragone chart.

in the first stage to some statistically reliable number. Having more experimental samples in the first stage may also solve the problem of overestimated CAL element, which predicts excessively rapid aging in Figure 6 (Left).

In the second form of implementation, predicted battery performance is more expressly shown. The method was verified by comparing predicted battery performance before load, and the actual measured value obtained after the load. The battery used in this experiment was a "used cell", which underwent charging and discharging under the SoC range of 50–90 at 1 C (30 Ah) current rate for 500 times under 35 degrees environment. At this point, the cell's capacity was 25.959 Ah, and the predicted cell capacity by the 1000th cycle was 21.65 Ah. The cell was then cycled for additional 500 cycles. The cell capacity decreased to 21.002 Ah, which was a 3.1% less than the predicted value. At this point, the scheme of cell capacity prediction using dQdV profiles remains at the level of demonstration, and a statistical assessment of reliability is an ongoing work.

4 CONCLUSION

We have developed a universally applicable method of battery life prediction, which takes advantage of the high sensitivity of dQdV profiles to battery aging. The method quantifies dQdV profile shapes as parameters, and changes to the parameters are used to predict the future battery performance. The method predicts battery aging more accurately since dQdV profile analysis yields more information than simple tracking of capacity over time, which is a current common method. The predicted result can be used to draw a Ragone plot, or to optimize the maintenance scheme.

REFERENCES

Rastler, D. 2010. Electric Energy Storage Technology Options: A White Paper Primer on Applications, Costs, and Benefits. EPRI, Palo Alto, CA.

Wang, J.S., Liu, P, Soukiazian, S. & Verbrugge, M.W. 2010. Method and apparatus for assessing battery state of health. US Patent, US 8531158 B2.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability prediction of electronic boards by analyzing field return data

S.V. Comert, H. Yadavari, M. Altun
Istanbul Technical University, Istanbul, Turkey

E.N. Erturk
ARCELIK A.S. R&D Center, Istanbul, Turkey

ABSTRACT: In this study, we perform field return data analysis of electronic boards. We cooperate with one of the Europe's largest manufacturers and use their well-maintained data with over 1000 electronic board failures. We follow two steps that are filtering the return data and modeling the filtered data with probabilistic distribution functions. In the first step of filtering we propose a new technique to eliminate improper data, correlated to incomplete and poorly collected data, from the whole field return data. In the second step of modeling, we use the filtered data to develop our reliability model. Rather than conventionally using a single distribution for all service times that does not accurately model the substantial changes of the electronic boards reliability performance over time, we use different distributions for different service time intervals. In order to determine the distributions we propose a technique that deals with forward and backward time analysis of the data.

1 INTRODUCTION

The rapid developments in electronics, especially in the last decade, have initiated the inception of electronics reliability (O'Connor & Kleyner, 2011). Conventionally used accelerated reliability tests have lost their significance; time consuming and expensive feature of these tests is against the demands of today's very *rapid electronic product cycles* (Pecht, 2010). This underlines the importance of using the product's field return data for reliability analysis that is relatively cheap and time saving (Kleyner & Sandborn, 2004; Wu, 2012). In this study, we propose a complete reliability methodology exploiting field return data of electronic boards.

Field return data can be used for variety of purposes that include the prediction of future claims, the estimation of field reliability, and the identification of opportunities for quality and reliability improvement. (O'Connor & Kleyner, 2011). If one assumes that the return data is error free then it is not difficult to claim that it is the most trustworthy data in analyzing reliability of a product compared to accelerated test or simulation based data. However, in reality field return data contains errors corresponding to improper, correlated, incomplete, and poorly collected data that result in misleading reliability predictions. In this study, we first deal with this problem. We propose a systematic approach to eliminate errors from field return data. We call this process of elimination as "filtering".

In the filtering process, we classify errors into two categories: obvious and hidden errors. Obvious errors are the errors that can be easily determined with applying one-by-one data check. Changing data orderings make this process even faster. Examples for such errors are unknown assembly dates, invalid time-to-failure values, and quality related errors. In contrary to the obvious errors, hidden errors and their probable sources cannot be directly determined from the data. Examples for hidden errors are significant changes in product manufacturing process, data loss, and inappropriate data recording in services. Hidden errors are fatal and overwhelm obvious errors in terms the number of occurrences. This obligates us to eliminate hidden errors before starting statistical analysis. In this work, we propose a new systematic approach to determine and eliminate both obvious and hidden errors. After eliminating the errors, now we have "filtered data" that is accurate and ready to be used in our statistical modeling.

In statistical modeling, the hazard rate of an industrial product is an important parameter especially for companies which have high volume products in the field. Additionally, hazard rate functions can directly be used for warranty forecasting. In this study, we mainly construct our model on hazard rate functions. In the literature it is well accepted to assume that the hazard

rate function of a product shows a bathtub characteristic. In general hazard rate models depict an entire bathtub curve as a combine of two Weibull distributions for early failure and wear out periods (Dhillon, 1999; Kececioglu, 2002). This is illustrated in Figure 1. Although the models using all regions of the bathtub curve are theoretically correct, they are not practically applicable to some industrial product groups with relatively long lives (Kleyner & Sandborn, 2004). Electronic boards, studied in this work, fall into these product groups. Electronic boards are expected to work at least 10–15 years with a warranty period of at most 5 years. This is illustrated in Figure 1.

In this study, we propose a model regarding early failure and useful life periods of electronic boards. Our model is based on Exponential and Weibull distributions among many other distribution options regarding the optimum curve fitting. Rather than conventionally using a single distribution for all time-to-failures that does not accurately model the substantial changes of the board's reliability performance over time, we use different distributions for different service time intervals. For this purpose we propose a new technique that deals with forward and backward time analysis of the data. In the fitting process we use "rank regression" and "maximum likelihood" methods.

The data used in this study (filtering and modeling analysis) contains assembly and return dates for each warranty call. Warranty period of the board is three years. The maintenance policy for electronic boards under this study is to replace the board with a new one in any suspected case such as stopping from time to time or breaking down entirely in the field. Therefore the analyzed data has no record of repaired boards. Throughout our analysis we benefit from Weibull++ by ReliaSoft Corporation.

The structure of this paper is as follows. In Section 2-Filtering, we describe the filtering procedure of field return data. In Section 3-Modeling, we work with the filtered data to develop our statistical model. Finally, Section 4 reports the conclusion of the work.

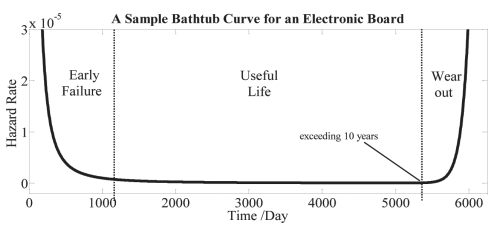


Figure 1. A bathtub curve—hazard rate function over time.

2 FILTERING

In order to guarantee accuracy of the analysis and eliminate errors, field return data must be filtered. For this purpose, we use a step by step procedure. In the first step, we filter obvious errors from the whole data. We filter data having unknown assembly date, data with quality failure records that result in zero time to failure (TTF), and data with negative TTF or unreasonable TTF.

In the second step which is the main target of this section we are dedicated to find and eliminate hidden errors. As it is mentioned before, obvious errors can be easily found by applying one-by-one data check. But, we cannot find hidden errors as direct as we find obvious errors. Here, a systematic approach is needed. By using Weibull++ ReliaSoft Corporation software we survey the consistency of the data and systematically investigate if there are hidden errors or not. We use 2 parameter Weibull distribution for our analysis because of being mathematically more tractable than other distributions (Reliasoft, 2014; Babington et al., 2007). Also using Weibull distribution to model reliability has long been approved in the literature. Maximum likelihood method (MLE) is selected for parameter estimation since regression methods generally work best for large data sets (O'Connor & Kleyner, 2011). In analysis, we deal with six month assembly time intervals. Selecting 6 month intervals is quite reasonable because we have 54 month return data.

The proposed methodology targeting hidden errors is as follows. We first perform forward analysis for 1–6, 1–12, 1–18, 1–24, 1–30, 1–36, 1–42, 1–48 and 1–54 month time intervals. This is illustrated in Figure 2. For example, 1–6 time interval represents products assembled in the first six months. Similarly, 1–42 time interval represents the whole data excluding the ones assembled in the last six months. In forward analysis we expand time window from left to right where the left edge is fixed. We then perform backward analysis for time intervals of 48–54, 42–54, 36–54,…,12–54, and 1–54. This is illustrated in Figure 3. Here, we expand time window from right to left where the right edge is fixed. Finally we perform analysis for seperate 6 month time intervals of 1–6, 7–12, 13–18, 19–24, 25–30, 31–36, 37–42, 43–48, 49–54. This is illustrated in Figure 4. Note that X-axes in figures represent assembly times (not TTF). As a result, using parameters of Weibull distributions of these three analysis, we filter improper time intervals corresponding to hidden errors.

We develop our filtering systematic mainly on a Weibull parameter β that explains the hazard rate function's behavior. If $\beta < 1$, it indicates a decreasing hazard rate and is usually associated with the early failure region. If $\beta \approx 1$, it means a constant

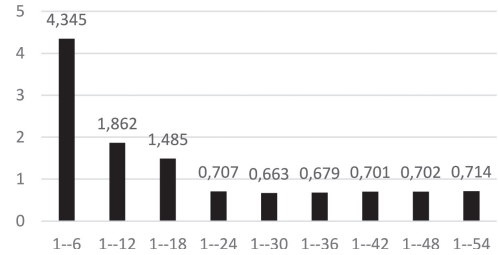


Figure 2. Beta (β) values for forward analysis.

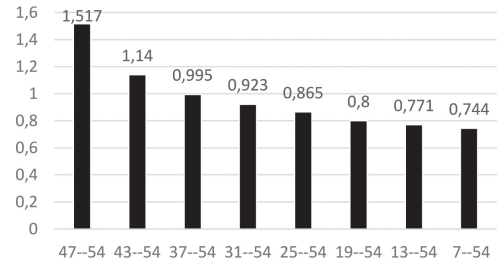


Figure 3. Beta (β) values for backward analysis.

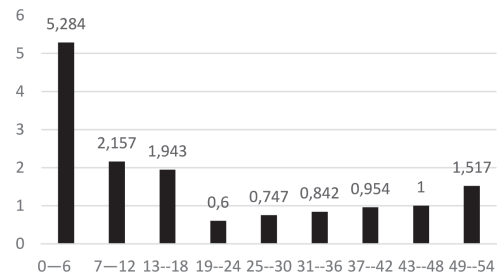


Figure 4. Beta (β) values for analysis of 6-month periods starting from the beginning.

hazard rate and is usually associated with the useful life region. If $\beta > 1$, it indicates an increasing hazard rate and is usually associated with the wear out region, corresponding to the end life of the product. As a reminder, the early failure, useful life, and wear out regions are illustrated n Figure 1. As follows we investigate Figure 2, Figure 3, and Figure 4 in details regarding β values.

Figure 2 shows β parameters of Weibull distributions for the forward analysis. Looking at β values we can derive that there are problems in the first 3 intervals 1–6, 1–12, and 1–18. These β values are greater than one, meaning that we are in the wear out region. This is impossible; the first 18 months of the field return data are suspected. Figure 3 shows β parameters of Weibull distributions for the backward analysis. Again, by looking at the β values we see that the last 6 months have $\beta > 1$. Here, we cannot come to a conclusion since we have insufficient data (sample size of 10) for the products assembled in the last six months. This low amount of sample size is not enough to perform accurate statistical analysis. Finally, Figure 4 shows β parameters of Weibull distributions for 6 month periods. If we look at β values we can derive that the first 3 intervals 1–6, 7–12, and 13–18 having $\beta > 1$ are suspected.

In conclusion, we should filter the first 18 months of the field return data corresponding to hidden errors. In other words, the products assembled in the first 18 months have insufficient field return data with hidden errors. Note that if we just performed backward analysis, we would not find any hidden errors. This could also happen for only performing forward or 6-month analysis for a different case. However, with performing backward, forward, and 6-month analysis together, as suggested in this study, we consider all aspects of hidden errors. We have now 36 month field data to be safely used in statistical reliability modeling.

3 MODELING

As we discussed in introduction, the field return data can not be used for analysis of the wear out region since electronic boards get into this region long after their warranties expire. Therefore, we only deal with early failure and useful time periods. We develop our hazard rate function with phases having "Decreasing Failure/Hazard Rate (DFR)" and "Constant Failure Rate (CFR)" like those proposed by Yuan et al. (2010) and Chen et al. (1999). Here, DFR and CFR correspond to early failure and useful life regions, respectively. The proposed overall hazard rate function $h_0(t)$ is presented in Equation 1 where $h_1(t)$ = hazard rate function in early failure period, $h_2(t)$ = hazard rate function in useful-life period, t = time (TTF), and τ = change point from DFR to CFR.

$$h_0(t) = \begin{cases} h_1, & t < \tau \\ h_2, & t \geq \tau \end{cases} \quad (1)$$

Using a piecewise hazard rate function for reliability modeling, as we suggest, is a well-studied subject in the reliability and statistics literature. This includes the determination of τ often called as change point problem. In some sources τ is even called as burn-in time. Studies on parametric change point analysis of nonmonotonic hazard rate functions consider the change point as a parameter and propose statistical estimation methods like MLE and least squares (Yuan & Kuo, 2010;

Blischke 2011). Also nonparametric methods were studied widely. Bayesian estimation method with prior distribution belief about change point was discussed using test data in Yuan & Kuo, (2010). A confidence interval for parametric estimation of change point in two phase hazard model was given by Chen et al. (2001). In this study, we propose a novel change point detection method with determination of the separate hazard rate functions $h_1(t)$ and $h_2(t)$ via parametric analysis and processing the data with graphical inferences.

The data that we use, have TTF values between 1 and 36 months, since the product has 3 year warranty period. In our model, we do analysis for forward and backward time windows. While forward analysis is a widely used method in warranty analysis, investigating TTF values from backward is a new method that we introduce for accurate determination of the change point τ and the hazard functions $h_1(t)$ and $h_2(t)$. In our method, M_f and M_b are used as the number of months that constitute the boundaries of time windows. In Figure 5, an explicit demonstration of the time windows are shown.

The forward analysis is conducted by using the filtered data with TTF values less than or equal to M_f. For example, if $M_f = 3$, the data to be analyzed will contain TTF values of 1, 2 or 3 months. After starting with $M_f = 1$, M_f is increased by adding months one-by-one (M_f = 2, 3, 4,…,36). In other words, the forward time window is gradually expanding to the end of the TTF line as seen in the upper part of Figure 5. In forward time window analysis, we see that 2 parameter Weibull distribution is a good fit for almost all different M_f values. Although in some cases the best fitting is achieved with Lognormal or Gamma distribution, these distributions show almost the same DFR pattern as that from Weibull distribution in our analysis. Therefore we determine Weibull distribution for $h_1(t)$. Note that in forward analysis we do not see a change point for M_f from which the DFR pattern changes significantly.

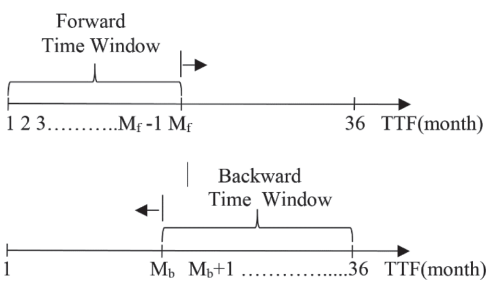


Figure 5. Demonstration of forward and backward time windows.

The backward analysis is conducted by using the filtered data with TTF values between M_b and 36 months (1–36, 2–36 …30–36…). In other words, one end of the backward time window is fixed at 36-month and the other is gradually expanding to the beginning of the TTF line as seen in the lower part of Figure 5. In the backward time window analysis, we always achieve the best fitting with Lognormal or Gamma distribution for $M_b < 14$ (months) and Exponential distribution for $M_b \geq 14$ (months). Therefore there is a change point approximately in the 14th month and we determine Exponential distribution for $h_2(t)$. The change point $\tau = 14$ (months) also results in $M_f = 14$ for $h_1(t)$ and $M_b = 14$ for $h_2(t)$ that are shown in Figure 6 and Figure 7, respectively.

Note that in this study we determine the change point from the backward analysis, but this is not a necessary and sufficient condition. For different field data, corresponding to different products, we could have had multiple change points or a single change point derived from the forward analysis. These cases are beyond the scope of this paper and considered as future work.

After determination of the change point, two phase hazard rate function, consisting of Weibull and Exponential distributions, can be constructed directly. In this case, there is a discontinuity problem at the change point; overall hazard rate function is not continuous. In order to solve this problem, we

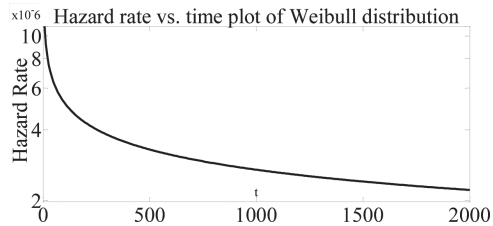


Figure 6. Hazard rate function h_1 (t) of forward analysis with Weibull distribution for Mf = 14 months. Beta: 0,715 Eta (Day): 2.44E + 6.

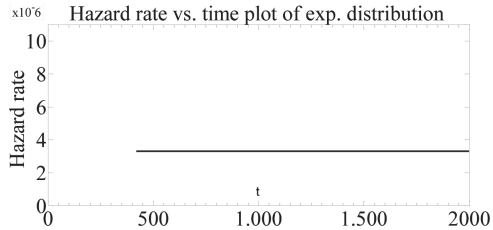


Figure 7. Hazard rate function h_2 (t) of backward analysis with Exponential distribution for Mb = 14 months. Mean time (Day): 303179.252, Gamma (Day): 382.086.

propose a smoothing and fitting method similar to the method suggested by Selmic & Levis (2002) for neural networks.

We achieve smoothing with a sigmoid function as a smooth step function approximation. Sigmoid function is given as follows.

$$s(t,\tau)=\frac{1}{1+e^{-b(t-\tau)}} \tag{2}$$

In Equation 2, τ is the change point in a unit of day. In our case its value is 14×30 days. Sharpness parameter b of the sigmoid function, can be calculated empirically. As a result, overall hazard rate function is given as:

$$h_0=\big(1-s(t,420)\big)\times h_1+s(t,420)\times h_2 \tag{3}$$

$$h_0=\left(1-\frac{1}{1+e^{-b(t-420)}}\right)\frac{\beta t^{\beta-1}}{\eta^{\beta}}+\frac{1}{1+e^{-b(t-420)}}\lambda \tag{4}$$

where β and η are the shape and scale parameters of the Weibull distribution $h_1(t)$, respectively. Additionally, λ is the hazard rate of the Exponential distribution $h_2(t)$. A plot of $h_0(t)$, $h_1(t)$ and $h_2(t)$ are shown in Figure 8 that clearly shows the idea under our smoothing operation.

A small distortion and error around the change point is an expected situation with this kind of smoothing. In our smoothing process, there is a slight difference between the overall hazard function $h_0(t)$ and $h_1(t)$ just before the change point at the 14th month (420th day). This can be seen in Figure 8. Fortunately, hazard rate values of $h_1(t)$ and $h_2(t)$ near the change point are very close to each other's because of neutrality of the data that results in very low error values.

It should be noted that there may be seen different distributions in the forward and backward analysis. The distributions do not have to be only Weibull and Exponential. We already know that distributions like Gamma, Lognormal, etc. can give all phases of bathtub curves with DFR, CFR and IFR tendencies according to values of the distribution parameters. Therefore, the proposed method of having continuous hazard rate functions can be directly applicable to different distributions.

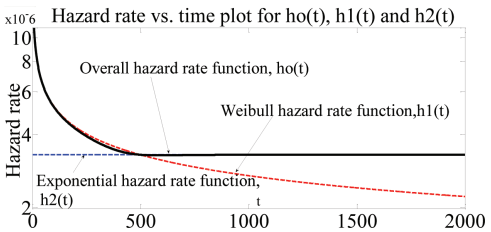


Figure 8. Proposed modeling approach. Plot of h_o (t), h_1 (t) and h_2 (t).

4 CONCLUSION

In this study, we propose a methodology to process field return data and model the hazard rate function of electronic boards. We cooperate with one of the Europe's largest manufacturers and use their well-maintained data with over 1000 electronic board failures. The main goal of our study is developing a precise reliability model for electronic boards including warranty forecasting. To reach our goal, we follow two steps that are filtering and modeling.

In the filtering step, we propose a new systematic approach to determine and eliminate both obvious and hidden errors. Our method separately investigates the data in six-month time intervals, and shows us the problematic time spans corresponding to incomplete data that need to be excluded. In the modeling step, we use the filtered data to develop our reliability model. Our model is achieved by performing forward and backward time analysis of the data, and eventually finding the best fitting distributions for different time-to-failure intervals. In the fitting process we use "rank regression" and "maximum likelihood" methods. Throughout our analysis we benefit from Weibull++ by ReliaSoft Corporation.

The proposed methodology, targeting a specific electronic board, can also be applied to the return data of other electronic boards. We apply it and the results, not to be disclosed here, show us clear evidence of our methodology's success.

ACKNOWLEDGEMENTS

We would like to thank Dr. Aydogan Ozdemir from Electrical and Electronics Faculty of Istanbul Technical University for his comments and suggestions regarding this work. We are also grateful to Tunay Çakar and Hasan Avcı for their helps.

This work is cooperated with Arcelik A.Ş. and supported by TUBITAK (The Scientific and Technological Council of Turkey) University-Industry Collaboration Grant Program (1505).

REFERENCES

Bebbington, M., Chin-Diew, L., Zitiks, R. 2007. Estimating the turning point of a bathtub-shaped failure distribution. Journal of Statistical Planning and Inference.138: 1157–1166.

Blischke, W.R., Karim, M.R., Murthy, D.N.P. 2011. Warranty data collection and analysis. London: Springer.

Chen, S., Sun, F., Yang, J. 1999. A new method of hard disk drive MTTF projection using data from early life test. Reliability and Maintainability Symposium, Washington DC, 18–21 January 1999.

Chen, Z., Ferger, D., Mi, J. 2001. Estimation of the change point of distribution based on the number of failed test items. Metrika. 53: 31–38.

Dhillon, B.S. 1999. Design Reliability: Fundamentals and Applications. New York: CRC Press.

Kececioglu, D. 2002. Reliability Engineering Handbook. Pennsylvania: Destech Publications.

Kleyner, A. & Sandborn, P. 2004. A warranty forecasting model based on piecewise statistical distribution and stochastic simulation. Reliability Engineering and System Safety. 88(3): 207–214.

O'Connor, P. & Kleyner, A. (5th) 2012. Practical Reliability Engineering. West Sussex: John Wiley & Sons.

Pecht, Michael, ed. Product reliability, maintainability, and supportability handbook. CRC Press, 2010.

Reliasoft Corporation website. 2014: http://www.reliasoft.com.

Selmic, R.R. & Levis, F.L. 2002. Neural-network approximation of piecewise continuous functions: application to function compensation. IEEE Transactions on Neural Networks. 13(3): 745–751.

Wu, Shaomin. "Warranty data analysis: a review." Quality and Reliability Engineering International 28.8 (2012): 795–805.

Yuan, T.R. & Kuo, Y. 2010. Bayesian analysis of hazard rate, change point and cost optimal burn-in time for electronic devices. IEEE Transactions on Reliability. 59(1): 132–138.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A double-loop Monte Carlo approach for Part Life Data Base reconstruction and scheduled maintenance improvement

F. Di Maio
Energy Department, Politecnico di Milano, Milan, Italy

M. Compare
Aramis Srl, Milan, Italy

S. Mattafirri
General Electric—Nuovo Pignone, Florence, Italy

E. Zio
Energy Department, Politecnico di Milano, Milan, Italy
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy, Electricité de France, Ecole Centrale Paris and Supelec, France
Aramis Srl, Milan, Italy

ABSTRACT: This paper describes a Monte Carlo (MC) based approach for reconstructing missing information in a Part Life DataBase (PLDB) used by General Electric (GE) for reliability analysis in support to the optimization of scheduled maintenance strategies. The PLDB contains quantitative and qualitative data coming from field observations at inspection of GE turbines. The approach is based on the Maximum Likelihood Estimation (MLE) technique to identify the parameters of the GE turbine binary degradation model, on the Fisher Information Matrix to estimate the confidence intervals on the estimated parameters, on a double-loop MC approach to propagate these confidence intervals onto the probabilities of occupying one of the degradation states over time, and, thus, estimate the missing equivalent starts (i.e., the up-time) to be associated to the recorded inspection observations (i.e., the degradation state) within the incomplete PLDB. Results of the application of the novel approach to a real industrial PLDB are discussed.

1 INTRODUCTION

General Electric (GE) offers to its customers a maintenance service on a set of components, such as the nozzles of the turbines, which is based on the subsequent steps:

I. The customer sends GE the component removed from the system upon a maintenance inspection. GE experts check the component and qualitatively classify its health state into 'Good', 'Light', 'Medium' and 'Heavy' (see Fig. 1).
II. The component ID, the information about its working time and the result of the inspection are stored in a Part Life Data Base (PLDB) for reliability life data analysis. This can be used to infer the component future failure behavior and identify the corresponding optimal maintenance decision that minimizes a cost objective function. Moreover, PLDB can be used to produce the cost estimate of maintenance service contracts to be signed with customers.
III. Components that can be fixed (with different repair procedures according to the entity of the damage) are sent back to the costumer in an As Good As New (AGAN) state.

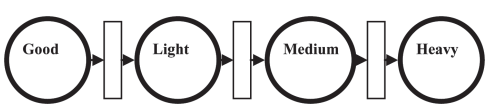


Figure 1. Scheme of the degradation mechanism.

With regards to step II, currently GE carries out the reliability life data analysis by modeling the component behavior as binary, i.e., there are only two possible component states: 'working' and 'failed'. This is done by treating 'Good' as 'working' state and combining 'Light'', 'Medium', 'Heavy' into a single 'failed' state (Fig. 2). In this work, we also adopt this latter simplified binary

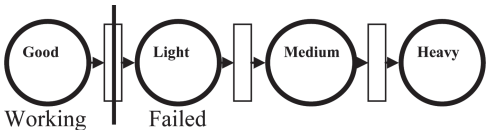


Figure 2. Simplified scheme of the binary degradation mechanism.

degradation model to describe the evolution of the erosion mechanism affecting the nozzle system of the turbines. The statistical evidence gathered by GE is exploited to improve their reliability prediction.

2 AVAILABLE DATA

The available dataset, i.e., the PLDB, consists of a set $N = 30$ records regarding field observations of the nozzle system of turbines operated by GE. Each record contains:

1. The machine (i.e., turbine) ID;
2. The inspection time (i.e., equivalent starts);
3. The degradation state of the component. This field may have four possible ordinal entries: 'Good', 'Light', 'Medium', 'Heavy';
4. The time at which the observation started, to give due account to the left censored data;
5. The value of the main covariate of the degradation process (e.g., temperature);
6. The machine total working time; this constitutes an upper bound for the missing time instants (to be estimated) at which the inspections have been performed.

When the i-th machine with $n = 22$ nozzles is inspected, a number n_s^i and n_f^i of nozzles can be found in 'working' and 'failed' states, respectively. In the latter case, records are referred to as interval censored records, whereas in the former case, records are right censored.

Beside the $N = 30$ complete data, another dataset is available containing the data of $M = 32$ additional machine inspections with unknown equivalent starts, i.e., the degradation state of every nozzle in the turbine is known, but the inspection time at which this situation has been encountered is missing.

In this context, the goal is to:

– Develop a method based on the Maximum Likelihood Estimation (MLE) technique to estimate the parameters of the binary degradation model, based on quantitative and qualitative data coming from field observations at inspection;

  Implement a technique based on the Fisher Information Matrix to estimate the confidence intervals on the estimated parameters;

Table 1. Example of data in PLDB.

	# Components safe	# Components failed
27.2 [units of time]	18	4
Missing	13	9
…	…	…

– Develop and implement a technique for propagating the estimated uncertainties (confidence intervals) onto the probabilities of occupying the degradation states over time;
– Develop a technique to estimate the missing equivalent starts to be associated to the recorded inspection outcomes.

Notice that the data considered in this paper and the corresponding results shown are different from the real ones from GE field experience, in respect of GE policy on confidential information.

3 ESTIMATION OF THE MODEL PARAMETERS

The aim of the first task of the work is to exploit the evidence contained in the available dataset with $N = 30$ complete data to estimate the values of the parameters of the stochastic model describing the degradation mechanism under study. The assumption is that the transition from 'working' to 'failed' state obeys a two-parameter $\underline{\theta} = \{\beta, \eta\}$ Weibull distribution, where β is the shape factor and η the scale factor. This latter represents the number of equivalent starts before which 63% of turbine nozzles fail.

Resorting to the Maximum Likelihood Estimation (MLE) technique (Kendall & Stuart 1979), the LogLikelihood function L can be written as:

$$L(\beta,\eta) \propto \log\left(\prod_{i=1}^{N} F\left(t_i|\beta,\eta\right)^{n_f^i} R\left(t_i|\beta,\eta\right)^{n_s^i}\right) \qquad (1)$$

where $R\left(t|\beta,\eta\right) = e^{-(t/\eta)^{\beta}}$ is the reliability of the n_s^i nozzles of the i-th machine which is found in 'working' state upon inspection, whereas $F\left(t|\beta,\eta\right) = 1 - e^{-(t/\eta)^{\beta}}$ is the unreliability of the n_f^i nozzles that are found in 'fault' state. In this respect, notice that the available dataset contains right-censored data in case of survived components, and interval censored data (where the intervals in which the failures occurred start at time $t = 0$) in case of failed components (Zio 2007).

Figure 3 shows the shape of the Log-Likelihood function L relevant to the $N = 30$ data contained in the PLDB dataset, whereas

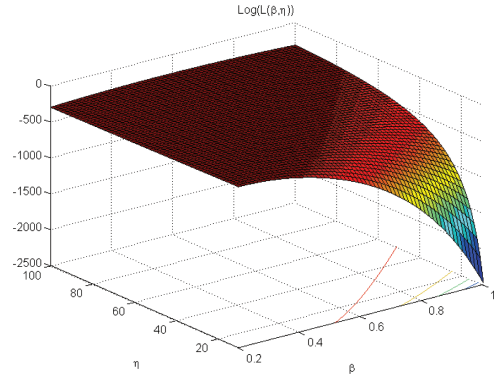


Figure 3. Log-likelihood function L.

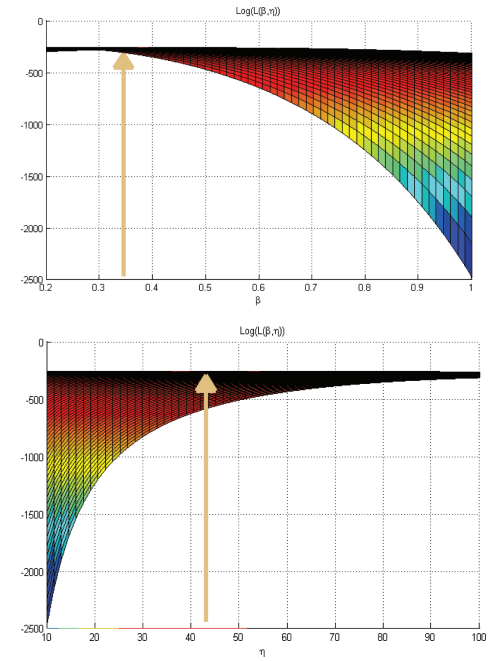


Figure 4. Log-likelihood function L, projected on the β and η axes.

Figure 4 shows that its maximum value is located in $\underline{\hat{\theta}} = \{\hat{\beta}, \hat{\eta}, \} = \{0.36, 45.23\}$.

Figure 5 shows, in log-log scale, the Cumulative distribution Function (cdf) of the Weibull distribution corresponding to the MLE values of its parameters $\underline{\hat{\theta}}$.

3.1 *Uncertainty of the model parameters*

An estimation of the confidence intervals on the parameters of a stochastic 2-parameter model can

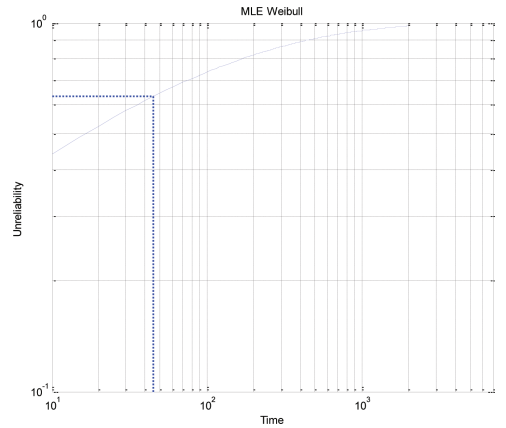


Figure 5. Point estimate of the unreliability plot.

be obtained by exploiting the asymptotic properties of the ML estimator $\underline{\hat{\theta}} = \{\hat{\beta}, \hat{\eta}, \}$. In fact, if $\underline{\hat{\theta}}$ is a unique solution to the maximization problem of $L(\beta, \eta)$, then (Papoulis & Pillai 2002, Kendall & Stuart 1979):

$$\text{i. } E(\hat{\theta}) \to \theta \tag{2}$$

$$\text{ii. } (\hat{\sigma}_\beta, \hat{\sigma}_\eta) \to (\sigma_\beta, \sigma_\eta)_{CR} \tag{3}$$

where $(\sigma_\beta, \sigma_\eta)_{CR}$ are the Cramer-Rao lower bounds (Papoulis & Pillai 2002) of the standard deviations of any unbiased estimator of $\underline{\theta} = \{\beta, \eta\}$. That is, any choice of an unbiased estimator of $\underline{\theta}$ brings a variability in the ML estimate which is necessarily larger than $(\sigma_\beta, \sigma_\eta)_{CR}$.

$$\hat{\theta} \text{ is asymptotically normal.} \tag{4}$$

With respect to ii), the approximated values of the variances $\underline{\hat{\sigma}} = (\hat{\sigma}_\beta, \hat{\sigma}_\eta)$ of the parameters $\underline{\hat{\theta}} = \{\hat{\beta}, \hat{\eta}, \}$ are provided by the main diagonal of their covariance matrix (Kendall & Stuart 1979). This can be computed as the inverse $J(\underline{\theta})^{-1}$ of the expected Fisher information matrix $J(\underline{\theta})$ whose generic (i, j) entry, $i, j = 1,2$ is (Kendall & Stuart 1979):

$$J_{ij} = E\left(\frac{\partial \log L(\underline{\theta})}{\partial \theta_i} \cdot \frac{\partial \log L(\underline{\theta})}{\partial \theta_j} \right) \tag{5}$$

where $L(\underline{\theta}) = L(\beta, \eta)$ is the likelihood function, and $\theta_1 = \eta$, $\theta_2 = \beta$.

In the reference case study, the estimated standard deviations $\underline{\hat{\sigma}} = (\hat{\sigma}_\beta, \hat{\sigma}_\eta)$ of $\underline{\hat{\theta}} = \{\hat{\beta}, \hat{\eta}, \}$ are given

by the entries (1,1) and (2,2) of the matrix $J(\underline{\theta})^{-1}$, respectively:

$$\begin{bmatrix} E\left(\left[\frac{\partial \log L(\beta,\eta)}{\partial \beta}\right]^2\right) & E\left(\frac{\partial \log L(\beta,\eta)}{\partial \beta}\cdot\frac{\partial \log L(\beta,\eta)}{\partial \eta}\right) \\ E\left(\frac{\partial \log L(\beta,\eta)}{\partial \eta}\cdot\frac{\partial \log L(\beta,\eta)}{\partial \beta}\right) & E\left(\left[\frac{\partial \log L(\beta,\eta)}{\partial \eta}\right]^2\right) \end{bmatrix}^{-1} \tag{6}$$

It is worth noticing that under mild regularity conditions, the matrix in Eq. (6) is equal to:

$$\begin{bmatrix} -E\left(\frac{\partial^2 \log L(\beta,\eta)}{\partial \beta^2}\right) & -E\left(\frac{\partial^2 \log L(\beta,\eta)}{\partial \beta \partial \eta}\right) \\ -E\left(\frac{\partial^2 \log L(\beta,\eta)}{\partial \beta \partial \eta}\right) & -E\left(\frac{\partial^2 \log L(\beta,\eta)}{\partial \eta^2}\right) \end{bmatrix}^{-1} \tag{7}$$

This allows us giving a rough, informal interpretation of Fisher information. In fact, notice that in general:

$$\frac{\partial^2 \log L(\underline{\theta})}{\partial \theta_i^2} = \frac{L'(\underline{\theta})}{L(\underline{\theta})} \tag{8}$$

Then, this second derivative can be interpreted as a measure of how quickly the probability distribution function (pdf) changes when we change the parameter in the proximity of the MLE estimation. The expectation of the square of this value gives us a more robust version of this measure: if Fisher information is large, then the distribution quickly changes when we move from the MLE value of the parameter (i.e., the distribution with parameter $\underline{\hat{\theta}}$ is different from the distributions with parameters close to $\underline{\hat{\theta}}$); on the other hand, if Fisher information is small, this means that the distribution corresponding to $\underline{\theta} = \underline{\hat{\theta}}$ is 'very similar' to distributions with values of the parameter not so close to $\underline{\hat{\theta}}$. In the former case, we should be able to robustly estimate $\underline{\hat{\theta}}$ based on the data, whereas in the latter case the robustness of the estimation is worse.

3.2 *Confidence intervals on the probability plot*

In this case study, the values of $\underline{\hat{\sigma}} = (\hat{\sigma}_\beta, \hat{\sigma}_\eta)$ are $\underline{\hat{\sigma}} = (0.17, 28.1)$. Figure 6 shows the distribution of $\hat{\beta}$ and $\hat{\eta}$ (top and bottom, respectively). Derivatives of $L(\beta,\eta)$ are computed resorting to the MATLAB symbolic toolbox.

Figure 7 shows the cdf of the unreliability and its pointwise double-sided 90% confidence interval. The width W_η of the double-sided 90% confidence intervals for η is equal to $W_\eta = 70 - 17 = 53$,

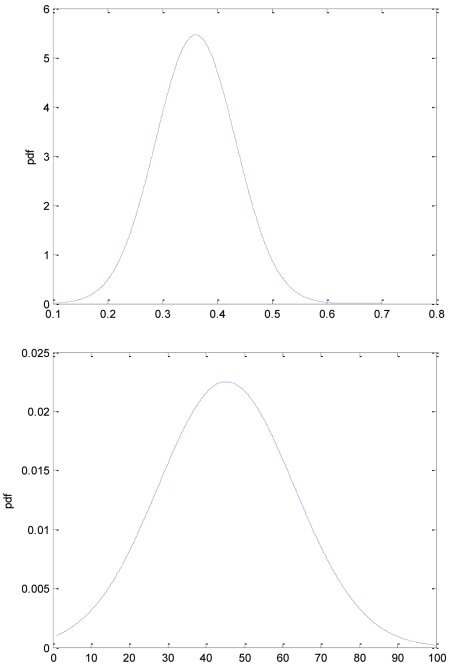


Figure 6. Distributions of $\hat{\beta}$ (top) and $\hat{\eta}$ (bottom).

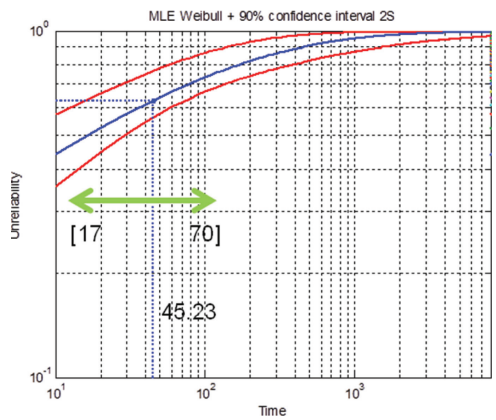


Figure 7. Unreliability and confidence intervals.

whereas the width W_U of the double-sided 90% confidence intervals for the unreliability at $t = \hat{\eta}$ is equal to $W_U = 0.78 - 0.56 = 0.22$.

In particular, the upper and lower bounds are found resorting to a MC sampling method implemented by the following procedure (Zio, 2013):

i. Partition the time axis into C small channels of length Δt.
ii. Sample β from $N(\hat{\beta}, \hat{\sigma}_\beta)$;
iii. Sample η from $N(\hat{\eta}, \hat{\sigma}_\eta)$;

iv. For each channel i of the time axis, compute $R(t_i|\beta,\eta)$, where $t_i = i \cdot \Delta t$, $i = 1, \ldots, C$.
v. Repeat steps ii–iv a large number of times (e.g., 500 in this work).
vi. For each time channel i, find the 5th and 95th percentiles of the gathered statistics, i.e., the pointwise double-sided 90% confidence interval.

4 ESTIMATION OF THE EQUIVALENT STARTS

The aim of this Section is to propose a procedure to infer such equivalent starts, on the basis of the statistical evidence made up of the N complete data. Two different approaches to the missing data problem are typically proposed. The first approach consists in developing models to reconstruct the missing data based on Artificial Neural Networks (AANN) (Hines, 1996), Principal Component Analysis (PCA) (Luh, 2011), Auto-Associative Kernel Regression Methods (AAKR) (Baraldi, 2012), Fuzzy Similarity methods (Baraldi, 2013) and similarity measures computed taking the correlation (Kim et al., 2005) and entropy (Brock et al., 2008) of information. The second approach consists in substituting the missing data by statistical values, e.g., the mean value of the available data (Schafer, 2002). However, the performance of especially the latter approach tends to decrease when applied to datasets containing few complete data. In our approach, we make use of a MC based approach for reconstructing missing information in the PLDB: as anticipated above, a number M of additional turbine inspection outcomes have been collected by GE, which report the degradation state at inspection of each of the $n = n_f^i + n_s^i$ components of the i-th machine, but not the time (expressed in equivalent turbine starts) at which that inspection has been performed.

From the statistical standpoint, every machine inspection can be regarded as the result of n repeated trials, each one consisting in testing the health state of the nozzle after it has been working for a time interval [0, t]. For each trial, two mutually exclusive events can occur: 'nozzle is in failed state', and 'nozzle is in working state'. For the sake of simplicity, we assume that the n trials are independent on each other. From the practical point of view, this means that the evolution of the degradation mechanism affecting any nozzle does not influence the evolution of any other degradation process relevant to any other nozzle of the turbine.

The probability of having a failed nozzle in a single trial reads:

$$p = F(t|\beta,\eta) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{9}$$

Simple analytical manipulations of Eq. (9) yield:

$$t = \eta \sqrt[\beta]{-\log(1-p)} \tag{10}$$

Eq. (10) allows us relating t with the degradation states recorded on the i-th machine at time t. Data in the original database allows us to calculate the ML estimators $\underline{\hat{\theta}} = \{\hat{\beta},\hat{\eta},\}$ of $\underline{\theta} = \{\beta,\eta,\}$: these are normally distributed random variables with $N(\hat{\beta},\hat{\sigma}_\beta)$ and $N(\hat{\eta},\hat{\sigma}_\eta)$, respectively, as shown in Section 3. It is important to notice that also p is a random variable, as it depends on the inspection outcome n_f^i of the i-th machine at time t, as shown in the following. Therefore, t turns out to be a random variable, that is a function of the random variables β, η and p.

Our objective is to find the ML estimate $\hat{p}^i$ of the probability p^i of having at inspection of the i-th turbine, $i = 1, \ldots, N$, a given value n_f^i of failed components and, thus, $n_s^i = n - n_f^i$ of safe components.

To do this, first notice that the number of failed components N_f^i is a binomially distributed random variable. Therefore,

$$P(N_f^i = n_f^i) = \binom{n}{n_f^i} p^{i\,n_f^i} (1-p^i)^{n-n_f^i} \tag{11}$$

Then, given the outcome n_f^i of N_f^i, the ML estimate of the probability p^i is given by the value $\hat{p}^i$ that maximizes the likelihood function $L(n_f^i \mid p)$:

$$L(n_f^i \mid p) = \binom{n}{n_f^i} p^{i\,n_f^i} (1-p^i)^{n-n_f^i} \tag{12}$$

from which we get that the maximum likelihood estimate $\hat{p}^i = n_f^i/n$ (Papoulis & Pillai 2002).

The second step of the proposed procedure aims at describing the uncertainty in the ML estimator $\hat{p}^i$, which is a random variable with its own distribution. In this respect, notice that the probability of having a number N_f^i of observations of 'failed' components not larger than n_f^i is:

$$P(0 \le N_f^i \le n_f^i) = \sum_{k=0}^{n_f^i} \binom{n}{k} p^{i\,k} (1-p^i)^{n-k} \tag{13}$$

with $0 \le n_f^i \le n$. Being p a random variable, the probability that $\hat{p}^i \ge p_u^i$ is given by (Birolini, 2004):

$$P\left(\hat{p}^i \ge p_u^i\right) = \sum_{k=0}^{n_f^i} \binom{n}{k} p_u^{i\,k} (1-p_u^i)^{n-k} \tag{14}$$

Eq. (14) defines the incomplete Beta function $I_{1-p}(n-n_f^i, n_f^i+1)$ (Kendall & Stuart 1979), which is the distribution of $\hat{p}^i$. We can sample a possible realization of p for a given n_f^i from this distribution.

On the basis of the considerations above, for any outcome n_f^i we can exploit Eq. (10) to estimate its missing equivalent inspection time t, by sampling α, β and p from the respective distributions.

For example, if $n_f^i = 16$, then $\hat{p}^i = n_f^i/n = 0.727$. The probability, e.g., 0.95, that $\hat{p}^i$ is larger than a given value p_u^i, e.g., 0.848, is given by the probability of having at most $n_f^i = 16$ outcomes out of n, when the probability of finding a fault component in a single trial is p_u^i. That is, larger values of $\hat{p}^i$ are more 'compatible' with experimental results accounting for larger values of n_f^i. In other words, there is a small probability, e.g., 0.05, of having the evidence n_f^i out of n with values of p larger than p_u^i. For clarity sake, the CDF of $I_{1-p}(6,17)$ is shown in Figure 8.

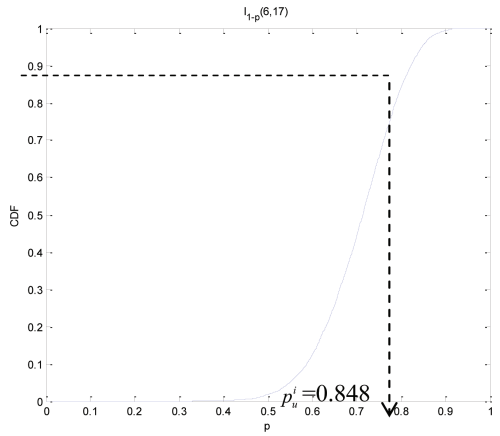


Figure 8. CDF of the incomplete beta function for $n_f^i = 16$ and $n = 22$.

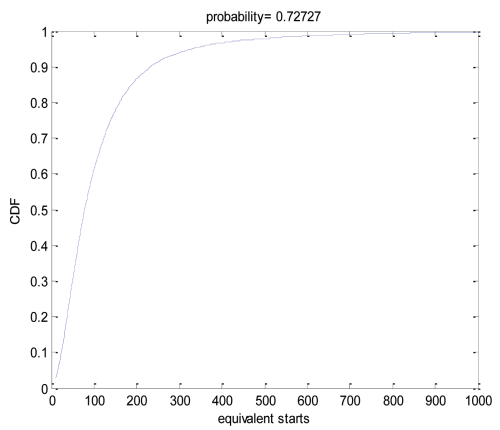


Figure 9. Distribution of t for $n_f^i = 16$ and $n = 22$.

The following MC sampling procedure is implemented to find a possible realization of the missing equivalent starts t for an inspection on the i-th turbine with $n_f^i = 16$:

i. Sample β from $N(\hat{\beta}, \hat{\sigma}_\beta)$;
ii. Sample η from $N(\hat{\eta}, \hat{\sigma}_\eta)$;
iii. Sample p from $I_{1-p}(n-n_f^i, n_f^i+1)$;
iv. Compute t with Eq. (10).

The MC procedure from i) to iv) is repeated a large number of times (i.e., 10^4); this allows building the probability distribution of t (Fig. 9) and to calculate its percentiles (e.g., 50th percentile), to be assumed as reconstructed missing equivalent starts.

5 ESTIMATION OF THE PARAMETERS ON THE MERGED DATASET

Hereafter, the merged dataset containing $N+M$ turbine inspections is considered, where the

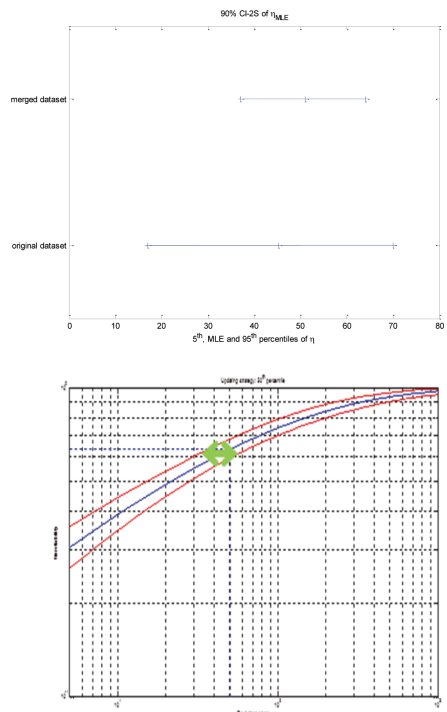


Figure 10. Uncertainty reduction in the estimation of η (top) and unreliability and confidence intervals (down).

equivalent starts t corresponding to the M turbine inspections are taken from the corresponding distribution estimated as in Section 4. In this case, the Log-Likelihood function L can be written as:

$$L(\beta,\eta) \propto \log\left(\prod_{i=1}^{N+M} F\left(t_i|\beta,\eta\right)^{n_f^i} R\left(t_i|\beta,\eta\right)^{n_s^i} \right) \quad (15)$$

where $R\left(t|\beta,\eta\right) = e^{-(t/\eta)^{\beta}}$ is the reliability of the n_s^i nozzles of the i-th machine which are found in 'working' state upon inspection, whereas $F\left(t|\beta,\eta\right) = 1 - e^{-(t/\eta)^{\beta}}$ is the unreliability of the n_f^i nozzles that are found in 'fault' state. If $i \le N$, then t_i is the equivalent starts value reported in the original complete dataset, otherwise, t_i is the 50th percentile of the distribution of t corresponding to n_f^i.

Parameters $\hat{\beta}$ and $\hat{\eta}$ can be calculated following the procedure detailed in Section 3, on the merged original and reconstructed datasets (N+M machine inspections). Figure 10 shows the reduced $\hat{\sigma}_{\eta}$ when the merged dataset is used,

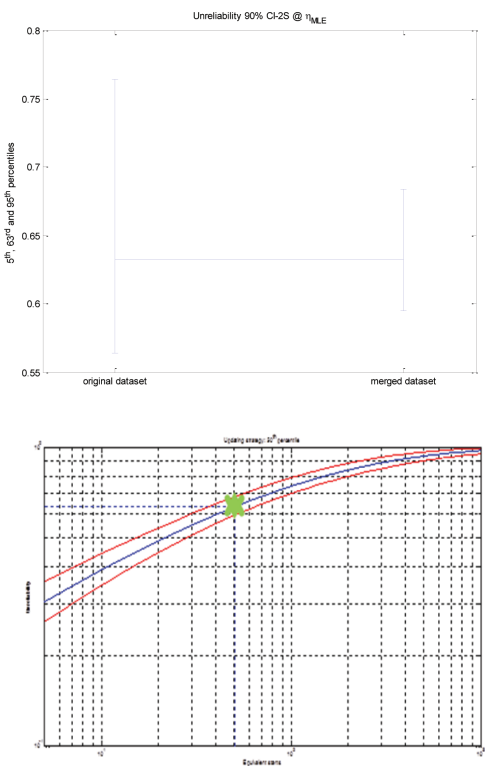


Figure 11. Uncertainty reduction in the estimation of the unreliability at t = $\hat{\eta}$ (top) and unreliability and confidence intervals (down).

with respect to the original dataset (N machine inspections, as shown in Fig. 7). In particular, on the left, the pointwise double-sided 90% confidence intervals for η are plotted for these two cases. Similarly, Figure 11, shows the contribution of the additional M outcomes in reducing the uncertainty of the estimation of the unreliability at $t = \hat{\eta}$.

6 CONCLUSIONS

In this work, a procedure has been presented to complete the data collected at field inspections of components and, thus, exploit all available data gathered. The procedure has been illustrated with reference to nozzle system of turbines operated by GE. It has been shown that such procedure is capable of:

- Estimating the parameters of a Weibull distribution as well as the related uncertainties;
- Reconstructing missing equivalent starts to reduce the uncertainty on the estimation, relying on an enlarged database that contains original (complete) data and additional (reconstructed) data.

In this respect, it has been shown that the reduction of the uncertainty in the estimates depends on the number of records collected in the field inspections, and that, in some particular cases, the proposed procedure conservatively leads to estimations of the scale factor of the Weibull distribution heavily shifted towards zero. Future work will be focused on solutions to avoid such anomalous situations.

REFERENCES

Baraldi, P., Di Maio, F., Pappaglione, L., Zio, E. and Seraoui R, 2012, Condition Monitoring of Electrical Power Plant Components During Operational Transients, Proceeding of the Institution of Mechanical Engineers, Part 0, Journal of Risk and Reliability, 226(6), pp. 568–583.

Baraldi, P., Di Maio, F., Genini, D. and Zio E., 2013, A fuzzy similarity based method for signal reconstruction during plant transients, Chemical Engineering Transactions, 33, pp. 889–894.

Birolini A. 2004. Reliability Engineering, Theory and Practice, 4th Ed., Springer-Verlag.

Brock, G.N., Shaffer, J.R. and Blakesley R.E. 2008 Which missing value imputation method to use in expression profiles: a comparative study and two selection schemes. Bioinformatics 2008;9:12.

Hines, J.W., Wrest, D.J., and Uhrig R.E. 1996, Plant Wide Sensor Calibration Monitoring, In Proceedings of the 1996 IEEE International Symposium on Intelligent Control, Dearborn, Michigan. IEEE, Piscataway, New Jersey, pp. 378–383. September 15–18.

Kendall, M. and Stuart A. 1979. The Advanced Theory of Statistics, Vol. 2, Charles Griffin and Company limited, London & High Wycombe.

Kim, H., Golub, G.H. and Park H., 2005, Missing Value Estimation for DNA microarray gene expression data: local least squares imputation, Bioinformatics, 21(2):187–98.

Luh, G.C. and Lin C.Y. 2011, PCA based immune networks for human face recognition Applied Soft Computing Journal, 11(2), pp. 1743–1752.

Papoulis, A. and Pillai S.U. 2002. Probability, Random Variables and Stochastic Processes, 4th edition, International Edition, Mc-Graw-Hill.

Schafer, J.L. and Graham J.W., 2002, Missing data: our view of the state of the art, Psychological Methods, Vol. 2, pp. 147–177.

Zio, E. 2007, An Introduction to the basics of reliability and risk analysis. World Scientific Publishing, Singapore.

Zio, E. 2013, The Monte Carlo Simulation Method for System Reliability and Risk Analysis Springer Series in Reliability Engineering.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Using field experience in the treatment of Common Cause Failures in reliability assessment

S. Hauge & S. Håbrekke
SINTEF Technology and Society, Safety Research, Trondheim, Norway

M.A. Lundteigen
The Norwegian University of Science and Technology (NTNU), Norway

ABSTRACT: The reliability of Safety Instrumented Systems (SISs) that employ redundancy is highly influenced by Common Cause Failures (CCFs). A widely used CCF model is the beta factor model, but a general challenge is lack of data to support the model parameters. Few initiatives have been taken to collect operating experience, except for the nuclear industry whose results are not directly applicable to other sectors. Use of checklists represents an alternative approach, but their underlying assumptions are not always well documented. Their applicability for the large variety of safety-critical equipment has also been criticized. This paper presents recent experience with CCFs and systematic failures (which are closely interrelated) along with new CCF checklists, based on an ongoing research project financed by the Research Council of Norway and the PDS forum members (www.sintef.no/pds).

1 INTRODUCTION

Safety Instrumented Systems (SISs), i.e. safety-critical systems that are based on electrical/electronic or programmable electronic technology, often employ redundancy to enhance their performance. The intended reliability effects of redundancy may however, be reduced if the system components are exposed to similar environmental exposures, design errors, and errors made during operation and maintenance. When multiple failures are attributed to a shared cause, they are often referred to as Common Cause Failures (CCFs). Standards that frame the development of SIS, such as IEC 61508 (2010), IEC 62061 (IEC 62061, 2005) and IEC 61511 (IEC 61511, 2003), require that measures are implemented to avoid CCFs and that the remaining effects of CCFs are included in reliability analyses.

Models for including CCFs in reliability analyses of SISs have evolved since the 1970s, and several models have been proposed for this purpose (Rausand and Hokstad, 2008). Excluding this failure category would lead to a significant underestimation of the calculated reliability (Rausand and Høyland, 2004), and most reliability experts would question analyses that would do so. The most common CCF model adapted by the process industry is the standard beta factor model (IEC 61511, 2003, ISA TR 84.00.02, 2002, SINTEF, 2013b). The PDS method (SINTEF, 2013b) has been developed with basis in this model and an extension of this, the multiple beta factor model (Hokstad and Corneliussen, 2004).

A common challenge for all CCF models is the lack of suitable data to support the model parameters. The nuclear industry has given CCFs considerable attention and carried out several CCF data collection projects to build generic data bases on CCFs (NEA, 2004, NEA, 2014, SKI, 1998). The process industry and the petroleum industry have not run similar projects, not as part of large data collection projects, like e.g. OREDA (OREDA, 2009) nor through other known initiatives. Hauge et al. (2006) investigated how the industry control CCF, but the study was of a qualitative nature. The PDS data handbook (SINTEF, 2013a) is one of few data sources that propose values of beta for commonly used components, but these are mainly established on the basis of expert judgments, comparison with other data sources and some results from operational reviews. The value of having generic data bases for CCFs may also be questioned. As discussed by Rausand (2012), the contribution from CCFs is strongly influenced by local, plant-specific conditions. This is also supported by results from operational failure reviews as discussed later in this paper.

Expert judgment is therefore often used in the process of determining the CCF model parameters, and checklists are used as a means of structuring such input. Two widely accepted examples

are found in IEC 61508 (2010) and IEC 62061 (2005), but even for these the foundation has been questioned: First, the same checklist questions are suggested for a wide range of component types with very diverse properties and failure modes. Second, the selection of checklist questions is not well explained, and rationales for weight and scores in relation to the checklist questions are not presented. Third, several of the checklist questions tend to be very general and "high level", and users of the checklists may interpret the meaning quite differently. A better approach may therefore be to develop equipment-specific CCF checklists, preferably with a content and structure that build on operating experience taking into account facility specific conditions.

The main purpose of this paper is to discuss the extent of CCFs and to suggest CCF component specific checklists, with basis in an extensive review of failures recorded for SISs in the oil and gas industry.

The content of this paper is based on an ongoing research project funded by the Norwegian Research Council and the member of the PDS forum.[1] Failures reported for a large variety of SIS components at offshore and onshore oil and gas facilities in Norway have been included in the review (totaling up to more than 10000 maintenance notifications). Based on this, the most typical CCF causes and their relative importance are being presented and discussed. The new knowledge has been used as basis for developing component specific checklists, targeted to address the most important CCFs for each of these.

Operational failure reviews have been carried out at six facilities, allowing the results to be considered as rather general for both onshore and offshore facilities, in particular for facilities located in environments similar to those in Norway and on the Norwegian Continental Shelf.

2 RESEARCH APPROACH (PDS PROJECT)

The main approach in this research project has been as follows:

Step 1: Carry out a literature review and a workshop on the treatment of CCFs in PDS forum. The results were used as input to steps 2–4. **Step 2:** Review of reported failures (maintenance notifications). The operational reviews were facilitated by SINTEF, but involved key discipline personnel (automation, mechanical, process) from the specific facility and company in question. Each notification was reviewed with the purpose of classifying failures according to IEC 61508 (2010). **Step 3**: Analysis of results. The results from all six facilities were reviewed, and the failures associated with the same type of components with shared causes were—given a set of associated criteria—classified as complete CCFs or failures that could have caused a CCF. Some of the results are given in Section 5 of this paper. **Step 4:** Development of component-specific CCF checklists based on the results in Step 3. Two examples of preliminary checklists are given in Section 6.

2.1 *Literature review*

The main purpose of the literature review was to investigate the state of the art for methods for determining model parameters of CCF models. Very comprehensive approaches like what is used in the nuclear power industry to support multiple-Greek letter CCF models, see e.g., NUREG/CR-5485 (1998) and NUREG/CR-6268 (2007), have not been studied in detail in this paper. Instead, the focus has been on identifying methods available for determining the β in the beta factor model, and on the definitions of CCF that may be useful as assistance in the analysis and classification of failures reported for safety-critical components. Literature referenced in a study by Rausand and Hokstad (2008) has been key for the review.

3 CCF DEFINITIONS AND APPLICATION

3.1 *CCF attributes*

CCF definitions have been proposed and refined over several decades. Smith and Watson (1980) did a detailed review of definitions available as early as in 1980. They concluded that a set of multiple failures could be defined as a CCF if *all* the following conditions are met: (1) The components affected are unable to perform as required, (2) multiple failures exist within (but are not limited to) redundant configurations, (3) The failures are "first in line" type of failures and not the result of cascading failures (i.e. where a failure of one component has triggered the failure of another component), (4) the failures occur within a defined critical time period (e.g., the time a plane is in the air during a flight or the time between two test intervals), (5) the failures are due to a single underlying defect or a physical phenomenon (the common cause of failures), and (6) the effect of failures must lead to some major disabling of the system's ability to perform as required.

In this paper, the term *complete CCF* is used to denote multiple events that fulfill all six criteria, with an extension of criterion 2. Multiple failures

[1] www.sintef.no/pds.

are considered for the whole category of similar components, and not only for similar components within the same safety function.

Regarding criterion six, it may be open to interpretation what to define as a major disabling. For example NEA (2004) defines a complete CCF as the event where *all* components in a population of interest have failed due to a common cause. In this paper, we include more events in the definition of complete CCFs. For example, in a 1oo3 configuration, the NEA definition requires failure of all three components to define it as a complete CCF, whereas in this paper a simultaneous failure of two components is considered sufficient. Actually, in the failure reviews, any simultaneous failures of two (or more) components due to a shared cause, is defined as a CCF event, although the components do not necessarily belong to the same safety function. This is further discussed in section 5.

The identification of CCFs among reported failures would overlook many possible causes of CCFs if focusing on complete CCFs alone. Systematic failures, i.e., failures that are due to errors made in specification, design, installation, or operation and maintenance, and which are not due to natural degradation of the component state, may be replicated for several components. When a systematic failure is found, it is important to also ask if other components may have been affected. Therefore, in the failure reviews, it has, for each systematic failure, been questioned whether the failure could have resulted in multiple failures within a relatively short time window. If yes, the failure has been defined as a potential CCF.

The term *potential* CCFs is thus used to capture a broader category of CCFs, and includes all foreseeable causes that may result in a CCF based on a review of recorded failures. This term is also mentioned in the ICDE guideline, but not formally defined. In practice we see that a potential CCF very much resembles a systematic failure. The two are however not identical; A failure may be systematic without necessarily having the potential to create a CCF (under given conditions and configurations). On the other hand, a potential CCF will always have the properties of a systematic failure.

The two categories complete and potential CCFs have been introduced to serve two different purposes. Complete CCFs may, when counted up, be used to estimate how often CCFs have occurred. The main problem is that a plant specific CCF failure rate will have a high level of uncertainty, due to limited amount of samples. Potential CCFs cannot be included, at least with the same weight as complete CCFs, in the estimation of CCF failure rates. However, potential CCFs are important for identifying potential failure causes as well as vulnerabilities in design or its operating environment that, if prevented or modified, could reduce the future occurrence of CCFs.

3.2 *Root cause, coupling factors and defenses*

Parry (1991) and Paula et al. (1991) split CCF causes into root causes and coupling factors, and this concept has been adapted in many types of CCF analyses (NUREG/CR-5485, 1998, NUREG/CR-6268, 2007, Lundteigen and Rausand, 2007).

A **root cause** is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence (NUREG/CR-5485, 1998). Examples of root causes are high or low temperature, excessive sand production, large vibrations, earthquake, fire, sudden changes in loads, high or low pressures, moisture or high humidity, heat radiation, electrical failure, lack of procedures, failure to follow repair or test procedure, systematic calibration failures, design failure, inadequate testing/inspection/follow-up etc.

All too often, the description of a failure is limited to the most obvious cause or a simple statement that "the component has failed". Without a proper identification of the root cause, it is difficult to select the most efficient defense measure. For example, in the review of reported failures, we see that failed detectors are often just replaced by a similar type without further analysis. We also see that valves being stuck during a functional test may be lubricated and then operated successfully. Lubrication has a short term effect on the valve performance, and actual root cause is seldom revealed. Such strategies are often insufficient for the purpose of selecting the most effective defense measures.

A **coupling factor** is a characteristic of a group of components or parts that identifies them as susceptible to the same causal mechanisms of failure (NUREG/CR-5485, 1998). Such characteristics may be related to the use of common procedures, common design principles, the same environmental exposure and/or operating environment, and the same personnel involved in design, installation, operation, or maintenance. Some examples of coupling factors may be that the same operator calibrates all level transmitters mounted on the same vessel. Another example is that a whole set of flame detectors are located in an area exposed to sea water spraying. A coupling does not trigger any failure by itself, but its presence may replicate or allow the replication of the same failure onto several components.

3.3 *Defense strategies*

It may be argued that the occurrence of root causes mainly impacts the total (i.e. independent

and dependent) failure rate, whereas a change in coupling impacts the beta factor in the beta factor model. Defenses against CCFs may therefore aim for both of these tactics (Lundteigen and Rausand, 2007). In practice, there may be operational constraints that limit the freedom in available defense measures. For example, root causes that are external, such as snow, sea spray, low or high ambient temperatures, or process parameters such as acidity and sand content in fluid, cannot always be modified, and their effects must be catered for when selecting defense measures.

Development of component-specific checklists for CCFs should therefore ideally capture the relevant coupling factors as well as typical failure causes associated with a component group, and these may be identified by review and analysis of reported failures.

4 DETERMINING THE BETA FACTOR

Several authors have suggested ways (checklists, influence diagrams) for determining beta values (Humphreys, 1987, Brand, 1996, Johnston, 1987, Zitrou and Bedford, 2003, Zitrou et al., 2003, IEC 61508, 2010, IEC 62061, 2005). An overview of these approaches is provided in Rausand and Hokstad (2008). The first approaches, such as Humphreys (1987) and Brand (1996) were developed with basis in the Nuclear industry, and build on insight and experience from this sector. Zitrou and Bedford (2003) and Zitrou et al. (2003) have extended the approach by Brand (1996) to include site-specific factors into influence diagrams. Insight to these methods has to some extent been used as inspiration for the checklists proposed in Section 6.

5 OPERATIONAL REVIEWS

In general, limited attention is given to CCFs during daily plant operation and during failure registration and follow-up in particular. This impression was also supported by the operational reviews which looked into various component groups of safety critical equipment on six facilities. Many multiple failures revealed in these reviews were not identified or registered as CCFs, even if the same type of failure had been notified by alarms or observed in many subsequent tests. This can be explained by inadequate investigation of the failure cause in the first place, inadequate overview of the failure history and last but not least a limited focus on CCFs in general.

In this paper we look into some results for three equipment groups; Shutdown valves, point gas detectors and level transmitters. Selected summary figures are given in Table 1.

The table lists the number of observed DU-failures, the number of registered CCF events among these DU failures, the number of DU-failures that are part of these CCF events (in brackets), and the aggregated operational time of the population. Note that a CCF can comprise from two to several DU-failures. At most 19 DU-failures have been registered for one CCF. Also note that potential CCFs are not included in the tables. More details for each of the three component groups are given below.

5.1 *Shutdown valves*

The shutdown valves shall close upon a demand. Several of them also have requirements with respect to closing time and some of them to maximum leakage rate in closed position. In total, 221 DU failures were observed for the shutdown valves from the six operational reviews. The DU failures mainly include the three failure modes fail to close on demand, leakage in closed position and delayed operation. The 11 CCF events registered involved the following failures:

- 19 DU failures (delayed operation) were due to poor design of hydraulic connections resulting in too long closing times.
- 11 other DU failures (fail to close) were due to incorrect valve type for the specific application (fail-open valves installed in fail-close application).
- Additional six DU failures (fail to close) of another type of valve were due to poor design (these were not designed for the intended use and degraded immediately). All these valves had to be replaced.
- Six DU failures (delayed operation) were due to changing hydraulic oil viscosity (caused by temperature variations).
- Four DU failures (fail to close) were due to actuator capacity. The operation of these valves is normally assisted by pipeline pressure, but when testing with no (delta) pressure over the valve they were unable to close.
- Three DU failures (fail to close) were due to damaged gaskets combined with dirt from operation.

Table 1. Results from operational reviews.

Component group	DU	CCF	Operational time
Shutdown valves	221	11 (59)	37 000 000 hrs
Point gas detectors	36	2 (14)	49 000 000 hrs
Level transmitters	52	2 (11)	12 000 000 hrs

– Three DU failures (leakage in closed position) were due to a leakage problem with a group of valves of similar type. No root cause of this problem was revealed.
– Two DU failures (fail to close?) were caused by wrong mounting of solenoid valves made while modifying the control of these valves.
– Two DU failures (failure to close) on similar types of valves were detected simultaneously (unknown cause).
– Two DU failures (fail to close) were caused by corrosion on the actuator stem due to wrong material selection.

An additional (unknown) number of DU failures (delayed operation) were due to inadequate bleed-off (wrong tuning of bleed-off valve).

In addition, several systematic failures were observed with a potential of causing CCF events. Examples are valves that did function due to low temperatures and ice/freezing, stuck hand wheel due to rust, insufficient lubrication and cleaning of valves, nitrogen leakage from valve accumulators and incorrect adjustment of valve during previous maintenance.

5.2 *Point gas detectors*

Gas detectors shall detect the presence of gas and initiate an alarm at specified concentration(s). Besides hydrocarbon gas, some H_2S, CO_2 and O_2 detectors are also included in the sample. In total, 36 failures were defined as DU failures for point gas detectors from the six operational reviews. The failure modes included e.g. no measurement ("dead"), unsteady measurement and wrong measurement. The two CCFs registered involved the following failures:

– Ten DU failures (incorrect measurement) were due to poor design of a detector type, such that all the detectors had to be replaced.
– Four DU failures (incorrect measurement) were all detected at the same time by random observations (no alarm). The four detectors had frozen measurement and had to be replaced.

Potential CCFs included detectors that did not function due to environmental influences causing dirty lenses, dense filter due to inadequate maintenance procedures, poor design of the detector mirror, and erroneous calibration.

5.3 *Level transmitters*

Level transmitters shall measure correct level in a tank or vessel and initiate alarm(s) at specified level(s). In total, 52 failures were defined as DU failures for level transmitters from the six operational reviews. These include failure modes such as wrong measurement, unsteady measurement and frozen measurement. The two registered CCFs involved:

– Nine DU failures (incorrect measurement) were due to wrong measuring principle for the specific application, resulting in wrong level measurements (revealed randomly or on tests). It should be noted that many vessels have very challenging measurement conditions, and a suitable level measurement principle hardly exist for all operational situations.
– Two DU failures (incorrect measurement) due to wrong data values in their data sheet.

Systematic failures that could potentially have resulted in CCFs included transmitters exposed to cold temperatures resulting in icing/hydrate formation in impulse lines, incorrect mounting of transmitter, and a transmitter exposed to an electrical failure.

5.4 *Estimation of beta*

Estimation of beta based on the results from Table 1 can be performed using various estimators. The well recognized estimator is (NUREG/CR-4780, 1989):

$$\hat{\beta}_1 = \frac{N_{\mathrm{DU,CCF}}}{N_{DU}} \tag{1}$$

Here $N_{DU,CCF}$ is the number of DU failures included in a CCF event (e.g. 59 for shutdown valves, ref. Table 1) and N_{DU} is the total number of DU failures experienced for the population. As discussed in section 3.1, in the failure reviews simultaneous failures of two (or more) components have been classified as CCF events, although the components do not necessarily go into the same safety function. Therefore, the above estimator will be rather conservative when estimating betas in general. A more appropriate estimate for the beta value may be (NUREG/CR-4780, 1989):

$$\hat{\beta}_2 = \frac{2 \cdot N_{CCF}}{N_{DU,I} + 2 \cdot N_{CCF}} \tag{2}$$

Here, N_{CCF} is the number of actual CCF events, e.g., two for level transmitters, and $N_{DU,I}$ are those DU-failures that are not affected by any CCF, e.g., 41 for level transmitters. This estimate assumes that each CCF event results in failures of two components. In reliability calculations CCF is mainly considered for two (or three) redundant components. Also in the PDS method, beta is defined as the fraction of failures of a single component that causes both components of a redundant pair to fail due to a CCF. In addition,

Table 2. Estimated beta values.

Component group	$\hat{\beta}_1$	$\hat{\beta}_2$
Shutdown valves	27%	12%
Point gas detectors	39%	15%
Level transmitters	21%	9%

modification factors are introduced to cater for different voting configurations (SINTEF, 2013b). Estimated beta values for each of our three component groups are shown in Table 2.

From the results we see that shutdown valves and gas detectors seem to have a somewhat higher estimated beta value than level transmitters. Also, the estimated beta indicates that beta values around 10% (and even more for valves and detectors) seem realistic. However, it should be noted that these estimates are based on a rather limited number of CCF events, although the accumulated operational period is rather extensive.

Most of the CCFs are facility specific and the same type of CCF may not necessarily appear on more than one facility. E.g. for point gas detectors and level transmitters, no complete CCF events have been observed on several facilities. On the other hand the data collected from the operational reviews are "the best available" and will together with expert judgments and component specific checklists hopefully result in an improvement in the estimation of CCFs taking facility specific conditions into considerations.

6 NEW EQUIPMENT SPECIFIC CHECKLISTS

As discussed above, the fraction of CCFs will vary significantly between installations and equipment types. Therefore, development of equipment specific checklists is a main activity in the ongoing research project. The purpose of developing such checklists is not necessarily limited to only estimating a value for beta after having judged a specific design in light of control questions. A checklist may also be used to point at possible defense tactics that, if implemented, will result in a reduction of the beta-factor. It may for example be of interest to reassess the value of beta in operation, and it is therefore relevant to document what kind of defenses that are assumed implemented and how these are followed-up in actual operation. Table 3 and Table 4 show some preliminary examples of checklists.

The structure of the suggested checklist is based on the following assumptions: (i) Component specific CCF vulnerabilities can be listed with basis in the review of reported failures: These are specific conditions known to affect the vulnerability to CCFs (e.g. sand in the production flow, presence of ice and snow, same operators calibrating several transmitters, etc.). These conditions are assumed to affect the beta-value regardless of defenses in place. (ii) Defenses may be introduced to reduce the impact of CCF vulnerabilities, but not to a zero level. For example, sand detectors, heat tracing of impulse lines, 3rd part control of work, etc.).

The columns of the table include: **Category:** A categorization of CCF vulnerabilities. These may be underlying (coupling) factors and causes that may increase the likelihood of experiencing a CCF. **Weight:** The assessed weight of the associated cause/factor based on results from the operational reviews. **Relevance:** Whether the specific cause/factor is relevant for the application under consideration. **Defenses:** Measures or strategies that may prevent or reduce the likelihood of the associated cause or coupling to come into force. A division between procedural/training/documentation meas-ures and physical measures has been made. **Efficiency (Eff):** A scaling comparable to the scaling used for potential CCFs in (NUREG/CR-6268, 2007), with one added level. The following scaling factors are suggested:

2.0: No measure is implemented resulting in a "penalty" of a factor 2. **1.0:** The measure is judged to have a *low* efficiency and does not go beyond what is considered "state of the art" in protection. **0.5:** Measures have been taken, but the effect of the measure is considered *medium*/limited or it has not been documented that the foreseen effects have been achieved. **0.1**: Measures have been taken, and it has been documented that the measures have a *high*/significant (and positive) effect on the issue in question.

Modification factor (Mod Factor): The product of efficiency factors assigned to each defense. The factor is used to update the weight of beta for this particular category.

When establishing the checklists, six main categories of underlying causes and coupling factors (threats) that may increase the likelihood of experiencing a CCF have been defined:

Design properties: Covering aspects related to redundancy, diversity and functionality of the specific equipment (see example in Table 3). *Special considerations*: Aspects related to previous experience with/maturity of the equipment, complexity of the design, possible weak points in the design, etc.

Human machine interface: Aspects related to accessibility to and maintainability of the equipment, including planned level of human interaction in

Table 3. Example checklist—environmental control category.

Category	Weight	Relevance	Procedure, training and documentation defenses		Technical/physical/separation defenses		Mod Factor
Design properties	30%	Y/N	Defenses/evaluation	Eff.	Defenses/evaluation	Eff.	
Are redundant valves of the same type (make, manufacturer, material selection, etc.)?	5%	Y	Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection and so on	2.0 (no)	Have measures identified in the design review been implemented to reduce the identified negative impacts of similar valve types?	0.5 (M)	1.0
Have max and/or min closing time been defined for the redundant valves in question	20%	Y	Have design reviews been carried out with the purpose of identifying possible design constraints in view of response time requirements?	1.0 (L)	Has it been confirmed that utility systems have sufficient capacity, as well as the individual valve actuators?	0.5 (M)	0.5
Is leak tightness an issue for the redundant valves in question	5%		Have max leakage rates been uniquely defined, i.e. consistency between all documentation specifying maximum internal leakage rates are ensured?	1.0 (L)	Has it been confirmed that the valves are suited for keeping fully tight in closed position? May the operating condition alter this capability?	2.0 (No)	2.0
Environmental control	15%	Y/N	Defenses/evaluation	Eff.	Defenses/evaluation	Eff.	
Are valves exposed to an internal environment such as dirt, sand, hydrate formation, etc. possibly affecting valve performance?	6%	Y	Has specific procedures for control of sand, dirt, hydrate formation, etc. been implemented, including procedures for cleaning and lubrication of valves?	1.0 (L)	Have physical measures for control of internal environmental influences such as sand traps, inhibitors, etc. been implemented?	0.5 (M)	0.5
Must the valve function under a large variety of pressure and flow conditions?	3%	Y	Have the valves, actuators and hydraulic blocks been verified and tested for all relevant pressure, temperature and flow conditions?	1.0 (L)	Has extra sizing/dimensioning of actuator, etc. been implemented to ensure that the valve will function under all foreseeable process conditions?	0.5 (M)	0.5
Are the valves exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting valve performance?	6%	Y	Are procedures for removing ice, build-up of snow, etc. during periods with cold temperatures in place and implemented (including procedures to check that e.g. heat tracing is functioning/is on)?	0.5 (M)	Are valves exposed to snow, ice, sea spray, cold temperatures equipped with separate weather protection/ isolation/heat tracing?	0.5 (M)	0.25

operation and maintenance. *Environmental control*: Covering aspects related to suitability of the equipment versus the design envelope (fit for purpose), and the level of alternating environmental conditions (see example in Table 3). *Operation & Maintenance*: Covering the operational personnel's proneness to perform errors and failures as well as the organization's readiness to prevent such failures. Aspects related to procedures, competency and training are included here. *Operational follow-up and management of change:* Aspects related to how experienced failures are treated and followed-up, alignment of test intervals in light of experienced failure history, root cause analysis incl. identification of systematic and common/shared failure causes, implantation of failure reducing measures as well as handling of changes and modifications affecting the particular equipment.

Each of these six categories have, based on experiences from the operational reviews, been assigned a generic weight (e.g. 30% of the CCFs can be explained by design related properties). It should be remarked that the weights at this stage are preliminary. For each category a number of checklist questions have been suggested, each with a weight summing up to the total weight of the associated category. For example, from Table 3 it can be seen that the closing time question is given a weight of 20%, since much problems have been experienced related to this issue. If a generic beta of 10% is assumed for shutdown valves, then, in effect, 2% of this beta can be related to closing time problems.

Based on an evaluation of the defenses related to each particular threat, this contribution can increase (no defenses implemented), remain unchanged (only "state of the art" defenses implemented) or decrease (additional defenses implemented). For example, for the referred closing time question, the resulting modification factor is 0.5, meaning that the beta contribution is reduced from 2% to 1%. Following this procedure for all questions will then yield an updated beta factor for shutdown valves based on plant specific conditions.

Defenses are per today predefined in the checklists. As part of the ongoing work it is being considered whether the checklists should have an added flexibility of the users being able to add their own defenses.

7 CONCLUSIONS AND FURTHER WORK

This paper has proposed a new type of CCF checklist, with basis in experience collected for the oil and gas industry. The approach, i.e. the definition of CCF categories and defenses, is as such generic, and may be applied also to other industry sectors. The weighting and detailed formulation of underlying information in the checklist should, however, be updated to reflect the industry sector experience in question.

Further work is needed to finalize the checklists. The next step is to present the checklist the PDS members and include their input and feedback in the final stage of the checklist development. Additional data may be gathered if needed from future operational reviews. The authors would like to present a more complete checklist proposal in a new and more extended publication, covering not only the shutdown valves but also detectors and transmitters.

The overall aim is to provide a more comprehensive framework for the treatment of CCFs in reliability assessments that may be applied in the design phase and updated to monitor status of CCFs at regular stages in the operational phase

ACKNOWLEDGEMENT

The present work has been carried out as part of the research project "*Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry*", a project that has been sponsored by the Research Council of Norway and the PDS participants (www.sintef.no/pds).

REFERENCES

Brand, P. (1996) *UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems*, Cheshire, UK: SRD Association, AEA Technology plc.

Hauge, S., Onshus, T., Øien, K., Grøtan, T.O., Holmstrøm, S. & Lundteigen, M.A. (2006) STF50 A06011 Uavhengighet av sikkerhetssystemer offshore—status og utfordringer (in Norwegian).

Hokstad, P. & Corneliussen, K. (2004) Loss of safety assessment and the IEC 61508 standard *Reliability Engineering and System Safety* 83: 111–120.

Humphreys, R. (1987) Assigning a numerical value to the beta factor common cause evaluation. *Proceedings of the sixth conference (Reliability '87)*. Birmingham.

IEC 61508 (2010) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Parts 1–7. eneva: International Electrotechnical Commission.

IEC 61511 (2003) Functional Safety—Safety Instrumented Systems for the Process Industry Sector. Geneva: International Electrotechnical Committee.

IEC 62061 (2005) Safety of Machinery—Functional Safety of Safety-Related Electrical/Electronic and Programmable Electronic Control Systems. Geneva: International Electrotechnical Commission.

ISA TR 84.00.02 (2002) Safety Instrumented Functions (SIF)—Safety Integrity Level (SIL) Evaluation Techniques. Parts 1–5.: The instrumentation, Systems, and Automation Society.

Johnston, B. (1987) A structured procedure for Dependent Failure Analysis (DFA). *Reliability Engineering* 19: 125–136.

Lundteigen, M.A. & Rausand, M. (2007) Common cause failures in safety instrumented systems on oil and gas installations: Implementing defenses through function testing. *Journal of Loss Prevention in the Process Industries* 20: 218–229.

NEA (2004) *International Common-Cause Failure Data Exchange. ICDE General Coding Guidelines. Technical Note NEA/CSNI/R(2004)4*.: Nuclear Energy Agency.

NEA (2014) International Common Cause Failure Data Exchange Project webpage http://www.nea.fr/html/jointproj/icde.html. Accessed 30 March 2014.

NUREG/CR-4780 (1989) *Procedures for Treating Common Cause Failures in Safety and Reliability Studies (Vol. 2)*, Washington DC: U.S. Nuclear Regulatory Commmission.

NUREG/CR-5485 (1998) *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.*, Washington DC: U.S. Nuclear Regulatory Commmission.

NUREG/CR-6268 (2007) *Common-Cause Failure Databases and Analysis System: Event Data Collection, Classification, and Coding*, Washington DC: U.S. Nuclear Regulatory Commission.

OREDA (2009) *OREDA Reliability Data (5th ed.)*, Oslo: OREDA Participants.

Parry, G. (1991) Common cause failure analysis: A critique and some suggestions. *Reliability Engineering and System Safety* 34: 309–320.

Paula, H.M., Campbell, D.J. & Rasmuson, D.M. (1991) Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering and System Safety* 34: 389–415.

Rausand, M. (2012) *Reliability of Safety-Critical Systems: Theory and Applications*, Hoboken, New Jersey: Wiley.

Rausand, M. & Hokstad, P. (2008) Common Cause Failure Modeling: Status and Trends. *Handbook of Performability Engineering.* London: Springer.

Rausand, M. & Høyland, A. (2004) *System Reliability Theory. Models, Statistical Methods, and Applications*, New York: Wiley.

SINTEF (2013a) Reliability Data for Safety Instrumented Systems, Trondheim, Norway.

SINTEF (2013b) Reliability Prediction Method for Safety Instrumented Systems. Trondheim, Norway.

SKI (1998) *Investigates events that (potentially) lead to CCF. SKI Technical Report 98:09*.: Swedish Nuclear Power Inspectorate.

Smith, A. & Watson, I. (1980) Common cause failures—a dilemma in perspective. *Reliability Engineering* 1: 127–142.

Zitrou, A. & Bedford, T. (2003) Foundations of the UPM common cause model. In T., B. & van Gelder, P.H. (eds.) *ESREL 2003.* Balkema.

Zitrou, A., Bedford, T. & Walls, L. (2003) Developing soft factors inputs to common cause failure models. In Spitzer, C., Schmocker, U. & Dang, V.N. (eds.) *ESREL 2003.* Springer, Berlin.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A geometric test for the analysis of contingency tables

J. Quigley & K.J. Wilson
Department of Management Science, University of Strathclyde, Glasgow, UK

ABSTRACT: The Chi-squared test for contingency tables has good performance when sample sizes are sufficiently large but is not appropriate with small samples. This is particularly relevant to reliability analysis where some failure types will occur infrequently. When this condition is violated, Fisher's exact test is often used as it is valid for all sample sizes. However, Fisher's test has been criticised for being overly conservative. Alternatives have been proposed but typically involve more complex computations. In this paper we propose an alternative test based on a geometric projection of the multinomial distribution onto the n-sphere. Each multinomial observation is represented by a single point on this sphere. The angle between two points representing two different multinomial observations can then be compared to the distribution of the angle under the assumption that the realisations come from the same underlying distribution. The null hypothesis distribution is simulated and easy to compute. This new test is compared to the Chi-Squared test and Fisher's Test in terms of both Type I and Type II errors and its potential use in reliability modelling is indicated using a real case study concerned with a manufacturer assessing different patterns of failures of machines across different regions.

1 INTRODUCTION

Contingency tables are used in the areas of safety and reliability modelling when there are several machines, systems or failure types which are possibly spread over different locations. That is, whenever data are in form of frequency of events for categorical variables. Typically we wish to know whether there are differences between the probability of failure between the different states of two of the different factors such as failure type and location. Examples include (Conte,Rubio, Garcia, & Cano 2011, Maiti & Khanzode 2009, Colombo & Ihm 1988, Schneidewind 1992).

Conte et al. (Conte, Rubio, Garcia, & Cano 2011) considered a 19×19 risk-injury contingency table of the accident rates in Spanish companies over an 11 year period to identify separate risk and injury groups. Maiti and Khanzode (Maiti & Khanzode 2009) investigated a relative risk model using a two way contingency table for fatal roof and side fall accidents at coal mines in India.

In Colombo and Ihm (Colombo & Ihm 1988) failure rates at nuclear power plants were considered. The failure rates of components were broken down by plant location and reactor system. This led to a contingency table for the numbers of failures which was further complicated by the different exposures at each of the plants. Schneidewind (Schneidewind 1992) was interested in the validation of software metrics. His proposed methodology used contingency tables as an important part of this validation process, counting up the numbers of correct and incorrect classifications of each type.

An example of a contingency table, based on the two factors in Colombo and Ihm (Colombo & Ihm 1988), is given in Table 1.

In such a contingency table we would typically be interested in whether there were differences in the probabilities or rates of failures which result in the observed numbers of failures $n_{i,j}, i, j = 1,2,3$ between the different locations or systems. Thereare two main statistical tests which could be used to do this; the Chi-Squared Test and Fisher's Exact Test (Pearson 1900, Fisher 1922).

In the Chi-Squared test expected frequencies are calculated for each of the cells in the contingency table $e_{i,j}$ and these are then compared to the observed frequencies to form the Chi-Squared test statistic

$$\chi^2 = \sum_{i=1}^{I} \sum_{j=1}^{J} \frac{(n_{i,j} - e_{i,j})^2}{e_{i,j}^2},$$

Table 1. An example contingency table with factors location and system.

	Location		
System type 1	$n_{1,1}$	$n_{1,2}$	$n_{1,3}$
System type 2	$n_{2,1}$	$n_{2,2}$	$n_{2,3}$
System type 3	$n_{3,1}$	$n_{3,2}$	$n_{3,3}$

which is compared to the χ^2 distribution on $(I-1)(J-1)$ degrees of freedom. The Chi-Squared Test is useful when all of the observed frequencies are equal to at least 5 but performance becomes poor when at least one of the frequencies is smaller than this (Cochran 1954). It cannot be carried out with multiple observed frequencies of 0.

Variants to the Chi-Squared Test have been proposed for small sample sizes. Two of the most prominent are the Yates correction and Fisher's Test. In Fisher's Test an exact p-value is calculated based on the assumption that the row and column totals are fixed. While the Fisher Test is exact and so is suitable for small sample sizes it has been criticised for being overly conservative (Liddell 1976). This conservatism stems from the discrete nature of the test statistic and the assumption of fixed marginals. Several other variants have been proposed in the literature but many of these rely on intensive numerical methods and are therefore, for practitioners wishing to test for differences quickly and simply, not always suitable or appropriate.

(Olbrich 1965) proposed a geometric projection of the multinomial distribution onto the n-sphere. Each multinomial observation was represented by a single point on this sphere and the difference between two multinomial realisations of the same degree was represented by the angle between the two points on the sphere. This representation had the nice property that it was variance stabilising. The representation was not commutative, however; if the order of the categories were switched in the multinomial distributions then the points on the sphere and the angle between the points did not remain the same.

In this paper we propose a commutative version of the (Olbrich 1965) representation. We then use this version to define a hypothesis test to test for differences in contingency tables. The test statistic is the angle between the two multinomial realisations. We use the variance stabilising property of the transformation in order to approximate the distribution under the null hypothesis that the two realisations come from the same underlying probability vector. The test does not require intensive numerical methods.

The remainder of the paper is structured as follows. In Section 2 we review the method of (Olbrich 1965), give our proposed commutative adaption and outline the geometric hypothesis test. In Section 3 we investigate the properties of the proposed transformation and in Section 4 we conduct a simulation study to assess the performance of the Geometric Test against the Chi-Squared Test and Fisher's Test for both Type I and Type II errors. Finally, in Section 5 we give an illustrative example of the method and we conclude the paper in Section 6.

2 GEOMETRIC TRANSFORMATION OF MULTINOMIALS

2.1 *The Olbrich transformation*

Consider two realisations from a multinomial distribution in n dimensions, $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$. Let

$$x_T = \sum_{i=1}^{n} x_i,\ y_T = \sum_{i=1}^{n} y_i,$$

be the total number of observations from each of these multinomials. Then the proportions of the observations in each of the categories are

$$p_i = \frac{x_i}{x_T},\ q_i = \frac{y_i}{y_T}.$$

Olbrich proposed representing the multinomials in spherical co-ordinates as points on an n-shphere using these proportions. Denote these points by $\underline{\theta}, \underline{\phi}$ respectively. Then

$$\underline{\theta} = \left(\cos^{-1}\left(\sqrt{p_1}\right), \ldots, \cos^{-1}\left(\sqrt{p_n}\right)\right),$$
$$\underline{\phi} = \left(\cos^{-1}\left(\sqrt{q_1}\right), \ldots, \cos^{-1}\left(\sqrt{q_n}\right)\right).$$

We can use such a transformation to calculate the angle between any two multinomial realisations on the n-sphere. This is given in the below result.

Theorem 1. *The angle A_O between two multinomial realisations $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ with proportions of observations in each category $p_i = x_i/x_T, q_i = y_i/y_T$ is given by*

$$A_O = \cos^{-1}\left\{\sum_{i=1}^{n+1}\sqrt{p_i q_i\left[\prod_{j=0}^{i-1}(1-p_j)(1-q_j)\right]}\right\},$$

where $p_0 = q_0 = 0$, and $p_1 = q_1 = 1$.

Proof. We can represent these points in Cartesian co-ordinates in $(n+1)$ dimensions. That is,

$$\begin{aligned}
c_1 &= r\cos(\cos^{-1}(\sqrt{p_1})),\\
c_2 &= r\cos(\cos^{-1}(\sqrt{p_2}))\sin(\cos^{-1}(\sqrt{p_1})),\\
&\vdots\\
c_n &= r\cos(\cos^{-1}(\sqrt{p_n}))\prod_{i=1}^{n-1}\sin(\cos^{-1}(\sqrt{p_i})),\\
c_{n+1} &= r\prod_{i=1}^{n}\sin(\cos^{-1}(\sqrt{p_i})).
\end{aligned}$$

The radius is $r = \sqrt{\sum_{i=1}^{n+1} c_i^2}$. This representation can be tidied up, using the fact that $\sin(\cos^{-1}(z)) = \sqrt{1-z^2}$, to

$$
\begin{aligned}
c_1 &= r\sqrt{p_1}, \\
c_2 &= r\sqrt{p_2(1-p_1)}, \\
&\vdots \\
c_n &= r\sqrt{p_n\prod_{i=1}^{n-1}(1-p_i)}, \\
c_{n+1} &= r\sqrt{\prod_{i=1}^{n}(1-p_i)}.
\end{aligned}
$$

We denote the Euclidian co-ordinates for $\underline{\theta}$ as $(c_1(\underline{\theta}), \ldots, c_{n+1}(\underline{\theta}))$ and for $\underline{\phi}$ as $(c_1(\underline{\phi}), \ldots, c_{n+1}(\underline{\phi}))$. Then the angle between these two points is

$$
A_O = \cos^{-1}\left(\frac{\sum_{i=1}^{n+1} c_i(\underline{\theta})c_i(\underline{\phi})}{\sqrt{\sum_{i=1}^{n+1} c_i(\underline{\theta})^2 \sum_{i=1}^{n+1} c_i(\underline{\phi})^2}}\right).
$$

This reduces to the result given.

The angle has the nice property that it tends to zero for two multinomial realisations from the same underlying distribution as the sample sizes go to infinity. To see this, consider

$$
\begin{aligned}
\lim_{x_T, y_T \to \infty} A &= \cos^{-1}\left(1-\rho_n + \sum_{i=1}^{n}\sqrt{\rho_i^2\prod_{j=1}^{i-1}(1-\rho_j)^2}\right) \\
&= \cos^{-1}\left(1-\rho_n + \sum_{i=1}^{n}\rho_i\prod_{j=1}^{i-1}(1-\rho_j)\right) \\
&= \cos^{-1}(1) \\
&= 0.
\end{aligned}
$$

2.2 *The commutative property*

Upon inspection of the angle, A_O, in Theorem 1, it is apparent that the choice of label, i.e., i, which a category is assigned will influence the resulting value of the angle. That is, if the categories of the multinomial variables are re-ordered, then the angle between them using the Olbrich transformation will be different.

Consider a simple 2×2 table with the two categories being "blue" and "not blue". Here the test statistic reduces to one of the two following test statistics depending on which category is assigned to be the first category.

$$
\begin{aligned}
a_O &= \cos^{-1}\left(\sqrt{p_{blue}q_{blue}} + (1-p_{blue})(1-q_{blue})\right) \\
&\neq \cos^{-1}\left(\sqrt{(1-p_{blue})(1-q_{blue})} + p_{blue}q_{blue}\right).
\end{aligned}
$$

This non-commutative property is a result of the dependence structure in the probabilities which ensures that they sum to 1 over all categories. As such, if we re-define the probabilities used within the test such that they are conditionally independent then we will have a commutative representation of the angle between two multinomial realisations.

As such, by using probabilities conditionally independent on categories with a lower index value and following the same geometric transformation as in Olbrich's work we can obtain a commutative formula for the angle. This is given in the following theorem. The proof follows the same form as that for Theorem 1. It is left to the reader.

Theorem 2. *The angle A_G between two multinomial realisations $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ with conditional proportions of observations in each category given that they weren't in any previous categories $\gamma_i = x_i/x_{T_i}$, $\beta_i = y_i/y_{T_i}$, where $X_{T_i} = \sum_{j=i}^{n} x_j, Y_{T_i} = \sum_{j=i}^{n} y_j$, is given by*

$$
\begin{aligned}
A_G &= \cos^{-1}\left(\sum_{i=1}^{n+1}\sqrt{\gamma_i\beta_i\left[\prod_{j=1}^{i-1}(1-\gamma_i)(1-\beta_i)\right]}\right) \\
&= \cos^{-1}\left(\sum_{i=1}^{n}\sqrt{p_iq_i}\right),
\end{aligned}
$$

where $p_0 = q_0 = 0$, and $p_1 = q_1 = 1$.

2.3 *Geometric hypothesis test*

Suppose we have two multinomial realisations $\underline{x}$ and $\underline{y}$ with underlying probability vectors $\underline{p}$ and $\underline{q}$ respectively. We wish to test whether the two vectors come from the same underlying multinomial distribution. The hypothesis test will take the form

$$
\begin{aligned}
H_0 &: \underline{p} = \underline{q}, \\
H_1 &: \underline{p} \neq \underline{q}.
\end{aligned}
$$

The test statistic is

$$
A_G = \cos^{-1}\left(\sqrt{\sum_{i=1}^{n}\hat{p}_i\hat{q}_i}\right),
$$

for observed $\hat{p}_i = x_i/x_T, \hat{q}_i = y_i/y_T$. The p-value is then

$$
\Pr(a \geq A_G) \approx \frac{1}{N}\sum_{i=1}^{N} I(a_i \geq A_G),
$$

where N is a large number of simulated values of A_G under the assumption that H_0 is true. To calculate $a_1, \ldots, a_N$ we need to estimate the probability vector under the null hypothesis, $\underline{p}_0$. This is

$$
\underline{\hat{p}}_0 = \frac{1}{2} \times (\underline{\hat{p}}_1 + \underline{\hat{p}}_2).
$$

Thus we see that to perform the test we carry out a parametric bootstrap (Efron & Tibshirani 1993) on $\underline{p_0}$.

3 PROPERTIES OF THE TRANSFORMATION

We have evaluated the mean and standard deviation of the angle A_G resulting from the transformation of one multinomial variable compared with its mean. The aim is to develop some intuition concerning the behaviour of this transformation. We have considered the mean and standard deviation with respect to the underlying probabilities and sample size.

Specifically, we have used Maple 17 software to calculate the mean and standard deviation exactly for multinomial distributions with 3 to 10 categories. In varying the underlying probabilities we used the standard deviation of the probabilities, as this is related to the Euclidean distance of the vector of probabilities from the vector of equal probabilities. Our standard deviations range from 0 to 0.5. We give two figures below to illustrate the analysis. The overall conclusions made are based on the more comprehensive investigation.

In Figure 1 we see the change in the mean and standard deviation of A_G for a 3-dimensional multinomial distribution over different sample sizes. In the left hand plot the standard deviation is 0 and in the right hand plot it is 0.29. In Figure 2 we see the same two plots for a 10 dimensional multinomial distribution.

An interesting pattern in the mean of angle from the transformation is that it monotonically decreases as sample size increases. Our study considered 99 different combinations of probabilities, number of categories and sample sizes, from which we are ableto fit a curve to the relationship between the mean angle, the standard deviation of the probabilities and the number of samples. That is,

$$\overline{x}_A = 1.356 - 2.8 \times s_p + (0.8 \times s_p - 0.34)\log(n),$$

where $\overline{x}_A$ is the mean of A_G and s_p is the standard deviation of the probabilities. This excludes the cases with equal probability. The fit of the curve was very good with $R^2 = 87.8\%$, and it shows that the mean decreases at a rate $o(\log(n))$ and is not affected by the number of categories m. The standard deviation of the probabilities influences the mean in two ways; it decreases the mode and increases the rate of decay with respect to sample size.

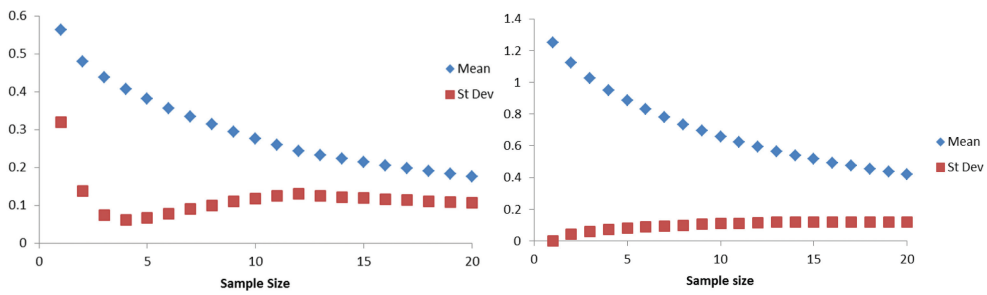


Figure 1. Mean and standard deviation of A_G for $m = 3$ with standard deviations of 0 (left) and 0.29 (right).

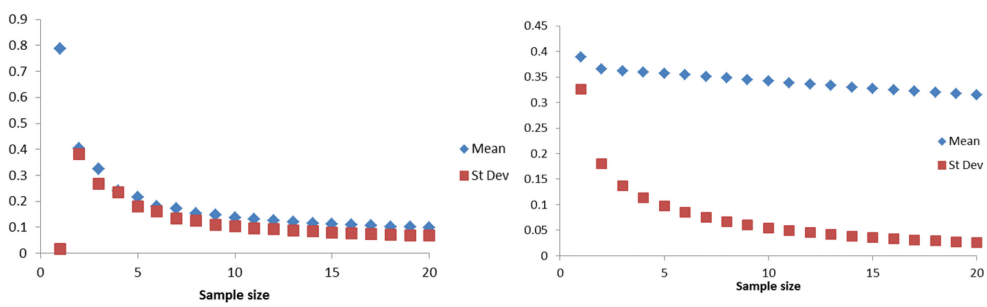


Figure 2. Mean and standard deviation of A_G for $m = 10$ with standard deviations of 0 (left) and 0.29 (right).

4 SIMULATION STUDY

4.1 *The distribution of A_G*

We wish to compare two multinomial realisations to test if they come from the same underlying distribution, i.e., if the have the same probability vector.

In Figure 3 we give histograms of the angle A_G for the trinomial distribution simulated with the same underlying probabilities for a range of different parameter vectors. In each case 10,000 pairs of points are simulated and there are 50 observations for each simulated point.

We see that in all cases the distribution of A_G has a mode which is close to zero and is right skewed. Of course, if the two realisations are the same then the angle between them will be 0.

We can carry out a similar simulation exercise for trinomial realisations which come from distributions with different underlying probability vectors. The resulting histograms are given in Figure 4. Again, each graph is the result of 10,000 simulations.

This time we see that the distributions of A_G are generally much more symmetric and have modes which are typically larger than in Figure 3. This suggests that A_G may be a useful statistic within the hypothesis test we have outlined in Section 2.3.

4.2 *Type I and Type II errors*

We will investigate the properties of the test with respect to Type I and Type II errors. All results are based on 1000 samples. The Type I error probabilities are given in Table 3 in the Appendix for two different probability vectors and different sample sizes. The probabilities from the Pearson Chi-squared test are also given.

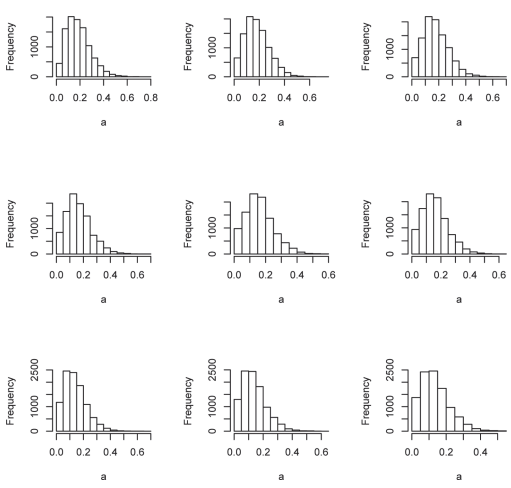


Figure 3. The distribution of A_G for 10,000 simulated pairs from the trinomial distribution with the same probability vector.

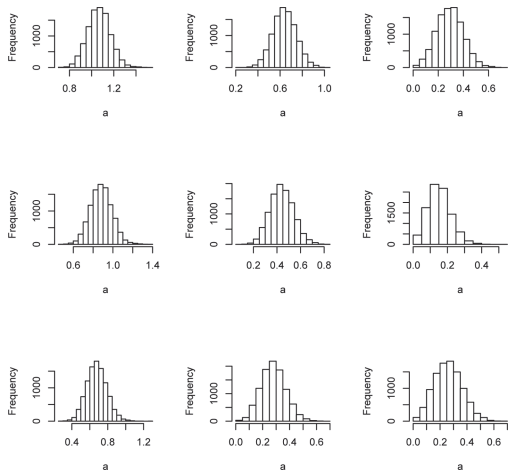


Figure 4. The distribution of A_G for 10,000 simulated pairs from the trinomial distribution with different probability vectors.

We see that, for $\underline{p}_1$ and $\underline{p}_2$ all three tests are performing fairly well, with the proportions of Type I errors being close to 0.05 for all tests over almost all sample sizes. This indicates that, for trinomials in which all of the categories have reasonably large probabilities, all of the tests perform satisfactorally with respect to Type I errors. However, for $\underline{p}_3$ in which there are small probabilities of being in some of the categories and hence small numbers of observations in those categories, all three tests have proportions of Type I errors well below 0.05 for a sample size of 5. The geometric test then performs well from a sample size of 10 whereas the other two tests are still making too few Type I errors up to a sample size of approximately 30.

The Type II errors are given in Table 4 in the Appendix. In Table 4 probabilities are $\underline{p}_1 = (1/3, 1/3, 1/3)$, $\underline{p}_2 = (1/2, 1/4, 1/4)$ and $\underline{p}_3 = (8/10, 1/10, 1/10)$. We see that the Geometric Test outperforms the other two tests for all combinations of probability vectors for sample sizes of 5 and 10. Beyond a sample size of 10 the Fisher Test, in particular, typically out-performs the Geometric Test. However, in this paper we are interested in situations where we have small probabilities and possibly few data and the in this case the Geometric Test give an improvement, albeit small, over the other two tests. When combined with its superior Type I error probabilities for the trinomial distribution with low probability events and this new Geomet-

ric Test looks to have some strengths over the two traditional tests.

5 ILLUSTRATIVE EXAMPLE

The illustrative example in this section is based on a desensitised version of real data. The numbers used are typical rather than specific values.

A company manufactures machinery which is then sold to operators in the power sector. As part of the contracts for the machinery the manufacturer guarantees specific levels of performance including reliability levels. There are different possible failure types of the machines which at a high level can be classified as Design, Installation, Maintenance and No Fault Found.

The reliability of the machinery depends on how it is operated and how it is maintained. This is not in the control of the manufacturer. It is suspected that there could be systematic differences between different regions as to the reliability of the sameequipment as a result of different operating procedures and different operating and maintenance capabilities.

Data have been collected on the numbers of failures by failure type and region and are given in Table 2.

We wish to test whether there are differences in the failure patterns across the different regions. The expected numbers of failures in each of the cells conditional on fixing the totals across rows and columns are given in brackets in Table 2.

Suppose we ask the question: is there a difference in the pattern of failures between Europe and North America? For the Pearson Test $p = 0.074$, for Fisher's Test $p = 0.090$ and so you cannot reject the null hypothesis that there is no difference in the pattern of failures between the two areas.

If we use the Geometric Test, however, we get a Test Statistic $A_G = 0.465$ which corresponds to a p-value of $p = 0.049$. Thus we see that the Geometric Test detects the difference between the two areas in this case when the Fisher and Pearson tests do not. This would make a difference to automatic identification of associations between factors that might provide insights into reliability behaviours.

Table 2. Contingency table of the number of failures of specific failure types across different regions.

Type/region	Europe	N America	Africa	Asia
Design	2 (5)	12 (12)	7 (6)	6 (4)
Installation	15 (11)	20 (25)	12 (12)	10 (9)
Maintenance	1 (1)	7 (3)	0 (1)	0 (1)
None Found	0 (1)	4 (3)	2 (1)	0 (1)

6 CONCLUSIONS

In this paper we have considered the analysis on contingency tables for numbers of failures in a reliability context. There will typically be some failure types with low probability and as such small numbers of realised failures in some of the cells in the contingency table. This means that the traditional Chi-Squared Test will be unsuitable and the most common alternative, Fisher's Test, is conservative meaning that statistically significant differences will be missed.

We have considered an alternative to these tests, which we have named the Geometric Test, which represents multinomial observations as points on the n-sphere. The test statistic is then the angle between the points and the p-value is approximated by sampling from the distribution under the null hypothesis. This new test out-performed the other two tests with respect to the Type I errors when some categories of the multinomial variable had small probability and with respect to Type II errors for small sample sizes.

There is much work still to be done for this method from both theoretical and applied perspectives. The test needs to be validated on a much larger simulation study and an investigation could be carried out into the theoretical properties of both the teststatistic and the test. There is also work to be done in evaluating the performance of the test in more than 3 dimensions and extending the test to more than two simultaneous miultinomial variables. It would also be interesting to benchmark the commutative test against the non-commutative transformation of Olbrich.

From an applied perspective, in order for the method to be useable for reliability practitioners it will be needed to be automated so that large numbers of simulations do not have to be run every time the test is performed.

REFERENCES

Cochran, W.G. (1954). Some methods for strengthening the common 2 tests. *Biometrics 10*(4), pp. 417–451.

Colombo, A. & P. Ihm (1988). A quasi-independence model to estimate failure rates. *Reliability Engineering and System Safety 21*, 309–318.

Conte, J., E. Rubio, A. Garcia, & F. Cano (2011). Occupational accidents model based on risk-injury affinity groups. *Safety Science 49*, 306–314.

Efron, B. & R. Tibshirani (1993). *An Introduction to the Bootstrap*. FL: Chapman and Hall/CRC.

Fisher, R.A. (1922). On the interpretation of 2 from contingency tables, and the calculation of p. *Journal of the Royal Statistical Society 85*(1), pp. 87–94.

Liddell, D. (1976). Practical tests of 2 2 contingency tables. *Journal of the Royal Statistical Society. Series D (The Statistician) 25*(4), pp. 295–304.

Maiti, J. & V. Khanzode (2009). Development of a relative risk model for roof and side fall fatal accidents in underground coal mines in india. *Safety Science 47*, 1068–1076.

Olbrich, E. (1965). Geometrische deutung der polynomialverteilung und einige folgerungen daraus. *Biometrische Zeitschrift 7*(2), 96–101.

Pearson, K. (1900). X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine Series 5 50*(302), 157–175.

Schneidewind, N. (1992). Methodology for validation software metrics. *IEEE Transactions on Software Engineering 18(5)*, 410–422.

APPENDIX

Table 3. Type I error probabilities for the three tests for various sample sizes.

Test	Probabilities	5	10	20	30	40	50	100
Geometric	$\underline{p}_1$	0.061	0.062	0.051	0.055	0.046	0.049	0.043
	$\underline{p}_2$	0.042	0.062	0.038	0.043	0.039	0.050	0.062
	$\underline{p}_3$	0.017	0.052	0.057	0.049	0.052	0.043	0.053
Pearson	$\underline{p}_1$	0.042	0.037	0.049	0.043	0.040	0.047	0.049
	$\underline{p}_2$	0.031	0.047	0.059	0.035	0.051	0.049	0.048
	$\underline{p}_3$	0.005	0.011	0.037	0.040	0.040	0.056	0.043
Fisher	$\underline{p}_1$	0.033	0.056	0.050	0.047	0.040	0.046	0.043
	$\underline{p}_2$	0.022	0.050	0.044	0.045	0.037	0.046	0.061
	$\underline{p}_3$	0.006	0.011	0.032	0.031	0.045	0.039	0.052

Table 4. Type II error probabilities for the three tests for various sample sizes.

Test	Probabilities	5	10	20	30	40	50	100
Geometric	$\underline{p}_1, \underline{p}_2$	0.917	0.915	0.885	0.790	0.741	0.688	0.449
	$\underline{p}_1, \underline{p}_3$	0.771	0.569	0.278	0.078	0.023	0.004	0.000
	$\underline{p}_2, \underline{p}_3$	0.893	0.783	0.643	0.448	0.292	0.171	0.011
Pearson	$\underline{p}_1, \underline{p}_2$	0.941	0.906	0.867	0.819	0.758	0.663	0.435
	$\underline{p}_1, \underline{p}_3$	0.812	0.540	0.197	0.061	0.021	0.003	0.000
	$\underline{p}_2, \underline{p}_3$	0.920	0.820	0.561	0.400	0.274	0.166	0.013
Fisher	$\underline{p}_1, \underline{p}_2$	0.953	0.924	0.885	0.797	0.753	0.698	0.443
	$\underline{p}_1, \underline{p}_3$	0.821	0.576	0.226	0.070	0.020	0.003	0.000
	$\underline{p}_2, \underline{p}_3$	0.913	0.818	0.601	0.416	0.281	0.172	0.009

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Assessment of a remaining working life of energetic devices using service data

M. Sykora, M. Holicky & J. Marková
Klokner Institute, Czech Technical University in Prague, Prague, Czech Republic

K. Presl
ČEZ, a.s., Prague, Czech Republic

ABSTRACT: Numerous fossil power stations in the Czech Republic and their key devices are reaching their design working life. The data from measurements and statistical methods may be applied with advantage for estimating a remaining working life. The paper discusses statistical methods appropriate for such analyses and provides suggestions for practical applications. Important steps of the analysis include selection of a suitable regression model and estimation of probability of exceeding a limiting value. Inherent randomness and trend of the observed parameter as well as statistical uncertainty due to a limited amount of the data should be taken into account. Aleatory uncertainties due to randomness and actual trend of the observed parameter as well as epistemic uncertainty due to lack of data and imprecision of a test method should be taken into account. Implementation of the theoretical procedures for the prediction of a remaining working life of important energetic devices is illustrated considering service data of the capacity of a generator and creep of steam piping.

1 INTRODUCTION

Numerous fossil power stations in the Czech Republic and their key devices are reaching their design working life. Effective maintenance plans, including time schedules, repair strategies and extent of repairs, should be based on credible estimates of the remaining working life of key energetic devices. That is why the monitoring systems are installed to provide operators with information concerning performance of energetic devices of production units of power stations.

Statistical analysis of monitoring data and outcomes of inspections may significantly improve estimates of the remaining working life of energetic devices. That is why the paper discusses statistical methods appropriate for such analyses. Basic tools, ready for daily use in the engineering practice, are recommended for major steps of the statistical analysis and suggestions for practical applications are provided.

2 BASIC STEPS OF STATISTICAL ANALYSIS

An operator of a power station commonly records an immense amount of measurements of technical parameters. Examples of the technical parameters (hereafter 'parameters') include:

- Parameters describing the creep of steam piping,
- Capacity of a generator,
- Outcomes of dissolved gas analysis, oil physical/chemical tests or tests of insulation of a transformer,
- Carbonation depths of concrete and corrosion rate of reinforcement in cooling towers etc.

Monitoring data can be used to predict a remaining working life of energetic devices (hereafter 'remaining life'). Statistical analysis of such data should include the following basic steps:

1. On the basis of expert judgements, parameters that may be used for prediction of a remaining life are identified and their measurements are collected. It is important to realise that different parameters may be selected for different production units.
2. The selected parameters are assigned by limiting values. When a limiting (critical) value is exceeded, a decision should be taken and device should be repaired or replaced.
3. Each statistical sample (set of measurements of a parameter) should be tested for outliers (minimum or maximum values). It is recommended to combine appropriate

graphical illustration of the data (e.g. by means of histograms) with statistical tests (for instance Grubbs' or Dixon's tests). Significance level (the probability that an extreme measurement is incorrectly detected as an outlier) is commonly selected as 0.05 or 0.01, Holicky (2013). When a cause of an outlying observation is identified (e.g. deviations from standard test conditions, human errors affecting measurements or incorrect records of data), the outlier is removed from the sample.

4. In case of the doubts about statistical dependence of parameters a correlation coefficient (Holicky (2013)) is determined. For a high degree of statistical dependence it may suffice to monitor one parameter only.
5. In the case of insufficient experimental data, Bayesian updating (JCSS (2001)) may be applied to combine information from different sources (few test results e.g. with measurements from different locations or devices with similar operating conditions, with results of theoretical models or with expert judgements). As an example, complex assessments of a steam turbine may be conducted in periods of about ten years and experience gained from other turbines can be then useful.

   Note that Bayesian updating allows updating estimates of remaining working life when new monitoring data become available.
6. To predict the trend of a parameter an appropriate regression model is selected on the basis of technical experience and its fit to the empirical data is verified.
7. When the parameter is proved to be dependent on a considered factor (device age, in-service time, number of starts etc.), boundaries of the regression curve and probabilities of exceeding limiting values are estimated.

Steps 6 and 7 concerning the prediction of parameters are described in detail in the following section.

3 PREDICTION OF PARAMETERS

Prediction aims to describe a principal trend of the parameter X with a considered time factor t. It may be important to take into account (or filter out) regular fluctuations around the regression curve caused by seasonal factors (such as increased power production in winter periods) and/or by long-term effects (resulting e.g. from a management plan of the power station).

In addition the parameter X is often fluctuating around the trend in a purely random manner. Such a random effect is normally time-independent and is caused by minor factors that are often difficult to identify. Examples of such factors may include unspecified deviations from 'standard' test conditions or measurement uncertainty (more specifically random component related to an individual measurement) due imprecision of a test method, testing device or minor human errors. Description of this random effect should be based on probabilistic methods and is an important part of the analysis.

Details of the regression analysis are provided in many publications, see e.g. Ang & Tang (2007) or Ryan (2008). In most cases linear, parabolic or exponential functions are used to describe the trend of X with t. An important assumption is that the operating conditions are same for a period covered by measurements and for a period of prediction.

The statistical prediction should consist of the following steps:

1. Considering technical experience with the parameter X, an appropriate regression model is selected. In common cases a linear model is appropriate:

$$X = \beta_0 + \beta_1 t + \varepsilon \tag{1}$$

   where β_0 and β_1 = regression coefficients; and ε = random error of the model.

   For some parameters physical evidence suggests a non-linear trend (e.g. exponential for parameters describing the creep of steam piping). If possible a non-linear relationship between X and t is then linearized by a suitable transform.
2. On the basis of a residual scatter (Ryan (2008)) a fit of a regression model and experimental data is assessed; normally the regression model is deemed appropriate for relatively high residual scatters, say over 0.6.
3. Dependence of X on t is verified by the test of a statistical hypothesis $\beta_1 = 0$ (commonly at a significance level of 0.05 or 0.01). If the hypothesis is rejected, the parameter X is assumed to be dependent on t. Otherwise the prediction hardly makes sense.
4. Prediction intervals of X are determined for a selected confidence level—probability that the parameter will be covered by the interval. A common confidence level is 0.95; however lower values (e.g. 0.75) may be accepted particularly in case of small sample sizes.
5. Probability P_{lim} of exceeding a limiting value is estimated for a selected value of t. Note that an acceptable value of P_{lim} should be established considering consequences associated with exceeding the limiting value. The consequences may considerably differ for various parameters—ranging from a requirement on the planned repair of a device to the need of

an immediate intervention causing unplanned outage of a production unit. That is why associated risks should be considered rather than probabilities, Sykora et al. (2013).

Relationships for prediction intervals and probability P_{lim} as well as more details on the prediction can be found in literature; Ang & Tang (2007), Holicky (2013) and Ryan (2008).

4 CASE STUDIES

4.1 *Capacity of generator*

The capacity of rod winding is considered as an important parameter for prediction of the remaining working life of a generator. Measurements of the capacity of a selected phase of the generator, taken at 100% of nominal voltage each about three years, are shown in Figure 1. No measurement is identified as an outlier. It appears that the capacity is significantly dependent on time (residual scatter is 0.63).

Figure 2 indicates variation of the probability P_{lim} of exceeding the limiting value with time. It follows that the probability is relatively high; for instance $P_{lim} = 0.15$ is predicted for year 2016.

It is important to realise that the width of the prediction interval (Fig. 1) and estimated probability P_{lim} (Fig. 2) are affected by different uncertainties:

- Aleatory uncertainties due to inherent variability of the observed parameter affected by properties of rod winding and service conditions,
- Epistemic uncertainties caused by lack of statistical data and imprecision of a test procedure (measurement uncertainty).

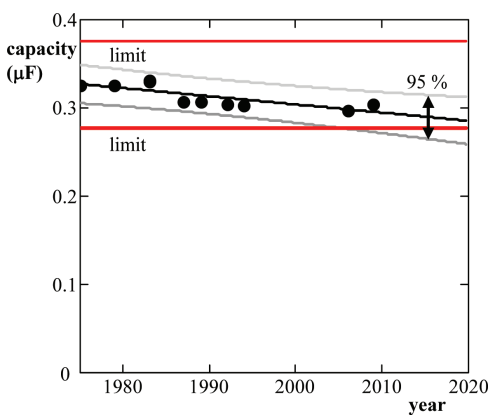


Figure 1. Variability of the capacity of a generator with time.

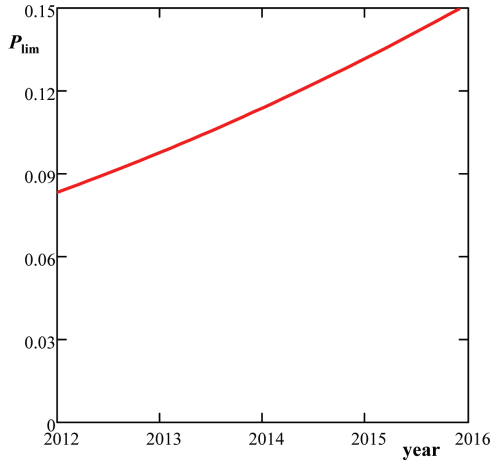


Figure 2. Variation of the probability P_{lim} of the capacity of a generator with time.

The former type of uncertainties is indeed a reason for regular monitoring. The latter uncertainties can be apparently reduced either by increased frequency of measurements or by the application of a more advanced test method.

In an illustrative example assume that a test method cannot be readily improved. The number of measurements n is then optimised to reduce the statistical uncertainty and minimise expected total costs C_{tot} related to a specified reference period. The optimum number of measurements can be assessed as:

$$\text{minimum}_n\ C_{tot}(n) = n \times C_1 + C_f \times P_{lim}(n) \qquad (2)$$

or, equivalently, using the standardised total costs:

$$\text{minimum}_n\ c_{tot}(n) = n + C_f / C_1 \times P_{lim}(n) \qquad (3)$$

where C_1 = all costs related to a single measurement; C_f = all costs related to exceeding the limiting value; and c_{tot} = total costs standardised by C_1.

The so-called pre-posterior analysis (JCSS (2008)) can be conducted to optimise decisions in regard to acquisition of new data. Consider that the total cost is optimised for a period from 2014 to 2020 and a decision can be to conduct zero to four measurements during this period (from 2014 each two years). In the pre-posterior analysis it is assumed that the future measurements will follow the trend indicated Figure 1. Note that in a more advanced analysis the assumption could be relaxed and e.g. influence of measurement uncertainty could be modelled.

The standardised total costs given in Equation (3) are optimised with respect to the

decision parameter n. Figure 3 shows the variation of the total costs c_{tot} and of the probability P_{lim} with the number of measurements n for two representative values of the cost ratio $C_f/C_1 = 10$ and 40. It can be concluded from Figure 3 that:

– For $C_f/C_1 = 10$: no measurement is taken since the total costs are affected more significantly by the cost of measurement than by the cost related to exceeding the limiting value,
– For $C_f/C_1 = 40$: one measurement is optimal.

Note that the optimum number of measurements may be significantly affected by a minimum period between the measurements. This period normally follows from a management plan, depending particularly on planned outages of a power plant.

In principle the result of a new measurement may affect an outcome of the prediction and thus a number of measurements should be re-optimised after each measurement.

4.2 *Creep of high-pressure steam piping*

The remaining working life of a high-pressure steam piping made of steel 15 128.5 is predicted. The piping has been in service for 22 years (absolute operating temperature 528 °C and pressure 9.6 MPa). The remaining working life is estimated using the Larson–Miller Parameter (LMP).

Values of LMP given by Rund et al. (2013) are based on results of creep tests that include stresses σ and time to rupture t provided by Kuboň (2011). Variation of σ with LMP is indicated in Figure 4. No measurement is identified as an outlier. Exponential relationship between LMP and σ is considered:

$$\sigma = \beta_0 - \exp \beta_1 t + \varepsilon \tag{4}$$

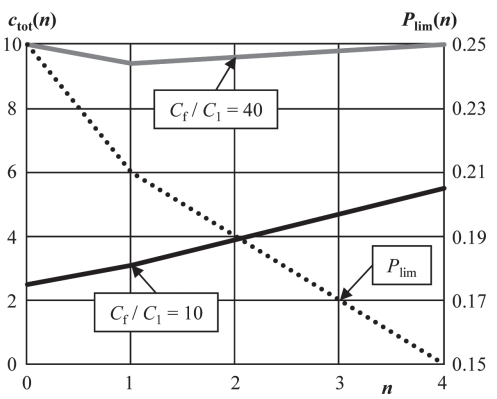


Figure 3. Variation of c_{tot} and P_{lim} with n for $C_f/C_1 = 10$ and 40 (example of the capacity of a generator).

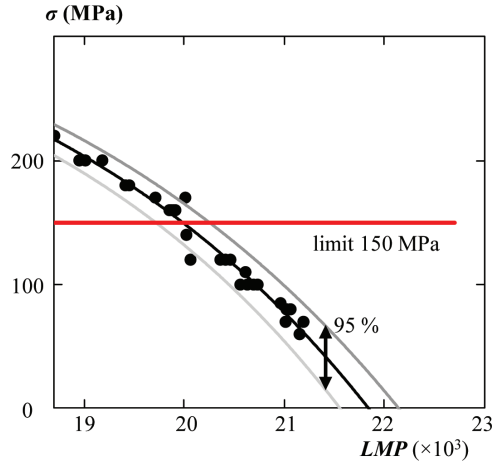


Figure 4. Variation of σ with parameter LMP (example of the creep of steam piping).

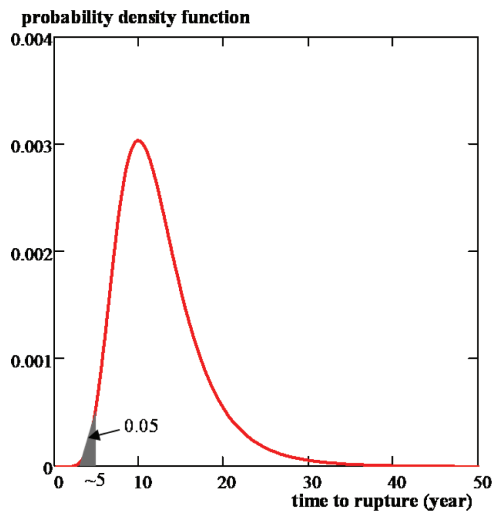


Figure 5. Probability density function of the time to exceeding the limiting value (example of the creep of steam piping).

The following transform enables to apply a linear regression:

$$\sigma' = \ln(\beta_0 - \sigma) \tag{5}$$

The following regression coefficients are obtained; $\beta_0 = 376$; and $\beta_1 = 2.71 \times 10^{-4}$. Prediction intervals and a limiting value are indicated in Figure 4.

It is assumed that the end of a working life of the piping is reached when the stress drops below 150 MPa. Probability density function of the time

to exceeding the limiting value (time to rupture) in shown in Figure 5.

The acceptable value of P_{lim}, needed to estimate a remaining working life, could be established on the basis of risk-informed decision making similarly as for the capacity of a generator. For illustrative purposes a value of 0.05 is considered and remaining working life is then estimated as about five years (Fig. 5).

5 DISCUSSION

The present contribution proposes a procedure for the prediction of a remaining life of energetic devices using monitoring data. The procedure is intentionally simplified for daily use in the engineering practice. It is recommended to supplement such an analysis by more advanced theoretical procedures whenever validity of the accepted assumptions is doubtful or significant deterioration mechanism (for instance with rapid progress) is detected. Examples of more advanced procedures were presented e.g. by Hammer et al. (2012), Wang et al. (2011), Wei et al. (2013) or in documents of the Electric Power Research Institute EPRI.

In particular due attention should be paid to effects of spatial variability of investigated technical parameters that may play an important role in the prediction. These effects should be taken into account when assessing large surfaces exposed to unfavourable environment such as for steam piping or cooling towers. Numerous models for spatial variability are available, see e.g. Allaix et al. (2009) or Sykora & Holicky (2013).

6 CONCLUSIONS

Methods of mathematical statistics provide efficient tools for the analysis of monitoring data concerning energetic devices. Important steps of the analysis include selection of a suitable regression model and estimation of probability of exceeding a limiting value. Aleatory uncertainties due to randomness and trend of the observed parameter as well as epistemic uncertainties due to lack of data and imprecision of a test method should be taken into account.

ACKNOWLEDGEMENTS

This study has been conducted at the Czech Technical University in Prague, Klokner Institute, within the research project TACR TE01020068 Centre of research and experimental development of reliable energy production supported by the Technology Agency of the Czech Republic.

REFERENCES

Allaix, D.L., Carbone, V.I. & Mancini, G. 2009. Recent advances in the modelling of space-variant structural properties. In H. Furuta, D.M. Frangopol & M. Shinozuka (eds.), *Proc. ICOSSAR 2009, Osaka, 13–17 September 2009.* Leiden: CRC Press/Balkema.

Ang, A.H.S. & Tang, W.H. 2007. *Probabilistic Concepts in Engineering Emphasis on Applications to Civil and Environmental Engineering*. USA: John Wiley & Sons.

Hammer, M., Ertl, J. & Janda, O. 2012. Estimation of Reliability Characteristics of Power Oil Transformers. *Engineering Mechanics* 19(1): 61–73.

Holicky, M. 2013. *Introduction to Probability and Statistics for Engineers*. Heidelberg: Springer.

JCSS 2001. *JCSS Probabilistic Model Code.* Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>.

JCSS 2008. *Risk Assessment in Engineering—Principles, System Representation & Risk Criteria*. Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>.

Kuboň, Z. 2011. Metody and způsoby hodnocení creepových vlastností ocelí and jejich úskalí (Methods and approaches to assessment of creep properties and their deficiencies—in Czech). *Proc. konference KOTLE A ENERGETICKÁ ZAŘÍZENÍ 2011, Brno, 14.–16.3.2011.*

Rund, M., Janovec, J. & Svobodová, M. 2013. Reziduální životnosti parovodů z oceli 15 128.5 (Residual service life of steam piping made of steel 15 128.5—in Czech). *Proc. 8. konference "Zvyšování životnosti komponent energetických zařízení v elektrárnách", Srní, 22.-24. říjen 2013.* Plzeň: Západočeská univerzita Plzeň.

Ryan, T.P. 2008. *Modern Regression Methods.* John Wiley & Sons.

Sykora, M. & Holicky, M. 2013. Durability assessment of large surfaces. In G. Deodatis, B.R. Ellingwood & D.M. Frangopol (eds.), *Proc. ICOSSAR 2013, New York, 16–20 June 2013.* Leiden (The Netherlands): CRC Press/Balkema.

Sykora, M., Holicky, M. & Markova, J. 2013. Risk Analysis of Production Units in a Power Station Using Bayesian Networks. In R.D.J.M. Steenbergen, P. Van Gelder, S. Miraglia & A.C.W.M. Vrouwenvelder (eds.), *Proc. ESREL 2013, Amsterdam, 29 September–2 October 2013.* Leiden: CRC Press/Balkema.

Wang, Y., Gong, S. & Grzybowski, S. 2011. Reliability Evaluation Method for Oil-Paper Insulation in Power Transformers. *Energies* 4(9): 1362–1375.

Wei, Z., Yang, F., Lin, B., Luo, L., Konson, D. & Nikbin, K. 2013. Deterministic and probabilistic creep–fatigue–oxidation crack growth modeling. *Probabilistic Engineering Mechanics* 33(0): 126–134.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Model for Information Quality determination of teleinformation systems of transport

M. Stawowy
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: This paper discusses a model for determining Information Quality (IQ) of teleinformation systems based on modeling the Certainty Factor (CF). This modeling practice is usually used for expert or artificial intelligence systems. Here, however, discussed are computer systems using data of teleinformation systems. Modeling CF is one of method, which can get information about properties of system when we have not full data to have it. Model was developed by Buchanan, Shortliffe for the rule system MYCIN at 1975 on Stanford University. I will try use this method to receive factor that will tell me "how good is this system which I analyzing". At the end I will show computer program to simulate different value to receive different result.

1 INTRODUCTION

In data communication systems intended for transport Information Quality (IQ) has a strong effect on traffic safety of vehicles. Particularly with regard to data communication information related to supervision over traffic received from different detectors. Data transmission and all measurements performed using those detectors can be burdened with various errors, which will introduce some scope of information uncertainty. The uncertainty may indicate the quality of information. The lower the uncertainty the higher the information quality.

Information quality is caused by many factors. As presented on Figure 1 information quality includes:

1. **relativity**—information meets the recipient's needs and is of essential importance for him/her,
2. **accuracy**—information is relevant to the level of knowledge represented by the recipient, defines the subject precisely,
3. **relevance**—information is never out-of-date, its updating cycle is consistent with its content,
4. **completeness**—information contains an optimal number of data, which is sufficient to process the information into specific knowledge, the level of detail depends on the recipient's needs,
5. **consistency**—particular elements and data correspond with each other, the form corresponds to the content, data updates are consistent with the objectives,
6. **suitability**—suitable presentation of information as well as description associated with the presentation ensuring correct interpretation,
7. **availability**—information is available when it is needed by competent recipients,
8. **credibility**—information confirms the authenticity of the data, contains elements ensuring the reliability of the message,
9. **congruence**—the information is consistent with different information, interpreted in the proper context.

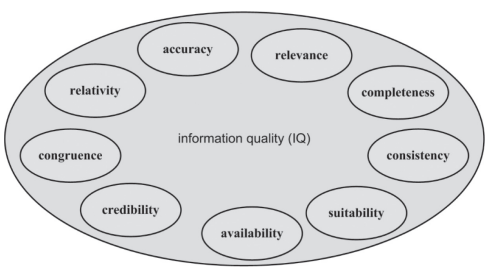


Figure 1. Components of information quality in technical terms. Prepared by the author based on Olaisen 1990 and Encyklopedia zarządzania and MITIQ.

In order to estimate the information quality of a selected system you should model the uncertainty the reverse of which could indicate IQ. Uncertainty can be modelled by using, among others, Bayesian networks. However, in this case, the data come from various sources and to simplify the modelling, and thereby calculation, could be used the theory mathematical evidence created by Dempster and Shafer. However, since we assess information from computer systems (modern detectors and

data transmission systems are controlled using microcontrollers), and the analysis they perform is a string of decisions (algorithms executed by the controllers), could be model the certainty factor of a hypothesis (CF Certainty Factor) (Shortliffe & Buchanan 1984, Heckerman 1992, Stawowy 2013) used in expert and artificial intelligence systems. Here it is necessary to make an assumption that the CF designated for a suggested model will be the sought IQ.

Usually, known publications talking about statistical models like Vinay & Khelil & Suri 2010 or Weng & Vespa 2011. Uncertainty models usually are used in management or logistic like in Rodrigues, Stantchev, Potter, Naim, & Whiteing, A. 2008. Presented work by Raghunathan 1999 was similar but not used presented in this article.

2 MODELLING THE CERTAINTY FACTOR OF A HYPOTHESIS FOR A DATA COMMUNICATION SYSTEM

The first part of this chapter specifies the dependencies used to calculate the values of the CF. It results from the variable directions of development of this method.

2.1 *Modelling the certainty factor of a hypothesis*

The formal simplified description of the certainty factor is as follows:

$$CF_{(s)} = MB_{(s)} - MD_{(s)} \tag{1}$$

where: *CF*—certainty factor, *MB*—reflection of knowledge, that is measure of belief, *MD*—reflection of ignorance, that is measure of disbelief, *s*—hypothesis based on some information.

It is important to remember that:

$$MB \to [0,1]; MD \to [0,1] \text{ that } CF \in [-1,1] \tag{2}$$

So, as it results from formula 2 the result of the calculations should fit within the range from –1 to 1. The value of 1 will indicate the highest IQ.

A model using the CF can be presented in the form of a graph where the nodes are the observations and the hypotheses. The branches are the certainty factors of the hypotheses. A simple models has been presented on Figure 2a and 2b.

The whole begins from observation nodes (e1, e2). The following dependence has been used for calculation of parallel CFs (Heckerman 1992):

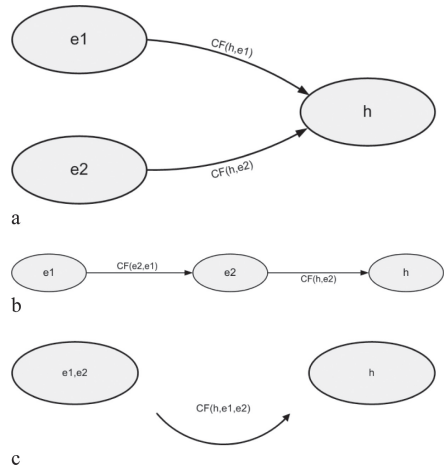


Figure 2. Sample CF models: a) parallel, b) serial, c) folded down. Prepared by the author.

$$CF_{(h,e1,e2)} = \begin{cases} CF_{(h,e1)} + CF_{(h,e2)} - CF_{(h,e1)} \cdot CF_{(h,e2)}, & CF_{(h,e1)} \text{ and } CF_{(h,e2)} \geq 0 \\ \dfrac{CF_{(h,e1)} + CF_{(h,e2)}}{1 - \min(|CF_{(h,e1)}|; |CF_{(h,e2)}|)}, & CF_{(h,e1)} \cdot CF_{(h,e2)} < 0 \\ CF_{(h,e1)} + CF_{(h,e2)} + CF_{(h,e1)} \cdot CF_{(h,e2)}, & CF_{(h,e1)} \text{ and } CF_{(h,e2)} < 0 \end{cases} \tag{3}$$

The following dependence has been used for calculation of serial CFs (Heckerman 1992):

$$CF_{(h,e1,e2)} = \begin{cases} CF_{(e2,e1)} \cdot CF_{(h,e2)}, & CF_{(e2,e1)} > 0 \\ 0, & CF_{(e2,e1)} \leq 0 \end{cases} \tag{4}$$

Using formulas 3 and 4 and the graphs (Fig. 2a and 2b) can folded down to a single branch with two nodes and the CF of this branch will be the sought value of the certainty factor of a hypothesis like on Figure 2c.

2.2 *Certainty factor model for a data communication system in transport*

A data communication system is a constituent part of a larger thematic system. For this reason, the telematic system has been described along with modelling in order to show the degree of influence on information quality held by the data communication part. A telematics system (e.g.: motorway) consists of many elements, such as: traffic supervision and measurement, monitoring, toll collection, meteo, display of information for drivers, signs with variable content, alert and service communication, data transmission, radio road information and integrated

control (Wawrzyński 2003). Each of these elements has specific requirements with regard to the quality and credibility of information. There is plenty of those characteristics and due to the limited volume of this study the modelling has been limited to one of the elements of motorway telematics. Traffic supervision and measurement has been chosen as this demonstratory element.

Traffic supervision and measurement usually include:

1. Proximity sensors such as inductive loops or detectors using infrared radiation.
2. Video detectors measuring the occupancy or speed of vehicles live and in the mean measurement value mode as well as identifying and counting the vehicles.
3. Data transmission routes.
4. Data interpretation tools.

Only one of the aforementioned components will be used for further modelling. Namely the video detector will be used to measure the speed of vehicles live (Jelušić, Anžek & Ivanković 2010, Stawowy 2013).

2.3 *Principle of measurement of the speed of vehicles using a video detector*

The sequence of images is transferred for analysis via cameras. The analyser detects the location of vehicles on subsequent frames of the image sequence. Displacement is then measured. After considering the time of the displacement one can determine the speed of those vehicles. Figure 3 presents the window of the speed measurement program using virtual vehicle displacement detectors (Stawowy 1997, Kędzierska, M. & Jasionek 2004).

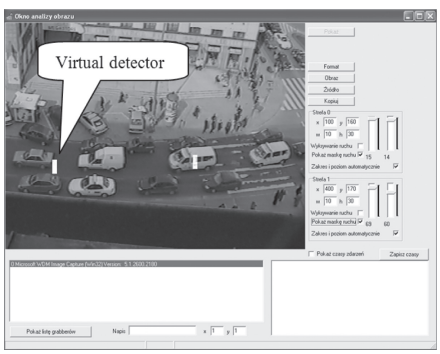


Figure 3. Window of the speed measurement program using virtual vehicle displacement detectors. Prepared by the author. The program has been written by the author of this article.

2.3.1 *Modelling the certainty factor of a hypothesis*

The first stage of analysis in such a measurement speed system is movement detection. The usual in this kind of video data analysis systems problem is interference (unwanted information). Especially in systems based on differential image analysis. Also the first stage of a decision will be whether we are dealing with motion of an object or noises or some other phenomena causing similar changes in the image as a moving vehicle. Therefore, it can be identified that we are dealing with two states of observation:

1. Movement occurred,
2. detection error.

A detection error can be broken down into different causes, which may be subsequent states of observation:

1. scene interference,
2. software failure,
3. data sent incorrectly.

So ultimately there may be more states of observation:

e1.1. movement occurred.
e1.2. scene image interference,
e1.3. software failure,
e1.4. data sent incorrectly.

At a further stage in order to measure the speed you should be certain that you have detected the locations of the same object of in two different places. Using the method of location of vehicles using virtual detectors you can distinguish such states of observation as:

e2.1. Moving object detected,
e2.2. software failure,
e2.3. data sent incorrectly.

The next node will have such states of observation as:

e3.1. Moving object detected by subsequent virtual detector,
e3.2. moving object not detected by subsequent virtual detector,
e3.3. detected object is not the same object as the one detected by the previous virtual detector,
e3.4. software failure,
e3.5. data sent incorrectly.

The last step is determination of the speed. The following states of observation will be present at this stage:

e4.1. speed determined,
e4.2. incorrect time measurement,
e4.3. software failure,
e4.4. computer system breakdown.

The graph for such a model is quite complicated, since we have transitions made of several layers. Intermediate hypotheses have been inserted to simplify the model. This is made possible by dependencies 3 and 4 described in the previous sub-chapter. Intermediate hypotheses can be subsequently determined in such a way:

h1. Movement detected,
h2. moving object detected,
h3. moving object detected by subsequent video detector,
h4. speed measured.

Figure 4 presents parallel graph of the model including all assumptions. Figure 5 presents serial graph of the model in second stage, after folded down parallel calculation. Graph is serial because

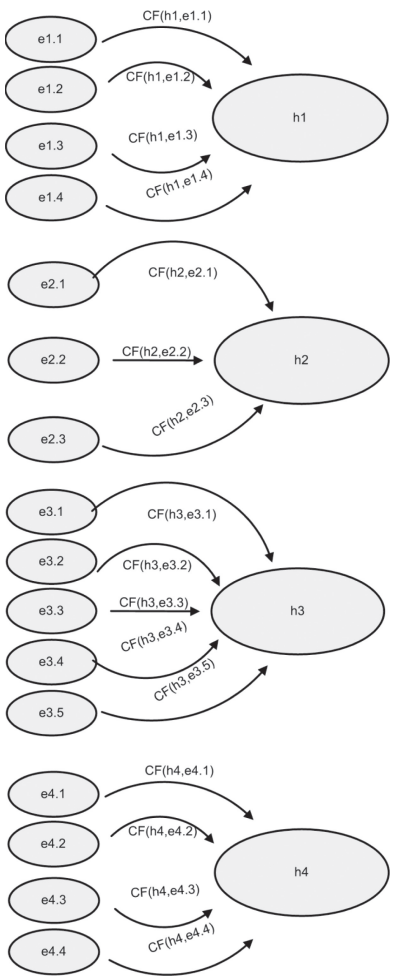


Figure 4. CF parallel model graphs. Prepared by the author.

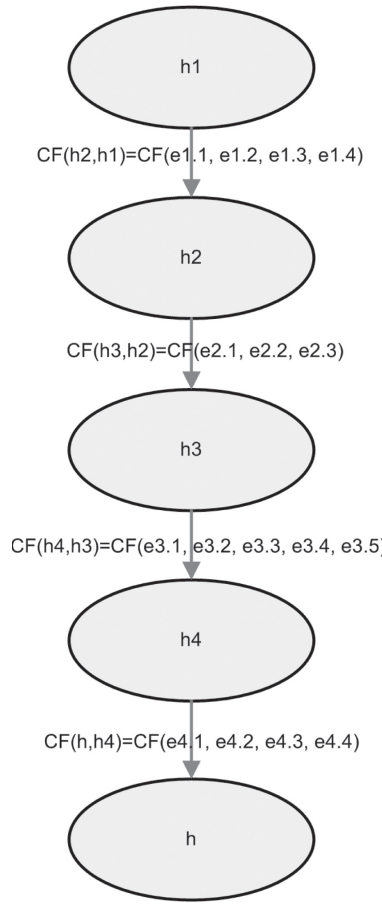


Figure 5. CF serial model graphs. Prepared by the author.

hypotheses are dependent on. It is mean that next hypotheses may not be met without previous. (Heckerman 1992, Stawowy 2013).

3 SAMPLE CALCULATION

The first calculation involves simplification aimed at determination of certainty factors of the intermediate hypotheses which will consist of subsequent CF calculations on the basis of formulas 3 and 4.

Subsequent values of certainty factors of the hypotheses are presented in Table 2. These values are not real but near to reals. Used only for demonstration methods possibilities.

According to the assumptions from chapter one the IQ of the modelled system is 0.5504. IQ was calculated by program special written for it.

4 SIMULATION OF EXAMPLE

A special program has been written in order to conduct the simulation. This program uses normal distributions with a standard deviation of 10% of the mean value. The distributions have been limited with a range of values that may be accepted by the CF according to formula 2. The values of subsequent CFs from Table 1 have been substituted as mean values. The number of repetitions of the simulation amounted to 10000. The result of the simulation is presented in Figure 6 (Meeker 1998). There is a density function of CF.

Comparing values $CF_{(h1, e1.1)}$ as well as $CF_{(h2, e2.1)}$ it would seem that $CF_{(e1.1, e1.2, e1.3, e1.4)}$ should be higher than $CF_{(e2.1, e2.2, e2.3)}$. However, this is not so due to the high impact of parameter $CF_{(h1, e1.2)}$. The courses also show which of the hypotheses affects the IQ the most negatively. In this case this was hypothesis h1 described as *movement detected* in chapter 2.3.1.

The next stage dealt with simulation of determination of hypothesis h1 using the same principles and values as in the IQ simulation. Figure 6 presents such a simulation. The courses of the distributions of parameters $CF_{(h1, e1.3)}$ and $CF_{(h1, e1.4)}$ overlap through a separated resolution of the simulation.

Figure 8 presents the simulation of hypothesis h1 with parameter $CF_{(h1, e1.2)}$ changed from –0.1 to –0.02. As a result, this significantly influenced the location of the values of hypothesis h1 during the simulation.

5 SUMMARY

This paper presents the method of determination of Information Quality (IQ) of a data communication system as a subsystem of motorway telematics with the use of modelling of the certainty factor of a hypothesis. After applying this type modelling gives

Table 1. Assignment of particular CF values. Prepared by the author.

h1	h2	h3	h4
CF(h1, e1.1) = 0.9	CF(h2, e2.1) = 0.8	CF(h3, e3.1) = 0.99	CF (h4, e4.1) = 0.99999
CF(h1, e1.2) = –0.1	CF(h2, e2.2) = –0.1 * 10^{-3}	CF(h3, e3.2) = –0.001	CF (h4, e4.2) = –0.1 * 10^{-3}
CF(h1, e1.3) = –0.1 * 10^{-3}	CF(h2, e2.3) = –0.3 * 10^{-4}	CF(h3, e3.3) = –0.1 * 10^{-3}	CF (h4, e4.3) = –0.3 * 10^{-4}
CF(h1, e1.4) = –0.5 * 10^{-6}		CF(h3, e3.4) = –0.3 * 10^{-4}	CF(h4, e4.4) = –0.3 * 10^{-4}
		CF(h3, e3.5) = –0.25 * 10^{-4}	

Table 2. Subsequent values of CF and value of IQ. Prepared by the author.

CF	Value
CF(e1.1, e1.2, e1.3, e1.4)	0,7098
CF(e2.1, e2.2, e2.3)	0,7998
CF(e3.1, e3.2, e3.3, e3.4, e3.5)	0,9698
CF(e4.1, e4.2, e4.3, e4.4)	0,9997
IQ	0,5504

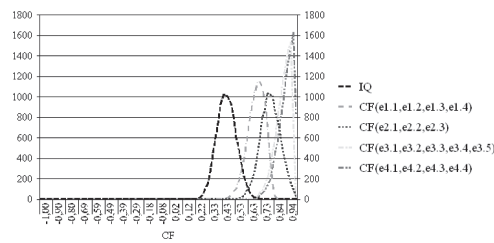


Figure 6. Result of simulation made for the examined example. Prepared by program written by the author.

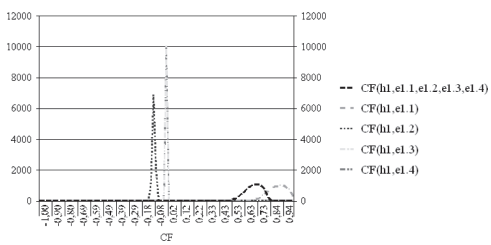


Figure 7. Result of simulation made for hypothesis h1 and unchanged CF parameters. Prepared by program written by the author.

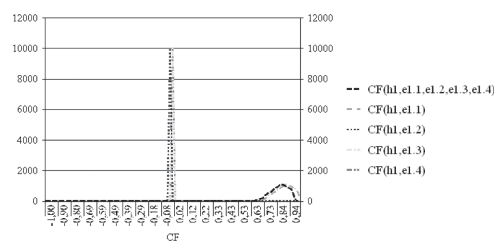


Figure 8. Result of simulation made for hypothesis h1 for $CF_{(h1, e1.2)}$ = –0.02. Prepared by program written by the author.

the possibility to connect many various properties of the examined analysis process such as: reliability of system elements, quality of the selected measuring method, quality of the data warehouse as well as safety resulting from the certainty of data.

It should be noted that subsequent stages of calculations are quite replicable and thereby easy to implement as a computer program or a computer simulation.

It also presents sample calculations for a real live speed measurement system. Used more and more for supervision of public road traffic.

Also a simulation of the example has been made using normal distributions of CF observations. The simulation demonstrated the possibility to identify the weakest link of the system. The simulation has also demonstrated the impact of the weakest link on the final result.

The results are intuitively correct, however, at the next stage this examination they should be compared with other methods of determining of information quality. One should also consider more measurement errors, which have not been considered in this model.

REFERENCES

Encyklopedia zarządzania. 2014. mfiles.pl/pl/index.php.

Heckerman D. 1992. The certainty-factor model. In S. Shapiro, editor, *Encyclopedia of Artificial Intelligence, Second Edition*, pages 131–138. New York: Wiley.

Jelušić, N., Anžek, M., & Ivanković, B. 2010. Information Source Quality in Intelligent Transport Systems. *PROMET-Traffic&Transportation*, 22(2), 125–131. Zagrzeb.

Kędzierska, M. & Jasionek P. 2004. Wizyjna detekcja ruchu pojazdów. M.Sc dissertation under supervision of Marek Stawowy. *Politechnika Warszawska Wydział Transportu*. Warszawa.

Meeker, W.Q., Escobar L. 1998. Statistical methods for reliability data. US and Canada: John Wiley & Sons Inc.

MITIQ MIT Information Quality Program. 2014. *http://mitiq.mit.edu*.

Olaisen, J. 1990. Information quality factors and the cognitive authority of electronic information. Wormell, I. (Ed.), *Information Quality: definitions and dimensions*, London: Taylor Graham.

Raghunathan, S. 1999. Impact of information quality and decision-maker quality on decision quality: a theoretical model and simulation analysis. *Decision Support Systems* 26 1999. 275–286. Dallas.

Rodrigues, V.S., Stantchev, D., Potter, A., Naim, M., & Whiteing, A. 2008. Establishing a transport operation focused uncertainty model for the supply chain. *International Journal of Physical Distribution & Logistics Management*, *38*(5), 388–411. UK.

Shortliffe, E.H. & Buchanan, B.G. 1984. Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. USA & Canada: *Addison-Wesley Publishing Co., Inc.*

Stawowy, M. 1997. Zastosowanie analizy obrazu do rozwiązywania zagadnień transportowych. *Raport Prace IPI PAN*, nr 862, Warszawa.

Stawowy, M. 2013. Wyznaczanie jakości informacji w telematyce autostradowej. *Prace naukowe—Transport* ISSN 1230-9265. 92/2013: 221–229. Warszawa.

Vinay, S. & Khelil, A. & Suri, N. 2010. Quality of information in wireless sensor networks: A survey. *International Conference on Information Quality 2010*. Germany.

Wawrzyński, W. 2003. Modelling elements of a telematic transportation system. *Zeszyty Naukowe. Transport/Politechnika Śląska*, 551–556. Poland.

Weng, Ning, I. Li, & Vespa, L. 2011. Information quality model and optimization for 802.15. 4-based wireless sensor networks. *Journal of Network and Computer Applications* 34.6 (2011): 1773–1783. USA.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A framework proposal to analyse the performance of assets under complex system

T. Grubessich, E. Johns, P. Viveros, R. Stegmaier & F. Kristjanpoller
Department of Industrial Engineering, Universidad Técnica Federico Santa María, Valparaíso, Chile

ABSTRACT: The historical analysis of the information is fundamental to support studies based on indicators of performance of a process and to feed representative models of the real system. Both studies are very im-portant for management and control of the processes as well as for the decision making of the enterprises. It is very important that this analysis represent effectively the system, since every deviation produced can lead to mistaken decisions. In this paper a methodological proposal is set up that incorporates additional activities to the traditional approach of the analysis and through which we can obtain results according to the reality of the system. The difference between both methodologies, is that in the methodological proposal is analysed the impact of the detentions of one equipment in the rest of the equipments, analyzing the consequences of the detention of the equipment of the system. The same effect is analysed when the detention in the system is produced by other reasons to the equipments. The differences between the results of both methodologies are appreciated to an equipment level, since to system level the indicators of performance are the same. However, the differences to an equipment level can be relevant, determining indicators significantly different and be-havior representations very different, being this last one of large importance at the moment of creating models to the system.

1 INTRODUCTION AND PROBLEM STATEMENT

The historical analysis of the information is fundamental for the realization of studies in varied areas within the organizations. The main benefit of this type of analysis is to increase the comprehension grade the system possesses, and taking this basis, varied possibilities are open to deepen the knowledge so much to support the management of the system as to support the process of the associated decision making.

Within the most concrete applications that can be done about the historical analysis of the information, is the definition of the actual and past state of the process through the indicators of performance. Some of the indicators considered are related to with reliability, maintenance, availability and utilization, among others (Ahmada & Dhafrb, 2002; Calixto, 2013; Muchiri et al, 2013, Van Horenbeek & Pintelon, 2014), in order to describe the functioning as much of the equipments, as of the system in a global manner. This analysis helps the detection of opportunities of improvement and the information here obtained is fundamental for a in a second analysis will be defined a behavior of the equipments according to the different perspectives that will be of interest (Sharma & Kumar, 2008; Viveros et al, 2012). Some of these perspectives of study are the time between failures, repairing time, production rates, among others.

In addition, when to this information we incorporate the logic of the functioning of the system (Distefano & Puliafito, 2009; Jau-Chuan & Yunn-Kuang, 2007; Singh & Goel, 1995; Zio et al, 2006) is possible to build a representation of the system that allows to carry out deeper and powerful studies from varied points of view and interests, such as impact of new investments in equipments in equipments, possible adjustments in the maintenance policies, changes in the design of the process, etc.

To carry out the above mentioned, appear diverse types of models that set up methodologies to represent the system (Bause & Kritzinger, 2002; Buzacott & Shanthikumar, 1993; Fuqua, 2003; Schryver et al, 2012; Zio & Pedroni, 2010). Some of these models are: mathematical models, stochastic models, deterministic models, simulation models for discrete events, Markov chains, among others. Each of these models, achieve different representation grades of the system, so its correct selection is relevant to accomplish with the desired objectives. On the other hand, each model possesses different requirements of information and development times, since many times is not possible to apply any model to a specific system.

Nevertheless, in order the model represent correctly the real system without matter of the type used, is fundamental that the behavior of the equipments and of the system will be well defined, and this will be closely related with the study of the historical information to be carried out. Any deficiency in this study directly rebounds in the model with such an impact that could invalidate the conclusions obtained. Is here where takes root the importance of the study of the historical information carried out.

Having in consideration the above mentioned, we present this document, which aims to propose a methodology for the historical information analysis of the assets in a complex process, in order to assure the correct presentation of the interactions between the equipments of the system.

With respect to the study of the historical information, where there have been detected in varied experiences in the national industry such as mining, cellulose, water treatment, present bankrupts that can engage the analysis validity, so it is considered that one methodology that guide the way to carry out the study of the historical information, is relevant and necessary.

As mentioned before, when there is a mistake, the main impact in the study of the historical information, are bankrupts in the definition of the behavior of the involved equipments and its aftermath in the system. These bankrupts lead to deviations between the generated model and the real system. The origins of these bankrupts are factors that aren't full analyze. Two of these factors are considered relevant due to the impact and the frequency they have are the way in which are analyzed the operational detentions. Will define what is understood for both factors as follows:

– The state change propagation consists of failures or detentions of individual equipments that induces an effect of total or partial functioning of the system.
– On the other hand, the operational detentions are produced by forced detentions, product of external phenomenon to the system by proper conditions of the process and that affect to the system in its grouping. Some examples of this type of detention are: supply failures, social problems, environmental, internal of the productive process (material lack to produce, accidents, etc.) design problems of the process that lead to detentions, among others.

When these effects are not considered in all its dimensions, is used to finish describing the behavior of the equipments with deviations to the reality, which generates mistakes at the moment to represent to the system through a model that incorporate those equipments. The impact of this deviation is difficult to quantify since it depends on the features of the system, however it is noticed that even can incite the model to miss its validity.

From the described situation, it is necessary to generate a methodology that supports the phase of the analysis of the historical information of the equipments of the process of the system and of the external factors that affect the system, in order to describe correctly the behavior of the system and its parts.

In order to ensure a correct description methodology proposal, this paper contains the following sections: a description of the proposed methodology and the traditional method, a numerical example where the proposed methodology is applied and compared with the traditional method and the conclusions of the study.

2 METHODOLOGY PROPOSAL

In order to explain the proposed methodology for the study of the historical information of a determined process, first it will be explained, in general, how to treat the historical information. As of this information, it will be shown how to work with it until reach the required information with an adequate format using the traditional focus. Then, will be shown how the methodology proposal functions from the same historical information and the differences with the present way of work.

2.1 *General scheme of analysis*

To start with the explanation, is necessary to understand what is the basis information needed, how and when is generated. For this, first is presented the following scheme that shows the main phases that lead, generally, to the study of the historical information (Fig. 1).

As we appreciate in the scheme, there exist activities that must be performed before applying the methodology of the historical information as with the traditional approach or the methodology proposal. These activities correspond to: to obtain the data base that contains the relevant information, the uprising of the logical configurations of the system failure and from the two formers, to create the unified data base with all the relevant information and in an adequate format. To understand a little more about these activities, will give a short description of each of them as following.

Data base of varied sources: the data required are those concerning to the events of failure and the repair of the equipments related to the system. These data generally come from operations and maintenance area of the organization (Bunea et al, 2008; Caldeira et al, 2013; Kans). Each organiza-

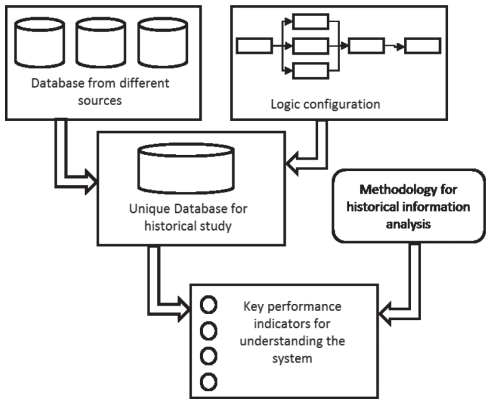


Figure 1. Scheme for historical analysis.

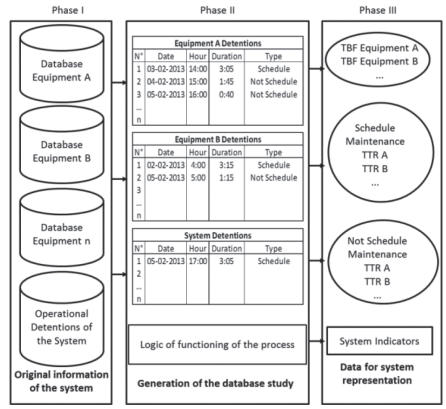


Figure 2. Traditional methodology for analysis.

tion defines the fields registered in each event, so they generally vary from organization to organization. Nevertheless, there are key fields that are required and which are the basis for a large number of studies. These fields correspond to: identify code of the equipment in which carry out a task, date and time of the activity starting, its duration and the work type performed (e.g. preventive, corrective, operational detention). As mentioned before, is probable that in order to get this information we have to use the database of different areas, as operations and maintenance. With this information, there are generated database for each equipment. In the type of events it must differentiate if they are scheduled or not still even they can specify other types.

Logical Configuration: It must be determined the logical configuration of the system, so for realize the functional dependencies in the equipments, subsystems and system respectively.

Data base unified for the historical study: Considering the data base related to the failure events and with failure logic of the system, it is generated a unique database withal this information and in which will be applied the methodology of historical analysis.

The final result of the analysis is the obtaining of required indicators such as the time between failures, repair times, availability, utilization, etc. All these seen for each equipment in separate form and for the general system.

2.2 *Traditional approach of analysis*

The following scheme introduces the traditional approach of analysis of the historical information with a more detailed description of the form in which it proceeds (include all the activities of the previous scheme). This scheme draws through phases, the activities of the former scheme. Next, is shown a diagram that will give an explanation of each one of these phases.

Phase I: Original information of the system: In this phase, the data are dispersed in different database of the organization, so there must be gathered the fields defined as necessary for the study. It must be verified the coherence of the information, since working with different database can produce incongruences due to the way the information is entered. Also in this phase the operational detentions are identified in the system.

Phase II: Generation of the database study: Once captured the required data they must be arranged giving a framework that allows to understand the relevant events that occurred in the system and its important features. On the other hand, it must be defined the logic of functioning of the process. In this step also are identified the operational detentions in the system.

Phase III: *Data for system representation*: To achieve a correct representation of the system, is commendable to set up the interesting events from which to characterize to the system. In this case, the events of interest can correspond to the changes in the states of the equipments and of the system. Already defined the equipments and system events, it can be possible to proceed to bunch the events by its type, taking into account the study approach. In this case, the events are bunched generating the periods between detentions, the periods of the detentions (Scheduled or not) and the key indicators of the system.

2.3 *New methodological proposal of analysis*

The proposed methodology is based on the traditional approach, but it incorporates an additional activity called Interaction of the system with equipments and other factors). To understand which is

the effect that is desired to reflect in the analysis, the following explicative schemes are shown.

To start, it is considered a system composed by a series of equipments with a determined logical configuration (Fig. 3).

Then, when some event occurs in one of the equipments or out of them, but affecting to system, it is registered a detention in the system, which is shown in the following scheme (Fig. 4).

The arrows towards the system reflect these possible events and the lozenge in one side of the system reflects the detention. This last is detected and measured in the traditional approach of the analysis and also in the methodology proposal. However, this detention has effects in the rest of the equipments expressed in the following scheme (Fig. 5).

This effect is not considered with the traditional approach and it is incorporated with the proposed methodology.

With the additional activity of the proposed methodology, it is possible in an integral way all the effect of the detentions in each one of the equipments, generating more representative information

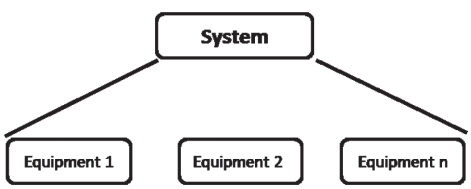


Figure 3. Scheme of a general system.

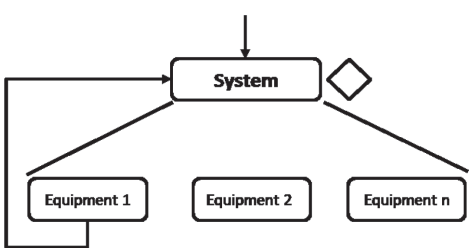


Figure 4. Scheme of a system with a detention.

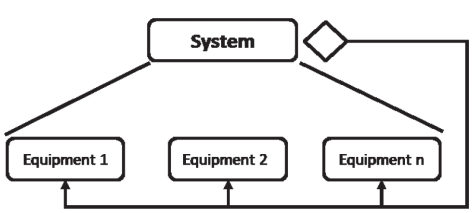


Figure 5. Effect of the detention on the equipments.

of each one of them. Is like that from the methodology with traditional approach, is incorporated the mentioned activity, achieving the following work scheme for the proposed methodology:

With respect to the interactions desired to be worked, is important to emphasize that they point to the same effect, but its causes are different. In respect to the effect, which must be in mind is that at the moment a detention occurs in the system (without matter the cause), this one generates that the hour meter of all the equipments stop, so the time lapse in the system is detained. Therefore, this time must be discounted from the time of the failures of all the equipments of the process.

Let's suppose a composed system by various components, among which are the equipments A and B that are in a parallel configuration. Let's suppose also that from step 2 of the scheme, the following information is obtained of the historical behavior of the system between the periods t_1 and t_2.

By the side of the system, it detained in the interval t_8 and t_7. The detentions of the equipments A and B do not affect the system due to the configuration of the existing failure. If we follow the traditional way of the analysis of the performance of the equipments in the step 3, the time of good functioning for the equipment A is $T_3 - t_4$, meanwhile for the equipment B is $t_5 - t_6$. However, it is not like that, since these two did not function between t_7 and t_8. In this way, the new methodology considers the impact of the detentions of the system, transmitting these times to each one of the equipments that compose it, achieving the following effect:

As of, in this example, the time of good functioning between failures of the equipment A would be: $t_3 - t_4 - (t_8 - t_7)$ and for equipment B: $t_6 - t_5 - (t_8 - t_7)$. It is necessary emphasize that the difference between both methodologies, may cause large variations in the results at the moment of measuring the time of good functioning of the equipments. However, calculating the indicators of performance of the system, the results must be the same with both methodologies.

With respect to the causes that lead to the detention of the system, are taken as focus the two more relevant. The external factors to the system and the design of him, related to the operational detentions and the equipment detentions that may cause detentions in the system or subsystem conditioned by the configuration in which the equipments are found. This last cause will be defined as state change propagation detention. It is necessary to have in mind that both methodologies include these detentions, but the traditional focus does not include the effect of these detentions in the rest of the equipments, generating differences in the result of the methodologies.

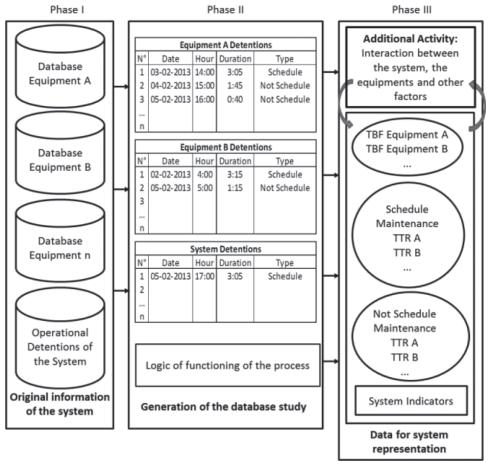


Figure 6. Proposal methodology for analysis.

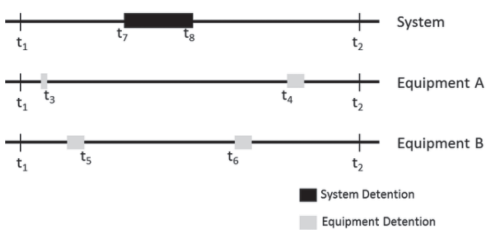


Figure 7. Sample of detentions on a system.

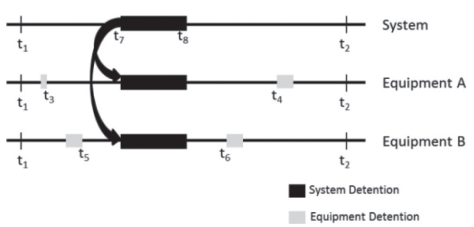


Figure 8. Detentions on a system an effect on equipments.

To deeper understand the application of this methodological proposal, next will show an application which will introduce both methodologies, its differences and the results as following.

3 NUMERICAL EXAMPLE

In order to understand how is executed the methodological proposal set up and the impact this have in the results, next will be shown an example in which will be used as much the traditional focus of analysis as the proposed methodology. In this way will appreciate the differences in the application of both analyses and in the results that are generated. Both methodologies will start from the same basis information that proceed from steps 1 and 2 of the Figures 2 and 6 already described, so the comparison will be totally valid. The case established, consist of a system composed by six equipments in a serial configuration. All of them begin to function at the same time and are considered new. After 1.040 chronological hours we have the following detentions data:

We must indicate that all the detentions of the equipment correspond to the not scheduled type, that is to say failures that are not expected by the equipment. On the other hand, exists the record of an operational detention of the system with duration of forty hours. These detentions are given by foreign factors to the system equipments, but it generates a detention in the same one.

The next step to be performed correspond to phase 3 represented in the Figures 2 and 6 where are differences between both methodologies. To follow with the analysis, will be indicated the steps that continue with the traditional focus, then will be performed with the proposed methodology and finally will be analysed the differences between results of the methodologies.

3.1 *Analysis with traditional approach*

3.1.1 *Application of the methodology in TBF*

Among the relevant indicators mentioned (such as TBF and TTR by equipment) will focus in the TBF that are produced by each equipment. To begin, will show Table 2 with the detentions of

Table 1. Detentions data of the example.

	Detentions		
Equipment	Time [hh:mm]	Duration [hh:mm]	Type
3	63:42	33:54	Not schedule
2	155:23	32:35	Not schedule
4	376:29	31:52	Not schedule
System	500:00	40:00	Operational detention
5	550:56	34:27	Not schedule
6	618:24	35:33	Not schedule
1	680:53	33:15	Not schedule
3	724:38	34:33	Not schedule
2	783:57	32:40	Not schedule
1	869:48	33:27	Not schedule
2	1001:09	35:15	Not schedule

each equipment, specifying the number of failures, the chronological hour in which the event was produced and the duration of it.

Using the traditional methodology to calculate the respective TBF, simply are taken the periods at the moment the equipment is available (from the moment zero or finishing its repair) and the nearest failure of the same equipment. Once this is applied, we conclude the following TBF in Table 3.

3.1.2 *Analysis of the % of utilization*

In order to calculate of the indicator of utilization, will be considered the next expression:

$$Utilization = \left(\frac{UPT}{UPT + DWT + OPT} \right)$$

where the UPT correspond to the time the equipment was functioning, el DWT correspond to the time the equipment was being repaired and ODT are the operational detentions that affect to all the system and whose causes are foreign to the equipments. Nevertheless with this analysis approach, the UPT is calculated as the total period it is evaluated, less the periods associated to the DWT and the OPT.

In this way, we obtain the following results in Table 4.

Table 2. Time of detention and duration per equipment.

Equipment	N° detentions	Hour of detention [hh:mm]	Duration [hh:mm]
1	2	680:53	33:15
		869:48	33:27
		155:23	32:35
2	3	783:57	32:40
		1001:09	35:15
3	2	63:42	33:54
		724:38	34:33
4	1	376:29	31:52
5	1	550:56	34:27
6	1	618:24	35:33
System	1	500:00	40:00

3.1.3 *Analysis of the TBF*

As third point of comparison, the first 15 TBF of each equipment are analysed with the aim to appreciate the differences produced between both methodologies. Table 5 shows this information for the traditional approach:

3.2 *Analysis with the proposed methodology*

3.2.1 *Application of the methodology of the TBF*

Beginning with the calculation of the TBF, applying the proposed methodology, we must consider the impact of each failure in the system and in the rest of the equipments. In this way, if we take as an example the first TBF of the equipment 1 the failure is produced at 668 hours and 53 minutes. However, in all this time failures were produced in the equipments 2, 3, 4, 5 and 6, each one with certain duration.

When analyzing the impact of those failures in the first TBF of the equipment 1, is determined that, given the configuration of the system, the hour meter of the equipment is stopped, so the total hours must be discounted, all the detention hours that generated the repair of the rest of the equipments. Applying this method in this case, we determine to the following results in Table 6.

3.2.2 *Analysis of the % of utilization*

With the proposed methodology in the calculation of the% of utilization for equipment, it is considered the propagated detentions of the equipments within the system, which leads to indicators up time fewer than those calculated with the traditional focus. To show this effect, Table 7 displays the up time of each equipment without consider-

Table 3. TBF with the traditional methodology.

Equipment	TBF equipment i	Hour of detention [hh:mm]	Duration [hh:mm]	TBF traditional methodology
1	1	680:53	33:15	680:53
	2	869:48	33:27	155:40
	1	155:23	32:35	155:23
2	2	783:57	32:40	595:58
	3	1001:09	35:15	184:31
3	1	63:42	33:54	63:42
	2	724:38	34:33	627:01
4	1	376:29	31:52	376:29
5	1	550:56	34:27	550:56
6	1	618:24	35:33	618:24
System	1	500:00	40:00	

Table 4. % of utilization with traditional methodology.

Equipment	Up time [HH]	Down time [HH]	Detention [HH]	Utilization (%)
1	933,28	66,72	40,00	93,33%
2	899,48	100,52	40,00	89,95%
3	931,53	68,47	40,00	93,15%
4	968,13	31,87	40,00	96,81%
5	965,55	34,45	40,00	96,55%
6	964,44	35,56	40,00	96,44%

Table 5. First 15 TBF using traditional methodology.

Equipment	Equipment 1	Equipment 2	Equipment 3	Equipment 4	Equipment 5	Equipment 6
1	680,89	155,38	63,71	376,50	550,94	618,41
2	155,67	595,97	627,02	1.122,07	618,86	820,06
3	535,14	184,52	382,64	1.603,71	467,60	661,77
4	449,51	1.369,46	855,31	535,45	225,82	613,66
5	902,82	1.697,34	1.252,89	563,48	458,20	502,12
6	845,40	530,34	87,86	996,99	278,06	649,03
7	745,96	349,06	210,59	286,01	291,55	584,11
8	324,09	1.716,08	253,10	477,32	482,72	938,28
9	410,82	479,39	281,86	269,09	442,58	1.373,89
10	912,94	99,43	519,44	366,86	674,81	977,01
11	1.259,93	489,02	355,79	1.131,80	443,54	770,62
12	731,33	899,09	698,33	535,25	235,70	1.080,63
13	553,52	239,03	143,35	1.010,87	334,13	482,00
14	666,53	677,11	19,04	651,97	418,55	890,76
15	425,76	765,34	472,46	451,41	553,19	761,18

Table 6. TBF with the proposal methodology.

Equipment	TBF equipment i	Hour of detention [hh:mm]	Duration [hh:mm]	TBF proposal methodology
1	1	680:53	33:15	472:30
	2	869:48	33:27	88:25
2	1	155:23	32:35	121:28
	2	783:57	32:40	386:16
	3	1001:09	35:15	151:03
3	1	63:42	33:54	63:42
	2	724:38	34:33	419:17
4	1	376:29	31:52	309:59
5	1	550:56	34:27	412:34
6	1	618:24	35:33	445:35
System	1	500:00	40:00	

Table 7. % of utilization with proposal methodology.

Equipment	Up time [HH]	Down time [HH]	Propagation [HH]	Detention [HH]	Utilization (%)
1	662,41	66,72	270,87	40,00	90,85%
2	662,41	100,52	237,07	40,00	86,82%
3	662,41	68,47	269,12	40,00	90,63%
4	662,41	31,87	305,72	40,00	95,41%
5	662,41	34,45	303,14	40,00	95,06%
6	662,41	35,56	302,03	40,00	94,91%

ing the propagated detentions and its respective percentage of utilization.

The expression that is used to calculate the indicator of utilization correspond to:

$$Utilization = \left(\frac{UPT}{UPT + DWT + PRT + OPT} \right)$$

where the period PRT is incorporated, associated to the propagated detentions, the UPT of the equipments is different to the previous methodology since the RPT periods are discounted, obtaining the real times of utilization.

3.2.3 *Analysis of the TBF*

Applying the proposed methodology to the same initial data, we can get the following TBF for each one of the six serial equipments in Table 8.

3.3 *Difference in the application and results of the methodology*

3.3.1 *Application of the methodology in the TBF*

In respect to the differences that arise from the generation of the TBF, Table 9 displays the results got through the distinct methodologies and its respective differences.

As we can appreciate, the differences between both methodologies are relevant, so that is imperative to define which is the most assertive to represent the behavior of the system. For this it will be analysed from two perspectives. The first one is to construct the representative models of the system and the second one the construction of key indicators of the performance, specifically, the utilization of the equipments.

With regard to the first point, at the moment of modeling the system behavior, the main thing is to represent correctly the behavior of each equipment and the relations between them that the system establishes. Then, in order to represent the random in the failure event of each equipment, it is used historical information of performance. This information must contain only periods of good functioning between failures, that is to say the times registered by hour meter. In the case the detentions will be foreign factors to the equipment, the hour meter must stop.

In the case of the traditional methodology, these detentions of hour meters are not considered so the period of good functioning is overestimated, while the proposed methodology is in charge of this issue, leaving the data clean in order to be used again.

On the other hand, and in order to assure a representative model of the system, they must consider the functional logic of the system, so in this way the model can stop the hour meters represented meanwhile the detentions of the system are produced.

With respect to the second point related to the indicators, will see the differences produced at moment of calculating the indicator of utilization of the equipments.

3.3.2 *Analysis of the % of utilization*

In order to begin, Table 10 shows the differences between the UPT and the% of utilization with each one of the methodologies.

As we can appreciate, exists a notorious difference in the value of the indicators of utilization with each methodology. It can be of importance that with the second methodology, the UPT of all the equipments is the same one, which is directly connected with equipments that posses a serial configuration, so the period in which each one works is exactly the same one at the rest. This reflects exactly what happens in the real system.

Table 8. First 15 TBF using the proposal methodology.

Equipment	Equipment 1	Equipment 2	Equipment 3	Equipment 4	Equipment 5	Equipment 6
1	472,51	121,48	63,71	310,00	412,57	445,59
2	88,43	386,27	419,29	658,09	334,71	501,32
3	385,42	151,06	241,25	1.087,68	318,27	390,85
4	298,77	879,05	555,63	295,38	183,06	467,48
5	572,75	983,90	807,12	327,48	311,14	283,05
6	520,40	358,64	52,89	578,11	238,06	407,73
7	436,91	171,03	176,01	175,90	222,16	379,94
8	186,26	1.064,13	150,65	297,21	259,85	491,67
9	287,10	309,13	179,21	197,41	236,05	860,25
10	543,88	99,43	315,40	253,88	435,92	595,89
11	804,38	284,37	210,51	649,20	232,89	485,28
12	436,25	511,69	435,32	384,41	140,28	612,59
13	344,27	205,48	103,35	614,32	270,46	285,02
14	453,87	394,10	19,04	338,95	210,83	624,24
15	213,01	465,61	299,98	307,33	379,45	444,53

Table 9. Difference between the TBF of both methodologies.

Equipment	TBF equipment i	TBF traditional methodology	TBF proposal methodology	Difference
1	1	680:53	472:30	208:22
	2	155:40	88:25	67:14
	1	155:23	121:28	33:54
2	2	595:58	386:16	209:42
	3	184:31	151:03	33:27
3	1	63:42	63:42	0:00
	2	627:01	419:17	207:44
4	1	376:29	309:59	66:29
5	1	550:56	412:34	138:22
6	1	618:24	445:35	132:49

Table 10. Difference between % of utilization.

	Up time [HH]		Utilization (%)	
Equipment	Traditional methodology	Proposal methodology	Traditional methodology	Proposal methodology
1	973,28	662,41	93,58%	90,85%
2	939,48	662,41	90,33%	86,82%
3	971,53	662,41	93,42%	90,63%
4	1.008,13	662,41	96,94%	95,41%
5	1.005,55	662,41	96,69%	95,06%
6	1.004,44	662,41	96,58%	94,91%

Table 11. Difference between MTBF of both methodologies.

MTBF	Equipment 1	Equipment 2	Equipment 3	Equipment 4	Equipment 5	Equipment 6
Proposal methodology	402,95	425,69	268,62	431,69	279,05	485,03
Traditional Methodology	640,02	683,10	414,89	691,92	431,75	781,57
difference	–237,07	–257,41	–146,27	–260,23	–152,70	–296,54

3.3.3 *Analysis of the TBF*

From the obtained information with each one of the methodologies, it is calculated the mean time between failures proving the following differences in Table 11.

This demonstrates that at the moment to make a curve fit to each one of the equipments it becomes to behaviors substantially different with each way of work. As appreciated, with the traditional approach the mean time between failures is much greater, since if not identifying the propagated detentions of the equipments, the periods of good functioning are overestimated in a greater size.

Having in mind these differences, it is assumed that the proposed methodology is substantially better than the traditional approach, since it represents the system in a better way, as from the perspective of the indicators as the representation of the behavior of the equipments of the system (being this crucial point for the creation of representative models of the system).

It is important to indicate that the differences between the results utilizing one or other methodology varies in accordance with the impact that have the propagated and operational detentions and these at the same time depend on the configuration of the system and of the foreign factors to the equipments.

4 CONCLUSIONS

In the present paper, it has been analysed the way in which usually has been made the analysis of the historical information of the system related to the indi-

cators of utilization and periods of good functioning. It has been explained how, generally, is made this type of analysis and the defects that it brings when not considering the interactions of the equipments with the system and the detentions that bear the system by the external factors. These two phenomenons are expressed through the propagated detentions and the operational detentions, which are considered at the moment of making the analysis of the complete system, but many times are not taken into account at the moment of making the analysis by equipment.

In order to incorporate these factors to the analysis by equipment and produce more representative results of the system, a methodological proposal is introduced, that mainly add activities to the traditional approach, which capture and identify clearly the phenomenon of interest and incorporate them to the analysis for equipment. In this way, we obtain real periods of good functioning, also the times of propagated detentions and operational detentions. The great impact obtained with this modification in the analysis, are more representative indicators of the equipment and real times of good functioning between failures.

Counting with this more purified information, is possible to get key indicators according with reality and also the basic information is got to make curve fit that represent the behavior of the equipments.

Together with describing the proposed methodology, it was developed a numerical example in which are detailed the differences utilizing one or other methodology and in the obtained results. The breach between the results proves that are not fewer. However, is necessary to emphasize that the differences are not easy to quantify from the first in any case, since they depends the most of the configuration of the system, behaviours of the equipments, present external factors, among other factors.

Certainly this document and the proposed methodology approached on indicators related to the management of the assets, the main contribution of the methodology take roots in the outlining that in the historical analysis of the system, we must take into account not only the impact of the events occurred in the equipments and that affect to the system, but also we must pay attention to the effect that these events have in the system and how they affect to the involved equipments. These events in the system can be caused by the same equipments or by foreign factors to them.

REFERENCES

Ahmada, M., Dhafrb, N., 2002. Establishing and improving manufacturing performance measures. Robotics and Computer-Integrated Manufacturing, 18: 171–176.

Bause, F., Kritzinger, P., 2002. Stochastic Petri Nets—An Introduction to the Theory (2nd edition).

Bunea, C, Mazzuchi, T., Sarkani, S. and Chang, H., 2008. Application of modern reliability database techniques to military system data. Reliability Engineering Safety, 93: 14–27.

Buzacott, J.A. and Shanthikumar, J.G., 1993. Stochastic models of manufacturing systems. Prentice-Hall, Englewood Cliffs, New Jersey.

Caldeira Duartea, J., Cunhaa, P. and Craveiroc, J., 2013. Maintenance Database. Procedia CIRP, 13: 551–556.

Calixto, E., 2013. Reliability, Availability, and Maintainability Analysis, Gas and Oil Reliability Engineering. Chapter 4: 169–347.

Distefano, S. and Puliafito, A., 2009. Reliability and availability analysis of dependent-dynamic systems with DRBD's. Reliability Engineering and System Safety, 94: 1381–1393.

Fuqua, Norman B., 2003. Markov Analysis. The Journal of the RAC, Third Quarter.

Jau-Chuan, K. and Yunn-Kuang, C., 2007. Comparative analysis of availability for a redundant repairable system. Applied Mathematics and Computation, 188: 332–338.

Kans, M. An approach for determining the requirements of computerized maintenance management systems, Computers in Industry: 59: 32–40.

Muchiri, P., Pintelon, L. and Martin, H., 2013. Development of maintenance function performance measurement framework and indicators. Int. J. Production Economics, 131: 295–302.

Schryver, J., Nutaro, J. and Haire, M.J., 2012. Metrics for availability analysis using a discrete event simulation method. Simulation Modelling Practice and Theory, 21: 114–122.

Sharma, R.K. and Kumar, S., 2008. Performance modeling in critical engineering systems using RAM analysis. Reliability Engineering and System Safety, 93: 891–897.

Singh, J. and Goel, P., 1995. Availability analyses of a standby complex system having imperfect switch-over device. Microelectron. Reliab., 35, No 2: 285–288.

Van Horenbeek, A., and Pintelon, L., 2014. Development of a maintenance performance measurement framework—using the Analytic Network Process (ANP) for maintenance performance indicator selection. Omega, 42: 33–46.

Viveros, P., Zio, E., Kristjanpoller, F. and Arata, A., 2012. Integrated system reliability and productive capacity analysis of a production line. A case study for a Chilean mining process. Proceeding of the Institution of Mechanical Engineers, Part O: Journal of Risk and Realibility, 226: 305–317.

Zio, E. and Pedroni, N., 2010. Reliability estimation by advanced Monte Carlo simulation. In Simulation methods for reliability and availability of complex systems. Springer Series in Reliability Engineering, Part I: 3–39.

Zio, E., Podofillini, L., and Zille, V., 2006. A combination of Monte Carlo simulation and cellular automata for computing the availability of complex network systems. Reliab. Engng Syst. Saf., 91, 181–190.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Proven in use in the machine tool industry for demonstrating the quantitative functional safety according to EN ISO 13849-1

B. Günnel & A. Meyna
University of Wuppertal, Wuppertal, Germany

M. Schlummer
Institute for Quality and Reliability Management GmbH, Wuppertal, Germany

H. Mödden & A. Broos
VDW—German Machine Tool Builders Association, Frankfurt, Germany

ABSTRACT: Since the standard EN ISO 13849-1 became effective in December 2012, manufacturers in the area of the machine tool industry have to assess the functional safety of the safety-related functions in a probabilistic quantitative way. Due to the specifications of the standard in combination with little experience and few existing quantitative data in the machine tool industry, manufacturers have huge problems by adapting the new requirements. The presented research project tries to develop an alternative and practicable procedure which shall allow the manufacturers to fulfil the normative requirements with a proven in use approach. Therefore, as shown in the ESREL-paper 2013, a first data analysis of real field data was performed to proof if the available field data in the machine tool industry is useful to develop a proven in use approach. Further the standard includes assumptions concerning the failure behaviour of the components, which were also checked with the first field data analysis. The first examination included the reliability of the analysed systems. To realise an approach for the Functional Safety of safety-related functions it is necessary to analyse these functions separately on the basis of field data. The aim and content of the presented paper is to extract the safety-relevant information out of the checked reliability field data. Afterwards, the safety-related field data has to be further analysed to identify those data that are responsible for one exemplified single safety-related function. Consequently, the received quantitative results can be compared with the requirements of the EN ISO 13849-1.

1 INTRODUCTION

The requirements on the safety and reliability of machine tools become more and more important. The manufacturers of machines have to fulfil several different guidelines and standards according to the Functional Safety and reliability before the machines were placed on the market.

The importance of the Functional Safety was underlined with the safety standard IEC 61508 which deals with Functional Safety of electrical/electronic/programmable electronic safety-related systems (IEC 2011). The innovation of this fundamental standard consists of the probabilistic examination of the Functional Safety with quantitative parameters. It is a universal standard, which is applicable in every industry sector. One aim of the IEC 61508 is that the standard should facilitate the development of application sector standards. Until today several derivates have been developed and transferred to different industry sectors.

In the area of machine tools there are two main standards that deal with the quantitative Functional Safety. The standard IEC 62061 "Safety of machinery—Functional Safety of safety-related electrical, electronic and programmable electronic control systems" is a derivate of the IEC 61508. It has been developed for machinery, which contains the examined machine tools as a subset. However, it deals exclusively with electrical/electronical control chains.

Because of the high amount of mechatronical systems in many types of machinery (e.g. machine tools), an additional standard for the mechatronical control chains of machinery has been prepared in parallel, the EN ISO 13849 "Safety of machinery—Safety-related parts of control systems" (ISO 2008). The standard consists of the two parts "General principles for design" and "Validation", but only the first part is relevant for this paper. The EN ISO 13849-1 replaced the former standard EN 954-1, which handled the

Functional Safety of machines in a descriptive and deterministic way. Consequently, a considerable paradigm change took place to a probabilistic point of view that causes many new demands for the manufacturers of any kind of machinery and consequently for the machine tool industry.

With the introduction of the EN ISO 13849-1 and the end of the transition period of EN 954-1 in December 2011, manufacturers in the machine tool industry are obliged to perform quantitative safety evaluations of their machines.

The new standard claims the quantitative evaluation of safety-related functions of a machine over an expected operation time of 20 years. This can only be realised by a probabilistic assessment of the Functional Safety of the relevant functions. The quantitative safety which is required by the EN ISO 13849-1 is specified by different "Performance Level" (PL). The PL is defined as an average probability of a dangerous failure per hour and is classified in different groups. An illustration of these different groups and the procedure to select a Performance Level for a safety-related function with the so called "Risk Graph" of the EN ISO 13849-1 was illustrated in the ESREL-paper 2013 "EN ISO 13849-1—New quantitative requirements for Functional Safety in the machine tool industry" (Günnel et al. 2013).

2 CONSEQUENCES OF EN ISO 13849-1

According to the EN ISO 13849-1, the appointment of a Performance Level represents the capability of a safety-related component to perform a safety-function. To determine the PL of a safety-function, the standard advises to use different aspects that contribute to the failure prevention of the safety-related function. One aspect is the $MTTF_D$-value (mean time to dangerous failure) of the single considered components which is the inverse failure rate of the exponential failure distribution.

The consequence of using the $MTTF_D$-value for calculation of the PL is that the standard assumes a constant failure rate (exponential distribution) for the failure behaviour of the components (Meyna & Pauli 2010). The problem with constant failure rates and the exponential failure behaviour is that components and systems with this behaviour are considered to have no ageing process. This assumption of the EN ISO 13849-1 is arguable, because machine tools that are used in real production environment are clearly subject to ageing processes.

The new probabilistic requirements of the EN ISO 13849-1 cause tough challenges for the manufacturers and huge uncertainty by the developers of machine tools, because they have no experience with this way of assessing their machines. The manufacturers have no or very insufficient documented quantitative data about the safety of the machines that can be used for a quantitative evaluation. Consequently, a few general quantitative parameters were developed that can be used by every company for the assessment.

A consequence of the general available parameters is that the existing machine tool concepts, which were built according to type C product standards for more than 10 years and which have a real and high Functional Safety in the field, appear not to be adequate to reach the required Performance Level at the first glance. Thus the machine tool manufacturers are exposed to new requirements to install additional safety equipment in their machines that causes extra costs and therewith an economical risk. The amount of maintenance can also increase when more components are assembled. This causes additional investments and costs for the user, too.

The assumption of the EN ISO 13849-1 and the existing general quantitative parameter leads to the theoretically wrong impression that the Functional Safety of some functions of the existing machine tools is not adequate.

3 APPROACH "PROVEN IN USE"

In order to correct this misleading conclusion, the VDW initiated the presented research project.

The aim of this project is to determine quantitative reliability parameters of existing machine tool concepts on the basis of real operational field data. Thus, it can be checked, whether the failure behaviour of the machines, functions and components is really exponential distributed or not. Additionally, it can be determined if the Functional Safety of the present machine tool concepts, which are well tried proven to be safe for many years, are practically sufficient according to the new requirements of the EN ISO 13849-1.

Furthermore, the research project shall proof the capability of a proven in use approach on the basis of the identified field data. Thus, a complementary procedure to the EN ISO 13849-1 could be developed, that is able to support the manufacturers of machine tools with a quantitative calculation of the Functional Safety that complies with the standard.

A first study, which was presented in the ESREL-paper 2013, should prove, if the existing operational field data in the machine tool industry is sufficient for a proven in use approach (Günnel et al. 2013).

Further quantitative reliability parameters of machine tools should be determined on the

basis of operational field data for the first time. Therewith, the assumption of the standard EN ISO 13849-1 should be proven, if exponential failure behaviour of the machines and components really exists.

In the context of the first study, the field data of the clamping function of a turning machine were selected to be analysed. The field data of two different companies that are involved in the life cycle of a turning machine were examined. The first company was a manufacturer of components and subsystems that are used in the clamping function of a turning machine. The data in this case were service data of one component and one subsystem of the clamping function, which consist of warranty-, goodwill- and bill-cases. The second company was an operator of turning machines, whose field data of three turning machines were malfunction messages that are automatically generated by the machines and send to a data base.

Both weekly documented field data could be screened after events that occur at the clamping function so that consequently the field data could be prepared and a very first reliability-related data analysis was executed. Thereby, the empirical failure probability was calculated and two theoretical reliability distributions (exponential and Weibull) were fitted.

The results of the analysis showed that the existing operational field data in the machine tool industry can generally be used for probabilistic reliability and safety assessments and consequently for a proven in use approach. The used field data included reliability events so that further researches were necessary to extract the subset of safety-relevant events.

The first outcomes of the data analysis clarified that the assumption of the EN ISO 13849-1 concerning the constant failure behaviour could not be confirmed. The empirical failure behaviour of the clamping function, the subsystem and the component could better be described with a Weibull distribution that is able to consider an ageing process of the systems. But there are additional analyses necessary to verify these first results. It is advisable to analyse different machine tools and different safety-related functions to find universal findings.

In summary the first study generated promising findings. It should be noted that the very first field data analysis just examined quantitatively the reliability of the whole clamping function. But for a proven in use approach it is essential to quantify the safety of the single safety-related functions.

Therefore, a second study was initiated that shall quantify the Functional Safety of safety-related functions for the first time. This study will be described in the content of this paper.

4 QUANTIFYING FUNCTIONAL SAFETY

As described before, the aim of the second VDW-study is to perform further field data analyses that quantify the Functional Safety of a safety-related function on the basis of real field data for the first time. This allows the possibility to demonstrate quantitatively the Functional Safety of existing safety-related functions that complies with the requirements of the EN ISO 13849-1.

The data base of the before mentioned operator of machine tools was used to generate and receive the field data for these analyses. To verify the findings of the first study a different machine tool was selected that has been analysed. After a first screening of the data base nine identical milling machines were identified that have a sufficient amount of data. The clamping function of the milling machines—comparable with the examined turning machines—is one of the most important functions. Consequently, one safety-related function of the clamping function was selected.

The safety function "prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece" of the standard prEN ISO 16090 (ISO 2013) was chosen to be analysed and quantified in order to keep the practical use of the researches.

The field data that has to be extracted from the data base of the operator could not be restricted to those data, which appear at the selected safety function. Thus, like in the first study, all field data must be collected that appear at the whole clamping function of the milling machine.

After the field data was determined, the manufacturer of the milling machines was contacted. As described before, the data consists of malfunction messages that are automatically sent to a data base. These messages are codes with a very short description of the malfunction. The meaning of the codes and the description is defined by the manufacturer so that only he knows which component or system is affected.

The entire field data of the data base represents the reliability of the whole clamping function. In cooperation with experts of the manufacturer of the milling machines it was possible to scan the detected malfunctions and to select those, who possibly can have an influence on the safety of the clamping function. The result of this procedure is that only the safety-relevant malfunctions remain in the data set. Therewith, it was possible to extract the subset of the safety-relevant events out of the complete reliability-relevant field data.

The reduced safety-relevant field data was checked again in cooperation with the experts of the milling machine manufacturer in the next step. Thereby, the malfunctions are identified that can

occur at the selected safety-related function. With this limitation the received reduced field data represent the safety-related malfunction messages which appear at the examined safety function.

Hence, it was possible with the support of expert judgments to constrict the reliability-related field data of the whole clamping function in two steps to the safety-related field data of one single safety function. Thereby, the allocation of the malfunction messages to the safety function is not definite, because the messages can also be relevant for further safety functions. Consequently, it is a worst case examination that needs to be stated more precisely in future researches.

Out of the determined field data the empirical failure probability is calculated. Afterwards, the theoretical failure probability of the exponential and Weibull distribution is determined on the basis of the empirical failure probability. To compare the goodness of fit of the probability distributions to the empirical distribution the respective coefficient of determination is calculated.

As shown in the ESREL-paper 2013 (Günnel et al. 2013), the exponential distribution cannot be used to describe the failure behaviour with an ageing process, as it is the case with machine tools. Thus, the following results contain the exponential distribution to verify the findings of the first study, but are not regarded further. The Weibull distribution in contrast can describe different ageing processes and is used in the following to describe the empirical failure behaviour.

The aim of the proven in use approach is a quantitative verification of the existing Functional Safety in the field, which can be compared with the quantitative requirements of the EN ISO 13849-1.

Therefore, it is necessary to determine a quantitative value out of the fitted Weibull distribution. The standard defines as quantitative value the Performance Level. The PL are shown in the following Table 1.

The definition of the PL is not explicit because there are several existing parameters that describe an average probability. However, a parameter is needed which is constant over the whole lifetime and represents an average probability.

Table 1. Classification of the Performance Level (ISO 2008).

Performance Level	Average probability of a dangerous failure per hour [1/h]
a	$\geq 10^{-5}$ to $<10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $<10^{-5}$
c	$\geq 10^{-6}$ to $<3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ to $<10^{-6}$
e	$\geq 10^{-8}$ to $<10^{-7}$

A very common value which is often used and also described in the EN ISO 13849-1 is the $MTTF_D$, which is the inverse failure rate of the exponential distribution. Next to the fact that the exponential distribution cannot be used for lifetime consideration, the failure rate does not agree with the definition of the Performance Level because the failure rate is not a probability value. Thus, a different value has to be selected.

The base standard of Functional Safety (IEC 61508) defines the PFH-value as the "average frequency of a dangerous failure per hour" as a comparable value in part four (IEC 61508-4). Under remark two to this definition the IEC 61508 states that the PFH is the mean value of the failure density function. This definition also fits to the definition of the EN ISO 13849-1, because the density function is a probability value. Consequently, the failure density is also useable to perform a proven in use approach.

But the mean value of the failure density function does not include the areas of high failure densities. In contrast the maximum of the failure density function as value includes all areas of the density function and consequently every existing failure density. This value is also consistent to the definition of the EN ISO 13849-1 and is therefore used for the presented proven in use approach.

5 RESULTS

As described before nine existing identical machines have been analysed. The results consist of the safety-related empirical and theoretical failure probability of the safety-related function. Further, the failure density function of the theoretical distribution function is calculated and illustrated to clarify how the maximum of the failure density function is obtained. The received maximum values can finally be compared with the quantitative requirements of the EN ISO 13849-1 and the Performance Level can be determined.

The results of the data analysis are shown in the following figures exemplarily for one milling machine. The reached PL of the safety-related functions of all nine machines are illustrated in Table 2.

In the following Figure 1 the results for the data analysis of the selected safety-related function of one milling machine are shown. The green dots represent the empirical failure probability, the blue line the fitted theoretical exponential failure probability and the green line the fitted theoretical Weibull failure probability. The operating time of

Table 2. Maximum value of the probability density function and achieved Performance Level of the selected safety-related function of the nine milling machines (* = not comparable).

Milling machine	Max. value [1/hour]	Achieved PL
A	$4{,}0690 \cdot 10^{-5}$	a
B*	–	–
C	$5{,}5897 \cdot 10^{-5}$	a
D	$5{,}3218 \cdot 10^{-5}$	a
E	$1{,}4594 \cdot 10^{-5}$	a
F	$1{,}6554 \cdot 10^{-5}$	a
G*	–	–
H	$9{,}2845 \cdot 10^{-6}$	b
I	$5{,}9164 \cdot 10^{-5}$	a

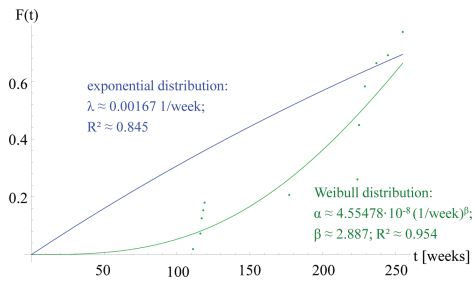


Figure 1. Empirical and theoretical failure probabilities of the selected safety-related function of a milling machine.

the milling machines was about five years at the time of data collection.

Figure 1 makes clear, that the empirical failure behaviour of the analysed safety-related function can approximately be illustrated with a Weibull distribution, because the theoretical failure probability of the Weibull distribution has a similar curve progression with the empirical failure probability. The coefficient of determination with $R^2 \approx 0.954$ is explicitly better than the coefficient of determination of the exponential distribution with $R^2 \approx 0.845$. The results of the other examined machines, which are not visualised here, also confirm the first outcomes of the first VDW-study that the exponential distribution in not adequate for field data analysis of systems with an ageing process.

With the determined Weibull distribution, which describes the empirical failure behaviour, it is now possible to calculate the failure density function that is used to determine the maximum value.

In the following Figure 2 the received failure density functions of both fitted distribution functions are visualised. Thereby, the same time period is shown like in Figure 1.

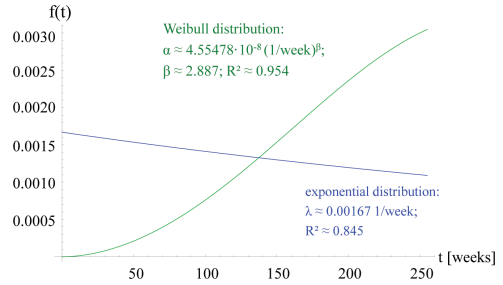


Figure 2. Theoretical failure density of the selected safety-related function of a milling machine.

With the density function of the Weibull distribution it is now possible to assess the maximum. As one can see in Figure 2, the displayed density function of the Weibull distribution does not have a maximum within the visualized time period. But the calculation of the peak value includes the entire progression of the density function.

As mentioned before and illustrated in Figure 1 and 2, the data analysis was performed on the basis of weekly documented field data so that the diagrams and distributions also have this time unit. In contrast the requirements of the EN ISO 13849-1 have the unit 1/hour. Thus, the determined nine maximum values of the machines have to be converted in this dimension.

Consequently, the obtained maximum values of all nine milling machines can be compared with the quantitative values of the Performance Level of the standard. The results of the comparison are displayed in the following Table 2.

As Table 2 makes clear, it is possible to demonstrate with the analysed field data for six safety-related functions a Performance Level a and for one also a PL b. Two regarded safety functions cannot be compared with the quantitative requirements because it was not possible to calculate a maximum of the failure density function. The reason for this is that the fitted Weibull distribution has a shape parameter λ of less than 1. The consequence is that the resulting density function has no explicit maximum. This failure behaviour is not usual for mechanical stressed systems like machine tools so that this has to be analysed more detailed in further researches.

In summary, the results of the second VDW-study make clear that it is possible to quantify existing safety-related functions of machine tools with a proven in use approach. The calculated maximum of the probability density function of the Weibull distribution is a useable value that can be compared with the quantitative requirements of the EN ISO 13849-1.

Furthermore, the findings of the first VDW-study concerning the incorrect assumed failure behaviour of the standard could be confirmed.

Nevertheless, there are further researches necessary to raise the accuracy of the proven in use approach. The mapping of the malfunction messages to the safety-related function, for example, could be more explicit so that the real amount of malfunction messages can be possibly reduced.

6 CONCLUSION

The introduction of the EN ISO 13849-1 requires a probabilistic quantitative assessment of the safety-related functions of machine tools and it causes huge uncertainty for many manufacturers and suppliers of machine tools, because there is only very little experiences with this kind of assessment among small and medium enterprises (i.e. machine tool builders). Furthermore, the released and existing quantitative data are universal and have no plausible connection to the single machine tool concepts and components of the manufacturers. With the use of these universal parameters many concepts of safety-related functions wrongly seem to be inadequate to achieve the new requirements, which cause extra costs for the manufacturers.

As the EN ISO 13849-1 requires the verification of average probabilities for the Functional Safety of safety-related functions over a lifetime of 20 years, which are called Performance Level, the assumed constant failure rate is problematic, because it considers no ageing of the machines.

The aim of this project is to detect and quantify the existing safety of the relevant functions of machine tools in the field. Thus, the assumption of the ISO EN 13849-1 and of the universal parameters can be checked. Afterwards, a proven in use approach shall be developed which complies with the requirements of the standard. The manufacturers can additionally calculate machine- or function-specific quantitative data.

In the lead VDW-founded study a first reliability-related data analysis was performed to survey, if the existing field data in the machine tool industry are useful to use them in a proven in use approach. Further, the assumed failure behaviour of the EN ISO 13849-1 was tested. The results of the analysis showed that the existing operational field data in the machine tool industry can generally be used for probabilistic reliability and safety assessments. The assumptions of the standard concerning the constant failure behaviour could not be confirmed.

Because of the positive results of the first study the second study was initiated to confirm the results of the first study and to quantify for the first time the safety of a safety-related function.

A different machine tool type was selected to be analysed for the confirmation of the results of the first study. The field data of the examined milling machines were collected at the same operator like in the first study. In cooperation with the manufacturer of the milling machines it was possible to extract the safety-relevant field data out of the entire reliability-related field data. With a second expert judgment of the manufacturer an allocation of the safety-relevant field data to a selected safety-relevant function was performed.

Further, a quantitative value was selected that can be determined out of a field data and afterwards be compared with the requirements of the EN ISO 13849-1.

The results of the field data analysis show that it is possible to quantify the Functional Safety of existing safety-relevant functions of machine tools with a proven in use approach. With the selected value it is possible to compare the determined quantitative safety with the specifications of the standard. Consequently, a quantitative proven in use approach of safety-relevant functions is possible that complies with the EN ISO 13849-1.

There are further researches necessary to raise the accuracy of the proven in use approach. It is advisable to quantify several safety-related functions of one subsystem and to analyse different machine tools.

Finally, the aim of this research project is to develop a general method to demonstrate the proven in use of the Functional Safety of existing and new safety-related functions of machine tools. This would help the manufacturers to perform a function—or machine-related verification that complies with the requirements of the standard EN ISO 13849-1. With this study a first quantification of existing safety-related functions with a proven in use approach has been realised.

The presented paper provides the findings of a VDW-funded study (VDW: German Machine Tool Builders Association, Frankfurt, Germany). This contribution made the researches possible so that the gratitude is aimed at the supporting people of the VDW.

REFERENCES

EN ISO 12100, 2010. *Safety of machinery—General principles for design—Risk assessment and risk reduction*. Berlin, Germany; Beuth Verlag GmbH.

EN ISO 23125, 2010. Safety of machine tools—Turning machines. Berlin, Germany; Beuth Verlag GmbH.

EN ISO 13849-1, 2008. *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design*. Berlin, Germany; Beuth Verlag GmbH.

EN ISO 13849-2, 2013. *Safety of machinery—Safety-related parts of control systems—Part 2: Validation*. Berlin, Germany; Beuth Verlag GmbH.

Günnel, B. et al. 2013. *EN ISO 13849-1—New quantitative requirements for Functional Safety in the machine tool industry*. ESREL Annual Conference 2013, Amsterdam, Netherlands.

IEC 61508-1, 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1: General requirements*. Berlin, Germany; Beuth Verlag GmbH.

IEC 61508-4, 2011. *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4: Definitions and abbreviations*. Berlin, Germany; Beuth Verlag GmbH.

Meyna, A. & Pauli, B. 2010. *Zuverlässigkeitstechnik—Quantitative Bewertungsverfahren*. Munich, Germany; Carl Hanser Verlag.

prEN ISO 16090, 2013. *Machine Tools—Machines for milling applications—Part 1: Safety*. Genf, Austria; ISO.

Schlummer, M. 2012. *Contribution to the Development of an Alternative Approach for a Proven-in-Use-Argumentation in the Automotive Industry*. Wuppertal, Germany; Dissertation.

The European parliament & the council of the European Union 2006. *Machinery Directive 2006/42/EC*.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Probabilities in safety of machinery—Part 1: Risk profiling and farmer matrix

Armin Bornemann
Deckel Maho, Pfronten, Germany

Yannick Froese
University of Applied Sciences, Frankfurt am Main, Germany

Luca Landi
Department of Engineering, University of Perugia, Italy

Heinrich Mödden
German Machine Tool Builders' Association (VDW), Frankfurt am Main, Germany

ABSTRACT: The new control system standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events; however, it avoids depicting them as relative frequencies. For the practical design engineers, a relative frequency approach is a more comprehensible form, because with the relative frequency a reconciliation with statistically acquired data is possible. This article closes some explanatory gaps caused by the one-sided emphasis on theoretical probability. In doing so, four contributions are provided in the context of field experience:

1. the concept of probability and the basic principles of distribution functions are elucidated using an "hourglass analogy",
2. fitting of an empirical Weibull distribution in order to evidence the theoretical requirements,
3. risk profiling method: plausibly stretched "risk snapshots" integrated to a "risk film" over the machine's lifetime,
4. proposals for a probabilistically founded dimensioning of enclosure.

This part 1 shall serve for a better understanding of the probabilistic concept, in particular for ongoing discussions of the merging of IEC 62061 & ISO 13849-1 into IEC/ISO 17305 in the Joint Working Group (JWG 1). Part 2 addresses more the practical design of machine tools and the corresponding standardization work of ISO/TC 39/SC 10 and before in CEN/TC 143. Together, part 1 and 2 are also intended to connect the world of International Standardization with the network of International Probabilistic Research, e.g. ESREL. For the sake of comparison with reality, a separate third paper of (Günnel et al., 2014) shows empiric findings of field data analyses.

1 INTRODUCTION

1.1 *Practical application problems*

The one-sided polarisation of ISO 13849-1 towards theoretical probabilities is a disadvantage, because the relative frequencies would enable the theory to be objectively verified. For the practical design engineer, a reconciliation with statistically acquired data or experimental results is necessary, as well as with subjective empirical values, e.g. by enumerating the relevant events (in the numerator) with regard to the total quantity of all events (in the denominator). This fraction is the original definition of a probability (see e.g., Montgomery), and it is a realistic introduction to probability theory, as also shown by the study of VDW (German Machine Tool Builder Builders Association) on operational dependability (Günnel et al., 2014). At the German Social Accident Insurance Scheme (BAuA 2010), the accident figures are recorded as frequencies, too, (with histograms), and they show two important results:

– a continuous improvement in safety due to decreased relative frequencies,
– an almost constant mutual relative percentage content of frequencies for individual degrees of seriousness (accident pyramids).

1.2 *Probability*

Mathematically viewed, probability has its unique definition within an axiomatic calculus. Yet, it is not at all clear what the term probability means, if it is applied to a non-mathematical situation (Main 2012).

As far as machine tools' safety is concerned, the terms "probability" or "likelihood" have not very often been used in developing the former product safety standards in CEN/TC 143. Their worldwide unique state of the art was established on a deterministic approach of the kind "identify hazard + compensate it with a bundle of safety measures = a safe machine" and is well-tried for more than a decade, now. Only when a second disconnecting channel in the control chains was discussed, the probability of a simultaneous failure of both channels was considered negligibly low. In contrast to this, since 2011 ISO 13849-1 made probability a key term in the standardization world. Most of the experts in the former deterministic approach are still in uncharted waters, when discussions circle around obviously different meanings of probability.

Here, in excerpted form only, the various manifestations of probability and certain fundamental relationships are explained: Probability as a theoretical value according to Laplace and Pascal is:

$$P(A) = \frac{number\ of\ events\ relevant\ for\ A}{number\ of\ all\ possible\ events} \tag{1}$$

e.g. rolling the dice

$$P(get\ a\ 6) = 1/6. \tag{2}$$

Probability as a relative frequency, e.g. of an experiment, according to von Mises:

$$F_{rel} = \frac{m(number\ of\ registered\ elements)}{n(number\ of\ all\ elements\ of\ a\ sample)} \tag{3}$$

Linking the two probability definitions with Bernoulli's Law of Large Numbers:

$$\lim_{n\to\infty} F_{rel} = P(A) \tag{4}$$

According to Bayes, probability can also mean a degree of personal belief, which however varies between different persons.

A well-defined mathematical fundament for calculating with probabilities was established by Kolmogorov. E.g. the first axiom postulated that every random event A has a probability $P(A)$, where:

$$0 \le P(A) \le 1 \tag{5}$$

Kolmogorov's Third Axiom on additivity, by the way, forms the basis for risk profiling, which is being proposed by the VDW for the superposition of individual "risk snapshots" to form a "risk film"; see below.

It needs no further explanation that the probability of mutual understanding can get very low, if students of Laplace and von Mises come across students of Bayes, even if they all apply the same mathematics of Kolmogorov.

For practical reliability engineering, the relationship between an experimentally determined histogram and an empirical density is very important and it has been compiled in very easily comprehensible form e.g. in Montgomery: several practical examples are adduced to explain how Bernoulli's Law of Large Numbers can be used to proceed from experimentally determined frequencies to theoretical probabilities and vice versa. In doing so, distribution functions can be derived, e.g. the normal distribution curve of Gauss.

ISO 13849-1 uses the Exponential distribution as a basis for describing the safety related reliability, without pointing it out. The probability of failure is then $F(t) = 1 - e^{(\lambda \cdot t)}$

In doing so, the failure rate λ plays an important role, several roles respectively, and it a priori assumes pure random failures. For the scope of the standard, which is "safety related parts of control systems", this is a very simple comparison standard. It fits quite well, if a constant failure rate λ can be suggested, e.g. for electronical products, which can be connected to the horizontal part of the "bathtub curve". In the VDW's study on operational dependability, by contrast, the Weibull distribution is used, because at machine tools the failures are not purely random, but the failure rate rises as the operating hours increase (as a consequence of wear and tear, ageing).

For the purpose of practical understanding, here the concept of probability and the basic principles of distribution functions are elucidated using an "hourglass analogy". This could help to improve the discussion about safety, in which the term "probability" still is mainly used in the sense "degree of belief" and not scientifically founded, but just subjectively emphasized.

1.3 *Hourglass analogy*

Detailed explanations of the basic probabilistic principles involved are provided e.g. in Montgomery. With a simplified model of an hourglass as an analogy, the basic concepts will be briefly outlined here; since with an hourglass the survival probability as "1 minus the probability of failure"

$$R(t) = 1 - F(t)$$

can be very vividly explained, because in the analogy it corresponds to the sand remaining in the glass. How are the various forms of a distribution function, namely:

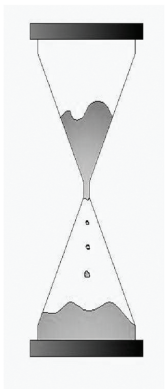
– density function $f(t)$
– failure probability $F(t)$ or survival probability $R(t) = 1 - F(t)$
– failure rate $\lambda(t)$

depicted in the hourglass analogy?

Figure 1 illustrates how the "distribution function of an hourglass" is developed from the density function. The basic assumptions required here are that per time unit approximately n grains of sand trickle through and there are a total of N grains in the glass (for the precise functioning of an hourglass are reference is given below).

All formulae apply only for $0 < t \le N/n$, because at $t^* = N/n$ the hourglass has run empty.

The definition of the PFH_d (Probability of Failure per Hour) as the average of the (dangerous) density function over an interval T shows that it corresponds quite well to the hourglass analogy. Fig. 2 shows an illustrating graphic, comparing the



Formulae (6)

$$f(t) = \frac{n}{N}$$

Density function

$$F_d(t) = \int_0^t f(\tau) \cdot d\tau = \frac{n}{N} \cdot t$$

Probability of failure

$$R_d(t) = 1 - \frac{n}{N} \cdot t$$

Probability of survival

$$\lambda(t) = \frac{f(t)}{R_d(t)} = \frac{\frac{n}{N}}{1 - \frac{n}{N} \cdot t}$$

Failure rate

Figure 1. Analogy to distribution functions with trickling sand.

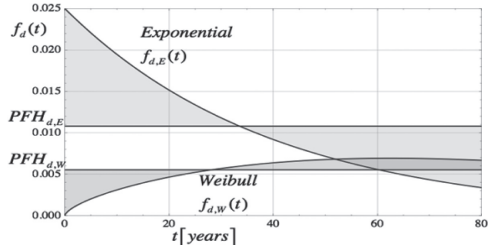


Figure 2. Comparison of PFH_d for Exponential and Weibull Distribution.

PFH_d-values of two different density functions, see also table 1 right column.

$$PFH_D = \frac{1}{T} \cdot \int_0^T \left(\frac{dF_d(t)}{dt} \right) \cdot dt = \bar{f}_d(t)$$
$$= \frac{1}{T} \cdot \int_0^T f_d(t) \cdot dt = \frac{F_d(t)}{T} \quad (7)$$

2 CRITICISM OF THE PERFORMANCE LEVEL

The PFH_d value is the crux of the matter in the studies of ISO 13849-1 and a "average variable in the kind of a frequency domain with the dimension [1/hour]". It is used not only for the quantifications, but also for the decision tree for determining target values as "performance level required" (PL_r, which is divided into PFH_d value ranges), see table 1. As explained above, an Exponential distribution is here assumed. For the example of "radioactive decay", it is true that in each second a fixed percentage of the atomic nuclei present in the substance will decay; the fewer nuclei are still present, the more slowly their number will decrease. This is not the case with the reliability of machine tools: the initial results from the VDW's studies on operational dependability show a significant deviation of the field data from an Exponential distribution (defining a temporally unchanging failure rate), because a time-dependence of the failure behaviour is clearly discernible. Against this background, during field data analysis criticism was voiced concerning the assumptions of a constant failure rate. As an improved model for the real failure behaviour, the Weibull distribution was chosen, which is able to factor in a failure rate rising to a maximum after a certain time period.

In the VDW's first study on the operational dependability of lathes, a Weibull distribution was approximated from field data for the clamping function of a lathe, with the following parameters: $\alpha = 0.000443$ and $\beta = 1.64$. For the empiric analysis, at the end of the available time series it was accumulated that $F(t) = 1$, which is an assumption on

Table 1. Classification of performance level (ISO 13849-1).

Performance level	Average probability of a dangerous failure per hour PFH_d [1/h]
a	$\ge 10^{-5}$ to 10^{-4}
b	$\ge 3 \cdot 10^{-6}$ to 10^{-5}
c	$\ge 10^{-6}$ to $3 \cdot 10^{-6}$
d	$\ge 10^{-7}$ to 10^{-6}
e	$\ge 10^{-8}$ to 10^{-7}

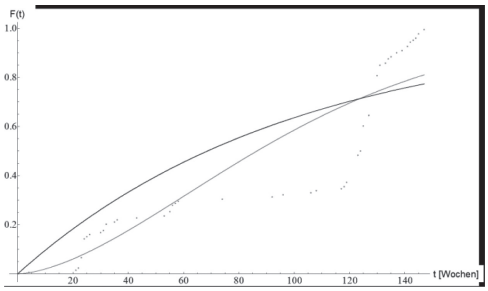


Figure 3. Empirical and theoretical failure probabilities for the clamping function of a lathe (Günnel et al., 2014).

the safe side. The curve for the empirical failure probability is shown separately in Fig. 3. It needs to be mentioned that all events influencing the reliability are incorporated in the empiric data, safety-related and non-safety-related events. How the separation of the safety-related share can be conducted by means of a fault tree, is explained in another ESREL 2014 paper of VDW (Günnel et al., 2014).

3 CRITICISM OF THE RISK MODEL AS SET OUT ON ISO 13849-1 AND CORRECTIONS

The phenomenon "risk" obeys a necessary causation. According to the ISO 12100 standard, which is meant to explain the Machinery Directive (MD) 2006/42/EG for the practical design, the risk assessment is the combination of risk analysis and risk evaluation. Risk analysis subsumes specifying the machine's limits (e.g., spatial and temporal limit), identifying the hazards involved, and estimating the extent of damage and the probability of its incidence. The risk $\mathfrak{R}$ is thus defined as a two-dimensional variable (damage severity S and expected frequency EF) which due to the EF element features a time-dependence:

$$\mathfrak{R} = S * EF \; where \; \mathfrak{R} = \mathfrak{R}(t) \tag{8}$$

Unfortunately, the risk increase due to time duration or number of repetitions of single hazards is not yet considered plausibly in ISO 12100.

Starting with the risk estimate, the risk assessment is used to decide whether, after executing the measures involved, the goals for risk reduction have been achieved.

For this purpose, the machine is divided into spatial and temporal limits, in accordance with 5.3.3./4 of the above-mentioned standard. In the risk assessments so far publicly available for machine tools, analysis concentrates on individual hazardous situations/events, typical for specific machines, in which the machines are being used (i.e., Man-Machine-Interaction, MMI). The modes of operation concept provide a standardized pattern for typical operator actions. From there, so called "stretched risk snapshots" can be derived as an abstracted MMI-model, which is needed as in input for the decision tree of ISO 13849-1. When this is done, the risk elements of ISO 12100 with regard to failure rates as "frequently based target values" are oddly compressed in ISO 13849-1, and the time slices of individual situations in relation to the machine's entire lifecycle is not plausibly recorded. For example, no distinction is drawn at all as to whether individual "risk snapshots" are frequently repeated or occur very rarely, although the risk content in the total risk for a particular machine is crucially determined thereby.

In order to cover the temporal limits appropriately in the risk assessment, in chapter 4 a VDW-proposal is explained for grouping together the individual "risk snapshots" in a holistic risk profile (the "risk film"). This proposal covers all relevant phases of the life-cycle (20 years in accordance with ISO 13849-1) of the machine tool involved together with their time slices t_j (as a weighting factor in the with $PFH_d \cdot t_j$ approximated exponential distribution). In doing so, realistic risk proportions are made available for risk assessment in accordance with ISO 12100. The aim of this "untangling" of the compressed risk elements in ISO 13849-1 is to enrich the current discussion in the standardisation working groups, in particular in sub group 5 of the "Joint Working Group" for the merging into IEC/ISO 17305.

A risk model that considers only PFH_d value ranges (without considering the time duration) is not plausibly congruent with the definition of risk in ISO 12100. This is because the relative frequency F_{rel} is closely dependent on the observation time t concerned, as can clearly be seen in Fig. 1 and Fig. 2; it is always the integral of the density function:

$$F_{rel}(t) = \int_0^t f(\tau) \cdot d(\tau) \tag{9}$$

This is a probability in the sense of a relative frequency.

In a recent publication (G. Gigerenzer), too, the misunderstandings and misdirections in risk estimation are vividly illustrated as "risk incompetence", which can be manifested even by high-ranking experts, if the risk is represented other than with relative frequencies in the Time Domain. Against this background, the risk definition provided in ISO 13849-1 can be seriously questioned

in regard to the PFH_d value ranges, because the time-dependence of the expected frequency of severity levels is not explicitly dealt with in the decision tree (called "risk graph") in Appendix A. Instead, the time-dependence is "accommodated" implausibly in risk parameter F, which is to be estimated out of the respective hazardous situation/event. Even recent discussions in the ISO working group in March 2014 for the ISO 13849-1 Amd 1 could not bring about a plausible definition of the parameter F, since it refers to the temporal ratio of hazardous exposure (which is plausible) *and in addition* to the frequency (*which is not plausible*). This risk model is therefore unsuitable for machine tools, because risk studies for machine tools must not simply ignore the temporally highly variable factor of man-machine interaction. It is precisely here that the greatest risk reductions can be achieved on the basis of defined access modalities within operating mode concepts, simply because the duration of the operator's exposure to hazard is minimised; temporally and spatially, e.g. with two-hand-control from a safely designed operator position. In the product standards for machine tools, there are detailed descriptions of how with the aid of fixed and movable guards the hazards resulting from random failures in the control chains can as far as possible be "kept away" from the operator. For risk assessment of machine tools, then one needs a "variable in the time domain", i.e. a reconciliation of:

– estimated expectable frequencies (EF) and corresponding severity levels (S) and
– tolerable limits for EF and S combinations.

From Meyna, the double-logarithmical Farmer diagram according to the Farmer graph (Farmer 1967) of Fig. 4 is explained in this context. A linear line represents a certain risk, comprising all possible combinations of EF and S of this risk. As regards machine tools, the S-axis could be normed to a maximum of one fatal accident, which can be considered—the very rarely occurring—worst case of injury. In the Farmer diagram, the individual steps for the risk reduction can be shown either as effect-related (reduced severity levels) or as cause-related (reduced frequencies) or as a mixture of the two; see Fig. 4 for the example of a flat-grinding machine with a primary wheel guard and an additional enclosure.

With the aid of the 3-step method of the Machinery Directive (or ISO 12100) in its specific implementation for machine tools, the effect of risk reduction can be illustrated as a vectorial variable, as described in VDMA Standard Sheet 34189; see the generalised principle in Fig. 4, starting with the "naked machine" by means of various measures:

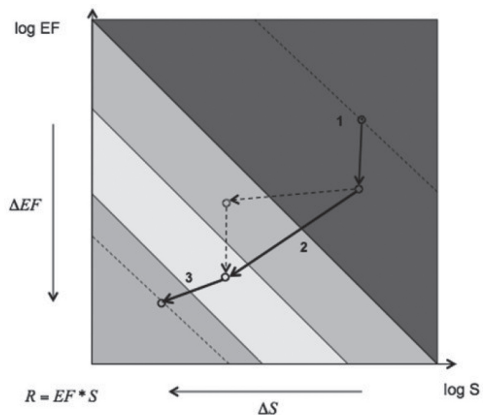


Figure 4. Theoretical risk reduction using the 3-step method acc. to ISO 16089 with primary wheel guard.

1. increase in inherent safety of the machine functions, in accordance with the technology-dependent state of the art
2. fixed or movable guard with interlocking and guard locking within an operating mode concept
3. instructive safety (operating instructions and training)

The functional safety plays a role only in the inherent safety of the machine functions and in the interlocking of the enclosure. With the third step a tolerable risk can be achieved, if the instructions for the intended application are followed by the user. Otherwise, only step 1 provides a risk reduction and an orange of even red risk range may put the operator in jeopardy, e.g. when defeating safeguards.

When applying ISO 13849-1, a case distinction drawn between a:

– Pure safety function pure (e.g., two-hand control with dependable stopping of the drives) and a
– technology-dependent machine function (e.g., tool clamping)

has so far not been defined.

The typical feature of a machine function is that the design engineer is in any case targeting a high level of reliability in order to optimise the machine's availability for the owner's benefit. The safety-related reliability (functional safety) is here always improved as well, because safety is a subset of the overall reliability/availability, since a failure of functional safety will be given full statistical weight in quantifying the dependability or availability of the machine concerned. A machine function can become a safety function if it has to be safely shut down when guard doors are opened, e.g. a gravity-loaded vertical axis. It is clear that in this context

time slices of the man-machine-interaction have to be factored in, because in the case of highly automated machines the transition to the safety function should have a far smaller time slice than the operation as a machine function. In fact, the trend to automation is going into this direction at least during the last decade.

Another unresolved discussion related to ISO 13849-1 is about the "overlapping of hazards". On the one hand side, safety functions are looked at very closely in order cope with every conceivable imponderability in the relevant control chain. On the other hand, these detailed dissections are not interpreted as regards the superposition of individual safety functions, i.e. a plausible composition that refers to the proportions of single effects is completely missing. This seems to be a considerable gap in the ISO 13849-1 on its way to probabilistic professionalism. As a consequence, the possible influence of an required increase of "Performance Level" on an improved operational safety is completely overestimated. This is at least true for machine tools, for which fixed and moveable guards within a safely defined modes of operations concept are the dominant risk reduction strategy. Uhlmann, Meister & Mödden are explaining the situation in detail (2012).

4 VDW'S PROPOSAL FOR RISK PROFILING

The overall machine risk is in the VDW's proposal totalled as a risk profile comprising the estimated individual contents of plausibly stretched "risk snapshots", as explained in VDMA Standard Sheet 34189, over:

- *all man-machine-activities and*
- *all hazards potentially caused by control system errors of*
- *all relevant machine components*
- *over all lifetime phases.*

In order to overcome the obstacles explained in chapter 4, VDW proposes an improved risk model in the Time Domain. Thereby, individual hazardous situations/events of man-machine interaction are modelled as (timely stretched) "risk snapshots" in order to follow ISO 12100, 5.5 (risk estimation), whereas the assumptions were made on the safe side for:

- the extent of damage in accordance with ISO 12100, 5.5.2.2 (Parameter *S* in accordance with accident statistics) and probability of occurrence of a damage in accordance with 5.5.2.3, with the influencing factors:

1. hazard exposure in accordance with 5.5.2.3.1 (Parameter F: activity-related),
2. probability of occurrence for the hazard in accordance with 5.5.2.3 (Parameter *O*: situation-related): the parameter *O* is in the risk profiles of the VDW mostly set to a value of 1, because the effects that reduce the probability of occurrence of damage are separately argued as a time share adducing a variable man-machine interaction. This is different from the utilization of parameter *O* in part 2 of this paper, because the "roof" of type A and B standards does not offer an explicit consideration of the time effect on the risk.
3. avoidability or controllability in accordance with 5.5.2.3.3 (Parameter *C*: operating-mode-dependent)

- and further relevant aspects in accordance with 5.5.3.

For a "risk snapshot", the connection between "cause" and "effect" can be depicted with the aid of the path diagram for mutually independent elements (*O*, *F*, and *C*) in Fig. 5:

1. The probability of a hazardous failure in all safety-relevant control chains $i = 1$ to m for the MMI activity $j = 1$ *to* n concerned $\sum_{i=1}^{m}\left(PFH_{d,i}\cdot t\right)$ as a possible "cause" and
2 The probability or relative frequency of an operator's injury with discrete severity levels Se 1 to Se 4 (in accordance with IEC 62061) as a possible "effect".

The result of the severity-level prognosis is directly dependent on risk parameters O_j, F_j and C_j. In order to arrive at the severity levels, the distribution of the severity levels Se 1 to Se 4 is connected with a histogram typical for machine tools (i.e., accident pyramids of the BAuA).

$$\mathfrak{R} = S_j \cdot F_j \cdot (1-C_j) \cdot O_j \cdot \left\lfloor \sum_{i=1}^{m} (-PFH_{d,i} \cdot t_j)_i \right\rfloor_j \quad (10)$$

Individual safety functions, with their expected frequencies are added together to form a superimposed failure probability $\sum_{i=1}^{m}(-PFH_{d,i}\cdot t_j)_i$, and multiplied by an occurrence probability O_j for the materialisation of a hazard.

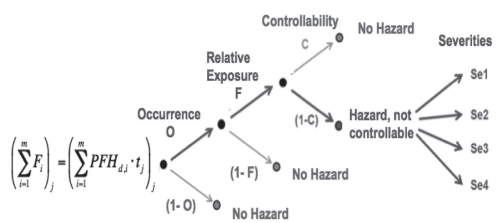


Figure 5. Risk path diagram, cause and effect relation.

The totalling function of the total risk $\mathfrak{R}(T)$ over all $j = 1$ to n risk snapshots during the time period $T = \sum_{j=1}^{n} \Delta T_j$ is obtained by totalling the snapshots with their temporal weighting in the approximated exponential function:

$$\mathfrak{R}(T) = \sum_{j=1}^{n} \mathfrak{R}_j(\Delta T_j) \tag{11}$$

$\mathfrak{R}(T)$

$$\sum_{j=1}^{n} \left[S_j \cdot F_j \cdot (1 - C_j) \cdot O_j \cdot \left(\sum_{i=1}^{m} PFH_{d,i} \cdot t_j \right) \right] \tag{12}$$

In this way, a plausible relationship is established between the multiplicity of causes (control system failures) and the bandwidth of possible effects (hazards and expectable severity levels) in the context of the highly time-variable man-machine interaction. The risk reductions can thus also be depicted in a time domain as an enclosure with interlock and locking in the context of an operating mode concept. This is what the product standards for machine tools are dealing with very successfully since more than a decade.

The risk profiling gives an interesting insight in the ongoing discussions about the "overlapping of hazards". The detailed dissections of single safety functions are dealt with in superposition (Kolmogorov's Third Axiom), and a plausible composition considering the proportions of single effects is introduced by this paper. This should not be neglected.

The risk profiling method is also intended to trigger a public discussion, particularly in the relevant standardisation bodies. For instance, in sub group 3 of the JWG 1 for the into IEC/ISO 17305, several machine examples have been discussed, for turning, grinding and milling machines, showing the significant risk reduction of guards, Fig. 8 to 12 are taken as examples from them. In addition, a presentation on this topic was given during the VDW's Technology Day at the METAV in March 2014. Furthermore, a comparison between different risk scoring systems (not yet compared e.g. in ISO/TR 14121–2) is feasible with the risk profiling, when a comparison object is selected, e.g. a machine as in fig. 8.

This risk snapshot, however, occurs more than once during a machine's service time (mission time), as a consequence a grouping of equivalent risk snapshots occurs. The factor with which the j-th snapshot has to be weighted over the exponential function as a group is reflected in the time slices; see Fig. 6, Fig. 7 and Fig. 9.

A practically useful risk model has to be able to depict the case that a reduction of activities with a comparatively increased risk of injury leads

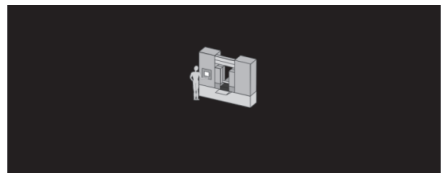


Figure 6. Individual risk snapshots within the service time (mission time).

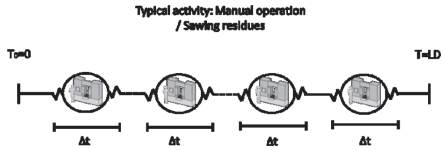


Figure 7. Repetition of risk snapshots and supsumption in a group as a a time share within the lifetime service time (mission time).



Figure 8. Example of a CNC milling machining center (5 axes).

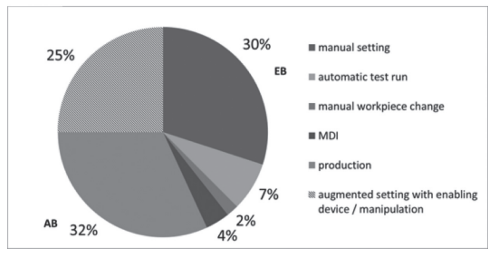


Figure 9. Time slices of different operating modes (AB = automatic mode, EB = setup mode, SBA = Special operating mode).

overall to a reduction in the total risk involved for the machine concerned. For example, for machine tools "offline setup" (instead of usual setup at the machine) is being developed using a 1-to-1 simulation model of the actual machine at a PC. This enables the risk to be significantly reduced by downsizing the amount of repeated activities during setup, see Fig. 10 with Operation Mode 2 (OM 2) as a significant risk share with 37,5%. This cannot, however, be argued with the risk model of ISO 13849-1, because it does not deal at all with a reduced repetition frequency of critical situations,

although this reduction (in the author's view) is the most important element in risk reduction for machine tools.

The result of the supsumption into groups of theequivalent risk snappshots of a time allocation over the service time (mission time) for the machine shown in Fig. 8 may resemble the diagram in Fig. 9.

The time shares of installation and troubleshooting are not listed, because these shares are relatively unimportant for the risk assumption caused by control failures on the other hand they represent accidents focuses caused by other reasons.

Furthermore, the cost-benefit ratio is for VDW companies an important issue in what is anyway a very predatory competition with low-price machines. This is another reason why a profiling method has been developed in the form of a Farmer Matrix and a two-dimensional Pareto diagram; see Figs. 10 and 11 below.

The risk presentation formats in Figs. 10 and 11 enable the design engineer to reduce the risk as best as possible, relating proposed additional

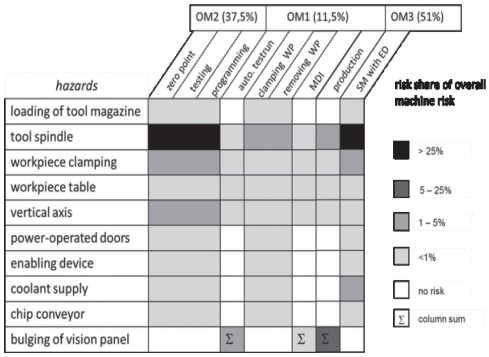


Figure 10. Two-dimensional Pareto diagram for the risk of a milling machine being used for its intended purpose, with a program test and enabling device in accordance with ISO 16090.

Expected frequency of a harm during a lifetime of the machine of 20 years acc. to PFH of PL of ISO 13849-1		Severity of a harm Acc. to IEC 62061 and 2010/16/EC			
		Se 1	Se 2	Se 3	Se 4
High	c,)c: 17,5 ÷ 100%	N	M	H	S
	d: 1,75 ÷ 17,5%	N	N	M	H
	e: 0,175 ÷ 1,75%	N	N	N	M
Low	<e: d. h. <0,175%	N	N	N	N

Severe Risk	S
High Risk	H
Medium Risk	M
Low Risk	N

Figure 11. (below): Proposal for a Farmer Matrix for comparing accumulated risk estimates.

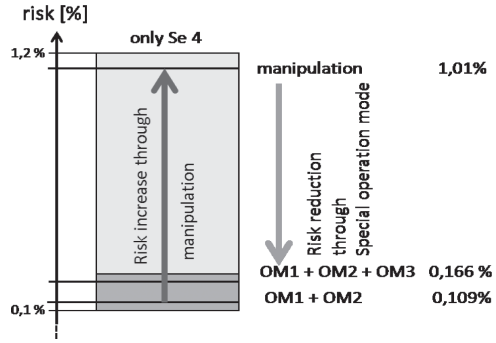


Figure 12. Risk comparison with standardised references for severity level Se 4.

efforts to the benefits obtained. Parameter studies are possible, answering the question: Which efforts leads to the highest risk reduction? Or the question (see Fig. 12: Is the special operation mode really the "lesser evil" compared to defeated safeguards (manipulation)?

5 PROBABILISTICALLY FOUNDED GUARD DIMENSIONING

The safety of a machine tool depends very much on the impact resistance of fixed and moveable guards (enclosure with vision panels). In the current product standards a non-probabilistic approach is still the basis for empiric tests to determine the required guard thicknesses. However, in reality all design variables are random variables, which can be described with statistical methods. The deterministic approach does not consider very unlikely events, but, it is desirable to know, what the probability P for a perforation event is, when the dimensioning is in compliance with the standard requirements: Is the probability tolerable? The probabilistic requirements for the functional safety can be directly compared with the requirements for the guard dimensioning, because both serve the same goal: operator protection. As a first step, it could be evaluated, how the deterministically defined state of the art in product standards performs in the probabilistic domain, i.e. if the impact resistance and the impact energy are being considered random variables.

Out of the density functions for the impact resistance R and the impact energy E, the probability P of a perforation event can be calculated. If e.g. impact resistance and impact energy follow a standard distribution, the relevant mean values and standard deviations can be empirically derived. The difference of both density functions, the "limit state function" is again a standard

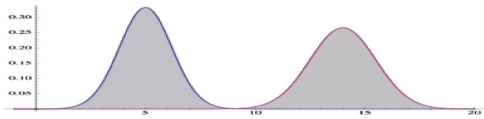


Figure 13. Intersection of two density functions.

distribution, of which the mean and standard deviation are functions of the input functions. The failure probability is the negative area element of the integrated limit state function. It is equivalent to the intersection area of the density functions of impact resistance and impact energy, see figure 13 and Montgomery. To start with, in Berlin and Tokio this approach is being studied for grinding machines, indicated in the CNC-Arena.

6 CONCLUSION

When comparing probabilistic theory and practice, the question arises, how the designer should consider a quantifiable tolerable risk in a responsible way. The deliberations above show that a quantitative risk assessment does not necessarily mean the numerical verification of the compliance with a tolerable limit. Due to the multi-dimensional variability of the man-machine-interaction as illustrated in the risk profiling in chapter 4, a precise proof is not feasible. However, showing the relative proportions of the risk reduction effects following the 3-step-method of ISO 12100 is much more important than giving an absolute value, which anyway depends on many subjective estimations. In doing so, estimates on the safe side that are summed up provide again a safe estimate. So, the essential effects become visible (see Fig. 10) and reproducible parameter studies can be conducted in a relatively objective manner (see Fig. 12). This enables the designer to justify that he derived a best possible design in the boundaries of technically available and economically acceptable means.

Depending on the specific aspects of a technology, numerically different tolerable risks develop as the significant differences in accident statistics of wood working and metal working machines clearly indicate, although the technologies are very similar except for the machined material (BAuA, 2010).

The best possible reference for a tolerable risk is the state of the art in well-tried product standards as ISO 16090 (before EN 12417). An increase of the requirements in the standard needs to be justified plausibly, and an appropriate consideration of the economic risk in Global competition is indispensable, not only in (small and medium) enterprises, but also from the Health and Safety experts.

Proving a tolerable risk can become a challenge, if product standards are not available. Then plausible probabilistic methods can be an useful argumentation platform, because the term "probability" in the law can be applied mathematically correct.

For the sake of comparison with reality, a separate third paper of Mödden & Günnel (ESREL, 2014) shows empiric findings of field data analyses.

Finally, a revealing oral statement on the quantitative consideration of safety, given by Dr. Heinrich Mushardt in 2013, an honoured VDW senior designer for machine tools, who retired recently, shall be quoted here:

"Under the obligation, to keep records of design analyses and to deal with potential hazards in a numerically plausible way, the designer can elude the allegation of culpable negligence. However, the completeness of analyses and the correctness of the decisions presumably can only be reviewed in case of damage. The numerically small values and the multitude of possible causes (for a hazardous effect) are located in the statistically limit range of small numbers. Statistically founded conclusions are not easy to obtain, when customers' requirements lead to a trend towards individual "one-off" designs. This causes scepticism whether the practical application of ISO 13849-1 can bring about significant improvements for the safety of machine tools. Risks due to foreseeable human behaviour shall be excluded, but there are also a not foreseeable misuse, technical failures and working errors. On this background, it should not be forgotten how rare severe injuries at machine tools occur altogether, and that if one severe accident happens, unforeseeable events or unforeseeable misuse of possibly criminal conduct play a major role but NOT primarily a lack of functional safety."

REFERENCES

Bundesministerium für Arbeit und Soziales 2010. Sicherheit und Gesundheit bei der Arbeit 2010, Unfallverhütungsbericht Arbeit, BAuA.

CNC-Arena:http://www.cnc-arena.com/de/emagazine/01-2014/, see page 24.

EN ISO 12100, 2010. Safety of machinery—General principles for design—Risk assessment and Risk reduction. Berlin: Beuth Verlag GmbH.

EN ISO 13849-1, 2008. Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design. Berlin: Beuth Verlag GmbH.

Farmer, F.R. 1967. Containment and sitting of nuclear power plants—Siting criteria—A new approach International Atom Energy Agency, Vienna, Austria.

Gigerenzer, Gerd 2013. Risiko—Wie man die richtigen Entscheigungen trifft, C.Bertelsmann, in English:

Risk Savvy, How to Make Godd Decisions, Penguin New York.
Günnel, B. et al., 2013. EN ISO 13849-1—New quantitative requirements for Functional Safety in the machine tool industry, ESREL 2013.
Günnel B. et al., 2014. Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849 1, ESREL 2014.
IEC 62061, 2005. Safety of machinery—Functional safety of electrical, electronic and programmable control systems for machinery. Berlin, Germany; Beuth Verlag GmbH.
IEC/ISO 17305, 2014. Safety functions of control systems, Joint Working Group 1 (draft 2014).
ISO/CD 16090, 2014. Machine tools—Safety—Milling machines (draft international standard) Berlin, Germany; Beuth Verlag GmbH.
Main, Bruce W. 2012 Risk Assessment—Challenges and Opportunities, Ann Arbor, USA; design safety engineering inc.
METAV 2014 press release VDW-Technology Day "Safe ty engineering for metal-cutting machining"
Meyna, A. & Pauli, B. 2010. Zuverlässigkeitstechnik-Quantitative Bewertungsverfahren. Munich, Germany; Carl Hanser Verlag.
Montgomery, D. et al., 2010. *Engineering Statistics*. Wiley; 5 Edition.
The European parliament & the council of the European Union 2006. Machinery Directive 2006/42/EC.
Uhlmann, E. et al., 2012. Sicherheit an Werkzeugmaschinen: Die Bedeutung der trennenden Schutzeinrichtung für die Risikoreduktion an Werkzeugmaschinen, ZWF Jahrgang 107 Hanser Verlag.
VDMA Einheitsblatt Nr. 34189 2013. Steuerung von Werk-zeugmaschinen—Risikobeurteilung, Draft 2013.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Probabilities in safety of machinery—Part 2: Theoretical and practical design

Armin Bornemann
Deckel Maho, Pfronten, Germany

Yannick Froese
University of Applied Sciences, Frankfurt am Main, Germany

Luca Landi
Department of Engineering, University of Perugia, Perugia, Italy

Heinrich Mödden
German Machine Tool Builders' Association (VDW), Frankfurt am Main, Germany

ABSTRACT: As stated in part 1 of the article, standard ISO 13849-1 deals with the theoretical probabilities of hypothetical individual events and the possibility of reconciliation of this theoretical approach with empiric field data is partly neglected.

In part 2 the problems arising during the real design of SRP/CS (Safety Related Part of a Control System) of machines are addressed on the background of relevant safety standards. Using the informative theoretical appendix A of ISO 13849-1 to determine the Performance Level required (PLr) may cause sometimes technically impracticable requirements, which are far beyond the state of the art in existing type C standards. For the sake of connection between theory and practice, the probability of occurrence of a hazardous situation must be taken into account in order to appropriately consider the required risk reduction of a SRP/CS in the context of the three-step-method of ISO 12100. For this purpose two practical solutions are provided:

– a methodology for PL_r definition for safety functions considering a realistic probability of occurrence of hazards, using a hybrid approach of ISO 13849-1 and IEC 62061,
– a "table based" methodology for the design of machine tool control system considering all the realistic "occurrences" as stated also in the "new" ISO/TR 14121-2. Those two contributions are extracted from the work during the ISO/TC 39/SC 10/WG4 meetings (ISO/CD 16090 for milling machines).

The selected safety function for 2.) is very similar to the safety function "prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece" of the standard ISO 16090-1. This safety function was chosen in another paper of Mödden, Günnel for ESREL 2014. Therein, the analysis of field data of real milling machines shows that a reliability between PL = a and PL = b is actually being achieved with state of the art design. This finding connects quite well theory and practice of state of the art milling machines.

1 INTRODUCTION

The design of Safety Related Parts of the Control System (SRP/CS) it is one of the emerging problems of the new standard requirements related to Machinery Directive (European Parliament and the Council of European Union, 2006).

The leading standards are ISO 13849-1:2008 and IEC 62061:2005 respectively from a "mechanical and electronic point of view".

If compared with the older "European standards" (EN 954-1:1996), the basic reliability concept of categories and design of systems with a given hardware fault tolerance has been rewritten in terms of reliability calculation.

Now the SRP/CS has to be designed using a validation procedure that requires a minimum reliability to be acquired in terms of Mean Time to Dangerous Failures ($MTTF_d$).

Also other very important concepts have been developed in the new standards mentioned above. Such as the requirement of a Diagnostic Coverage (DC) and the design of systems which considers the Common Cause Failures (CCF). Trying to

summarize with an understandable simplification, using the new standards a good architecture on the SRP/CS (for example doubled channels) is no longer sufficient to achieve the required minimum reliability.

The acronyms for the overall design safety concepts of the two standards are: PL (Performance Level, ISO 13849-1) and SIL (Safety Integrity Level, IEC 62061).

As it will be explained in detail in the next paragraphs those two different concepts, whose full calculation are performed in different ways, are comparable in terms of Average Probability of Dangerous Failure per Hour (PFH_D, expressed in terms of 1/h).

The main problem of those two "safety views", often sharing the same components on a real machine, is the results of risk assessment (see also Part 1 of this paper). The minimum PFH_D required for assuring a sufficient level of safety may be different if the calculation it is performed using the SIL or PL concept, because ISO 13849-1 is cutting at $MTTF_d$ at 100 year and IEC 62061 is doing it with 150 year.

And if some technologies are used for SRP/CS, e.g. pneumatic or hydraulic, only the PL concept according ISO 13849-1 is still valid for the full design process, but often both are valid.

The PL_r (required) needs to be derived from the risk assessment with the three-step-method of risk reduction according to ISO 12100:2010.

The Machine Directive only requires a risk assessment, but does not specify as it shall be done. Moreover also the ISO 12100, type A standard, specifies the principles of risk assessment and does not specify any method to do it.

In the following paragraphs some methods useful to calculate PL_r, in full accordance with the risk assessment principles of ISO 12100, will be presented. In the first paragraph, an hybrid method ISO 13849-1—IEC 62061 will be presented. In the second paragraph, a table method covering all the phase necessary to perform the risk estimation for a general safety function of a SRP/CS will be shown.

2 DEFINITION OF THE PL_r

Trying to merge the two different approaches of the two already mentioned standards, some preliminary consideration on the definition of a hazard occurrence probability in ISO 12100 has to be done.

2.1 *The "occurrence problem" on ISO 13849-1*

If somebody sees the element of risk of the Figure 1 ISO 12100, one can notice that the overall

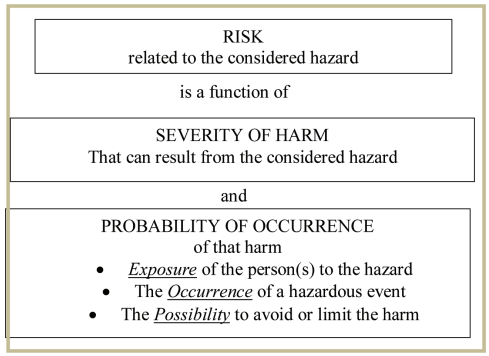


Figure 1. Elements of risk according to ISO 12100.

probability of occurrence of the harm depends on (see part 1 of the paper):

1. exposure,
2. occurrence of hazardous event,
3. possibility of avoiding or limiting the harm.

If one looks at the definition of Occurrence (point 5.5.2.3.2 of the ISO 12100), the relevant factors that influence the probability of occurrence of harm are:

1. reliability and other statistical data,
2. accident history,
3. history of damage to health,
4. comparison of risks.

The standard says clearly that *those factors shall be taken into account.*

Looking at informative Annex A of ISO 13849-1, concerned with the contribution to the reduction in risk made by the SRP/CS, amazingly, an explicit provision of the occurrence parameter is missing.

The method given here provides, as stated in ISO 13849-1: "only an estimation of risk reduction and is intended as guidance to the designer and standard maker in determining the PL_r for each necessary safety function to be carried out by an SRP/CS".

In our opinion this definition it is too conservative and some of the already mentioned relevant factors of ISO (e.g. real accident history) cannot be taken plausibly into consideration.

To give an example, we are looking at the Safety Function (SF) of limited speed monitoring—maximum spindle speed during some Modes of Safe Operation (MSO) for milling machines (ISO CD/16090, 2014, table J.2. paragraph 2). Among experts, there are no accidents known due to this risk. If the occurrence of a hazard is not taken into account, no risk reduction can be done. The same is true, if a real harm related with this risk

never occurs in the operational field. The point is that the machines are designed the last 10–15 years with high safety standards and the technology has been changed in the drive control system. Before this has been done, some accidents had occurred. This evidence/lack of injuries can be researched, for example, on national accident institution surveillance reports (e.g. INAIL 2013). From the "experience point of view" the theoretical severity of the harm is high, but in the "real world" we have no evidence of real accidents.

In the novel technical report ISO/TR 14121-2 (ISO 2012) the problem of *probability of occurrence of hazard* and its correlation with *probability of occurrence of harm* is clarified.

In point 5.4.3 of the ISO/TR it is clarified that occurrence of a real harm is a fundamental aspect to take into account and this occurrence is strictly connected not only with potential risk, but also with occurrence as stated in ISO 12100.

In all the risk estimation tools proposed in subsequent paragraph 6 of ISO/TR 14121-2 the occurrence is always taken into account.

For example if the risk graph method is used according to ISO 14121-2_2013, section 6.3.2, the occurrence is divided in three levels:

1. O1—low
2. O2—medium
3. O3—high.

In IEC 62061 there are even 5 levels as defined in table A.3.

In ISO 13849-1 one cannot find any definition or any variations or levels.

From statistical data on the market, usually we have data of occurrence of harm and not occurrence of hazard, which is different from a theoretical point of view. In other words, the SRP/CS designer has to be sure that there is no accident data recorded for a given SF, but this fact does not mean no occurrence of hazardous event. It only means that the designer managed to cope with the hazardous events by applying the right safety measures.

For instance usually we have designed and properly installed other protective measure (as guards) for a specific risk reductions (e.g. impact with moving parts) effecting also the SF risk estimation.

If the occurrence of hazard is low, the general hypothesis of reducing the risk index by one level appears to be a good compromise between the theoretical and the real application (see Fig. 2). This can be done, if you use the informative risk graph of ISO/TR 14121-2. On the other side, when the occurrence of hazard is high, the risk index is increased, if a possible severe injury is expected.

From the authors point of view, the entire machine tool is a very complex machine made of several hundreds or thousands of components and the correlation between different safety principles leading to a common risk reduction cannot be simply neglected, but needs to be considered properly (see chapter 4 of part 1 of the paper). If a very complex machine with several correlations between SF and other safety measures has to be taken into account, the designer has to take an overall view of the entire machine. The proposed risk estimation matrix method of ISO/TR 14121-2 (Table 1), taking into consideration directly the overall probability of harm it is a quite realistic approach.

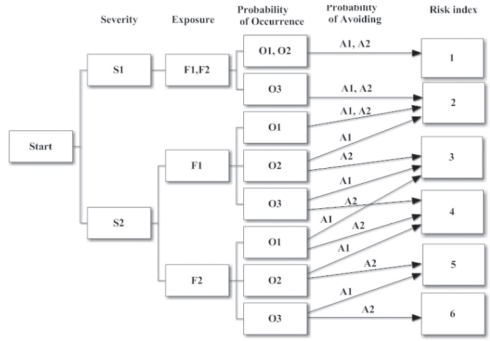


Figure 2. Risk graph from ISO/TR 14121-2.

Table 1. Risk estimation matrix from ISO/TR 14121-2.

Prob. of occurence of harm	Severity of harm			
	Catastrophic	Serious	Moderate	Minor
Very likely	High	High	High	Medium
Likely	High	High	Medium	Low
Unlikely	Medium	Medium	Low	Neglig.
Remote	Low	Low	Neglig.	Neglig.

2.2 *Element of risk in different standards and technical reports*

Before the merging project IEC/ISO 17305 is providing concrete results, we have at first to summarize the different meanings of risk element of ISO 13849-1 and IEC 62061.

2.2.1 *Severity (S or Se)*

In ISO 13849-1 only two severity levels are used, and they are called S1 and S2, where S2 is severe injuries. In contrast hereto, in IEC 62061 four severity levels are used, which largely correspond to the four severity levels of EU Decision on general safety of products (Decision 2010/15/EU, called RAPEX), see Table 2.

Table 2. SIL from IEC 62061.

Severity (Se)	Class (Cl)				
	3–4	5–7	8–10	11–13	14–15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

Comparing the severity, bruises and/or cut wounds without complications are classified as S1 in ISO 13849-1 (Table A.1.), that corresponds only partially to the grouped severity levels Se1 and Se 2 of ISO 62061.

The severity levels Se 3 and Se 4 of ISO 62061 are, in accordance with Table A.1, largely congruent with severity level S2 of ISO 13849-1.

2.2.2 *Exposure (F or Fr)*

In ISO 13849-1 only two exposure levels are used, and they are called F1 and F2 (the F2 is frequent exposure, a very rough method which even tries to compress the duration of hazardous situations into a frequency, which is not plausible, as already stated in part 1 of the article).

In IEC 62061 five exposure (*Fr*) levels are used (Table A.2) with numerical values that can to be assigned.

2.2.3 *Possibility of avoiding the hazard—harm (P or Av)*

In ISO 13849-1 again only two probabilities of avoiding of hazard levels are used, and they are called P1 and P2 (the P2 is to be used, if there are no/little chances to avoid the hazardous situation).

In IEC 62061, we have a different theoretical contribution, here we have three levels of probability of avoiding or limiting *harm* (*Av*) not hazard (Table A.4) with three different numerical results possible from an overall estimation.

2.2.4 *Occurrence of hazard (Pr)*

In ISO 13849-1 is not possible to take an occurrence probability explicitly into account. Very different from this, in IEC 62061 we have five levels available. As regards automatically controlled machines, especially the risk of unexpected start-up of a movement has to be taken into consideration in the context of the three-step-method of risk reduction of ISO 12100. Only then it is possible to estimate the occurrence probability that will be caused, if the SRP/CS fails. The intended use needs to be taken into consideration e.g. as regards the modes of operation (e.g. setup, manual or automatic working, maintenance). On the background of a kind of "naked" machine (i.e. only step 2 of 3 steps of risk reduction is considered), the occurrence probability of a hazard due SF failure cannot reasonably estimated. But, ISO 13849-1 tries to do exactly this, not surprisingly concluding that the occurrence probability rather should be equals to 1.

2.3 *A practical "partial merging" method for type C standards*

The risk classification method in accordance with IEC 62061 is of general validity, and not only restricted to electrical control systems. Therefore, it can also be applied to mechatronic control chains as ISO 13849-1 regards them. The requirement for a SF made of mechatronic components can thus be defined either with the informative decision tree, (wrongly called "risk graph") of ISO 13849-1, or with a risk classification in accordance with IEC 62061. Other parts of IEC 62061 however, for example the beta factors estimation for common cause failures, are not useable, when hydraulic and pneumatic systems are used.

In IEC standard the results of risk estimation leads to a class of probability of harm (not hazard) CL:

$$CL = Fr + Pr + Av \tag{1}$$

In Table 2, the result of IEC 62061 is a SIL.

So a defined PFH_d value range dependent of a SIL is stated (see IEC 62061, Table 3).

The resulting PFH_d value range is likewise defined in ISO 13849-1 Table 3, Table 4.

From the Tables 3 and 4 we can conclude that because the value ranges of PFH_d are largely

Table 3. PFH_d and SIL.

SIL	Probability of dangerous failures per hour (PFH_d)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 4. PL from IEC 13849-1.

PL	Average probability of dangerous failures per hour (1/h)
a	$\geq 10^{-5}$ to $<10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $<10^{-5}$
c	$\geq 10^{-6}$ to $3 <10^{-6}$
d	$\geq 10^{-7}$ to $<10^{-6}$
e	$\geq 10^{-8}$ to $<10^{-7}$

congruent, the risk graph and the risk classification can be plausibly linked to each other. The PFH_d parameter is a common mathematical platform between ISO 13849-1 and IEC 62061 (assuming that also the IEC 62061 definition is an "average", as illustrated in part 1 of this paper).

The PL = a has no correspondence with SIL.

In Figure 3, the result of the decision tree of ISO 13849-1 is a PL_r.

A SIL 1 is equivalent to PL = b and PL = c. Only for injuries with a lower severity of S1, PL = b can be derived, since for a severity of S2 at least PL = c is demanded. SIL 1, however, subsumes the entire PFH_d value range of PL = b and PL = c.

SIL 2 is completely equivalent to PL = d and SIL 3 is fully equivalent to PL = e.

Furthermore, IEC 62061 provides, as we have already seen, more "levels" for each parameters and the overall CL, see equation 1 and Table 2 above. This enables a substantially more realistic and more accurate assessment of the risk reduction to be achieved by the SRP/CS than in ISO 13849-1.

The requirement for SIL 1 is, in accordance with Table 2 detailed for the following combinations and risk classes:

– severity level Se 3 with CL 8–10,
– severity level Se 2 with CL 11–13,
– severity level Se 1 and CL 14–15.

On the basis of these requirements of SIL 1, the following case differentiations are derived for the minimum PL_r:

Se 1 and CL = 14, SIL 1 → $PL_{r,min}$ = b
Se 1 and CL = 15, SIL 1 → $PL_{r,min}$ = c
Se 2 and CL = 11, SIL 1 → $PL_{r,min}$ = b
Se 2 and CL = 12 or 13, SIL 1 → $PL_{r,min}$ = c
Se 3 and CL = 8 or 9 or 10, SIL 1 → $PL_{r,min}$ = c

because injuries of Se 3 are irreversible and comparable to S2 in ISO 13849-1, and there PL = c (S2, F1, P1) is the lowest possible PL.

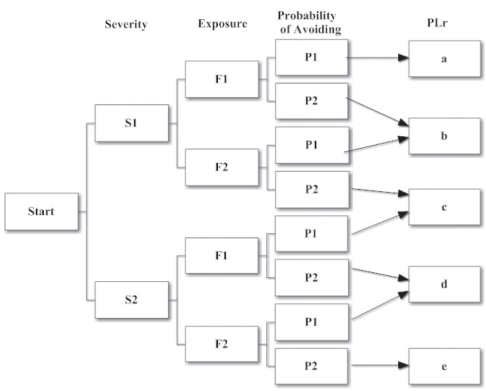


Figure 3. PL_r from IEC 13849-1.

In IEC 62061, below SIL 1 "other measures" must be provided at least (OM in Table 2). We have also a very important note to Table 3 point 5.2.4.2 in the IEC 62061. If we have less than SIL 1 from risk estimation, the minimum requirements are the ones of category B of ISO 13849-1.

The requirement of OM is, in accordance with Table 2, detailed for the following combinations and risk classes:

Se 1 and K = 11–13, AM → $PL_{r,min}$ = a
Se 2 and K = 8–10, AM → $PL_{r,min}$ = a
Se 3 and K = 5–7, AM → $PL_{r,min}$ = a

In addition to $PL_{r,min}$ = a, the wording "other measures" of IEC 62061 is used. Following this approach, the IEC 62061 OM + ISO 13849-1 PL = a become a kind of "safety integrity performance level" with the sum of the requirements of both.

In our opinion, this hybrid approach gives excellent results on removing the very rough risk estimation of ISO 13849-1 (see also Hedberg & others, 2011).

Example 1: the following example shows the difference that could be found using the direct approach of ISO 13849-1 instead of the hybrid one presented. The SF function being analysed here is *limited speed of spindle due to tool* being applied in different Modes of Safe Operation (MSO).

When exceeding the maximum processing speed of the tool, a controlled stopping of the tool spindle shall takes place according to IEC 60204-1: 2009, 9.2.2 depending on the technique applied.

Usually the maximum processing speed shall be provided in the tool parameters of the tool management (manual human data input).

The risk estimation of ISO 13849-1 leads for long stays during some operation to: S2-F2-P2 and then to PL = e. This is often far away from both, and from the state of the art of all the tooling machine technologies and from technical achievability.

If the risk estimation of IEC 62061 is used, we can find: CL = Fr + Pr + Av = 4 + 1 + 5 = 10 with a possible severity Se = 4 we have a SIL 2 and then with the partial merging approach PL = d. Then we have to define, if we have to use a category 2 or 3 system, because a PL = d can be designed in both ways. But when fixed or moveable guards are in operation (for example full enclosure with interlocked guards and guard locking during automatic machining), one can have longer stays according to IEC 62061, because the severity Se = 3 is sufficient.

The main difference between the two simplified risk estimation methods is that it is possible also to

take into consideration positive field experiences, e.g. that no accidents are known among experts for a certain machine type with a specific SF and so even Pr = 1 can be justified. The corresponding discussion is ongoing in the working groups of type C standards.

There are also some technical achievability problems with this SF, which will be considered in detail in the next paragraph.

3 A NOVEL TABLE METHOD FOR CONCISE RISK ESTIMATION OF A SAFETY FUNCTION OF A SRP/CS

From the machine builders point of view, a precise identification and explanation of all the SF's is needed in order to develop a model for both, the risk estimation and the quantification of the reliability (PL or SIL). However, in the current type C standards for machine tools, it is very difficult to find a precise identification and risk estimation for all the SF of a given machine.

Also some technical information of how to reach the required safety level is welcomed by machine designer (for example technical information based on state of the art of current machine on the market or technical achievability of a given PL).

A "technically design oriented" view leads to very detailed explanations of all the SF's, which could take several pages in the type C standard. The first ISO type C standard for machine tools with a small SF description is the ISO 23125:2010/Amd 1:2012—Safety of turning machines. In this standard the main SF are described in a single page (see point 5.11 b) trying to give the main information on PL_r regardless of the different requirements for similar SF in different zones of the machine. For example in this standard the enabling device SF has always a PL_r = d requirement, this is a very simplified approach.

It is clear that this simple table is not satisfactory at all, not even for a simple analysis: the PL_r of the SF depends on the kind of the control chain which builds the SF and it also depends on the risk reduction of an enabling device. So a realistic risk estimation has to consider all the factors of paragraph 2 of this paper for all the different risk reduction effects of an enabling device. Moreover this has to be done in all the specific applications, e.g. in every mode of operation there needs to be a specific requirement in a type C standard. Moreover an enabling device has always to fulfil at least two different safety functions: a "safe stop function", if it is released and "protection of unexpected movement", if the enabling device is not used.

Trying to summarise the main requirements for a methodology for SF requirement of a general type C standard, at least the following tasks have to be taken into consideration:

- identical SF in different zones of the machine (for example work zone, maintenance zone, tool magazine, tool changer) may lead to different required performance level depending on the individual risk estimations,
- identical SF used in different modes of operation may have different required performance level depending on the individual risk estimations. For example some "other protective measure" as partial guards or safe operator position may affect the risk estimation for the SF (se parameter P),
- detailed explanation of the risk reduction of a safety function and according additional normative requirements.
- remarks for details of SF which are not requirements, but can help the designer in defining a safe machine control system,
- classification with the parameter S, F, P, as explained above and with plausible description of why it was been chosen,
- additional explanations needed as stated in paragraph 1.1 of this paper. All those factors may affect the PL_r from a theoretical formulation to a realistic one as already explained.

It is also very important to give a clear definition of the main quantities to be used, especially when different definitions can be used. For example the definition of *short* and *long presence* differs from one standard to another, so a clear definition of what is a short stay and what is long stay is very important for exposure parameter (see paragraph 1.2.2).

The resulting concise table method comprises two different tables:

- ***SF_table 1***: list of SF with numbering, designation and cross reference to the occurrence probability of hazards that can be found later in the SF_Table 2 (see Table 5 below),
- ***SF_table 2***: table method for the concise risk estimation of every SF, see Table A.2, appendix A for the full table example.

Table 5. Example of SF_table1, numbering, designation and cross reference.

No. of SF	Designation	Cross-reference to SF_table 1
SF 01	Safety-related stop function	1.5, 1.9, 4.1, 5.3, 9.1, 10.1, …
SF 02	Manual reset function	
SF 03	Start/restart function	15.4, 20.4
SF 04	Local control function	1.7, 15.5

These two tables will be proposed as normative (mandatory) for the new type C standards of milling machines ISO 16090-1.

Going back to *example 1* of paragraph 2.3 the entire concise risk estimation in tabular method is presented in Table A.2 of appendix A.

The selected safety function is very similar to the safety function "prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece" of the standard prEN ISO 16090-1. This safety function was chosen in another paper of Mödden & Günnel for ESREL 2014. The analysis of field data of real milling machines shows that a reliability between PL = a and PL = b is actually being achieved with state of the art design.

3.1 *Typical demand rates of safety functions*

To perform the necessary $MTTF_d$ calculation and subsequent PL quantification according to ISO 13849-1, it is very important to give to the machine builder the *typical demand rates* of SF. This additional table will be informative, because different demand rates are possible for different machine types.

The demand rates are divided into groups of machine depending from the category defined in the standard. For the milling machine standard, it will define 4 different groups of machines: from the simple group 1 (manual machines) to the group 4 (complex transfer and special purpose machines). See Appendix A for the full table example of demand rates.

4 CONCLUSIONS

In this part 2 of the paper, the problems arising during the real design of SRP/CS using exclusively ISO 13849-1 are addressed. Using an ISO 13849-1/IEC 62061 "partial merging" approach based on the PFH_d, which is a common mathematical basis in both standards, proper risk reduction requirements for the SRP/CS or SF can be found both in terms of PL or SIL.

A novel "table based" methodology for concise risk estimation utilizable in type C standards is presented. The selected safety function is very similar to the safety function "prevention of unexpected start-up of a movement of a linear or rotational axis with an incorrectly clamped workpiece" of the standard ISO 16090-1. This safety function was chosen in another paper of Mödden & Günnel for ESREL 2014. The analysis of field data of real milling machines shows that a reliability between PL = a and PL = b is actually being achieved with state of the art design. This finding connects quite well theory and practice of state of the art milling machines.

Those two contributions are extracted from the work during the ISO/TC 39/SC 10/WG4 meetings (ISO/CD 16090-1 for milling machines).

REFERENCES

Decision 2010/15/EU, 2009. *Commission Decision of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System 'RAPEX' established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC* (the General Product Safety Directive) (notified under document C(2009) 9843).

EN, 1996. *EN 954-1—Safety of machinery—Safety-related parts of control systems—General principles for design.* International Organization for Standardization, Geneva, Switzerland.

European Parliament and the Council of European Union, 2006. *Directive2006/42/EC on machinery safety.* International Organization for Standardization, Geneva, Switzerland.

Günnel B., et al., 2014. *Proven in use in the machine tool industry for demonstrating the quantitative Functional Safety according to EN ISO 13849* 1, ESREL 2014.

Hedberg, J; Söderberg A. & Tegehall J., 2011. *How to design safe machine control systems—a guideline to EN ISO 13849-1*, SP Technical Research Institute of Sweden, SP REPORT 2011:81, ISBN 978-91-87017-14-8, ISSN 0284-5172.

IEC, 2012. IEC 62061:2005 + A1:2012. Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems. International Organization for Standardization, Geneva, Switzerland.

IEC/ISO 17305, 2014. *Safety functions of control systems*, Joint Working Group 1 (draft 2014).

INAIL, 2013. *7° Italian report on surveillance on the market*, Inail, Rome. Can be found and downloaded in Italian: http://www.ispesl.it/informazione/eventi/DTS/20137Rapporto.pdf.

ISO, 2008. *ISO 13849-1—Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2010. *ISO 12100 Safety of machinery—General principles for design—Risk assessment and risk reduction.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2012a. *ISO/TR 14121-2—Safety of machinery—Risk assessment—Part 2: Practical guidance and examples of methods.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2012b. *ISO 23125:2010/Amd 1:2012—Machine tools—Safety—Turning machines—Amendment 1.* International Organization for Standardization, Geneva, Switzerland.

ISO, 2014. ISO/CD 16090-1—Machine tools safety—Machining centres, Milling machines, Transfer machines—Part 1: Safety requirements. International Organization for Standardization, Geneva, Switzerland.

APPENDIX, TABLE METHOD FOR RISK ESTIMATION OF A SF OF A SRP/CS

Table A.1. Example of concise risk estimation of a SF, from ISO 16090:2014 (draft).

No.	Subject	No of SF	Explanation of safety function effect, other requirements*	Remarks**	Classification according to ISO 13849-1: 2006	Additional explanation see ISO 12100:2010, 5.5.2.3.2	PL_r
2	Tool spindle and tool clamping device						
2.2	Tool clamping	SF 16	***Limited speed—maximum processing speed of the tool in MSO 1, MSO 2, MSO 3*** When exceeding the maximum processing speed of the tool (see 3.6.1) a controlled stopping of the tool spindle takes place according to IEC 60204-1:2009, 9.2.2 depending on the technique applied. The possible input of the maximum processing speed (see 3.6.2) shall be provided in the tool parameters of the tool management.	Fault incident may occur unexpectedly in MSO 2 or MSO 3. Incorrect input of tool parameters is most common source of failure. Tool data may be provided manually as well as by a central control level of the machine. The maximum permitted processing speed depends on constructive limitations of the spindle, the clamping means and the size, mass and unbalance of the specific tool. These limitations are given by the manufacturer of the machine.	**S2**: – **F1:** In MSO 2 or MSO 3 short presence*** in hazard zone and limited speed depending on the mode of safe operation, (see 2.3 in this table). In MSO 1 protection by guards. **P2:** –	Rotational speed parameters may be provided by manual data input or Rotational speed parameters may be provided by a central control level of the machine State of the art is PL = a (technical achievability, see separate paper Mödden, Günnel 2014). Accidents in MSO 2 or MSO 3 due to lack of functional safety are not known.	PL_r = a

*In this column only normative requirements, no explanations.
***Remarks are not mandatory, here additional information can be provided.
**In this case the "short stay" in the hazardous zone is defined as less than 1 hour accumulated during a 8 hours shift, not more than 10 minutes per exposition (see IEC 62061:2005, table A.2).

Table A.2. Examples of typical demand rates of operations and SF.

No.	Function	Machine group			
		Group 1, number of operations	Group, number of operations	Group 3, number of operations	Group 4, number of operations
1	Mean operating time in days per year (d_{op})	300	300	300	300
2	Mean operating time in hours per day (h_{op})	8	8	16	24
3	Emergency STOP	Once per day	4-times per day	Once per week	Once per week

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Research on reliability qualification test design by considering inheritance factor

Yanlei Wang, Dinghai Xu & Longbo Liu
Naval Academy of Armament, Beijing, China

ABSTRACT: During the different development stages of the product, the approach that can design reliability qualification test plan scientifically, shorten testing time, improve test efficiency is needed. In order to use the test data from similar products in different development stages, the mixed Gamma distribution is used as prior distribution by considering product inheritance factor and correlation of testing data. After that a new reliability qualification test design method based on the Bayesian theory is established. Finally, the correctness and effectiveness of the proposed method is proved through examples.

1 INTRODUCTION

A large number of reliability tests must be carried out during the product development processes. But in different stages of development, the products are in different technology status. Generally speaking, the development process of product needs to go through virtual prototype, initial prototype and the formal prototype stages. Although the prototype states in different development stages are various, there has some continuity of inheritance. Therefore, the test data from the same kind of reliability test also has inheritance in different development stage. If the test information in different development stages can be combined properly (Wilson et al. 2006, Colombo 1990), the problems of the traditional reliability qualification test: the testing time is too long, lack of test samples and so on can be solved effectively.

Due to the test data in different development stages are not unified and from different populations, so it is difficult to solve the problem by only using the classical method based on large sample size (Ming 2009). While the Bayesian method (Huang et al. 2006, Gholizadeh et al. 2012) can make full use of priori information to make up the fact that the field test data is deficient, then the amount of field test can be effectively reduced in the premise of not reducing the degree of confidence.

In this paper, the inheritance factor is introduced to the development process of the product. This is better than the traditional Bayesian method to highlight the continuity of product technical states in different stages of development process, and also makes better use of reliability test data in different stages. Mixed Gamma prior distribution can be adopted to characterize differences of the product in different stages by using state inheritance factor. According to previous test data and the levels of risk of the producer and the user, the reliability qualification test program can be developed. The test program can not only make full use of the test information in each test phase, but also reasonably utilize different information from the whole development process and improvement process, and the guide line of the new method is presented for the reliability qualification test design.

2 MIXED PRIOR AND POSTERIOR DISTRIBUTION

Based on Bayesian method, it can significantly reduce the test sample size and shorten test time to make the product reliability qualification test plan by utilizing the priori information. How to use the priori information effectively and establish the prior distribution model is the key point to develop the Bayesian evaluation test programme.

2.1 *Determination of gamma prior distribution and posterior distribution*

The life of product is assumed to follow exponential distribution. The likelihood function of failure rate λ under fixed time censoring with replacement is given by

$$L(\lambda) = \frac{(T\lambda)^z}{z!}\exp(-\lambda T) \tag{1}$$

where T is the total test time, z is the number of failures.

For exponential distribution, the prior distribution of the failure rate λ is usually characterized by its conjugate distribution, Gamma distribution (Zhang & Jiang 2000, Wang 1993) whose probability density function is,

$$\pi(\lambda|a,b) = \frac{b^a}{\Gamma(a)} \lambda^{a-1} \exp(-b\lambda) \tag{2}$$

where, $\lambda > 0$, $a > 0$, $b > 0$, a and b is prior distribution parameters, it can be determined by the priori information (Coit & Jin 2000).

There are several kinds of methods to determine prior distribution parameters. The method using different quantiles of prior distribution proposed by Wang (1993) is adopted in this study. For different confidence levels, γ_1, γ_2, assuming the optimal precision confidence lower limit λ_1 and λ_2 of random failure rate of can be determined based on priori information of early prototypes. The quantiles of failure rate λ in the posterior distribution are λ_1 and λ_2, and the corresponding confidence levels are,

$$\begin{cases} \int_0^{\lambda_1} \pi(\lambda|a,b)\mathrm{d}\lambda = \gamma_1 \\ \int_0^{\lambda_2} \pi(\lambda|a,b)\mathrm{d}\lambda = \gamma_2 \end{cases} \tag{3}$$

From Equation (3), the parameters a and b can be solved based on the prior distribution.

According to Equation (1) and (2), the posterior distribution of the failure rate λ can be obtained based on Bayesian theorem,

$$\pi(\lambda|D) = \frac{(b+T)^{(a+z)}}{\Gamma(a+z)} \lambda^{a+z-1} e^{-\lambda(b+T)} \tag{4}$$

The upper confidence limit of failure rate, λ_U is given by

$$\int_0^{\lambda_U} \pi(\lambda|D)\mathrm{d}\lambda = \gamma \tag{5}$$

The lower confidence limit of reliability is given by

$$R_L = \exp(-\lambda_U T_0) \tag{6}$$

2.2 *The Gamma prior distribution with a mixed inheritance factor*

During the development process, the product would undergo testing, improvement and retesting. The product reliability is increasing in this process. Although conjugate distribution has strong adaptability and simple calculation, but it only considered the similarity and inheritance, and ignored the improvement and innovative uncertainty of the product. Hence, by combing the prior distribution with the test information before the initial prototype, it is necessary to introduce inheritance factor, namely the mixed Gamma distribution as advanced prior distribution. This is more reasonable, and the probability density function is expressed as follows,

$$\pi(\lambda|a,b) = \rho \frac{b^a}{\Gamma(a)} \lambda^{a-1} \exp(-b\lambda) + (1-\rho) \tag{7}$$

Assuming that the test data is D, based on the Bayesian formula, the posterior distribution can be obtained as

$$\begin{aligned} \Pi(\lambda \mid D) &= \frac{\pi(\lambda|a,b) \cdot L(\lambda)}{\int_0^{\infty} \pi(\lambda|a,b) L(\lambda)\mathrm{d}\lambda} \\ &= \frac{(1-\rho)\lambda^z e^{-\lambda T}\Gamma(a) + \rho b^a \lambda^{a+z-1} e^{-\lambda(b+T)}}{\dfrac{(1-\rho)\Gamma(z+1)\Gamma(a)}{T^{(z+1)}} + \dfrac{\rho b^a \Gamma(a+z)}{(b+T)^{(a+z)}}} \end{aligned} \tag{8}$$

where a and b are prior distribution parameters, determined in subsection 2.1; $0 \le \rho \le 1$ is called inheritance factor, reflecting the similarity between the initial prototype and the formal prototype in reliability point of view, describing degree of similarity and inheritance in function and structure of the product. Then $1 - \rho$ is the update factor, reflecting reliability uncertainty during improvement from the old product to the new one. When $\rho = 1$, the two populations are the same, mixed prior Gamma distribution is a generalized conjugate Gamma distribution. When $\rho = 0$, the two populations are completely different, there is no information useful for the prior distribution under the Bayesian assumption. Therefore, mixed Gamma prior distribution is based on prior information and prior distribution. Mixed distribution is used to describe the product reliability and uncertainty, and fully embodies the dialectical relationship of inheritance and development.

The parameter ρ reflects the degree of new product inherited from the original one. If the formal prototype compared to the initial one has made lots of changes, ρ is small, and conversely the value is large. Therefore, determining the value of ρ needs to consider the specific product in different development stages, it can give by experts based on the degree of the product's changes.

The upper confidence limit of failure rate, λ_U is

$$\int_0^{\lambda'_U} \Pi(\lambda|D)\mathrm{d}\lambda = \gamma \tag{9}$$

The lower confidence limit of reliability, R_L is,

$$R_L = \exp(-\lambda'_U T_0) \tag{10}$$

2.3 *Inheritance factor calculation*

In order to determine the degree of similarity between two products quantitatively, taking full account of the number of similar elements on the basis of similarity analysis should be carried out. First, define the number of similar elements between two systems is ρ_n; second, the similarity determined by each element is ρ_u; finally, the system similarity calculation formula is given by (Zhou 2004),

$$\rho_n = \frac{N}{K + L - N} \tag{11}$$

$$\rho_u = \sum_{i=1}^{N} \beta_i q(u_i) \tag{12}$$

$$\rho = \rho_n \bullet \rho_u = \frac{N}{K + L - N} \sum_{i=1}^{N} \beta_i q(u_i) \tag{13}$$

where, K, L, N stand for the numbers of elements for product A, B and their similar sections in one level respectively. $q(u_i)$ indicates the value of the similarity unit built by the similar feature in common of the similar products. And β_i is the weight coefficient of the similarity unit considered in $q(u_i)$. Equation (13) shows the similarity degree of two products accurately. From Equation (11)–(13), we can figure out that the similarity degree of the products is the quantized value acquired by comparing all information of two products actually.

In reliability engineering, while studying the similarity of different products, the differences between structure, function, design principle, working principle, material composition and working environment are mainly considered. Thus, in order to determining the similarity degree between the modified product and the original one, we only need to consider the six factors: structure, function, design principle, working principle, material composition and working environment of the product. Since new product is modified based on old one, the six factors considered usually refer to the similar elements, then we can consider as $K = L = N = 6$, that is $\rho_n = 1$. Thus, detailed values of weight coefficient and the inheritance factor of similar units could be determined by engineering information and expert experiences. This method directly uses the test data and has reduced the subjectivity. The format of the test data is time and number of failures.

3 RELIABILITY QUALIFICATION TEST PLAN BASED ON MIXED GAMMA DISTRIBUTION

On the base of posterior distribution from Equation (8), a reliability qualification test method can be developed. The basic idea is: first, use the formulae of both sides risk based on the posterior distribution to establish equations; second, solve the equations and obtain the qualification test plan (T, c), which must satisfy the producer's risk α_0, user's risk β_0 and distinguishing ratio D. For c must be an integer, the equations are always be solved by trial and error method (He & Dai 1995), but frequently the result is not objective.

By introducing optimization method, the solution procedure of the reliability qualification test plan would be divided into two sections, one section is to solve the equations with continuous variable; the second section is to obtain the final test plan by optimization process. Finally, an objective and steady plan can be obtained.

3.1 *Establishment of preliminary qualification test plan*

The concept of risk of the Bayesian theory based reliability qualification test plan is different from that of the classical qualification test plan. According to the posterior distribution, the producer's risk and user's risk are called posterior risk. (Ming 2009, Jiang & Zhang 2000, Chen et al. 2002). The reliability qualification test plan based on posterior risk often makes the user bear too much risk.

Suppose that the specified value and maximum acceptable value of the failure rate are λ_0 and λ_1, respectively. The test result of the fixed time censoring test is (T, z), and the following inequations will hold,

$$P(\lambda > \lambda_1 \mid z = x) > P(\lambda > \lambda_1 \mid z = x - 1) \tag{14}$$

$$P(\lambda < \lambda_0 \mid z = x) < P(\lambda < \lambda_0 \mid z = x - 1) \tag{15}$$

with

$$\begin{cases} P(\lambda > \lambda_1 \mid z = x) = \int_{\lambda_1}^{\infty} \Pi(\lambda \mid D, z = x) \mathrm{d}\lambda \\ P(\lambda < \lambda_0 \mid z = x) = \int_{0}^{\lambda_0} \Pi(\lambda \mid D, z = x) \mathrm{d}\lambda \end{cases} \tag{16}$$

Equation (14) and (15) are obviously in physical meaning: Equation (14) indicates the fact that for the same test time T, when the number of failure is z, the failure rate is greater than that when the number of failure is z–1. The physical meaning of Equation (15) is similar to Equation (14).

Let A_c denotes the maximum permitted failure number from the test samples for declaring the fact the product can pass the reliability qualification test; and R_e denotes the minimum number for refusing the fact that the reliability of the product can pass the test. Assuming the test plan is (T, c), then the maximum user's risk in the qualification test (the probability of which the product's real failure rate is larger than the maximum acceptable value but the product has passed the qualification test) is,

$$\max_{z\le c} P(\lambda > \lambda_1 \mid A_c) = P(\lambda > \lambda_1 \mid z = c) \tag{17}$$

The maximum producer's risk in the test (the probability of which the product's real failure rate is smaller than the specified value but the product has failed to pass the qualification test) is,

$$\max_{z\ge c} P(\lambda < \lambda_0 \mid R_e) = P(\lambda < \lambda_0 \mid z = c) \tag{18}$$

It should be noticed in Equation (18) that the range of rejection is $z \ge c$, not $z \ge c+1$. That's because when solving the test plan, T and c were assumed as continuous variables.

Plan (T,c) should satisfy

$$\begin{cases} P(\lambda < \lambda_0 \mid z = c) = \alpha \\ P(\lambda < \lambda_1 \mid z = c) = 1-\beta \end{cases} \tag{19}$$

By solving Equation (19), we can get a preliminary test plan (T', c') which satisfy the requirement of producer's risk α, user's risk β and the distinguishing ratio D.

3.2 *Establishing final test plan by optimization method*

For engineering practice, c must be an integer, researchers used to solve Equation (19) by tentative numerical method. But for different test plans, the prior information and inheritance factors are diverse, so it is not convenient to solve all of them by the tentative numerical method. Furthermore, the tentative numerical method will introduce too many subjective factors; and its repeatability is not good. Thus, the tentative numerical method cannot confirm that the derived results is the optimal one.

In subsection 3.1, we assume that c' is the judging failure number of preliminary test plan. Now we define that c denotes the judging failure number of the final test plan after rounded off. Let T be the decision variable, then set up optimization model as follows,

$$\begin{aligned} &\min \quad (\alpha-\alpha_0)^2 + (\beta-\beta_0)^2 \\ &\text{s.t} \\ &\begin{cases} \alpha = P(\lambda < \lambda_0 \mid z = c) \\ \beta = 1 - P(\lambda < \lambda_1 \mid z = c) \\ T > 0 \end{cases} \end{aligned} \tag{20}$$

The optimization objective function is the sum of the square of the risk values of the producer and the user. According to the solution of the proposed optimization model, parameter T can be obtained, thus final qualification test plan (T,c) can be obtained. For c must be an integer, after rounded off, the actual risk values α' and β' will deviate from the initial values slightly.

4 EXAMPLE

In this example, the development cycle of the product is assumed to be one year, and contains development processes of principle prototype A, B, early prototype A, B, and final prototype A, B. The reliability qualification test data in different stages are listed in Table 1.

According to engineering information and the experts' evaluated conclusion, the similarity degrees between product A and product B in the aspects of structure, function, design principle, working principle and material composition are 80%, 85%, 80%, 85% and 90%, respectively. As their work environment is different, we can set the similarity is 75% based on previous experience. According to Equation (13),

$$\rho = \rho_n \bullet \rho_u = \frac{N}{K+L-N}\sum_{i=1}^{N}\beta_i q(u_i) = 0.825 \tag{21}$$

In the same way, the inheritance factor of early prototype is 0.875.

Substitute test data of all process into Equations (3), (7) and (8) to obtain prior hyper-parameters $a = 0.4045$, $b = 1974.5$, then combine all the information above to derive inheritance factor. By calculating Equations (9) and (10), we can get the conclusion that the reliability of the product do not satisfy the requirement; it is needed to continue the reliability qualification test.

Normally, user's risk should not be higher than 0.2 in product qualification test.

By calculation of prior information of the principle prototype and the early prototype, when the confidence level of product failure rate is 0.8 and 0.9, the optimal confidence limit randomization is 1.246 and 1.536. That means the hyper-parameters can be obtained. After determining inheritance factor, test plan can be obtained by solution of Equations (19) and (20). In the case of that the failure number is 0, the total test time T is 0.6175 times of MTBF, in the case of that the failure number is 1, the total test time T is 1.932 times of MTBF.

Table 1. Reliability qualification test data of prototype A and prototype B in different stages.

Test stage	Accumulated time (h)	Failure number
Principle prototype A	2680	0
Principle prototype B	2400	1
Early prototype A	1600	1
Early prototype B	4248	0
Final prototype A	1840	0
Final prototype B	1720	0

5 CONCLUSIONS

The reliability qualification test plan established based on the proposed method both agrees well with classical qualification test plan based on large sample size, which makes it easy to be accepted in practical engineering; also it reflects the inheritance and development of the dialectical relations. Theoretically, it is more reasonable than traditional Bayesian plan of the reliability qualification test. An optimization model is purposely developed to solve the reliability qualification test plan. This model can make the test decision scientific and quantitative, and it has good robustness. Examples show that the proposed method can utilize test data fully and reasonably of all stages under the less sample condition. It can save test cost and time efficiently.

REFERENCES

Chen Y., Jiang L. and W., 2002. A Bayesian plan of qualification test in exponential case. Operations Research and Management Science, 11(2): 56–59.

Coit D.W. and Jin T., 2000. Gamma distribution parameter estimation for field reliability data with missing failure times. IIE Transactions, 32(12): 1161–1166.

Colombo A.G., 1990. Reliability parameter estimation by combination of data from various sources. Systems Reliability Assessment, 6: 273–283.

Gholizadeh R., Shirazi A.M, Hadian M., 2012. Bayesian system reliability and availability analysis under the vague environment based on exponential distribution. International Journal of Soft Computing, 3(1): 25–45.

He G. and Dai C., 1995. Technology of Reliability Test, Beijing: National Defence Industry Press. (in Chinese).

Huang H.Z., Ming J.Z. and Sun Z.Q., 2006. Bayesian reliability analysis for fuzzy lifetime data. Fuzzy Sets and Systems, 157(12): 1674–1686.

Jiang L. and Zhang Z., 2000. A Bayesian method of reliability qualification test in binomial case. Journal of Engineering Mathematics, 17(4): 25–29.

Ming Z., 2009. Research on Reliability Synthetically Assessment and Qualification Based on Bayes Analysis of Dynamic Distribution Parameter. PhD Dissertation, National University of Defense Technology. (in Chinese).

Wang L., 1993. Reliability of Bayesian demonstration testing under exponential distribution. Journal of East China Normal University (Natural Science), 3: 1–10.

Wilson A.G., Graves T.L., Hamada M.S. and Reese C.S., 2006. Advances in data combination, analysis and collection for system reliability assessment. Statistical Science, 21(4): 514–531.

Zhang Z. and Jiang L., 2000. A Bayesian plan of testing for production acceptance in exponential case. Chinese Journal of Applied Probability, 16(1): 66–70.

Zhou M., 2004. Science of Similarity, Beijing: Science Press. (in Chinese).

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimal design on Accelerated Degradation Testing with Gamma process for reliability demonstration

C. Zhang, X. Lu, X. Chen & Y. Wang
Science and Technology on Integrated Logistics Support Laboratory, National University of Defense Technology, Changsha, Hunan, P.R. China

ABSTRACT: For products with high reliability and long lifetime, Accelerated Degradation Testing (ADT) may be adopted during product development phase to verify whether its reliability satisfies the predetermined level within feasible test duration. The optimal design of accelerated degradation testing for efficient reliability demonstration becomes a research focus to increase demonstration accuracy and to reduce test cost. The actual degradation from engineering is usually a strict monotonic process, such as fatigue crack growth, wear, and erosion. However, the method for reliability demonstration by ADT with monotonic degradation process hasn't been investigated so far. This paper proposes an optimal reliability demonstration method by ADT for this kind of products. We first apply Gamma process to describe the monotonic degradation. Next, we convert the required reliability into allowable cumulative degradation in ADT, and demonstrate the reliability by comparing the actual accumulative degradation with the allowable level. Further, we suggest an optimal ADT design for efficient reliability demonstration by minimizing the asymptotic variance of decision variable under the constraints of sample size, test duration, and test cost. The method is validated and illustrated with example on reliability demonstration of alloy product in the end.

1 INTRODUCTION

Reliability demonstration test is commonly adopted in product development phase to validate whether its reliability meets the specified requirement. Accelerated Life Test (ALT) could reduce test duration and has been applied in reliability demonstration for highly reliable products with long lifetime (Bris 2000, Krasich 2003).

For engineering circumstances, the reliability of highly reliable product is usually dominated by its performance degradation. Accelerated Degradation Test (ADT) is consequently promoted as feasible solution to reliability demonstration of this kind of products, for it reduces test duration further by comparison with ALT. Yang (Yang 2009) presented a reliability demonstration method based on degradation test under normal stress level using linear degradation model, and Huang (Huang 2012) proposed an optimal ADT plan for reliability demonstration based on linear degradation model.

Compared with linear degradation model, stochastic process model can reasonably identify the random variation in degradation process. Baussaron (Baussaron 2011) proposed a reliability demonstration method based on ADT using Wiener process model. Generally speaking, the performance degradation of product is usually a monotonic process, such as fatigue crack growth, wear, and erosion. Gamma process model is a strict monotonic process model, and it is more reasonable for these occasions than Wiener process model (Park 2005). Unfortunately, few literatures can be identified to deal with reliability demonstration by ADT using Gamma process model.

This paper proposes a reliability demonstration method by ADT for products with Gamma process. The rest of this paper is organized as follows. Section 2 gives a motivating example. Section 3 delivers the models for the problem. Section 4 suggests a reliability demonstration method by judging the cumulative degradation in ADT. Section 5 presents an optimal ADT plan for efficient reliability demonstration. Section 6 offers the results that apply the proposed method to the motivating example. Section 7 concludes the paper.

2 MOTIVATING EXAMPLE

The metal component subject to cyclic load could rupture when the length of fatigue crack reaches the threshold, which accounts for a majority of failure for metal component. Meeker and Escobar (Meeker 1998) described such a problem. Fatigue crack development process of a kind of alloy product is a strict monotonic process as shown

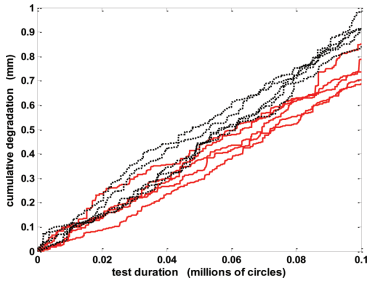


Figure 1. Typical fatigue crack development process of an alloy product from CSADT. (The red lines denote the degradation of 5 products under an elevated stress level, and the black lines denote a higher stress level.).

in Fig. 1, and should be described properly by Gamma process.

Suppose that the reliability of the alloy product required by consumer is $R_\beta = 0.9016$ with risk $\beta = 0.10$ at $t_0 = 0.1286$ millions of circles, and that the acceptable reliability for producer is required to be $R_\alpha = 0.9832$ with risk $\alpha = 0.30$ at the same time. If such a high reliability with long service duration is demonstrated by traditional fatigue life test, it will be unfeasible for the too lengthy test duration. So the reliability demonstration method by ADT for such kind of products with Gamma process should be investigated.

For this problem, there exist some issues worthy of further consideration.

1. If ADT is employed, how can we judge whether the reliability satisfies the requirement according to the degradation data acquired in ADT?
2. Can we possibly optimize the test plan for efficient reliability demonstration, which means better demonstration confidence with the constraints on sample size, test duration, and test cost?

3 MODELS

3.1 *Degradation model*

Let $\{X(t), t \geq 0\}$ represent Gamma process with shape parameter v and scale parameter u, $X(t) \sim Ga(vt, u)$, and its basic properties are as follows.

1. $P\{X(0) = 0\} = 1$.
2. $E(X(t)) = uvt$, $Var(X(t)) = u^2 vt$.
3. $X(t_j) - X(t_i)$ is s-independent from $X(t_k) - X(t_j)$ for $0 < t_i < t_j < t_k$.
4. $\Delta X(t) = X(t + \Delta t) - X(t)$, $\Delta X(t) \sim Ga(v\Delta t, u)$, $\Delta t > 0$, and its probability density function is defined as

$$f(\Delta x) = \frac{1}{\Gamma(v\Delta t)u^{v\Delta t}} \Delta x^{v\Delta t - 1} e^{-\frac{\Delta x}{u}}, \Delta x > 0 \qquad (1)$$

where, $\Gamma(v) = \int_0^\infty x^{v-1} e^{-x} dx$.

Gamma process is a strictly monotonic process with s-independent and non-negative increments. Suppose a failure occurs when the degradation reaches the specified threshold ω, then failure time T can be defined as the time when the degradation path cross ω, and the reliability at t can be expressed as

$$R(t) = P(T > t) = P(X(t) < \omega) = Ga(\omega \mid vt, u) \qquad (2)$$

The probability density function of T at t could be obtained from (2), but the formulation is too complex to be used in practice. Fortunately, the cumulative distribution of T could approximate to Birnbaum-Saunders distribution (Bris 2000, Padgett 2004).

$$F(t) = P(T < t) = P(X(t) > \omega) = \Phi(\sqrt{vt} - \sqrt{\frac{\omega^2}{u^2 vt}}) \qquad (3)$$

where, $\Phi(\bullet)$ is standard s-normal cumulative distribution function, u and ω are s-independent from stress levels. Refer to (3), the reliability for a given Gamma degradation process with u and ω is determined by vt.

3.2 *Acceleration model*

In an ADT for products with Gamma degradation process, the shape parameter v reflects the effect of stress level S_k on the performance. Acceleration model can be denoted as

$$\ln v_k = a + b\varphi(S_k) \qquad (4)$$

where, a and b are unknown coefficients of acceleration model, and $\varphi(S_k)$ is a known function of S_k. If $\varphi(S_k) = \ln S_k$, acceleration model is Inverse Power Law. If $\varphi(S_k) = 1/S_k$, it is Arrhenius equation.

The scale parameter u of Gamma degradation process reflects the random variation of the performance, and it is s-independent from stress levels.

4 RELIABILITY DEMONSTRATION BY ADT

Let R_β denote limit quality from consumer under use condition S_0 at time t_0 with corresponding consumer's risk β, and R_α denote acceptable quality

from producer under use condition S_0 at the same time with corresponding producer's risk α. Generally, $R_\beta < R_\alpha$.

4.1 *MLE for the models*

Suppose a constant stress ADT with N stress levels, n_k samples are tested under the stress level S_k, and the performance of the samples under S_k is measured as Δx_{kij} for m_k times with identical measuring interval Δt, $k = 1,2,...,N$, $i = 1,2,...,n_k$, $j = 1,2,...,m_k$.

According to (1), the likelihood function of such an ADT is

$$L(a,b,u) = \prod_{k=1}^{N}\prod_{i=1}^{n_k}\prod_{j=1}^{m_k}\left[\frac{1}{\Gamma(v_k\Delta t)u^{v_k\Delta t}}\Delta x_{kij}^{\,v_k\Delta t-1}e^{-\frac{\Delta x_{kij}}{u}}\right] \quad (5)$$

where, v_k can be expressed as (4).

Further, the log-likelihood function from (5) is

$$\ln L(a,b,u) = \sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}[-\ln\Gamma(v_k\Delta t) - v_k\Delta t\ln u + (v_k\Delta t - 1)\ln\Delta x_{kij} - \frac{\Delta x_{kij}}{u}] \quad (6)$$

MLE of parameters $(\hat{a},\hat{b},\hat{u})$ can be solved from (6).

4.2 *Reliability demonstration method*

Similar to Cumulative Exposure Model (Nelson 1980), the remaining life of a degradation process also depends only on the current cumulative degradation and current stress regardless how the degradation accumulated. This is to say if the reliability of a degradation process at time t_0 under use condition S_0 is $R_0(t_0)$, and its reliability at time τ_k under elevated stress level S_k is $R_k(\tau_k)$, $R_0(t_0) = R_k(\tau_k)$, when and only when

$$E\left(X_0(t_0)\right) = E\left(X_k(\tau_k)\right) \quad (7)$$

where, $E\left(X_0(t_0)\right)$ is the performance degradation expectation at t_0 subject to use condition S_0, and $E\left(X_k(\tau_k)\right)$ is the performance degradation expectation at τ_k subject to elevated stress level S_k. From (7), we can obtain

$$\mu v_k\tau_k = \mu v_0 t_0 \quad (8)$$

$$\tau_k = \frac{v_0 t_0}{v_k} \quad (9)$$

where, $k = 1,2,...,N$.

From (3), we can denote the required reliability under the elevated stress level as

$$1 - \Phi(\sqrt{v_k\tau_k} - \sqrt{\frac{\omega^2}{u_\beta^{\,2}v_k\tau_k}}) = R_\beta \quad (10)$$

$$1 - \Phi(\sqrt{v_k\tau_k} - \sqrt{\frac{\omega^2}{u_\alpha^{\,2}v_k\tau_k}}) = R_\alpha \quad (11)$$

where, u_β and u_α are scale parameters corresponding to R_β and R_α respectively subject to S_k. Further,

$$u_\beta = \frac{\omega}{v_k\tau_k - \gamma_{1-R_\beta}\sqrt{v_k\tau_k}} \quad (12)$$

$$u_\alpha = \frac{\omega}{v_k\tau_k - \gamma_{1-R_\alpha}\sqrt{v_k\tau_k}} \quad (13)$$

where, γ_p is the 100 *pth* percentile from $\Phi(\bullet)$. we use (9), (12) and (13) to convert the required reliability $R_\beta(t_0)$ and $R_\alpha(t_0)$ under use condition S_0 into the equivalent reliability requirement $R_\beta(\tau_k)$ and $R_\alpha(\tau_k)$ under elevated stress level S_k.

After n_k products are tested under S_k, the cumulative degradation of n_k samples under S_k at time t_k

$$CD(t_k) = \sum_{i=1}^{n_k} X_i(t_k) \sim Ga(nv_k t_k, u) \quad (14)$$

where, $X_i(t_k)$ is the measured degradation under S_k, and $t_k = m_k\Delta t$. The observed reliability under S_k is exclusively determined by the cumulative degradation, so we can demonstrate the reliability by judging whether $CD(t_k)$ reaches the allowable level. In the rest of this section, we derive the allowable level.

Let Ac denote the allowable cumulative degradation level of n_k samples corresponding to the required reliability. If $CD(t_k) \le Ac$, the reliability will be accepted, otherwise the reliability will be rejected. So the customer's risk and the producer's risk associated with the demonstration above are as follows.

$$\beta = Ga(Ac \mid nv_k t_k, u_\beta) \quad (15)$$

$$\alpha = 1 - Ga(Ac \mid nv_k t_k, u_\alpha) \quad (16)$$

According to (3),

$$\beta = 1 - \Phi(\sqrt{n_k v_k t_k} - \sqrt{\frac{Ac^2}{u_\beta^2 n_k v_k t_k}}) \quad (17)$$

$$\alpha = \Phi(\sqrt{n_k v_k t_k} - \sqrt{\frac{Ac^2}{u_\alpha^2 n_k v_k t_k}}) \tag{18}$$

So Ac can be expressed as

$$Ac = \mu_\beta(n_k v_k t_k - \gamma_{1-\beta}\sqrt{n_k v_k t_k}) \tag{19}$$

or,

$$Ac = \mu_\alpha(n_k v_k t_k - \gamma_\alpha \sqrt{n_k v_k t_k}) \tag{20}$$

where, γ_p denotes the $100pth$ percentile from $\Phi(\bullet)$.

5 OPTIMAL ADT PLAN FOR RELIABILITY DEMONSTRATION

Demonstrating reliability by ADT on sampled specimens from a lot causes the type I and type II risk. The actual risk varies with the test plan, and it consequently has an influence on the sample size, test duration and test cost demanded for the ADT. This section investigates the optimal ADT plan for efficient reliability demonstration.

5.1 *Objective function*

From the reliability demonstration procedure in section 4, we find that the value of Ac determines the type I and type II risks. The larger asymptotic variance of $\hat{A}c$ is, the greater deviation of actual risks will be. Thus, we set the asymptotic variance of $\hat{A}c$ as objective function.

$$\min \hat{AV}ar(\hat{Ac} \mid n_k, m_k, \Delta t) \tag{21}$$

The asymptotic variance of $\hat{Ac}$ can be expressed as

$$\hat{AVar}(\hat{Ac}) = \left[\left(\frac{\partial \hat{Ac}}{\partial \hat{a}}\right), \left(\frac{\partial \hat{Ac}}{\partial \hat{b}}\right), 0\right] F^{-1} \left[\left(\frac{\partial \hat{Ac}}{\partial \hat{a}}\right), \left(\frac{\partial \hat{Ac}}{\partial \hat{b}}\right), 0\right]' \tag{22}$$

where, F denotes the Fisher information matrix. The detailed expressions for calculating $\hat{AVar}(\hat{Ac})$ are listed in the Appendix.

5.2 *Constraints*

The constraints in reliability demonstration by ADT usually include (Park):

1. The test time t_k under S_k should not exceed the specified test duration t_{Mk}.
2. The sample size should not exceed the number of the test units available.
3. The risks should not exceed the pre-determined level.
4. The total test cost Tc should not exceed the budget C_b.

Further, the total cost of conducting a reliability demonstration by constant stress ADT is given by

$$Tc(n_k, m_k, \Delta t) = C_{op}\Delta t \sum_{k=1}^{N} m_k + C_{mea} \sum_{k=1}^{N} n_k m_k + C_{it} \sum_{k=1}^{N} n_k \tag{23}$$

where, C_{op} denotes the unit cost for each operation, C_{mea} denotes the unit cost for each measurement, C_{it} denotes the unit cost for each test unit.

According to the above analysis, the optimization problem can be formulated as

$$\min \hat{AV}ar(\hat{Ac} \mid n_k, m_k, \Delta t) \quad s.t. \begin{cases} Tc(n_k, m_k, \Delta t) \le C_b \\ m_k \Delta t \le t_{Mk} \\ \sum_{k=1}^{N} n_k \le n_M \\ \alpha = \alpha_1 \end{cases} \tag{24}$$

where, $n_k, m_k \in \{1,2,3,...\}$, $\Delta t > 0$, $t_{Mk} \le \tau_k$. We adopt (19) to obtain $\hat{Ac}$, so the objective function contains the constraint on consumer's risk β.

5.3 *Solving optimal test plan*

We suggest the following procedure to solve the optimal ADT plan.

Step 1. Conduct the preliminary test to acquire the prior degradation data of products, and calculate the prior estimation of (a,b,u) by MLE.

Step 2. Deduce the objective function and constraints using the prior estimator $(\hat{a},\hat{b},\hat{u})$, and search optimal solution $(n_k^*, m_k^*, \Delta t^*)$ with nonlinear optimization method.

(Due to the complex objective function, the closed expression does not exist for $(n_k^*, m_k^*, \Delta t^*)$, but the optimal solution can be solved by nonlinear optimization method.)

Step 3. Conduct the reliability demonstration test according to the optimal test plan, and demonstrate the reliability by cumulative degradation in ADT, usually together with the degradation in the preliminary test.

(After acquiring new degradation data, MLE of (a,b,u) and Ac are renewed, and the decision of acceptance or rejection can be made accordingly.)

6 SOLUTION TO MOTIVATING EXAMPLE

In this section, we illustrate the proposed method with the motivating example by MC simulation.

We suppose $C_{op}=0.6$, $C_{mea}=1.3$, $C_{it}=55$ (Laiao 2006), and $(a,b,u)=(6.4906,1.8,0.009297)$, $\omega=0.9$ inch.

6.1 *Preliminary test*

Let $S_0=1$ and the relationship between v_k and S_k be Inverse Power Law. A preliminary test is simulated with two elevated constant stress levels $S_1=1.15$ and $S_2=1.25$. The number of test unit and measurement for S_1 and S_2 are $n_1=5$, $m_1=900$, $n_2=5$, $m_2=900$ respectively. The measurement interval is $\Delta t=0.0001$ millions of circles.

According to the true value of (a,b,u), a set of simulated degradation for preliminary test is shown as Fig. 1. Refer to (6), MLE of the parameters is $(\hat{a},\hat{b},\hat{u})=(6.4982,1.7288,0.009451)$.

6.2 *Optimal test plan*

Given the constraints configuration (C_b,t_{M1},t_{M2},n_M), the optimal test plan can be derived by the method in section 5. Let $(C_b,t_{M1},t_{M2},n_M)=(3000,0.1010,0.0874,30)$, the process for solving the optimal test plan is shown as follows. In this example, the cumulative degradation under S_1 is selected as decision variable, so the optimization model should be

$$\min A\hat{V}ar(\hat{A}c\,|\,n_1,n_2,m_1,m_2,\Delta t)$$
$$s.t.\begin{cases}0.6(m_1+m_2)\Delta t+1.3(n_1m_1+n_2m_2)+55(n_1+n_2)\le 3000\\ m_1\Delta t\le 0.1010\\ m_2\Delta t\le 0.0874\\ n_1+n_2\le 30\\ \alpha=30\%\end{cases} \tag{25}$$

where,

$$Ac=\frac{\omega(d-\lambda_{0.9}\sqrt{d})}{0.1286e^{6.4982}-\lambda_{0.0984}\sqrt{0.1286e^{6.4982}}} \tag{26}$$

$$\alpha=\Phi\left(d-\frac{(d-\lambda_{0.9})(\sqrt{0.1286e^{6.4982}}-\lambda_{0.0984})}{\sqrt{0.1286e^{6.4982}-\lambda_{0.0168}}}\right) \tag{27}$$

$$d=n_1m_1\Delta t\exp(6.4982+1.7288\times\ln 1.15) \tag{28}$$

$$A\hat{V}ar(\hat{A}c)=\left(\frac{\partial\hat{A}c}{\partial\hat{a}}\right)^2\hat{V}ar(\hat{a})+\left(\frac{\partial\hat{A}c}{\partial\hat{b}}\right)^2\hat{V}ar(\hat{b})+2\left(\frac{\partial\hat{A}c}{\partial\hat{a}}\right)\left(\frac{\partial\hat{A}c}{\partial\hat{b}}\right)\hat{C}ov(\hat{a},\hat{b}) \tag{29}$$

Using the constrained nonlinear optimization method, the optimal test plan is

$$(\Delta t^*,n_1^*,n_2^*,m_1^*,m_2^*,Ac)=(0.0011,7,11,91,79,5.1903) \tag{30}$$

So the optimal test is to measure 7 and 11 units under S_1 and S_2 respectively, the corresponding measurement number are 91 and 79, and the measurement interval is 0.0011 millions of circles. If the actual cumulative degradation under S_1 $CD>5.1903$ inch during the test, the reliability will be rejected; otherwise the reliability will be accepted.

The optimal test plans with different budget C_b, test time constraint t_{Mk} and specimen constraint n_M are as shown in Table 1, 2 and 3 respectively, and some conclusions can be drawn by comparison as follows by comparison.

1. C_b, t_{Mk}, and n_M have definite influence on the optimal test plan. More test budget, longer test duration and more specimens will be beneficial to objective function, and will help us achieve better reliability demonstration confidence.

Table 1. Optimal test plans under different budget C_b.

C_b, t_{M1}, t_{M2}, n_M	Δt^*	n_1^*	n_2^*	m_1^*	m_2^*	Ac	$AVar(Ac)$
2000,0.1010,0.0874,30	0.0053	7	19	19	16	5.2223	0.0826
2500,0.1010,0.0874,30	0.0017	7	13	58	50	5.1104	0.0724
3000,0.1010,0.0874,30	0.0011	7	11	91	79	5.1903	0.0661

Table 2. Optimal test plans under different time constraint t_{Mk}.

C_b, t_{M1}, t_{M2}, n_M	Δt^*	n_1^*	n_2^*	m_1^*	m_2^*	Ac	$AVar(Ac)$
3000,**0.0202,0.0175**,30	-	-	-	-	-	-	-
3000,**0.0505,0.0437**,30	0.0014	14	16	36	31	5.2276	0.0862
3000,**0.1010,0.0874**,30	0.0011	7	11	91	79	5.1903	0.0661

The optimal test plan in the first row cannot be constructed for the too short test duration.

2. If C_b, t_{Mk}, and n_M are too small, the asymptotic variance will not converge, and the optimal test plan may not exist.
3. t_{Mk} has greater influence on asymptotic variance than C_b and n_M, so longer test duration as possible is recommended.

6.3 *Sensitivity analysis for optimal test plan*

The optimal test plan depends on the prior information about a, b, and u. Usually the prior information may deviate from the actual value. Next, we evaluate how the deviation affects the optimal test plan in terms of the relative error $RB(\hat{AVar}(\hat{Ac}))$.

Let ε_1, ε_2 and ε_3 denote the error for a, b and u respectively, and the prior estimator deviates ±10% from the true value. $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \{-10\%, 0, 10\%\}$. The error of a, b, and u are combined to display the sensitivity of the optimal test plan under same C_b, t_{Mk}, and n_M configuration. The results are shown in Table 4. Some conclusions about sensitivity of the optimal test plan can be drawn.

1. The deviation of u has no obvious influence on optimal test plan.
2. The deviation of b has perceptible influence on optimal test plan, but the optimal test plan is reasonably robust against the deviation of b.
3. The deviation of a has major influence on optimal test plan. In order to get a reasonable optimal test plan, it is recommended that the prior estimation of a be paid more attention.

6.4 *Validation for optimal test plan*

Next, we investigate the validity of the optimal test plan of (30) by MC simulation. Set $(n_1^*, n_2^*) = (7,11)$, 1000 sets of degradation data were generated by MC simulation with different combinations of $(\Delta t, m_1, m_2)$, and the corresponding Mean Squared Error (MSE) of Ac is investigated.

$$\hat{MSE}(Ac) = \frac{1}{N_{MC}} \sum_{w=1}^{N_{MC}} (\hat{Ac}_w - Ac)^2 \tag{31}$$

where, N_{MC} is the number of MC simulations for each test plan, $\hat{Ac}_w$ is the estimated Ac in the wth simulation for the test plan, Ac is the true value of decision variable corresponding to the actual value.

The results are shown in Table 5. It shows that the proposed optimal test plan yields the smallest

Table 3. Optimal test plans under different specimen constraint n_M.

C_b, t_{M1}, t_{M2}, n_M	Δt^*	n_1^*	n_2^*	m_1^*	m_2^*	Ac	$AVar(Ac)$
3000,0.1010,0.0874,**10**	-	-	-	-	-	-	-
3000,0.1010,0.0874,**15**	0.0008	7	8	120	104	4.9719	0.0624
3000,0.1010,0.0874,**30**	0.0011	7	11	91	79	5.1903	0.0661

The optimal test plan in the first row cannot be constructed for the too small sample size.

Table 4. Optimal test plans under different combination of ε_1, ε_2, ε_3.

ε_1, ε_2, ε_3,	Δt^*	n_1^*	n_2^*	m_1^*	m_2^*	Ac	$RB(AVar(Ac))$
-10%,-10%,-10%	0.0010	8	9	101	86	5.5320	40.88%
-10%,0,0	0.0010	8	9	99	88	5.5616	33.59%
-10%,10%,10%	0.0009	8	9	103	85	5.3323	18.69%
0,-10%,0	0.0011	7	11	93	81	5.2217	3.95%
0,0,10%	0.0011	7	11	91	79	5.2401	0
0,10%,-10%	0.0010	7	11	95	80	5.0959	-9.88%
10%,-10%,10%	0.0027	6	24	38	33	4.7042	-39.51%
10%,0,-10%	0.0026	6	24	39	33	4.7690	-41.64%
10%,10%,0	0.0025	6	24	39	33	4.7010	-45.74%
0,0,0	0.0011	7	11	91	79	5.2401	0

Table 5. Simulation results under different combinations of $(\Delta t, m_1, m_2)$.

$\Delta t^*, n_1^*, n_2^*, m_1^*, m_2^*$	0.0022,7,11,45,39	**0.0011,7,11,91,79**	0.0011,7,11,91,39	0.0008,7,11,125,45
$AVar(Ac)$	0.0838	**0.0661**	0.0956	0.0904
$\hat{MSE}(Ac)$	0.1260	**0.0995**	0.1428	0.1346

MSE for Ac, which illustrates the validity of the proposed method.

7 CONCLUSIONS

This paper discussed the reliability demonstration by ADT for highly-reliable products with Gamma degradation process. We proposed a reliability demonstration method by judging the cumulative degradation in ADT with the allowable level, and also presented an optimal test plan design for reliability demonstration with ADT by minimizing asymptotic variance of decision variable to increase demonstration accuracy under the constraints on available test samples, test duration, and test cost. The method was illustrated by the motivating example.

8 APPENDIX

The expression of Fisher information matrix is

$$F=\begin{bmatrix} E\left(-\frac{\partial^2 \ln L}{\partial a^2}\right) & E\left(-\frac{\partial^2 \ln L}{\partial a\partial b}\right) & E\left(-\frac{\partial^2 \ln L}{\partial a\partial u}\right) \\ E\left(-\frac{\partial^2 \ln L}{\partial b\partial a}\right) & E\left(-\frac{\partial^2 \ln L}{\partial b^2}\right) & E\left(-\frac{\partial^2 \ln L}{\partial b\partial u}\right) \\ E\left(-\frac{\partial^2 \ln L}{\partial u\partial a}\right) & E\left(-\frac{\partial^2 \ln L}{\partial u\partial b}\right) & E\left(-\frac{\partial^2 \ln L}{\partial u^2}\right) \end{bmatrix}$$

where,

$$E\left(-\frac{\partial^2 \ln L}{\partial a^2}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\psi_1(v_k\Delta t)(v_k\Delta t)^2 =\sum_{k=1}^{N}\psi_1(v_k\Delta t)(v_k\Delta t)^2 n_k m_k$$

$$E\left(-\frac{\partial^2 \ln L}{\partial a\partial b}\right)=E\left(-\frac{\partial^2 \ln L}{\partial b\partial a}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\psi_1(v_k\Delta t)(v_k\Delta t)^2\varphi(S_k) =\sum_{k=1}^{N}\psi_1(v_k\Delta t)(v_k\Delta t)^2 n_k m_k\varphi(S_k)$$

$$E\left(-\frac{\partial^2 \ln L}{\partial a\partial u}\right)=E\left(-\frac{\partial^2 \ln L}{\partial u\partial a}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\frac{v_k\Delta t}{u}=\frac{\Delta t}{u}\sum_{k=1}^{N}v_k n_k m_k$$

$$E\left(-\frac{\partial^2 \ln L}{\partial b^2}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\psi_1(v_k\Delta t)(v_k\Delta t)^2\varphi^2(S_k) =\sum_{k=1}^{N}\psi_1(v_k\Delta t)(v_k\Delta t)^2 n_k m_k\varphi^2(S_k)$$

$$E\left(-\frac{\partial^2 \ln L}{\partial b\partial u}\right)=E\left(-\frac{\partial^2 \ln L}{\partial u\partial b}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\frac{v_k\Delta t\varphi(S_k)}{u} =\frac{\Delta t}{u}\sum_{k=1}^{N}v_k n_k m_k\varphi(S_k)$$

$$E\left(-\frac{\partial^2 \ln L}{\partial u^2}\right)=\sum_{k=1}^{N}\sum_{i=1}^{n_k}\sum_{j=1}^{m_k}\frac{v_k\Delta t}{u^2}=\frac{\Delta t}{u^2}\sum_{k=1}^{N}v_k n_k m_k$$

and,

$\psi_1(z)=\dfrac{d\ln^2\Gamma(z)}{dz^2}$ is trigamma function.

The expression of asymptotic variance-covariance matrix is

$$V=F^{-1}=\begin{bmatrix} Var(a) & Cov(a,b) & Cov(a,u) \\ Cov(b,a) & Var(b) & Cov(b,u) \\ Cov(u,a) & Cov(u,b) & Var(u) \end{bmatrix}$$

By δ method, the asymptotic variance of $\hat{A}c$ can be calculated by using the following formulation

$$A\hat{V}ar(\hat{A}c)=\left[\left(\frac{\partial\hat{A}c}{\partial\hat{a}}\right),\left(\frac{\partial\hat{A}c}{\partial\hat{b}}\right),0\right]F^{-1}\left[\left(\frac{\partial\hat{A}c}{\partial\hat{a}}\right),\left(\frac{\partial\hat{A}c}{\partial\hat{b}}\right),0\right]'$$

where,

$$\frac{\partial\hat{A}c}{\partial\hat{a}}=\frac{\omega(2n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k-\gamma_{1-\beta}\sqrt{n_k t_k e^{\hat{a}+\hat{b}\varphi(S_k)}})}{2(e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\gamma_{1-R_\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0})}- \frac{\omega(n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k-\gamma_{1-\beta}\sqrt{n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k})(2e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\gamma_{1-R_\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0})}{2(e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\gamma_{1-R_\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0})^2} =\frac{\omega\sqrt{n_k t_k e^{2\hat{a}+\hat{b}\varphi(S_0)+\hat{b}\varphi(S_k)}t_0}(\gamma_{1-\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0}-\gamma_{1-R_\beta}\sqrt{n_k t_k e^{\hat{a}+\hat{b}\varphi(S_k)}})}{2(e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\gamma_{1-R_\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0})^2}$$

$$\frac{\partial\hat{A}c}{\partial\hat{b}}=\frac{\omega(2n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k\varphi(S_k)-\gamma_{1-\beta}\varphi(S_k)\sqrt{n_k t_k e^{\hat{a}+\hat{b}\varphi(S_k)}})}{2(e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\gamma_{1-R_\beta}\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0})}- \frac{\omega(n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k-\gamma_{1-\beta}\sqrt{n_k e^{\hat{a}+\hat{b}\varphi(S_k)}t_k})}{2(e^{\hat{a}+\hat{b}\varphi(S_0)}t_0-\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0}\gamma_{1-R_\beta})^2} \cdot(2e^{\hat{a}+\hat{b}\varphi(S_0)}t_0\varphi(S_0)-\sqrt{e^{\hat{a}+\hat{b}\varphi(S_0)}t_0}\varphi(S_0)\gamma_{1-R_\beta})$$

REFERENCES

Baussaron, J. "Degradation test plan for Wiener degradation process," In Proceeding of Annual Reliability and Maintainability Symposium, pp.1–6, 2011.

Bris, R. "Bayes approach in RDT using accelerated and long-term life data," Reliability Engineering and System Safety, vol. 67, pp. 9–16, 2000.

Huang, X. "Reliability demonstration through accelerated degradation zero-failure testing under binomial distribution," Systems Engineering and Electronics, vol. 34, no. 9, pp. 1951–1956, 2012.

Krasich, M. "Accelerated testing for demonstration of product lifetime reliability," In Proceedings of Annual Reliability and Maintainability Symposium, pp.117–123, 2003.

Liao, C. & S. Tseng, "Optimal design for step-stress accelerated degradation tests", IEEE Transactions on Reliability, vol. 55, no. 1, pp. 59–66, Mar. 2006.

Meeker, W. & Escobar, L. “Statistical Methods for Reliability Data,” New York: Wiley, 1998.
Nelson, W. “Accelerated life testing: step-stress models and data analysis”, IEEE Transactions on Reliability, vol. 29, no. 2, pp. 103–108, 1980.
Padgett, W. & Tomlinson, M. “Inference from accelerated degradation and failure data based on gaussian process models,” Lifetime Data Analysis, vol. 10, pp. 191–206, 2004.
Park, C. & Padgett, W. “Accelerated degradation models for failure based on geometric brownian motion and gamma processes,” Lifetime Data Analysis, vol. 11, pp. 511–527, 2005.
Park, J. & Yum, B. “Design of Reliability Acceptance Sampling Plans Based on Accelerated Degradation Tests,” Asia Pacific Management Review, vol. 6, pp. 461–476.
Yang, G. “Reliability demonstration through degradation bogey testing,” IEEE Transactions on Reliability, vol. 58, no. 4, pp. 604–610, 2009.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

One producer, two brands: A comparison of car operating conditions

M. Jadwinska, T. Siekierka & M. Zając
Wroclaw University of Technology, Poland

ABSTRACT: Currently, car companies are the owners of several brands. It is associated with the marketing policy of companies (Min Han 1990). Some brands under one company to be sporty, other family or luxury—in line with the image of the brand. Regardless of the image—sharing cars within a group often use the same components. As a result, companies can save time on designing cars, and money—thanks to the production of the same item for several brands. Since the current vehicles of different brands are built from the same components leaving the factory, they should have a similar operational and reliability parameters. The aim of the article is to compare the number of vehicles manufactured by the same company: one of them is the average vehicle, while the other should be in your group to premium. Paper presents the results of their observations and analysis of the results.

1 INTRODUCTION

Today, maintaining the brand is basically the same as customer retention, and is to provide more and better products for a good price (Raff 1991). The market is global and ruled by globalized consumer, whose needs are diverse. In addition, the modern consumer freed almost entirely from unnecessary sentiments of loyalty anachronistic and actively looking for information about the products and the opportunity to buy them as cheaply as possible. The same applies to cars. Created divisions have their foundation in the techniques associated with marketing. For example, in the area of family vehicles distinguishes the following classes (Vinson & Scott & Lawrence 1977): safe family car, the car for a family with a child, a comfortable family car, roomy family car, family car trouble-free, economical family car, family car environmentally friendly, best family car, etc.

Regardless of the distribution of representatives of each class can have many features in common, not limited only to the functional features. They are simply made from the same components, elements, systems, for example, may be driven by the same engine. There are some engines passing into legend, and installed in many vehicles. There is no more popular diesel engines than 1.9 TDI Volkswagen Group produced and constantly modernized in the years 1991–2011. He has performed in over 40 different versions with different inter alia, torque, power, injection system, the assembly. He was installed in many cars of Volkswagen Group: from Skoda Fabia and VW Polo to Sharan and Ford Galaxy. Production finished with the introduction of EURO 5 standard, which was not able to fulfill, even by useing DPF.

Lowering the cost of production means that car companies use the same elements or components in different models. Since it uses the same elements and can therefore be concluded that cars today are characterized by similar operating costs and reliability.

The purpose of this article is to demonstrate differences in the operation of vehicles within the same group of different brands. The collected data come from an authorized service network, have been collected in the second quarter of 2014.

Maintenance strategies represent one of the many areas of maintenance research theory. Among the many listed models fulfill an important role in the maintenance system strategy is based on the control of main parameters of the model—the so-called strategies to control the state of the system (called inspection maintenance, inspection and replacement models). Computational problem in this type of strategies is the selection of optimal moments inspecting the object that operating costs were minimal (Koucky & Valis 2011). Overview of system status control models can be found, inter alia, in (Nowakowski & Werbinska-Wojciechowska 2012).

At the same time, it is worth emphasizing that in the available literature can find a number of works that address the problem (Werbinska 2008):

the impact of the changing environment on the functioning of the technical system,

the impact of technological progress on serviced component and system

as well as appear in works that compare, under certain assumptions, different operating strategies.

In the area of modeling maintenance of technical facilities used mathematical methods involving, among others. probability theory, renewal theory, or the theory of Markov processes. However, there are a number of issues, the complexity of which can't be described using analytical functions (Valis & Pokora 2014). Therefore, there are a number of studies involving the implementation of linear and nonlinear programming, dynamic programming, simulation methods or heuristic methods that have been mentioned only in developed literature review; preventive maintenance strategies, in its classical form, are hardly used in practice—there have been many modifications thereof which allow a more accurate reflection of the actual functioning of the technical process (Valis & Zak 2014).

In a situation where the system components are not dependent or relationship can't be properly defined, maintenance problems are solved by using the models to maintain a dedicated technical objects. In this case, two basic policy of maintaining technical facilities are used—Strategy Exchange BRP blocks (Block Replacement Policy) and the Strategy Exchange According to Age ARP (Age Replacement Policy). The first method is the most commonly used by car manufacturers as a recommendation for vehicle users. Nevertheless, there is often the need to implement corrective support. In time of increasing the competence and diagnostic systems inside a vehicles, successive producers decide to change their approach to cases of vehicle maintenance by the user and showing maximum period between every service preventive indicate the information from the system informing the user of the need to make the necessary adjustments (Loska 2011).

2 THE CASE

The data presented in this chapter come from two authorized Vehicle Service Station (VSS) in Poland. Both brands belong to the same group, one of them belongs to the premium class, the second class of vehicles popular.

During the study observed number of cars admitted to the (VSS) for repair or maintenance works. Were counted separately damage to individual components and the time of repair. The object of the study was the number of people visiting customer service. During the study reported more visits in the premium segment because of the greater amount of vehicles. As a subjective observation can be treated better assessment of clients of premium warranty terms in the premium segment, the overall culture of service and maintenance.

Figure 1 shows a graph of the typical numbers of visits to the service station in 2014. The direct

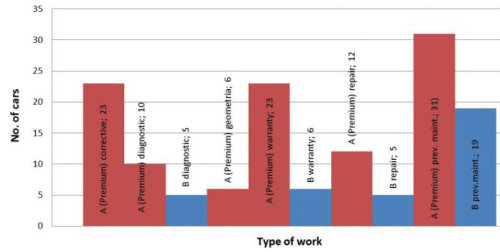


Figure 1. Graph of the numbers typical visits to the service station 2014.

relationship were presented two brand vehicles, one of which represents a group of cars in the premium segment. The first column of the chart shows the number of shares of default arising from various types of faults, especially new models introduced on the market.

These faults are often caused by flaws in the component reliability testing or are the result of errors in the manufacturing process. It is not possible to check all the parts and components of a new product in every possible way. In today's era of technology and the growing amount of electronic systems (eg., traction control) for vehicles more common are errors on the background of software drivers and modules of the car. Unfortunately, this type of defect also require manual servicing a car in order to update the software. There is no information about the vehicles not belonging to the premium brands. It may be caused by more complex systems installed in the premium brands, so default action to remove those defects than in the remaining brands.

The second group shown in Figure 1 is a comparison of the number of visits by the need to carry out a diagnosis of the vehicle. The procedure aims to establish and verify a fault in the vehicle. Here should not be surprising that a greater number of visits of vehicles in the premium segment is caused by greater complexity of the product, both the hardware and software. Each following group, which can be found in chart shows a comparison is visits to the site due to components or services covered by the warranty. There used to guarantee the distribution that is obtained when purchasing a new vehicle called. As it can be seen there were reported 23 visits vehicles of brand A (Premium), while in brand B only 6. The reason of this situation may be less extensive warranty of car brands B segment, as well as the general conviction customers a premium for better quality services in the authorized repairer (VSS). Direct comparison with the previous statement is related to repairs of both brands. Therefore, the argument is redundant results. Cars representing the brand A (Premium)

were on VSS 12 times, while Brand B vehicles only 5 repairs related to the scope of work not covered by the warranty.

Most owners owning Brands A (Premium) go to service vehicles to an authorized (here 31 times) than car owners Brands B (19 visits). Often this involves in Poland with a sense of the value of the product, but also, unfortunately, owner's wealth, which is the main reason the results presented.

In case of replacement it was compared to replacement of individual components of the vehicle. Here both Brand A and B, which can boast of nine visits to the service. It is possible to deliver the customer's own part, purchased privately. Service is obliged to request the customer's responsibility to replace the defective part on privately purchased replacement. The customer pays only for the service exchange.

When it comes to seasonal wheel exchange in the car, especially with winter tires to summer and vice versa, there is 31 visits reported for brand A (Premium), while brand B can score the result of 13 visits. When changing wheels often include a wheel alignment, which was mentioned above. Vehicle geometry on the example of Brand A (Premium), which is nothing else like setting toe in the car rarely be recorded in the site itself, however, is often typed as one of the steps to replace wheels.

The results of changing the oil in the cars of both brands are very similar. The exchange is based mainly on the exchange of the oil filter, oil and oil drainage. Therefore, the service rates depend largely on the capacity of the engine, and thus the amount of oil that is needed to be replaced. Nowadays, the boundaries between oil change intervals in gasoline and diesel, which are usually around 30k. miles.

Figure 2 shows the number of visits to the VSS premium brand vehicles and traditional to a specific service.

3 CONCLUSIONS

The selection of an appropriate strategy for maintaining complex systems requires the determination of policy for handling the group of elements, and not for each item separately working. The complexity of such a task is growing, especially when working elements are not identical, eg in the area of reliability whether there is between them, depending, for example in terms of economic or structural.

Preventive maintenance strategies, in its classical form, are hardly used in practice—there have been many modifications thereof which allow a more accurate reflection of the actual functioning of the technical process.

In the case of passenger cars, in an era of increasing the competence of information systems and diagnostic manufacturers are increasingly turning to the change in approach to terms of vehicle maintenance by the user.

The study indicates that the need to select an appropriate maintenance policy exists within a single company producing vehicles part of the same elements. Number of visits is higher in vehicles representing the premium class. This may seem surprising, but it should be noted that these vehicles are usually much better equipped, hence the number of possible points of damage or lack of functionality is greater. Hence the cost of vehicle maintenance premium compared to conventional vehicles is higher. As it comes from the research rule is repeated in different vehicle segments.

REFERENCES

Koucky, D., Valis, D. 2011. *Suitable approach for non-traditional determination of system health and prognostics*. In: Zeszyty Naukowe, Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki, 2011, 123–134.

Loska, A. 2011. *Przegląd modeli ocen eksploatacyjnych systemów technicznych*. Preceedings of Computer Integreted Management Conference, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, 2011, 2: 37–46.

Min Han, C. 1990. *Testing the Role of Country Image in Consumer Choice Behaviour*. European Journal of Marketing, Vol. 24 Iss: 6, pp. 24–40.

Nowakowski, T., Werbinska-Wojciechowska, S. 2012. Zagadnienie utrzymania środków transportu–system wsparcia decyzyjnego. Prace Naukowe Politechniki Warszawskiej. Transport, 37–54.

Raff, D. 1991. *Making cars and making money in the interwar automobile industry: economies of scale and scope and the manufacturing behind the marketing*. Business History Review 65.04 (1991): 721–753.

Valis, D., Žák, L. 2014 in prep. Contribution to oil data assessment for system condition determination. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Valis, D., Pokora, O. 2014 in prep. Application of Selected Diffusion Processes on System State Assessment. Article accepted for European Safety and Reliability Conference ESREL, 2014 Conference, 14–18 September, Wroclaw Poland.

Vinson, D.E., Scott, J.E., Lawrence, M. 1977. The role of personal values in marketing and consumer behavior. The Journal of Marketing, 44–50.

Werbinska, S. 2008. Model logistycznego wsparcia systemu eksploatacji środków transportu. Rozprawa doktorska Wydziału Mechanicznego PWr., Wrocław.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Ship voyage characteristics in Wuhan Yangtze River Bridge waterway

Ying-Ping Zhou
School of Logistics Engineering, Wuhan University of Technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

Ling-Zhi Sang & Zhe Mao
Intelligent Transportation System Research Center, Wuhan University of Technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

Qing Wu
School of Logistics Engineering, Wuhan University of Technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

ABSTRACT: To ensure the navigation safety of ships, the characteristics of ships that go through the bridge waterway of Wuhan Yangtze River Bridge need to be studied. Ships' AIS information was used as a data source to analyze the distributions of the ship speed when ships navigating into and out of the bridge waterway downstream, as well as when passing by the buoys and the navigable hole. Then the shortest distance between the ships and their nearest buoys, the ships and the bridge piers were all calculated, the relationship between the distribution of the shortest distance and the corresponding ship speed was studied. Statistic analysis and K-S testing prove that, the ship speed of the downstream ships that navigate into and out of the bridge waterway, pass by the buoys and the navigable hole, obeys positive skew distribution respectively. The shortest distance between ships and the bridge pier obeys negative skew distribution, the shortest distance between ships and the navigation buoy is almost normal distributed. There is no linear relationship between the ship speed and the shortest distance.

1 INTRODUCTION

The ship traffic of the Wuhan Yangtze River Bridge Waterway is intensive, whilst the navigable hole of this bridge is narrow (128 metres), accidents occur in this waterway area frequently every year, so it is necessary and of significance study on the voyage characteristics of ships in this waterway area, which is important for the supervisor to ensure the safety of ships. Automatic Identification System (AIS) information can be obtained by parsing the AIS messages which are received through Vertical Horizontal Filter (VHF) by AIS base station. AIS information mainly includes the static, dynamic, and navigation information of the ship. Accident statistics, ship collision avoidance (Weng et al., 2012, Mou et al., 2010), statistics or modeling and simulation of traffic flow (Yan et al., 2010, Jin et al., 2012, Goerlandt et al., 2011), etc. can be researched by using the ship AIS information as a data source. At the same time, further study on the voyage behavior characteristics of ships can be carried out through the statistical analysis of AIS information. The voyage behavior characteristics of ships voyaging in the harbor waterway area and sea area are studied both domestically and overseas (De 2010, Gunnar et al., 2009, Zhu et al., 2012). Voyage behavior characteristics of ships, traffic flow (Mou et al., 2010), navigation ability (Zhou et al., 2013, Hu et al., 2013, Ai et al., 2013), ship speed and safe distance (Hou et al., 2010), etc. in the bridge waterway of the Yangtze River were studied by the domestic scholars. The linear regression model of the length, ship speed, ship course and the closest point of approach (CPA) was came up (LLOYD 2004), and the safe waterway space (MEINE et al., 2004) was studied by some scholars overseas. To sum up, study of the voyage characteristics of ships in the process of navigating into to navigating out of the bridge waterway of the Wuhan Yangtze River Bridge is relatively rare.

The ships' AIS information is used as a data source, the distributions of the ship speed when the ships navigating into and out of the bridge waterway, passing by the buoys and the navigable hole downstream are analyzed in this paper. Then the shortest distance between ships and their nearest buoys, ships and the bridge piers when ships passing by are calculated. The relationship between the distribution of the shortest distance

and the corresponding ship speed are studied. The model of the distribution function is built and then hypothesis testing is completed.

2 DATA PROCESSING

The AIS base station, which built in the Wuhan segment of the Yangtze River waterway can receive AIS messages broadly, all the information about the ships upstream and downstream in the bridge waterway of this segment can be received. As the distribution of the buoy start to become intensive about one nautical mile from the upstream of the Wuhan Yangtze River Bridge, the area between one nautical mile from the upstream and one nautical mile downstream of the bridge was chosen as the target bridge waterway. The AIS information of all the downstream ships whose ship speed were higher than 2 knots from January 7 to 16 in 2014 was chosen as preprocessing data, this preprocessing data includes 20275 pieces of information. Considering the loss of information in the process of receiving AIS messages, the preprocessing data are in discontinuous time.

This paper mainly studies the distribution law of the ship speed of the downstream ships from navigating into to leaving out of the bridge waterway, as well as the law of the shortest distance, and the relationship between the shortest distance and the corresponding ship speed. Therefore, the ship speed of the ships should be statistically analyzed, and the shortest distance should be calculated.

2.1 *Selection of ship speed*

In order to get the data of ship speed needed for the study, the moment when a ship arrives the place where is one mile away upstream from the Wuhan Yangtze River Bridge and the same distance downstream from the bridge, and this two moment are chosen as the time the ship navigates into or navigates out of the bridge waterway. The moment when a ship is closest to a buoy or the bridge pier is chosen as the time the ship voyages by them, the ship speed correspondingly is the average ship speed of that in two positions, where is the closest AIS information point to the buoy or the bridge pier.

To get the ship speed data for ships navigate into and out of the bridge waterway, the range of longitude and latitude of the axis, which parallel to and is one mile away from the Wuhan Yangtze River Bridge was used as the limited parameters to select ships' AIS information, 4566 pieces of information are obtained as the ship navigate into the bridge waterway, 1322 pieces of information are obtained as the ship navigate out of the bridge waterway. To get the ship speed information when the ship navigates by the buoy and the bridge pier, the information about the ship whose distance is farther than 500 metres from the buoy, or is farther than 200 metres from the bridge pier, is excluded, AIS information of 936 ships which navigate by the navigation, 506 ships which go through the navigable hole is finally obtained.

2.2 *The calculation of shortest distance*

In order to calculate the shortest distance between the ship and the buoy in the bridge waterway, as well as the shortest distance between the ship and the bridge pier, the position where AIS device is fixed for sending the ship AIS messages is regarded as the AIS information point, the buoy or bridge pier is regarded as the target object, the longitude and latitude of the buoy or bridge pier is set as target point. It is also assumed that the ship navigates in line between two AIS information points. The algorithm for calculating the shortest distance is shown in Figure 1.

1. Select the AIS information points which are at a certain distance from the target point. The data in this algorithm are the same as the former data of ship voyaging by the buoy and going through the bridge, the selection criteria is that the distance from these AIS information points to the

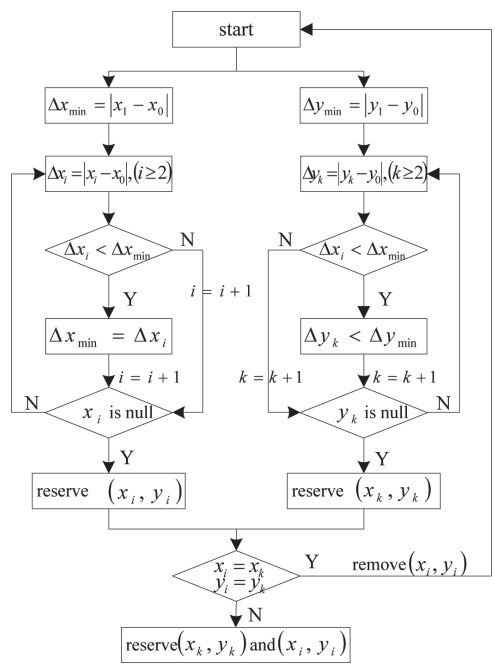


Figure 1. The algorithm of the shortest distance.

buoy is about 500 m, and to the bridge pier is about 200 metres.

2. All of the AIS information for one ship can be obtained in one day, according to the MMSI information in the received AIS messages, for a ship has a fixed MMSI number. All of these AIS information points are then listed in time sequence, and then subtract the longitude and latitude of ships with that of the target object (bridge pier or buoy) respectively. The obtained absolute value of the difference is then recurrently compared; the minimum absolute values of the longitude difference Δx_{min} and latitude difference Δy_{min} are kept, as well as the corresponding longitude and latitude value of the ship, (x_i,y_i), (x_k,y_k). If and $x_i = x_k$, the AIS information that has an inferior absolute value of the longitude difference and latitude difference is kept. Therefore, two or three AIS information points can be obtained where the absolute values of the longitude difference and latitude difference are minimum, and these AIS information points are called reserved points. The process of this step is shown in Figure 2.
3. As is discussed above, it is assumed that the ship navigates in line between two AIS information points. If there are two reserved points, the distance from the target point to the line formed by these two points is calculated and kept; if there are three reserved points, mark them by A, B, C in turn. The distances from the target point to the line formed by A, B and line formed by B, C are calculated respectively, compare these two distances and then keep the smaller one. On this basis, the minimum distance from the ship to the target object can be obtained, and that is the shortest distance.

The geographic location of the target buoy used in this paper is 114.283833° east longitude and 30.54833° north latitude. The two bridge piers of the downstream navigable opening (#7) of the Wuhan Yangtze River bridge are the target bridge pier. Actually, the calculated shortest distance is the distance from the point where AIS device is fixed for sending the messages to the middle point of the buoy and bridge pier.

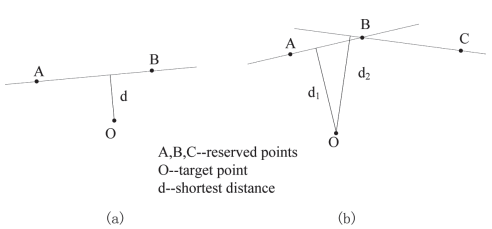


Figure 2. Step 2 of the shortest distance algorithm.

After the above calculation of the distance, 445 shortest distances from ships to the buoy are gained; the maximum value among the shortest distances is about 102 metres. 246 shortest distances from ships to the bridge pier are gained; the maximum value among these shortest distances is about 68.5 metres.

3 THE DISTRIBUTION LAW

3.1 *The distribution law of ship speed in the bridge waterway*

By selecting and counting the ship speed information of ships in the bridge waterway of the Wuhan Yangtze River Bridge, statistical analysis of 4 ship speed characteristics of the ships are carried out, the frequency histogram of the ship speed is drawn.

The distribution of the ship speed when ships navigate into the bridge waterway is shown in Figure 3. The unit of the speed is knot (kn) in the figure, the same as in the following figures.

The information indicates that, the ratio of the ships whose ship speed between 4 knots and 10 knots accounts for about 96.1%, whose ship speed between 5 knots and 7 knots accounts for about 58.56%, whose ship speed above 10 knots accounts for less than 2%.

Then use the testing of Kolmogorov-Smirnov (hereinafter referred to as K-S test) to test the speed distribution of ships when entering the bridge area. Let X be the sequence of speed value for the ship entering the Bridge area, let the significance level be 5%. Then put the vector X into the function H = kstest (X), consequently the value of H can be calculated out with the help of Matlab, that is H = 1. According to the principle of the K-S test, X is originally assumed to obey the

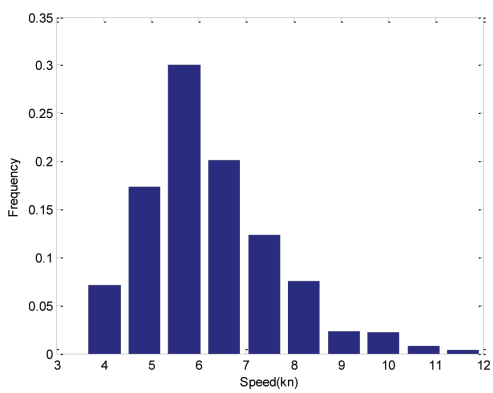


Figure 3. The ship speed distribution when ships navigate into the bridge waterway.

standard normal distribution, if H = 0, the original hypothesis cannot be rejected, if H = 1, the hypothesis is rejected. In summary, the speed of the ship entering the bridge area does not obey the normal distribution.

Skewness function is further applied to analyze the skewness of the speed distribution. As is known, skewness can be used as a statistic parameter to weigh the direction and degree of the distribution deflection. If the value of skewness *SK* is 0, it means that the distribution obeys a normal distribution. When *SK* is over 0, the distribution obeys positive skew distribution; while it is under 0, it obeys negative skew distribution. The *SK* can be calculated as:

$$SK = \frac{n\Sigma(x_i - \overline{x})^3}{(n-1)(n-2)sd^3} \quad (1)$$

Where n is the size of the speed sequence X, x_i is the i-th number, *sd* is the standard deviation of X, $\overline{\chi}$ is the mean of X. The skewness *SK* of the speed distribution which can be calculated out using Matlab is 0.8433 when ship entering the bridge area, obeying a positive skewness.

The distribution of the ship speed when ships navigate by a navigation buoy is shown in Figure 4.

The information indicates that, the ratio of the ships whose ship speed between 4 knots and 9 knots accounts for about 92.1%, whose ship speed between 6 knots and 8 knots accounts for about 54%, whose ship speed above 9 knots accounts for less than 8.3%.

Similarily, the value of the H can be calculated as 1 under this circumstance, the value of the skewness is 0.7563, the ship speed obeys positive skew distribution.

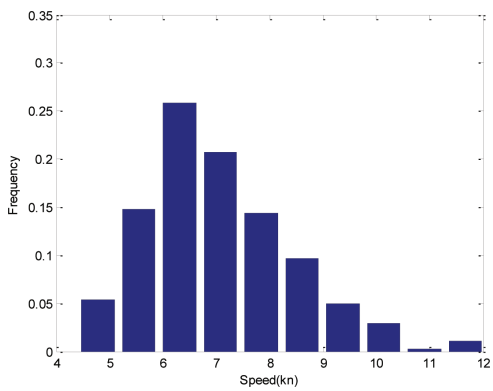


Figure 4. The ship speed distribution when ships navigate by the buoy.

The distribution of the ship speed when ships navigate by the bridge pier is shown in Figure 5.

The information indicates that, the ratio of the ships whose ship speed between 4 knots and 9 knots accounts for about 93.5%, whose ship speed between 6 knots and 8 knots accounts for about 54.9%, whose ship speed above 9 knots accounts for less than 7.3%.

The value of H equals 1 under this circumstance and the value of the skewness is 0.5813, the ship speed also obeys positive skew distribution.

The distribution of the ship speed when ships navigate out of the bridge waterway area is shown in Figure 6.

The information indicates that, the ratio of the ships whose ship speed between 5 knots and 13 knots accounts for about 91.1%, whose ship speed between 5 knots and 8 knots accounts for about 57.8%, whose ship speed above 10 knots accounts for less than 16.2%.

The value of H equals 1 under this circumstance and the value of the skewness is 0.8374, the ship speed obeys positive skew distribution.

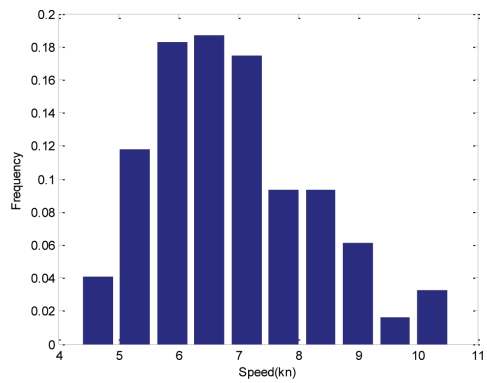


Figure 5. The ship speed distribution when ships navigate by the bridge pier.

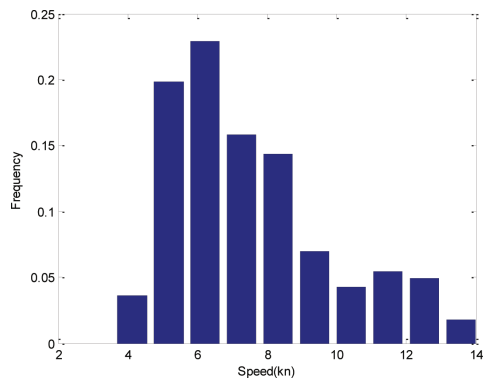


Figure 6. The ship speed distribution when ships navigate out of the bridge waterway.

3.2 *The distributive law of the shortest distance*

Through calculating and statistically analyzing the shortest distance, the frequency histogram of the shortest distance is drawn, and the hypothesis testing is completed.

The distribution of the shortest distance when ships passing by the buoy is shown in Figure 7. The unit of the distance is metre (m) in the figure, the same as in the following figures.

The information indicates that, the ratio of the ships whose distance from the navigation buoy is above 60 m accounts for about 91.93%.

The value of H equals 1 and the value of the skewness is 0.0053, which is much near zero, therefore the shortest distance under this circumstance is almost normal distributed.

The distribution of the shortest distance when ships navigating by the bridge pier is shown in Figure 8.

The information indicates that, the ratio of the ships whose distance from the navigation buoy is between 35 m and 65 m accounts for about 94.3%.

The value of H equals 1 and the value of the skewness is –0.5755, therefore the shortest distance under this circumstance obeys negative skew distribution.

At last, the distribution of the ship speed and shortest distance under different voyage circumstance (shown in figure 3 to figure 8) can be concluded, as shown in the table 1.

It can be seen that the ship speed of ships navigating in the bridge waterway obey positive skew distribution, which means that the low ship speed account for the majority, ships are more likely to choose a low speed when navigating in this special waterway. The shortest distance between ships and the bridge pier obeys negative skew distribution, which means that the bigger value of the shortest distance is dominated. The shortest distance between ships and the navigation buoy is almost normal distributed. In conclusion, when ships navigate in the bridge area waterway, a more conservative navigation method is usually adopted, that is low speed or far away from the buildings.

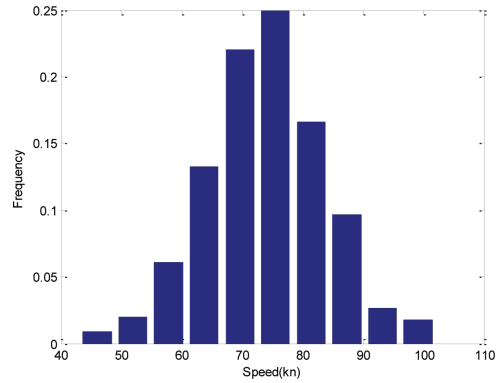


Figure 7. The shortest distance distribution when ships passing by the buoy.

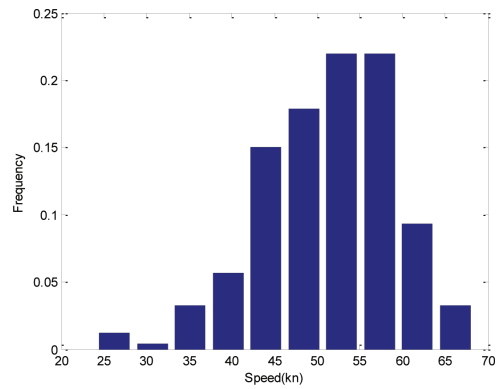
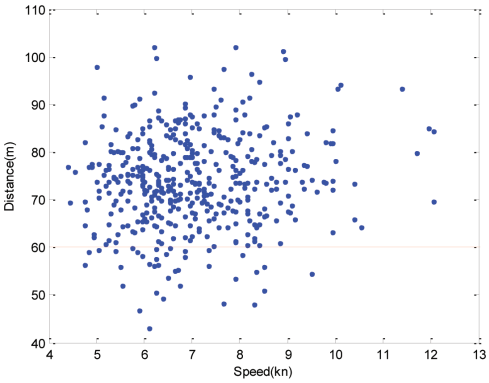


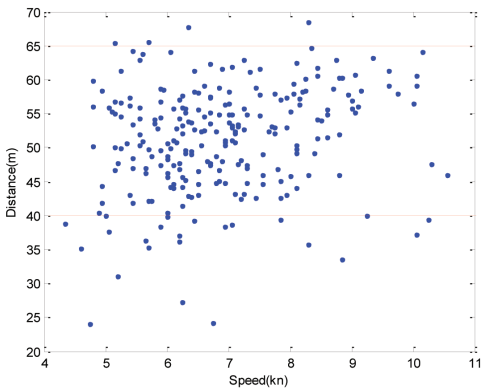
Figure 8. The shortest distance distribution when ships passing by the bridge pier.

Table 1. The distribution of the ship speed and shortest distance.

	Specific distribution	H	$\overline{\chi}$	sd	Skewness value	Distribution type
Ship speed Distribution	Refer to figure 3	1	6.2309	1.4034	0.8433	Positive skew distribution
	Refer to figure 4	1	7.0383	1.3683	0.7563	Positive skew distribution
	Refer to figure 5	1	6.8953	1.3048	0.5813	Positive skew distribution
	Refer to figure 6	1	7.5789	2.3078	0.8374	Positive skew distribution
Shortest Distance Distribution	Refer to figure 7	1	73.8007	9.8483	0.0053	Almost normal distributed
	Refer to figure 8	1	51.2226	7.8271	-0.5755	Negative skew distribution



(a)



(b)

Figure 9. The relationship between the ship speed and the shortest distance.

3.3 *The relationship between the ship speed and the shortest distance*

In order to study the relationship between the ship speed and the shortest distance, the ship speed is chosen as the horizontal axis, the shortest distance as the vertical axis, the relationship between them is shown in Figure 9.

As is shown in the Figure 9, there is no specific functional relationship between them, what can be observed is, most of the minimum shortest distance between the ships and the buoy are around 60 metres, there is little shorter than 60 metres (figure (a)); most of the minimum shortest distance between the ships and the bridge pier are between 40 metres and 65 metres, there is little shorter than 40 metres or farther than 65 metres (figure (b)).

4 CONCLUSION

According to the processing of the ships' AIS information which is received by the AIS base stations, the ship speed information related to ships which navigate downstream in the Wuhan Yangtze River bridge area at the following moment was selected out and analyzed statistically, that is when ships navigating in and out of the bridge area, passing by the buoys and the bridge piers. Then the shortest distance was calculated out using the former selected ship speed information between the downstream ships and their nearest buoys, between the ships and the bridges. The relationship between the distribution of shortest distance and the corresponding ship speed was also analyzed. Finally, Hypothesis testing was carried out aiming at the shortest distance and the ship speed.

The result shows that the ship speed is a positive skew distribution whenever the ship is navigating into the bridge area, voyaging by the navigation buoy, going through the bridge or navigating out the bridge area. Ships when navigating out the bridge area will normally ship speed up comparing with which when navigating in. The range of the ship speed is familiar when the ship voyage by the navigation buoy and the bridge pier. As for the shortest distance, it is negative skew distribution when the ship goes through the bridge, while it is almost normal distributed when the ship voyage by the navigation buoy and. However, the formerly noted ship speed does not have a linear relationship with the shortest distance. This result reflects that a certain rule exists in the distribution of ship speed and the shortest distance when ships navigate through the bridge area. It can provide a basis for the next research on the relationship between the ship types and the ship voyage behaviors in the bridge area, as well as the research on the behavior characteristics and rules for ships navigating in the continuous bridge area.

ACKNOWLEDGEMENTS

This paper is supported by Western Communications Construction Scientific and Technological Project of Ministry of Transportation of the People's Republic of China (Grant No. 201132820190), Natural Science Foundation of Hubei Province, China (Grant No. 51309187), and FP7 Marie Curie IRSES of European Union (Grant No. 314836).

REFERENCES

Ai, W.Z., & Hu, B.H. 2013. Research on Fairway Condition for Safety Navigation in Bridge Waters. *Applied Mechanics and Materials*, 275, 2807–2810.

De Boer, T. 2010. An analysis of vessel behaviour based on AIS data (*Doctoral dissertation, Master Thesis, Delft University of Technology*).

Goerlandt, F., & Kujala, P. 2011. Traffic simulation based ship collision probability modeling. *Reliability Engineering & System Safety*, 96(1), 91–107.

Gunnar Aarsæther, K., & Moan, T. 2009. Estimating navigation patterns from AIS. *Journal of Navigation*, 62(04), 587–607.

Hou, H.Q., LI, Y.C., Chu, X.M. 2013. Vessel clearance model al in busy waters of the Yangtze river. *Journal of Dalian Maritime University*, 39(4):21–24.

Hu, Y.M., Zhou Y., & Chen B. 2013. The Measure for Up-bound Ships to Pass by the Nanjing Yangtze River Bridge piers with Safe Distance. *Navigation of China*. 36(3):65–69.

Jin, X., Fu, Y., & Zhang, L. 2012. Research on vessel traffic flow at Chengshantou water area based on AIS Data. *Journal of Dalian Maritime University*, 38(1), 33–36.

Lloyd D.N. 2004. Integrating VTS with port operation. *In Proceedings of VTS*.

Meine J., Kramer M. 2004. Creation of a region VTS with data fusion and integration of vessel data and movement details over the area of several independent ports, coastal and inland waterways. *In Proceedings of VTS*.

Mou, J.M., Tak, C.V.D., & Ligteringen, H. 2010. Study on collision avoidance in busy waterways by using AIS data. *Ocean Engineering*, 37(5), 483–490.

Weng, J., Meng, Q., & Qu, X. 2012. Vessel collision frequency estimation in the Singapore Strait. *Journal of Navigation*, 65(02), 207–221.

Yan, X.P., Ma, F., Chu, X.M., & Chen, C. 2010. Key technology of collecting traffic flow on the yangtze river in real-time. *Navigation of China*, 33(2), 40–45.

Zhu, F., Zhang, Y., & Gao, Z. 2012. Research on Ship Behaviors Based on Data Mining. *Navigation of China*, 35(2), 50–54.

Zhou, H., Guo, G., & Wu, B. 2013. Nanjing Yangtze River Bridge Transit Capacity Based on Queuing Theory. *Procedia-Social and Behavioral Sciences*, 96, 2546–2552.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Fleet-level reliability estimation of repairable units

Amir H.S. Garmabaki, Alireza Ahmadi & Jan Block
Division of Operation and Maintenance Engineering, Luleå University of Technology, Luleå, Sweden

ABSTRACT: This paper investigates reliability analysis of a repairable unit at fleet level. In fleet, multiple similar systems are running in different operating environments. In fact, due to the highly censored data as well as high variations in failure rate within the fleet, merging the datasets becomes a challenge. The non-parametric analysis is used to capture the failure trend of repairable units at fleet level. Consequently, fleet data have been aggregated and the actual number of failure has been compared with the expected total number of failures. In addition, parametric models are used to model the reliability trend obtained through a non-parametric approach to identify the reliability parameters at fleet level. Real data are used to demonstrate the applicability and validity of the proposed method. Results shows the accuracy of log-linear process is reasonably acceptable.

1 INTRODUCTION

Repairable systems are those systems that can be restored to fully satisfactory performance by a method other than replacement of the entire system (Ascher and Feingold, 1984). Reliability analysis of repairable units can be classified into parametric and non-parametric methods.

The parametric method entails stochastic point processes, including the Homogeneous Poisson Process (HPP), the Renewal Process (RP), the Non-Homogeneous Poisson Process (NHPP), and the Generalized Renewal Process (GRP). For further discussion, see e.g., (Kijima and Sumita, 1986), (Rigdon and Basu, 2000), (Rausand and Høyland, 2004), (Ebeling, 2010), and (Kumar and Klefsjo, 1992). Application of parametric methods require a lot of statistical assumptions and analytical skills for implementation, which make these methods inapplicable for some real-world cases. The application of these methods for a single system/unit is fairly straightforward. However, in practice, the analyst is often dealing with multiple similar systems that are installed in different equipment/plants, that are running in different operating environments and with varying influencing factors.

The application of parametric reliability analysis methods at fleet level, even if very limited in scope, is quite complex and time-consuming for a variety of reasons. For instance, failure analysis is made more difficult by the highly multi-censored nature of the reliability data belonging to different failure modes (Block et al., 2013a). The analysis of time-censored and failure-censored data need different treatment and application of different methods. Moreover, drawing conclusions at fleet level from these individual analyses requires statistical assumptions that, in practice, entail a degree of uncertainty.

The non-parametric method provides a graphical estimate of the number of recurrences (repairs/failures) per unit and per the whole population, versus utilization/age. The method is non-parametric in the sense that it does not use a parametric model for the population. This estimation involves no assumptions about the form of the mean function or the process generating the system histories.

Within available non-parametric methods, Mean Cumulative Function (MCF) was introduced to estimate the expected average number of failures per unit within population of a fleet, see (Nelson, 2003). In this process, the number of systems at risk at each failure node is the basis of computation. MCF results, in combination with total utilization at fleet level, can be used to estimate the total expected number of failures at fleet level.

In addition, Ebeling (2010) used a method to aggregate data at failure nodes in order to calculate the cumulative number of failures for a whole fleet of jet engines. That methodology considers the cumulative operation time of all other engines at any failure nodes/dates and considers that the failure nodes are not chronologically ordered. This requires complete information on the status of all systems at all failure nodes. However, in some cases; specifically for the case of this study, such complete information is not available due to the variety of operational bases and operators.

Recently, Block et al. (2013b) discussed the reliability behavior of repairable units at fleet level. They performed a case study and evaluated the goodness of fit of the estimated linear curves

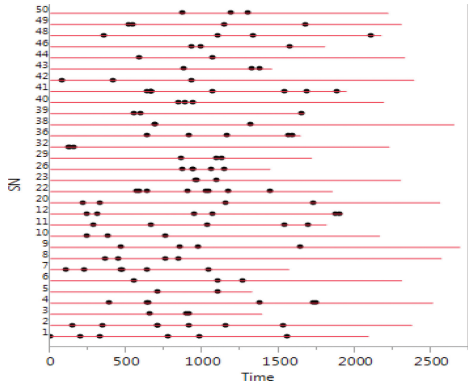


Figure 1. Event plot of units' failures.

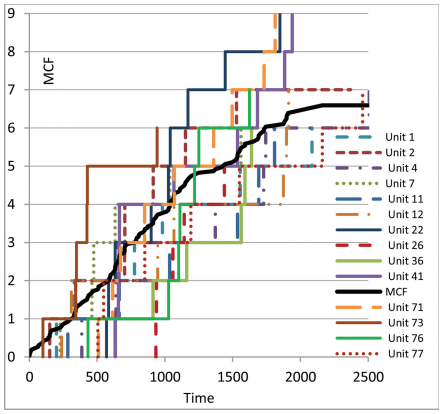


Figure 2. Cumulative failure events for 14 units.

against the actual MCF. In addition, Block et al. (2013a) used the power law process to calculate the expected number of failures at fleet level.

In this study, we have introduced an approach to compute the cumulative number of failures at fleet level, in which the recurrent failure events of units within the fleet are chronologically ordered (see Fig. 1).

In addition, we have used the power law as well as the log-linear and homogeneous poisson processes to fit a curve on the MCF, and to the variation of estimation by different models.

The rest of this paper is designed as follows: In Section 2, MCF is introduced; Section 3 reviews some parametric models. The proposed non-parametric model is discussed in Section 4. Aircraft Radar Transmitter Unit (Case Study) is studied by parametric and non-parametric methods in Section 5. Finally, conclusions and discussions are given in Section 6.

2 MEAN CUMULATIVE FUNCTION (MCF)

Here, we discuss a simple and informative plot for analyzing recurrent repair data. The plotting method provides a non-parametric graphical estimate of the number/cost of repairs per unit versus age. This estimate can be used to evaluate the repair rate of the population with respect to age and predict future number/cost of repairs. The MCF plot reveals most of the information that we are searching for in recurrent data (Nelson, 2003). A key advantage of the MCF plot is that it provides a single summary plot for a group of units, which is easily compared with other MCF plots of different populations. The MCF plot is the population of staircase functions for all the studied units. This staircase is a consequence of the non-parametric estimation. Non-parametric MCF estimation methods have been described by (Nelson, 2003, Block et al., 2013b, Meeker and Escobar, 1998). The mathematical formulation of MCF is discussed as follows, see (Nelson, 2003).

Let n denote the number of observed units, and let m denote the number of unique failure times. Also, let $t_1, \ldots, t_m$ be the unique failure times. Then the non-parametric estimator of the MCF is

$$\hat{\mu}_{NP}(\mathrm{t_j}) = \sum_{k=1}^{j}\left[\frac{\sum_{i=1}^{n}\delta_i(t_k)\times d_i(t_k)}{\sum_{i=1}^{n}\delta_i(t_k)}\right] = \sum_{k=1}^{j}\left[\frac{\sum_{i=1}^{n} d\cdot(t_k)}{\sum_{i=1}^{n}\delta\cdot(t_k)}\right], \quad j=1,\ldots,m \tag{1}$$

where $d_i(t_k)$ is the number of failures recorded at time t_k for unit i, and

$$\delta_i(t_k) = \begin{cases} 1 & \text{if unit } i \text{ is still functioning} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Also, the total number of failures reported at time t_k is given by

$$d.(t_k) = \sum_{i=1}^{n}\delta\cdot(t_k)\times d_i(t_k) \tag{3}$$

And $\delta\cdot(t_k) = \sum_{i=1}^{n}\delta_i(t_k)$ is the number of systems at risk for failure. Figure 2 depicts the MCF of 13 transmitter unit failures which are plotted by JMP/SAS software.

3 PARAMETRIC MODELS

In practice, one may want to know in what cases the parametric or non-parametric model are suitable. However, one should always do a MCF plot, as it

reveals information that parametric model fitting does not, see (Nelson, 2003). However, information given by non-parametric approaches are valid for the associated set of data and utilization, and failure prediction during the future operations is not possible. Hence the application of parametric approaches arises. Here we discuss fitting different models to the MCF data regarding our case study. We attempt to fit the power law process, log-linear process, and homogeneous poisson process to the MCF curve.

3.1 *Power law model*

The power law model is part of parametric NHPP models when the ROCOF of the NHPP is considered as

$$w(t) = \frac{\beta}{\theta}\left(\frac{t}{\theta}\right)^{\beta-1}, \ \theta > 0, \beta > 0, t \geq 0 \tag{4}$$

where $W(t) = \int_0^t w(s)\, ds$ and θ, β are scale and shape parameters, respectively, see (Ascher and Feingold, 1984).

3.2 *Log-linear model*

The log-linear form of intensity function also allows for increasing and decreasing the rate of occurrence. This model was proposed by (Cox and Lewis, 1966). The ROCOF of an NHPP is defined by

$$w(t) = e^{\alpha+\beta t} \ ; -\infty < \alpha, \beta < \infty \tag{5}$$

Where $W(t) = \int_0^t w(s)\, ds$ and α, β are scale and shape parameters, respectively.

3.3 *HPP model*

The HPP is the simplest statistical model for repairable systems. The HPP is a poisson process with a constant intensity function. In this process, the system does not wear out during the time between failures. The HPP cannot be used to model systems that are improving or deteriorating. Hence, it should be applied with caution. It is worth noting that the PLP and log-linear model reduce to the HPP model when $\beta = 0$. Here, we consider that

$$w(t) = e^{\alpha} = \lambda \text{ and } W(t) = \lambda t \tag{6}$$

4 PROPOSED NON-PARAMETRIC MODEL

Here, we discuss how to calculate and plot the Actual Total Number of Failures (ATNF) with/without censoring age at the fleet level. Let us consider a fleet consisting of k units/components and assume that the i:th unit, $i = 1, ..., k.$, is observed during the period $[0, T_i]$, which experienced N_i failures in their time horizon, $i = 1, ..., k$. Let T_i be the total operation time of the i:th component. And let t_{ri} be the age of the i:th component at the r:th occurrence of failure, $r = 1, ..., N_i$; $i = 1, ..., k$. Also, $m = \sum_{i=1}^{k} N_i + k$, $m' = \sum_{i=1}^{k} N_i$ and order all t_{ri} from smallest to largest. Let $S_c^{'}$ *and* S_w' where $c = 1 ... m$ and $w = 1 ... m'$, be the chronologically merged data: $S_1 \leq S_2 \leq ... \leq S_m$ and $S_1' \leq S_2' \leq ... \leq S_{m'}'$ for data with/without censored, respectivily. Then the actual failure time is given by:

$$\text{Actual failure time for fleet with time censor} = S_c' \times k, \tag{7}$$

$$\text{Actual failure time for fleet without time censor} = S_w \times k, \tag{8}$$

and

$$ATNF = \text{Actual number of failure with/without censoring} \times k$$

5 CASE STUDY: AIRCRAFT'S RADAR TRANSMITTER UNIT

We studied a (repairable) radar transmitter unit. This transmitter was the part of the main surveillance radar (PS-37) of the AJ 37 strike aircraft. The data were right-hand censored by two processes: failure and discard. The study considers 83 repairable units. Figure 1 displays the transmitter repair data of 50 units, separately. Each line in the figure shows the failure history of a component and each bullet point shows the aircraft unit's age in hours when a transmitter was repaired. For example, Transmitter S/N 40 was repaired at 840.72, 884.18, and 932.74 hours, and was observed for 2186.47 hours. The latest age is called the unit's "censoring age."

The successive repair pattern of 13 units is plotted simultaneously in Figure 2.

As described in Section 2, equation 1 is used to estimate the MCF. Figures 3 and 4 show the MCF

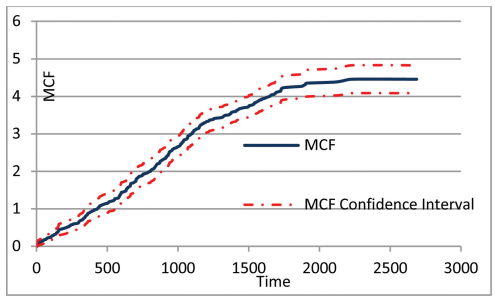


Figure 3. MCF plot of the units within the fleet.

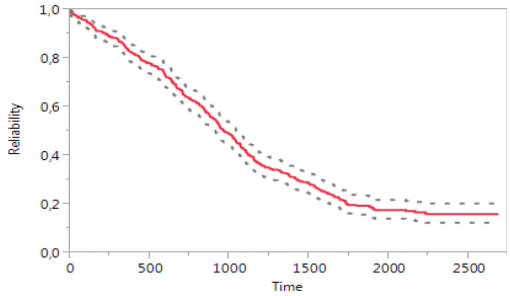


Figure 4. Reliability of fleet-level failure vs time.

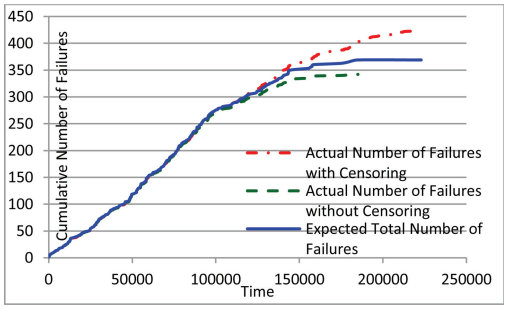


Figure 5. Actual total number of failure and ETNF for all unit.

and reliability plot, respectively, with a two-sided, 95% confidence bound.

5.1 *Non-parametric failure behavior ETNF vs the proposed model*

In addition, we calculate the Expected Total Number of Failures (ETNF) for all components and the relation of MCF with proposed model is depicted in Figure 5, simultaneously. We observe that the behavior of both curves are mostly the same until 125,000 operating hours, after which time the effects of age censoring appear.

To better understand the behavior of the above categories and to check the validity of the fleet data aggregation for estimatation of the number of failures, we select three random sample data from the data set and apply the same procedure as discussed earlier. The first random data consists of 26 random units and the second and third consist of 25 and 21 random units, respectively. The behavior of ETNF along with the actual total operational time (with/without censoring age) are plotted in Figures 6, 7, and 8, respectively. Results show similar behavior as in the first case (for analysis of all components, see Fig. 5).

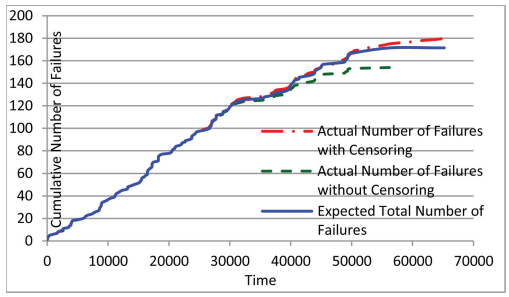


Figure 6. Actual number of failures and ETNF estimate for 26 random components.

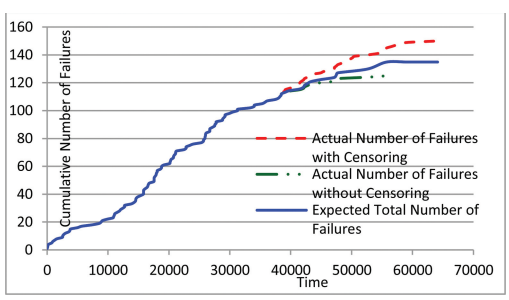


Figure 7. Actual number of failures and ETNF estimate for 25 random components.

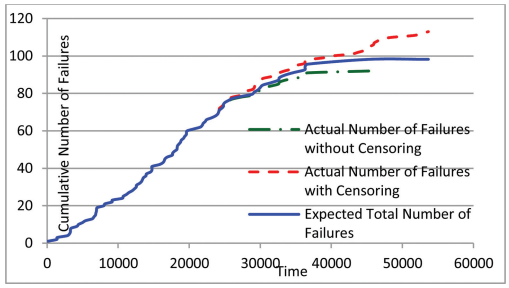


Figure 8. Actual number of failures and ETNF estimate for 21 random components.

5.2 *Fitting the parametric model to the MCF*

Here, we discuss the fitting of different models to the MCF data from our case study. We try to fit the power law process, log-linear process, and homogeneous poisson process to the MCF curve. Parameter estimations of the models are given in Table 1.

In addition, Figure 9 shows the goodness of fit of each model, separately. Also, we plot two-sided confidence levels at a significance level of 95% for our case study. The width of the confidence interval

Table 1. Parameter estimations of PLP, LLP, and HPP with censoring age data.

Model	Parameter	Estimate	Std error
Power law	θ	361,344	40,1399
	β	0,8466	0,04514
Log-linear	α	–5,7004	0,09406
	β	–0,0005	9,19e^{-5}
HPP	α	–6,1517	0,05404

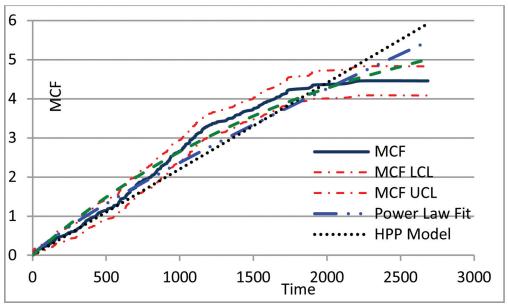


Figure 9. Goodness of fit of the power law, log-linear, and HPP.

after 2000 hours increases because several components are censored and will increases by increasing the numbers of censored units.

5.3 *Model evaluation*

Performance analysis of the proposed model is done using the four common criteria defined below (Kapur et al., 2010).

– The ***Bias*** is defined as

$$Bias = \sum_{i=1}^{k} \frac{(\hat{m}(t_i) - y_i)}{k} \tag{9}$$

The difference between the observed and predicted number of failures at any instant in time is known as PE_i (prediction error). The average of PE's is known as bias. The lower the value of Bias, the better the goodness of fit.

– The ***Variation*** is defined as:

$$Variation = \sqrt{\frac{\sum_{i=1}^{k} (PE_i - Bias)^2}{k-1}} \tag{10}$$

The average of the prediction errors is called the prediction Bias, and its standard deviation is often used as a measure of prediction variation.

– The Root Mean Square Prediction Error (RMSPE) is defined as

$$RMSPE = \sqrt{Variation^2 + Bias^2} \tag{11}$$

RMSPE is a measure of how closely the model predicts the observation.

– The Mean Square Error (MSE) is defined as

The difference between the expected values $\hat{m}(t_i)$ and the observed data y_i is measured by MSE as follows:

$$MSE = \sum_{i=1}^{k} \frac{(\hat{m}(t_i) - y_i)^2}{k} \tag{12}$$

where k is the number of observations. Low MSE indicates less fitting errors and, thus, better goodness of fit.

Table 3 show the values of MSE, Variation, RMSPE, and Bias for the power law, log-linear, and HPP models, for both censored and non-censored data sets. As the results show, the log-linear model has better comparison values than PLP and HPP for the censored data set.

However, as is evident in Figure 9, the curves associated with the proposed models do not fit properly to the MCF curve. This is due to the censoring ages at the end of the MCF curves, which have falsified effects on parameter estimation of the models. Therefore, the time censors in the data sets have been converted to failure censored, to protect against false estimation, see Table 3 (Without Censored Data Set). As shown in that table, the log-linear model fits the MCF better than the PLP and HPP models; however, the difference between them is not significant. For simplicity, we therefore suggest use of the HPP model. It may noted that the value of the shape parameter of the power law tends to 1, see Tables 2 and 3.

Figure 10 shows the goodness of fit of the log linear, PLP, and HPP models with the MCF. As is evident, the associated models provide more accuate estimation compared to the models with censored age data.

Table 2. Parameter estimation of models with failure censoring.

Model	Parameter	Estimate	Std error
Power law	θ	398.56839	39.0811
	β	0.966112	0.057858
Log-linear	α	–5.943227	0.112218
	β	–0.000124	0.000135
HPP	α	–6.025952	0.062017

Table 3. Best fit value.

	PLP	Log-linear	HPP
With censored data set			
MSE	0.0874	0.048116	0.18411
Variation	0.295631	0.219341	0.42906
RMSPE	0.295218	0.219076	0.42848
Bias	0.087655	0.048248	0.18462
Without censored data set			
MSE	0.01916	0.016207	0.02058
Variation	0.00865	0.007932	0.00881
RMSPE	0.01139	0.015056	0.02927
Bias	0.00741	–0.0128	0.02792

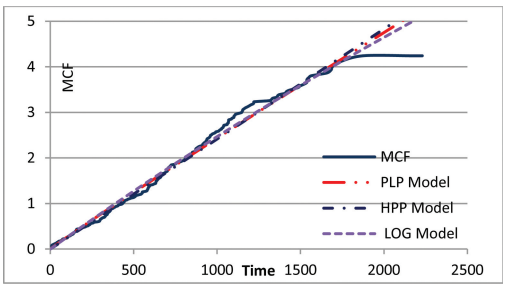


Figure 10. Goodness of fit of the power law, log-linear, and HPP (without the censored data set).

6 DISCUSSION AND CONCLUSION

In this paper, we have introduced an approach to compute the cumulative number of failures at fleet level when the recurrent failure events of units within the fleet are chronologically ordered. The proposed model is examined with three random samples. It is observed that in all three samples, the actual total number of failures (estimated by the proposed model) are slightly higher than the expected total number of failures (using the MCF). It is also observed that when the data set is non-censored, the ATNF for all three cases is slightly lower than the ETNF. In addition, the plots show that until around 125,000 fleet-wise operation hours, the ETNF and ATNF approach generates the same results for both censored and non-censored data sets. Therefore, the results obtained by the ATNF of a mature fleet can be used to estimate the number of failures for a new fleet, when the fleet is operated under approximately the same conditions.

In addition, to enhance the prediction power of the MCF, parametric models, such as the power law, log-linear, and homogeneous poisson process, are used to fit a curve on the MCF based on time-censored and failure-censored data. The results show that for both cases the log linear model provides the better fit to the MCF curve.

ACKNOWLEDGEMENT

We would like to acknowledge gratefully the financial support provided by the Swedish National Aeronautics Research Programme and granted through the NFFP6 project "Efficient Performance Based Air Vehicle Maintenance".

REFERENCES

Ascher, H. & Feingold, H. 1984. *Repairable Systems Modelling, Inferences, Misconceptions and their causes,* New York, Marcel Decker.

Block, J., Ahmadi, A. & Kumar, U. 2013a. Fleet-level Reliability of Multiple Repairable Units: a Parametric Approach using the Power Law Process. *International Journal of Performability Engineering*, Accepted.

Block, J., Ahmadi, A., Tyrberg, T. & Kumar, U. 2013b. Fleet-Level Reliability Analysis of Repairable Units: A Non-Parametric Approach using the Mean Cumulative Function. *International Journal of Performability Engineering,* 9, 335–346.

Cox, D.R. & Lewis, P.A. 1966. *The statistical analysis of series of events,* London, Methuen.

Ebeling, C.E. 2010. *An Introduction to Reliability and Maintainability Engineering,* Waveland Press.

Kapur, P.K., Singh, O., Garmabaki, A.S. & Singh, J. 2010. Multi up-gradation software reliability growth model with imperfect debugging. *International Journal of System Assurance Engineering and Management,* 1, 299–306.

Kijima, M. & Sumita, U. 1986. A Useful Generalisation of Renewal Theory: Counting Processes Governed by Non-Negative Markovian Increments. *Journal of Applied Probability,* 23, 71–88.

Kumar, U. & Klefsjo, B. 1992. Reliability analysis of hydraulic systems of LHD Machines using the power law process model. *Reliability Engineering and System safety,* 35, 217–224.

Meeker, W.Q. & Escobar, L.A. 1998. *Statistical Methods For Reliability Data,* New York, Johan Wiley.

Nelson, W.B. 2003. *Recurrent Events Data Analysis for Product Repairs, Disease Recurrences, and Other Applications,* Philidelphia, Pa, SIAM.

Rausand, M. & Høyland, A. 2004. System Reliability Theory: Models, Statistical Methods, and Applications, Hoboken, NJ Wiley.

Rigdon, S.E. & Basu, A.P. 2000. *Statistical Methods for the reliability of Repairable Systems.,* New York, John Wiley.

Reliability and safety education and training

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Learning from failures: The case of Deepwater Horizon disaster

A.W. Labib
University of Portsmouth, UK

ABSTRACT: In this work, it is argued that learning from failures and safety competence should be an important part of the curriculum of engineering and management students. The case of Deepwater Horizon will be used to illustrate how to learn about learning from failures using multi-models inspired by reliability and risk analysis in order to investigate disasters. This type of analysis can offer richness to our understanding of the root causes and provide insight into policy making and support decisions for resource allocations for prevention of such disasters. The concept of learning and unlearning from failures is relevant to the reliability and safety community.

1 INTRODUCTION—CASE STUDY DEEPWATER HORIZON

Authoritative in-depth description of the Deepwater Horizon oil spill can be found in the Deepwater Horizon Study Group Report (DHSG, 2011), the BP Commission Report (2011) and the USDOI Report (2010).

While it can be argued that this section—which provides a summarised yet extensive description of the accident and the background to it—could have been made much shorter by referring to the abundant information in this literature, it is suggested that a primary data collection would be of lower quality because with the passage of time, memories would have faded and key personnel dispersed. Therefore a secondary data analysis (a proven and widely-used research method) has been used for structuring the problem. This also gives the possibility of triangulating sources—and the analysis can be easily checked by other researchers.

Students were briefed regarding the background to the disaster (Section 1.1 below). The technical cause of the failure (Section 1.2) and the consequences and their severity (Section 1.3). They were then divided into three groups, each of which was required to use reliability engineering techniques to analyse the failure and make recommendations based on the analytic tools that were used.

1.1 *Background to the disaster*

On 20 April 2010 a massive explosion destroyed the Deepwater Horizon drilling rig in the northern Gulf of Mexico, followed by the leakage of millions of barrels of oil. The drilling rig (see Fig. 1), which was owned and operated by Transocean, had resumed the drilling of the Macondo well in the sea floor in the Gulf of Mexico, which at this point was at a depth of 8,000 ft.

The drilling operation, which had been resumed on 6th February 2010, incorporated a Blowout Preventer (BOP) that consisted of hydraulic valves designed to regulate the pressure of the oil and gases released from the well simultaneously with the drilling mud and sea water that is introduced into the well. The function of the BOP is to seal off a well that is being worked upon or drilled over, and this can happen during well interventions or drilling if there is an over pressure that threaten the proper functioning of the rig. During the drilling



Figure 1. The Deepwater Horizon drilling rig in operation (Source: Rigzone, How do Semisubmersibles Work?, Accessed November 23, 2010). (http://www.rigzone.com/training/insight.asp?insight_id=338&c_id=24).

stage the pressure increased, due to two factors: the mud and sea water that were introduced into the well and the pressure that was produced by oil and gas coming from the well bottom. Figure 2 shows the components of the blowout preventer.

Sea water and drilling mud were injected into the well to control the pressure. However, when the well pressure overcame the pressure of the mud and the sea water, the mud, accompanied by hydrocarbon gas, started to overflow on to the rig surface. Although it was controlled and diverted to the mud and gas separator, the gas source was unknown. Investigations revealed that hydrocarbon was being released through the poorly designed cement barrier, which was cast in order to isolate the well. The released gas mixed with mud, and at this stage the hydrocarbon, produced high pressure and damaged the gasket inside the blowout preventer. As a consequence, a larger quantity of gas, oil and mud flowed up to the rig surface. Minutes later, the first explosion occurred and damaged the cables that connect the control room and the blowout preventer. As a result, the blowout was completely isolated and uncontrollable. Over time, the huge amount of hydrocarbon entered the still functioning engine room which provided the ignition source of a second, massive explosion.

1.2 *Technical cause of the failure*

Investigations indicated that there were many reasons for the disaster. However, whatever these were, the consequences were disastrous. The causes can be classified into several categories as outlined below (DHSG, 2011).

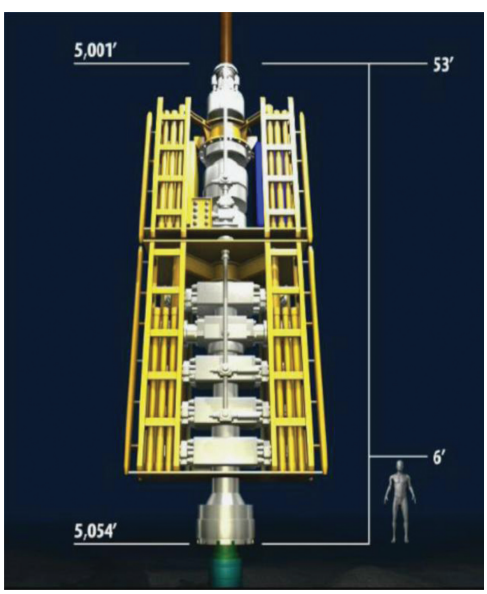


Figure 2. Blowout preventer (DHSG, 2011).

1.2.1 *Poor design of cement barrier*

It was believed that the main cause of the explosion was the leakage of hydrocarbon from the bottom of the well to the drilling tower, which resulted in the leakage of gas into the engine room. Investigators succeeded in analysing the scenario. From the beginning, the cement barrier that was used to prevent the gases from getting into the well was not successfully designed. In addition, it was not tested in order to see whether it could sustain the pressure. As a consequence, hydrocarbon was released through the cement barrier into the well.

1.2.2 *Mechanical failure of the blowout preventer*

The Blowout Preventer (BOP) is a mechanical arrangement that consists of different parts which work as valves to regulate the well pressure and prevent oil and gas from reaching the rig surface. In this case, this equipment seriously failed. The high pressure hydrocarbon that was released through the cement layer damaged the gasket inside the BOP. As a result, the well pressure became uncontrollable. This resulted in the release of large amounts of oil and gas up to the rig surface. Mud and gas separators ventilate the hydrocarbon on to the rig surface. However, the ventilated hydrocarbon gas entered the power generator room, which provided the ignition source. Furthermore, the fire safety and gas system, which is designed to prevent fire and gas mixing, was not working or was incapable of overcoming the problem. Therefore, the explosion occurred.

1.2.3 *Damage of control cables*

There were two explosions ten seconds apart. The first damaged the control cables which connected the BOP with the control room, causing the BOP to become out of control. Consequently there were no signals between the control room and the blowout preventer.

1.2.4 *Fire and gas system*

There was a safety system, to prevent fire. In oil exploration operations, frequent fire accidents are expected. However, in the Deepwater Horizon case, the system was not working, which reflected the poor maintenance of the safety systems.

1.3 *Consequences and severity*

1.3.1 *Fatalities and injuries*

At the time of the accident there were 126 personnel on the Deepwater rig, and most of them did not realise that a serious problem had occurred because

the safety system alarms were not functioning. They were subsequently instructed to evacuate the rig as early as possible. During that time there was chaos on the bridge because the shift crew members were still trying to understand what was happening. In addition, emergency plan procedures were not clear to the shift crew. However, many of them were preparing to jump into the sea and others were waiting for the lifeboats to be launched. But only two lifeboats were ready and they were partially full. Unfortunately, evacuation routes were blocked because of the explosion and the atmosphere was saturated with large amounts of carbon dioxide as the ventilation systems failed. Near the rig, there was a supply ship, the Damon Bankston. It was called for help and, due to its fast response, the people who jumped into the sea were rescued first and the injured were airlifted to the nearest hospital. The consequences were 11 fatalities and 15 injuries (DHSG, 2011).

1.3.2 *Environmental impact*

It is undeniable that the environmental impact of the disaster was catastrophic. The oil spill lasted for about 87 days before it was stopped. An independent analysis indicated that the total spilled oil was around 185 million gallons plus another 33.8 million gallons that were captured by BP. As a result, hundreds of miles of shoreline were oiled and large areas of the sea were closed to fishermen. Moreover, wildlife was affected by the oil spill; thousands of birds, fish, turtles and marine mammals were killed.

2 ANALYSIS OF 1ST GROUP OF STUDENTS

The disaster happened for various reasons, some of them technical, some organisational, some financial and yet there were problems of safety-related design.

2.1 *The technical reasons*

1. The cement barrier was incapable of preventing hydrocarbon gas from entering the well. Thus, the gas mixed with the drilling mud and was released under high pressure on to the rig surface.
2. The blowout preventer failed to isolate the well which in turn allowed hydrocarbon and oil to seep on to the rig surface.
3. The first explosion severed the control cables between the blowout preventer and control room. Consequently, the blowout preventer was out of control.
4. The fire and gas system broke down, so it could not prevent the hydrocarbon ignition.

2.2 *The design and safety reasons*

1. The well was cemented before the laboratory test results were provided to BP. Halliburton (the contractor who was responsible for testing the cement layer design) reported to BP that the well cement barrier was not effectively designed and that it was probable that a serious gas flow could occur.
2. The design of the gas and mud separator was poor. That is to say, when hydrocarbon was separated from the mud, it had not been burned or safely disposed of. It was released into the engine room where its ignition led to the massive explosion.
3. The blowout preventer was critical equipment which was used to isolate the well and regulate the oil and gas pressure. As such it should have been redundantly designed. To be more precise, there should have been a redundant blowout preventer connected in series. This would have reduced the probability of oil and gas leakage to the rig surface.
4. The design of the control room was poor. That is to say, influx of the hydrocarbon was not recognised until it reached the riser. The control room systems were either outdated or failed.
5. Safety system alarms were suspended (for some unknown reason), so most personnel did not realise what was happening and that the situation required evacuation.
6. The safety system had suffered various failures in the past. However, no actions had been taken to correct them.
7. There were only two evacuation boats. In the absence of evacuation procedures most of the workers jumped into the sea.

2.3 *Financial and organisational factors*

1. In an attempt to cut costs and increase profits BP had been cutting maintenance budgets during the previous few years. This led to inefficient maintenance programmes and a backlog of deferred corrective work, especially on critical safety items.
2. Within the BP group excessive changing of leadership positions was widespread, generating problems with work control and long term planning.
3. Financial and time pressure was one of the main reasons for the disaster. The changing of the drilling rig took a long time and thus put workers under pressure. In addition, managers were under financial pressure as the drilling process could have taken longer than planned and the company would have been forced to pay a penalty for any overrun.

2.4 *Fault Tree Analysis (FTA)*

FTA is a reliability analysis technique. Through FTA, basic events that led to the disaster can be explored. Figure 3 illustrates all the probable causes of the disaster.

From the diagram it can be concluded that the basic causes are as follows:

1. The fire and gas system failed to detect the gas leakage, either because it failed or was overloaded.
2. The blowout preventer failed to isolate the well for various possible reasons:
   - It was uncontrollable because the control cables were severed.
   - The operator was incompetent.
   - The design of the control panel was poor.
   - The pressure regulation valve failed to close.
3. The shoe track failed to isolate the well because it was badly designed or damaged.
4. The cement barrier was incapable of isolating the well for various possible reasons:
   - The design was not accurately tested in the laboratory.
   - The cementing process was inefficient.

The barrier itself was damaged by the high pressure of hydrocarbon.

Having analysed the likely disaster causes, the next step is to evaluate the reliability of the whole system by applying the Reliability Block Diagram technique to an investigation of the possible design modifications that could enhance reliability.

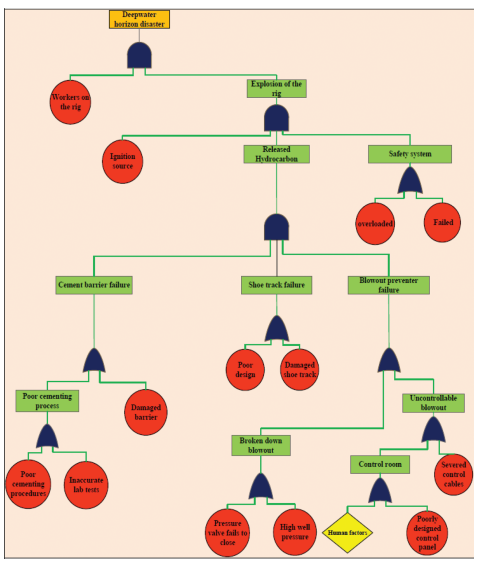


Figure 3. The Deepwater Horizon disaster fault tree analysis.

2.5 *Reliability Block Diagram (RBD)*

RBD is the next reliability assessment step following the FTA. It assesses the reliability of a system. Furthermore, designers can learn from the mistakes that might be the reasons for the disaster. Figure 4 shows, for the Deepwater Horizon case, the basic causes and their interdependencies.

2.6 *Recommendations and reliability improvement*

Technical recommendations:

2.6.1 *Blowout preventer*

- Cover the control cables so that they can be protected against damage.
- Install a redundant blowout preventer, which will increase the system reliability.
- Ensure that the BOP operator is competent.

2.6.2 *Cement barrier*

- Cementing procedures need to be revised and assessed.
- Carry out accurate experimental work to ensure the reliability of the cement barrier.
- Study the possibility of a cement barrier replacement e.g. using a metallic barrier.

2.6.3 *Shoe track*

- Needs to be redesigned and assessed.

2.6.4 *Fire and gas system*

- Replace the old system with a high capability one.
- Install a safety system that can give an indication of a high concentration of gas.

Management and financial recommendations

- Improve skills of personnel, especially for critical tasks.
- Focus on work planning and allocate enough time for work achievement.

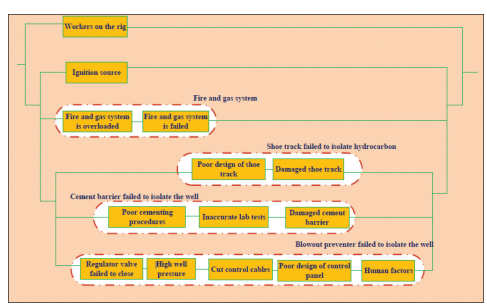


Figure 4. Reliability block diagram of Deepwater Horizon disaster.

– Allocate maintenance budget sufficient for reliability enhancement.
– Focus on safety procedures.
– Review emergency evacuation arrangements.

3 ANALYSIS OF 2ND GROUP OF STUDENTS

3.1 *Summary of the technical cause of the disaster*

– Cement-casing barrier failed to isolate.
– Incorrect interpretation of negative-pressure test.
– Fire and gas system did not prevent release of gas and its ignition.
– BOP emergency response mode failed to seal.

These technical causes are outlined in Figure 5. The resulting Fault Tree, Reliability Block Diagram and Failure Mode and Effect Analyses are illustrated in Figures 6, 7 and 8.

3.2 *Lessons learned*

– Human: Best practice and heightened vigilance in all steps from design to any variations during drilling are essential.
– Use better technology: Independent BOP activation control (e,g, audio-transmission), either from onshore or from standby vessels, is desirable.
– Installation: Ensure equipment and materials (e.g. cement) are used correctly.
– Re-design: Improve BOP so that it can show its real-time conditions.
– Data transmission: Transmission of data onshore so that situation can be further monitored.
– Contingency: Back-up Blind Shear Ram (BSR), i.e. introduce redundancy.

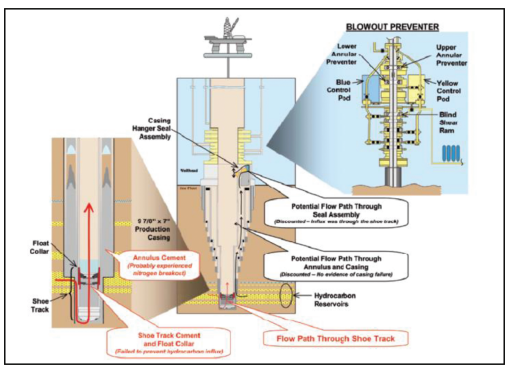


Figure 5. Technical causes of the failure (adapted from DHSG, 2011).

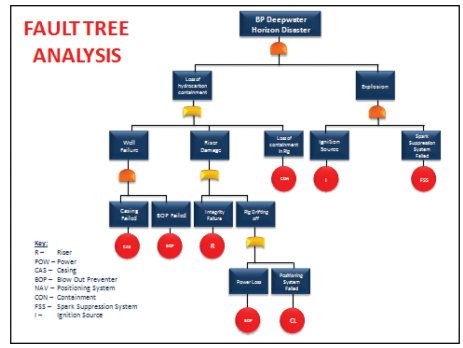


Figure 6. Fault tree analysis.

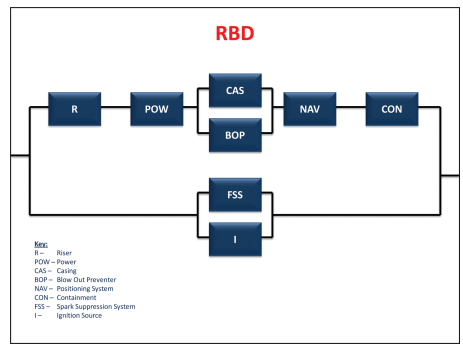


Figure 7. The reliability block diagram of Deepwater Horizon.

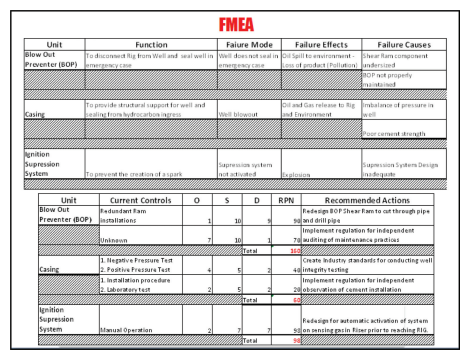


Figure 8. FMEA model of Deepwater Horizon.

4 ANALYSIS OF 3RD GROUP OF STUDENTS

4.1 *Technical cause of the disaster*

– Design and engineering flaws
  – BOP poor design had been indicated previously: (failed in 2006, 50% of usage).

  - Incorrect cement composition: use of nitrite and other additives reduces the strength of the required composition.
- Poor communication
  - Lack of effective communication Between Parties (BP, Halliburton and Transocean).
- Poor management decisions
  - Deviation from design specification (only 6 centralizers used rather than the recommended 21).
  - No dedicated BP representative.
- Mechanical failure
  - BOP failure (of battery, blind shear ram and emergency disconnect system).
- Operational implementation
  - Poor judgment of pressure reading (drill line reads 1400psi and kill line reads 0 psi) (BP and Transocean personnel could not have analyzed and interpreted pressure reading, thinking it false).
  - No action was taken due to lack of investigation of pressure reading.
  - Well integrity not established.

Figure 9 shows the barriers that were breached and subsequently led to the disaster. Figure 10 show the equivalent FTA. Figure 11 shows the related RBD with its estimated probabilities.

Not that estimated probabilities in Figure 11 are guesses based on the author's judgment. Based on Figure 11, one can then estimate overall (un)reliability, viz:

Reliability calculation:

$$\text{Line 1: } 0.5 \times 1 - (1 - 0.4925)^2 = 0.2442$$
$$\text{Line 2: } 0.2425 = 0.2425$$
$$\text{Line 3: } 0.985 \times 0.2925 = 0.288$$
$$\text{Line 4: } 1 - (1 - 0.5)^3 = 0.8768$$
$$\text{Line 5: } 1 - (1 - 0.4851)^2 = 0.7348$$
$$R = 1 - (1 - 0.2442)(1 - 0.2425)(1 - 0.288)(1 - 0.8768)(1 - 0.7348)$$
$$R = 0.986$$

Therefore: Unreliability

$$U = 1 - 0.986$$
$$U = 0.0133.$$

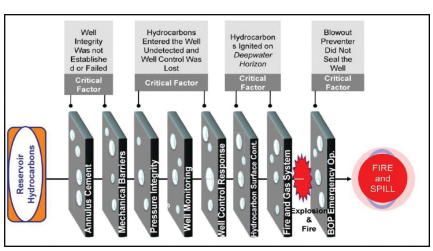


Figure 9. Barriers for Deepwater Horizon (adapted from DHSG, 2011).

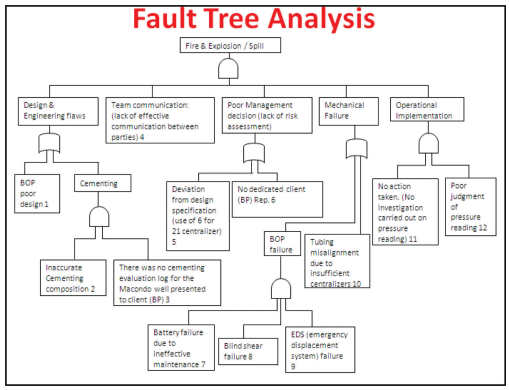


Figure 10. FTA for Deepwater Horizon.

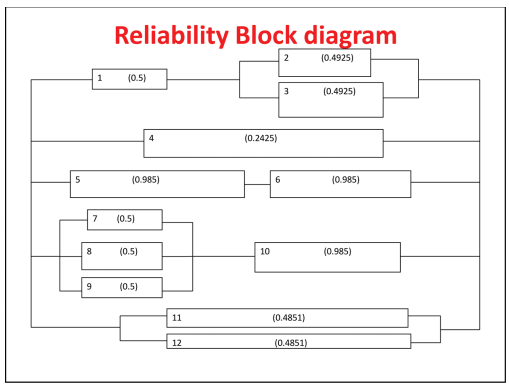


Figure 11. RBD for Deepwater Horizon.

4.2 *Lessons learned*

There was evidence of the following deficiencies in the management of the operation:

- Communication gap between parties.
- Non-compliance with design specification and procedures.
- Lack of peer review.
- Ineffective process safety management.
- Lack of monitoring and supervising operational team, from client to contractors.
- Disregard for team members' judgment.
- Insufficient organizational cultural change (from focus on cost saving to focus on ensuring safety).

Improvements needed:

- Full compliance to design specification and requirements (adequately centralized).
- More advanced BOP design.
- More effective communication.

– Establishment of on-going risk assessment procedures.
– Appointment of dedicated client representative.

5 FEEDBACK AND GENERIC LESSONS

Here the tutor (the author of the current work) offered feedback to the three student groups. This was intended to provide more insight into the accident—as an incident, as a company and as a culture—hence addressing both specific and wider generic lessons.

Each group produced a slightly different mental model, although each was exposed to the same narrative. The main differences were in the level of detail each group went into with respect to the FTA, and its use of qualitative analysis (the strength of Group 1) as opposed to its emphasis on quantitative modelling using FMEA (the strength of Group 2) and use of reliability calculations (the strength of Group 3). Nevertheless, on the whole, there were more agreements than otherwise between the findings of the groups.

The students were then directed to read a well balanced review of quantitative versus qualitative analysis of risk (Apostolakis 2004), and a good account of possible approaches for assessing and managing risks from extreme events (Bier et al. 1999).

It was also noticed that the RBDs of all three groups had an AND-gate at the top which signifying a parallel structure. As mentioned earlier, this implies the existence of a set of barriers that were all insufficient to prevent the disaster (as illustrated in the Swiss cheese model proposed by Reason (1997)).

As regards to specific regulatory lessons, the American regulatory agency of the industry—Minerals Management Service (MMS) had dual roles which can be seen as conflicting. On the one hand it had a role in promoting oil and gas leasing and collecting revenues, while on the other hand it acted as regulator and enforcer on the other (Flouron 2011). Since the accident the MMS dual functions have been separated.

In terms of BP as a company and culture the report by the Deepwater Horizon Study Group (DHSG 2011) conclude that this disaster also has eerie similarities to the BP Texas City refinery disaster as outlined in the BP Texas City report (2007). These similarities include:

a. multiple system operator malfunctions during a critical period in operations;
b. not following required or accepted operations guidelines (so-called "casual compliance");
c. neglected maintenance;
d. instrumentation that either did not work properly or whose data interpretation gave *false positives*;
e. inappropriate assessment and management of operations risks;
f. multiple operations conducted at critical times with unanticipated interactions;
g. inadequate communication between members of the operations groups;
h. unawareness of risks;
i. diversion of attention at critical times;
j. a culture with incentives that provided increases in productivity without commensurate increases in protection;
k. inappropriate cost and corner cutting;
l. lack of appropriate selection and training of personnel;
m. improper management of change (as outlined by the Baker Panel 2007 and Hopkins 2009).

The DHSG (2011) report also suggested that in both cases—Texas City and the Deepwater—meetings were held with operations personnel at the same time and place as the initial failures were developing. These meetings were intended to congratulate the operating crews and organizations for their excellent records for *worker safety*. Both of these disasters have served—as many others have served—to clearly show there are important differences between *worker safety* and *system safety*. One does not assure the other.

The DHSG (2011) report contains four strategic findings. Firstly, it warns about the apparent under-estimation of the hazard caused by the 'next generation' series of oil and gas exploration in the ultra-deep waters of the northern Gulf of Mexico. Secondly, it warns that the consequences of major offshore oil and gas system failures can be several orders of magnitude greater than those of previous generations of these activities, and that major developments are needed to address the consequences of major failures. Reliable systems are needed to enable effective and reliable containment and recovery of large releases of hydrocarbons in the marine environment. Thirdly, it suggests that strategies related to non-renewables as an energy source need to be re-examined. Fourthly, it encourages collaborative efforts in benchmarking best practice in safety.

It is clear from the analysis that the Deepwater Horizon operation had many lines of defence (safety barriers) that were breached. This view is supported by research on the Texas City refinery disaster report (Holmstrom et al. 2005) which identified several deficiencies in observability and diagnosability of the condition of safety barriers in the refinery's isomerisation unit.

Since safety barrier problems were common to both accidents, and both accidents are attributed to BP, students were then provided with some theory on safety barriers as regards their definition,

classification and performance (Sklet 2006 and Svenson 1991). For example, according to Svenson a safety barrier represents a function (and not for example an object) which can arrest the execution of the accident so that the next event in the accident chain is never realized, while a barrier system is maintains the barrier function.

Also as feedback, the students were exposed to some related industrial standards that address reduction of risk through safety barriers. For example, with respect to the concepts of risk prevention, control and mitigation, ISO:13702 (1991), a standard for the oil & gas industry) states that *prevention* means reduction of the likelihood of a hazardous event, *control* means limiting the extent and/or duration of a hazardous event to prevent escalation, while *mitigation* means reduction of the effects of a hazardous event. Hence, a barrier function is a one planned to prevent, control, or mitigate undesired events or accidents (Sklet 2006).

In another development regarding barriers related to software systems, Leveson (1995) distinguished between three types of barrier function: lockout, lockin and interlock. A lockout "prevents a dangerous event from occurring or prevents someone or something from entering a dangerous area or state", a lockin is "something that maintains a condition or preserves a system state", while an interlock serves "to enforce correct sequencing or to isolate two events in time".

As outlined by the Department of Environment (DOE, 1999), when analysing barriers in an accident investigation, the following topics need to be addressed:

1. barriers that were in place, and how they performed,
2. barriers that were in place but not used, and
3. barriers that were not in place but were required.

It is important that after their analysis of the deepwater event, students be made aware of the above theories regarding safety barriers. In this way they can better appreciate the relevance of these concepts.

REFERENCES

BP Commission Report. National Commission on the BP Deepwater Horizon Oil Spill & Offshore Drilling, Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling 1. 2011.

BP Texas City Report. Investigation Report, Refinery Explosion and Fire, BP Texas City, Texas, U.S. Chemical Safety and Hazard Investigation Board. March 2007; Washington DC.

DHSG, 2011. Final report on the investigation of the Macondo well blowout. Deepwater Horizon study group.

DoE. Conducting accident investigations DOE workbook, revision 2. Washington, DC: US Department of Energy, 1999.

Flouron, A.C., Three Meta-Lessons Government and Industry Should Learn from the BP Deepwater Horizon Disaster and Why They Will Not, 2011; 38 (2), Boston College Environmental. Affairs Law Review.

Holmstrom, D., Altamirano, F., Banks, J., Joseph, G., Kaszniak, M., Mackenzie, C., Shroff, R., Cohen, H. & Wallace, P.E.S., 2006, CSB Investigation of the Explosions and Fire at the BP Texas City Refinery on March 23, 2005, Process Safety Progress, 25 (4), 345–349.

ISO:13702. Petroleum and natural gas industries—Control and mitigation of fires and explosions on offshore production installations—Requirements and guidelines. Geneva: International Organization for Standardization. 1999.

Leveson, N., Safeware: System Safety and Computers, Addison-Wesley Publishers, 1995.

Sklet, S., Safety barriers: definition, classification, and performance, Journal of Loss Prevention in the Process Industries, 19 (2006), 494–506.

Svenson, O. (1991). The Accident Evolution and Barrier function (AEB) model applied to incident analysis in the processing industries. Risk Analysis, 11(3), 499–507.

USDOI. Report regarding the causes of the April 20, 2010 Macondo well blowout. The Bureau of Ocean Energy Management, Regulation and Enforcement. United States Department of the Interior. USA, 2011.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The representation of nuclear power in cinema: The contribution of a filmic analysis to understanding the public debate

A. Portelli & C. Martin
CRC—MINES-ParisTech, Sophia Antipolis, France
ESAIP, Grasse, France

F. Guarnieri
CRC—MINES-ParisTech, Sophia Antipolis, France

ABSTRACT: Representations of the nuclear industry in European countries play a determining role in the public debate and the development of energy policies. Cinematic fiction as a media object contributes to our understanding of social reality and also exercises a major influence on public opinion, because of its ability to "colonize" awareness. The risk of nuclear conflict and the effects of radiation have inspired many filmmakers. However, there are far fewer films dedicated to the civilian use of nuclear power. Nevertheless, some notable works make it possible to investigate the topic through a focus on the relationship of man to their work in the sector, in particular the challenges of subcontracting maintenance activities, which is represented in terms of modern slavery.

The first part of this article outlines the methodology used to analyse how civilian nuclear power is represented in film. The second part puts the methodology into perspective and shows how workers in the sector are represented in a French film. Finally, the third part shows how this representation fits into the nuclear debate in France.

1 INTRODUCTION

Social representations encompasses concepts, beliefs, myths, objects or classes of individuals that appear as "shared cognitive schema that are developed by a group that allow its members to think, to represent the surrounding world and to orient and organise behaviour, often by prescribing or forbidding certain objects or practices" (Mannoni, 1998: 4). Not only can they represent a serious challenge, they can also be at the centre of controversy, such as that concerning nuclear technology (Martin *et al*., 2013). The representations that feed the public debate on nuclear power can thus have a significant impact on the development of energy policy. They can be examined through a wide variety of sources, such as photography, novels, newspaper articles and cartoons, advertising, televised debates, documentaries or cinematic fiction.

The theme of the radioactivity was initially addressed by filmmakers a few years before the Second World War. Many films were made, inspired by the destruction of Hiroshima and Nagasaki, and the subsequent tensions between the two superpowers during the Cold War. These films reflected the anxieties of the population, such as the risk of nuclear war, the destruction of humanity or mutations due to radiation. Representations of the nuclear apocalypse, which have been studied by researchers for many years (Puiseux, 1987) have fuelled the imagination of audiences and influenced their perception of nuclear technology.

However, there are far fewer films dedicated to civilian use of nuclear power. Nevertheless, a few works stand out, such as *The China Syndrome* (Bridges, 1979), the short film *Mont Fuji in Red* taken from *Dreams* (Kurosawa, 1990), *Land of Oblivion* (Boganim, 2012), *The Land of Hope* (Zion, 2012) and *Grand Central* (Zlotowski, 2013); the latter was shown at the Cannes Film Festival in 2013 in the *Un Certain Regard* category. This French film evokes, in the context of a romance, the relationship between a man and his work in the nuclear power industry; it specifically addresses the challenges of subcontracting, which is represented in terms of modern-day slavery (Fig. 1). Subcontractors intervene during scheduled power outages in order to undertake maintenance operations that are not carried out by the operator's employees.

The aim of our research is therefore to show how the film illustrates the power relationships that feed the debate on the nuclear industry and its extremely widespread practice of subcontracting in the sector. The first part of the article presents the methodology used to analyse the representations of nuclear power in film. The second part puts

Gary, the main character in *Grand Central*, has not completed his training as a boilermaker and has held down a series of temporary jobs, before becoming a subcontractor in the nuclear sector. The work is demanding and dangerous. The protagonist is integrated into a team of workers and has a secret relationship with Karole, the partner of his colleague Toni. He is slowly contaminated, by both love and radiation.

Figure 1. Summary of Grand Central.

the methodology into perspective and shows how the sector is represented in the film *Grand Central*. Finally, the third part illustrates how this representation fits into the public debate on nuclear energy in France.

2 ANALYSIS OF CINEMATIC REPRESENTATIONS

The issue of cinematic representations lies at the crossroads of filmic analysis and the social sciences. Our methodology is therefore the result of a (delicate) compromise between two disciplines that do not share the same background. Consequently, we must define the status of the filmic object. In the next step we demonstrate the relevance of the monographic approach to the study of the representation of civilian nuclear power, and we present our methodological framework.

2.1 *The status of the filmic object*

The question we seek to answer implies that the film is seen as a vector of representations that reflect the social reality which it forms part of. The researcher must therefore examine how the film restructures society in the form of entertainment, where the symbolism refers to the time it was made (Vanoye *et al*., 2001). Fiction, depending on its viewpoint, aligns itself with certain articulated and unarticulated practices and values (Ferro, 1993), which reflect a reconstructed world view. It is this ability to reinvent reality (rather than simply duplicate it) that enables the filmic object to become part of the development of social processes and influence, to a greater or lesser extent, the opinions and behaviour of the general public (Delage *et al*., 2004).

This approach requires a comparison of what is learned from the filmic analysis with its external sources. The first focuses on the description and interpretation of the fictional narrative and its audio-visual dimension, in which the analyst must remember that cinema is a collective art. In this context, the question of exactly who is the author of a film has given rise to an abundant literature, which shows that it is not the director alone. On the contrary, the film's author is considered as a "virtual meeting room" a "speaker" or the "subject of the filmic narrative" (Aumont *et al*., 2002: 13–14).

The cinema is also an industry, subject to economic and cultural considerations that affect production. A filmic analysis alone is therefore insufficient and must be supplemented by an external analysis that integrates the work into its production context. It is only with this condition in mind that the researcher can succeed in identifying the anchor points that connect the work of fiction to its place in social space-time.

The film is therefore defined as an object that is inseparable from the society that produces and watches it. Researchers can approach their work by focusing on significant sequences, or establish sets of themes. This choice not only depends on the research question; it is also determined by how the film itself is composed.

2.2 *The monographic analysis*

The corpus of films concerning the nuclear industry corpus consists of two sets. The first includes works of fiction where the part of the action takes place in a power station (*The China Syndrome*, *Grand Central*). The installation forms part of the scenery; work situations are recreated and the balance of power between the operator and workers is explored. The second set includes films that address the issue of nuclear power but do not take place inside a plant, which may be confined to the background (*Mount Fuji in Red, Land of Oblivion*, *The Land of Hope*). The operational and organizational dimension is neglected in favour of a description of the consequences of a nuclear disaster on man and the environment.

A study of the themes that are explored in these two sets makes it possible to put into perspective the representations they convey—the interior of the installation, the operator, the nuclear risk, etc. However this poses a significant problem for researchers: the corpus, at a national level, is insufficient to carry out an analysis. Given this situation, a thematic study must compare films from different countries and different eras. For example, it would lead to a comparison of an American film from 1979 (*The China Syndrome*) and a French film from 2013 (*Grand Central*). Under these conditions, it becomes difficult to contextualize representations, as they refer to different cultural objects.

On the other hand, the monograph invites the researcher to focus their efforts on a single film, which resolves contextual problems. Specifically, we chose *Grand Central* for two main reasons. It is the first French film to focus so closely on workers

in the nuclear sector, and second, its narrative is clearly centred on the relationship between the operator and subcontractors, which feeds the public debate on the sector. This work of fiction occupies an important place in the history of representations of the nuclear industry and clearly merits further analysis.

2.3 *Internal and external analysis*

For the internal analysis, the film must be considered from various angles, which correspond to the decomposition of its content. An internal analysis "does not consider the object (the film) in its entirety, but seeks to identify the various constituent components in order to identify organizational systems" (Journot, 2002: 6). The analysis begins by identifying the central plot themes, before dividing the film into sequences and describing the imagery and the soundtrack. The film cannot be studied in the same way as a novel as there are technical considerations which the analyst must identify and interpret. The objective is to formulate an explanation of the film, in other words to arrive at "an understanding of some of its *raisons d'être*" (Aumont *et al*., 2002: 6).

A sequence is a "series of scenes (or single scenes) that make up an individual or distinct piece of dramatic action" (Pinel, 2005: 365). *Grand Central* can be divided into 131 sequences. Most of them are diurnal (89) and filmed indoors (78). Our analysis is focused on sequences that address the nuclear industry (69). They concern segments where the work is mentioned but the installation does not appear onscreen, segments where the exterior of the plant is shown, and those where the action takes place in the facility. This brief description immediately highlights the importance of the relationship between the worker and the physical space in the film's narrative.

The external analysis takes a different point of view and focuses on the inspiration for the film—in terms of writing and filming—as well as sources generated by the film. The press pack provides valuable information about the project's genealogy, the documentation used in writing the script, shooting locations, the role of technicians, etc. However, as this is a communication tool used to promote the work the information it contains must be used with caution.

An evaluation of the film's reviews indicates how well it was received on theatrical release. One critical review describes the work as not only meeting "certain aesthetic criteria" (Journot, 2002: 30), but also as a system of representations around which a social consensus is formed. Consequently, this critique reveals certain connections between the film and public opinion and the ideas conveyed on the topic.

These connections are fed by multiple types of media. With respect to *Grand Central*, the post-Fukushima environment increased television and radio reporting of subcontracting. Similarly, newspaper articles addressed the issue of workers in the nuclear sector. An examination of these sources therefore serves, on the one hand, to contextualise the film, and on the other to determine how it fits into public debate on the sector.

These methodological details highlight the difficulty of linking internal and external analyses. Academic research can quickly lead to an overly mechanical cultural interpretation. In order to avoid this pitfall, external influences at the time when the sequences were filmed must be taken into account. The contextual analysis should not be seen as an alternative to the filmic analysis, but rather its endpoint.

The approach rests on a delicate balance between the two forms of analysis, which mean that the film is sufficiently contextualized but the key elements that are essential in order to understand it are not lost (Marie, 1992). Researchers are therefore limited to a form of internal-external compromise, and must be careful to avoid overly rigid causal links as "any hypotheses that are derived from a text remain hypothetical" (Jullier, 2013: 160). This suggestion is particularly applicable to the study of *Grand Central*, due to the complex relationships that link it to the debate on nuclear power.

3 THE IMAGE OF NUCLEAR POWER IN *GRAND CENTRAL*

This second section uses the methodology described above to examine how nuclear power is represented in *Grand Central*. First, it outlines the inspiration for the film, before showing how the plant, the work and subcontractors are presented.

3.1 *The film's inspiration*

The film's director Rebecca Zlotowski said in an interview that the concept for the film came from her co-writer Gaëlle Macé, who had read *La Centrale* (Filhol, 2010), which is a novel about subcontractors in the nuclear industry. Zlotowski became interested in a story that she considered to have "significant documentary rigour" and that was about "a completely fictional community". A former subcontractor and author of an essay on decontamination work (Debout, 2010) was hired as an adviser and participated at all stages of the making of the film. These details, extracted from the press pack, lend credit to the film and had a certain influence on its critical reception.

The director states she did not conceive of Grand Central as either pro- or anti-nuclear, "My film is political, it is not militant. (...) The description that I present leads to an observation and this observation may lead to further thought. But in no case was this critical reflection the inspiration for the story. (...) To describe this world, this marginalised community of social outcasts, who can be sacrificed, is a political process" (Nouchi, 2013). Although the argument is legitimate, the distinction between "politics" and "militancy" remains unclear. Zlotowski's attempt to clarify the question only emphasizes the ambiguity. The Fukushima accident, which occurred during the writing of the screenplay, had a determinant impact on the authors, "Dozens of articles were published in the press documenting the daily lives of nuclear workers who were sacrificed there, as in France, and this tragic coincidence made us sure that there was a good reason to write the script" (Press pack, 2013). The director therefore creates a link between the working conditions of subcontractors and nuclear disaster. However, this link is often repeated in the public debate to question the safety of facilities, and can become an argument in favour of a potential withdrawal from nuclear power. If *Grand Central*'s narrative is seen in the same vein as antinuclear activism, the film becomes very much a "political" object, although not in the sense that the director intended. The film's purported neutrality in the debate does not seem to hold true. The sequence analysis, in turn, tends to confirm this premise.

3.2 *The nuclear sector in images*

The representation of workers situates them in an imaginary space where the facility resembles a sacred place. Its cooling towers add to the aesthetic qualities and make us think of the bell towers of a cathedral, containing a mysterious power. They appear repeatedly, either in the background as visual elements of the landscape or as inserts, where they dominate the scene. These images represent the "nuclear brand", as the narrator says in the novel (Filhol, 2010: 25). The sacredness of the plant is again suggested when the main character first discovers the Cruas facility. The scene is shot from inside the plant. The door opens and the team leader enters first. He is followed by the others, while the door rumbles closed, as if the characters were entering an inner sanctum. The locker room is like a sacristy, where subcontractors get changed before entering the reactor to commune with the atom. The blue light emanating from the reactor's "choir" clearly represents the symbolism of this space where the profane are not allowed to enter—only the most experienced subcontractor is allowed to approach it. The sacred note, which is reflected in both the architecture and work processes (Bergé, 2010), therefore finds its place in the collective imagination related to the history of nuclear energy, which emerged from the development of the first French nuclear power centres (Hecht, 2004).

Subcontractors are proud to work in the sector. They value their profession, which requires motivation, concentration and a high level of precision. The team leader explains that the work is demanding, "If you do it, you do it well. You must be good, you must be capable". The film therefore portrays the characters as unsung heroes who are working for the public good. One of them makes it clear, "We bring light to the people!"

The industry's profit imperatives severely test worker's motivation and tend to the dehumanization of the job. A rapid recruitment process, a few days of training in radioprotection and a routine medical visit are the main character's introduction to the world of subcontracting. These steps are treated as mere formalities, and hiring procedures are immediately discredited. This representation also features in the novel, which compares the training of subcontractors to the training of young recruits in the Great War, "I was the one that trained the back of the front, lectures on theory, then ten days practice in the school yard, ten days made eight at the height of the offensive when we accelerated the training of recruits so that they were available as quickly as possible—after all, what was the point of investing any more time and money in people we knew would have a short career?" (Filhol, 2010: 18).

The film therefore treats the work of subcontractors as a struggle against radiation exposure. Their interventions are compared to a battle with a "colourless, odourless, invisible" enemy. In one sequence, workers wait in silence for the moment when they can enter the red zone. The team leader gives the signal and puts on his mask, quickly followed by the others. Time is suspended and the subcontractors seem to be preparing to mount an assault, as if in a war film.

Animal metaphors express the real danger of this confrontation. The protagonist rides a mechanical bull; in the same way workers try to tame the atom. The crocodile, seen during a visit to the zoo is as devious as radiation. It can sit still for hours in order to improve its chances of surprising its prey.

The films imagery highlights the solidarity between men who must face the risk of contamination. The team leader encourages the social relationships based on the value of sharing. He severely chastises the main character when he drinks all the water in the communal bottle. The team leader takes collective and equal responsibility for any mistakes, "Here it is nobody's fault, it's everyone's fault!" Subcontractors feel that

they belong to the same world, which is characterized by working and living conditions that seem to come from a bygone era. This class consciousness was highlighted by *Grand Central*'s technical advisor, who thinks that subcontractors are part of a large family, "They find themselves living in the same places: camping sites, hostels. They share the same worries about lack of security, separation from their families, the same risks, the same doubts, which brings them even closer together" (Press pack, 2013). In effect, the characters live in their own world, on the outskirts of the plant in cramped and uncomfortable mobile homes. Promiscuity cannot be avoided and the community likes to gather in the evening or for picnics in the countryside.

These very tight social relationships help the nuclear sector lumpenproletariat to endure the operator's domination. The film represents the relationship between the workers and the organization in a particularly distinctive dialectic: one car park is reserved for the "aristocrats" (employees of the operator) and another is for the "galley slaves" (the subcontractors). The team leader stipulates the privileges granted to the most important workers: lower exposure to radiation, better wages, a coffee machine, free electricity. The camera follows the characters as they leave the plant and head to their cars. The car park for the operator's employees remains off-screen, as if it is a place that is off-limits to subcontractors.

Domination is also takes the form of a sequence about decontamination. A female subcontractor is shot from behind, standing naked. Her face is not shown, which emphasises the anonymous nature of the operation, and she is cleaned with a water jet, which immediately suggests a prison environment. Radiation detectors indicate that young woman's hair is contaminated. She turns her head twice towards the radiation protection officers that stand round her. They decide to shave her head. Handfuls of hair are shown falling onto her legs. A close-up then shows the character's face; she is crying. The officer, who is partially out of the shot, carelessly shaves the woman's head. The physical assault evokes the idea of the concentration camp and the depersonalisation of workers.

A reduction in long-term outages increases not only tensions between the subcontractors, but also the accident rate. An intervention goes wrong and the main character is contaminated. During the medical examination, the doctor tells him that he must now work in the green zone. If he receives further exposure to radiation he will either be made unemployed for technical reasons, or sent to another site. The subcontractor refuses to accept the second option. The sequence continues silently as follows: the protagonist goes to the green zone and puts on his helmet. He then appears in the locker room, checking his dosimeter. The doctor (off camera) announces that he is now "suspended". In the film the operator is shown to fail to take responsibility for the health risks that the worker is exposed to and gets rid of him as soon as he becomes useless. The following sequence alternates between the young man and his lover, each in their respective locker rooms. The subcontractor asks, "What if I want to stay?" He does not receive any response. This decision on the part of the director lends a particular meaning to the sequence. The character approaches a stack of cylinders and hides his dosimeter, before recovering it at the end of the day. Consequently, the doctor's failure to answer can be interpreted as an incentive to circumvent regulations and behave irresponsibly, in contravention of any professional ethics.

The film therefore emphasizes the precarious situation of the subcontractor and the master-servant relationship between him and the operator. The latter takes advantage of the worker's lack of qualifications, deliberately puts his health at risk and does not acknowledge his contribution in any way. The characters' working and living conditions lead to individual and collective dramas: one worker becomes sterile, the team leader separates from his wife and no longer sees his children, some are contaminated, while the group gradually disintegrates. This representation of workers demonstrates the challenges of the debate on subcontracting, which itself is a controversy that is intrinsically linked to the development of nuclear technology (Boudia, 2007).

4 THE ROLE OF CINEMA IN PUBLIC DEBATE ON NUCLEAR POWER

This final section discusses how the narrative of *Grand Central* fits into public debate on the sector. An analysis of its critical reviews makes it possible to determine, aside from its aesthetic value, how credible the representation of nuclear power is. The reaction of the press, as much as the film itself, forms part of a broader network of representations of civilian nuclear power. Consequently, it appears to be difficult to challenge the narrative of *Grand Central*, as it seems off-limits for sociological, scientific and moral reasons. Nevertheless, there are other ways to view subcontractors and their relationships with operators.

4.1 *The critical reception of Grand Central*

The film received many positive reviews, both in the press and in specialised journals. These highlighted its intelligence and realism (Mandelbaum, 2103), its coherent aesthetic choices (Narbonne, 2013), the script's rigor (Ferenczi, 2013) and the actors'

talent (Raspiengeas, 2013). There were only a few unfavourable reviews, which focussed on the schematic plot, and suggested that the film was a half-incarnated "world of ideas" (Ferenczi & Strauss, 2013; Gester, 2013). While the harshest critics judged the narrative to be unconvincing, none questioned the way the industry was represented.

The plant is associated with several levels of symbolism. It is compared with a "nuclear hell" (Sotinel, 2013; Narbonne, 2013), an "evil stomach" or a "toxic bath" (Kaganski, 2013) in which workers are immersed. The reactors are seen as "modern mines" (*Le Parisien*, 2013) and the atmosphere of the facility is described as "prisonlike" (Delcroix, 2013). Such terminology dramatizes the workspace, which becomes a place of suffering and alienation for workers who are "dogsbodies" (Ferenczi, 2013).

The precarious situation of the characters caught the critics attention, who used very strong language. Subcontractors were described as outcasts, the underclass, the walking dead. They are a shadow proletariat, a small tribe of untouchables who live in a world without hope. Workers are represented as convicts, "In their own way, they spend their time breaking stones waiting for their release from prison. They wear their dosimonitors like chains, to calculate their degree of irradiation" (Delcroix, 2013). The representation of nuclear sector workers is said to be all the more fascinating as it is far removed from "the neat official image of engineers and highly qualified technicians that is so often conveyed" (Lacomme, 2013).

As one, critics noted the documentary nature of the film. The scenes showing the apprenticeship seem "larger than life" (Ferenzi, 2103). The narrative "places each protagonist and situation in a specific professional context, indicative of current socio-economic reality" (De Bruyn, 2013). This almost documentary-like immersion demonstrates to the pubic "the reality" of workers in the nuclear sector (Bernheim, 2013).

These analyses are interesting for several reasons. First they make it possible to identify the points where the fictional story corresponds to other representations of nuclear power. Comments about the film find similarities with the pessimism of Emile Zola's novel Germinal, to describe a new form of servitude through work.

Moreover, by giving the film documentary value, critics crystallize representations on the precarious nature of subcontracting in the nuclear power sector.

4.2 *Contextualization of the film in the public debate*

The debate on nuclear energy concerns questions about its impact on public health and the environment, lack of transparency and democratic dialogue, the safety of installations, the risk of proliferation, waste management, profitability and the cost of dismantling (Barré *et al*., 2013). The Fukushima accident revived media interest in safety issues in France, which was closely linked to the debate on subcontracting. The real nature of the power relationships between operating companies and subcontractors are understood by researchers (Thébaud-Mony, 2000). Furthermore, the idea of the subordinate subcontractor is not specific to the nuclear sector, and authors have examined the risks of subcontracting in other sectors (Mayhew & Quinlan, 1997).

The reasons for the use of subcontractors are at the heart of the controversy and are frequently cited by the media. The most common argument is without doubt the profitability imperative, which forces the operator to limit the duration of power outages and to use a cascade of subcontractors (Fayner, 2012). The outsourcing of health risks is a secondary argument: the health of workers is not given much weight and they are not under medical supervision, while the nuclear lobby refuses to recognize occupational cancers linked to ionizing radiation (Nicolas, 2013).

Another problem is the transmission of knowledge. This knowledge is lost as workers retire and subcontractors must train themselves on the job. The loss of continuity increases the potential for an accident, as "nothing can replace the memory and experience of workers who knew the installation" (Thébaud-Mony in Pascariello, 2011).

Finally, the acceleration in the pace of work due to the optimization of long-term outages (Gérard, 2011), increased levels of stress, the arduous nature of the work (Weiler, 2010) and loss of skills (Auffray, 2011) are seen as factors that threaten the safety of the facility and personnel. The narrative of *Grand Central* is consistent with this system of representations. Consequently, the film reflects the popular image of the sector presented in the media, which leaves little room for an alternative narrative.

4.3 *Factors that discourage discussion*

The visible part of a society consists of both the images producers broadcast and what audiences expect to see (Sorlin, 1977). In the context of our analysis, the subcontractor is only observed (and observable) in terms of insecurity and danger. Why is it therefore so difficult to develop an alternative representation and to criticize the film's medium? First, we must reformulate how modern society thinks about subcontracting. The transition to modernity is defined by a loss of confidence in technology and expertise. This discredit leads the

population to feel vulnerable, a sentiment that is amplified by the globalization of risks and the hypermediatisation of technological accidents. Consequently, the idea that science enables social progress has been called into question since the mid-1960s. It was in this context that civilian nuclear power became uncoupled from the idea of progress (Topçu, 2006). Since then, its detractors have associated it with counter-productivity at all levels. The nuclear disasters at Three Mile Island, Chernobyl and Fukushima crystallized this representation in the media, which structures the dissemination of information and influences civil society. However, this is only possible so long as the media makes clear its independence from the official line. This configuration of the public space, where the idea of a "nucleocracy" (a term coined to describe a mode of techno-political governance that combines various actors and pressure groups) has naturally tended to discredit arguments about power. Therefore, the media is obliged to criticise the nuclear sector in order to demonstrate its independence and usefulness.

The issue of subcontracting also highlights a problem linked to the accessibility of sources. The subject has received little attention from academics because of security issues related to nuclear energy and a lack of interest from social scientists in blue-collar workers. "In these conditions where it is difficult to access the situation on the ground, it is not surprising that journalists' treatment of the nuclear industry is confined to current concerns in all forms of televised news" (Fournier, 2012). This situation clearly limits the diversity of viewpoints.

One last factor explains the difficulty of criticizing the image of the subcontractor presented in *Grand Central*. The link that is made between work and social distress is what could be termed an "untouchable" representation. Developed societies are uncomfortable when faced with poverty, which is approached with great caution by the media. Calling into question the film's narrative could therefore be seen as an unacceptable attempt to justify the exploitation of the weak by the strong.

However, there are other potential representations that do not diminish the dignity of workers in the nuclear sector. In fact, the subcontractors depicted in *Grand Central* do not seem to be representative of this type of worker. While the film's bias helps to nourish the image of nuclear power in the popular imagination, it does not acknowledge the professionalism of subcontractors. It is clear that there is a part of the labour force in the nuclear sector that leads a precarious existence, and questions can be asked about why operators find it necessary to subcontract 80% of maintenance activities. However, the debate cannot be simply reduced to calling 20,000 subcontractors nomadic workers who are overexposed to radiation for the sake of economic efficiency. Subcontracting activities are many and varied, and while the lives of some workers are made precarious due to the nature of the contracts between operators and subcontracting companies (the social conflicts experienced by plants are witness to this), a large majority of subcontractors are employed in stable, long-term contracts.

The film does not mention the role of trade unions in the organization of nuclear industry workers. On the one hand, many workers are confident of their abilities and their professional identity, while on the other hand the distinction between employees of the operator and subcontractors is not entirely clear. Proof of this fact is found in real life, in the joint unionisation of the employees of the operator and subcontractors at the Cruas plant—precisely where the film's action is supposed to have taken place. Teams work together and the operator's employees are highly dependent on the skills of subcontractors. For example during delicate and complex cleaning and dismantling operations, contractors are clearly the experts and owners of the know-how. Such situations provide a less schematic image of subcontracting and open up perspectives that are more in line with the reality on the ground.

5 CONCLUSION

The presentation of the nuclear sector in *Grand Central* has attracted the attention of social scientists. The views presented in the film are indicative of current challenges in the public debate. They translate, starting with the description of subcontractors, concerns about working conditions in the sector and the security of French nuclear power plants. It is clearly essential, in the context of the post-Fukushima public debate, to examine the daily lives of subcontractors and once again question the human cost of energy. In this respect, Zlotowski's film contributes to the debate and provides a skilful look at aspects of the sector that are unknown to the general public.

In contrast, the relations between subcontractors and operators must also be analysed (and consequently be represented) in terms of joint operations. Interactions between subcontractors and operators are not based on simple dependency relations, but on strategies that lead to alliances (Martin *et al.*, 2012). This shows that it is necessary to investigate, rethink and eventually make visible the entire set of power struggles and relationships.

REFERENCES

Auffray, E. 21 March 2011. Dans les centrales françaises, le malaise de la viande à radiations. In *Libération*.

Aumont, M. & Marie, M. Dictionnaire théorique et critique du cinéma. Paris: Nathan.

Barré, B. & Majnoni d'Intignano, S. 2013. *Faut-il renoncer au nucléaire ?* Paris: Le Muscadier.

Bergé, C. 2010. *Superphenix, déconstruction d'un mythe*. Paris: La Découverte.

Bernheim, C. 21 August 2013. Nos coups de coeur de la semaine: Grand Central et Magic Magic. In *Femme actuelle*.

Boudia, S. 2007. Naissance et rebonds d'une controverse scientifique: les dangers de la radioactivité pendant la guerre froide. In *Mil neuf cent*, 25: 157–170.

De Bruyn, O. 28 August 2013. Grand Central: Rebecca Zlotowski secoue nerveusement le ciné français. In *Le Nouvel Observateur*.

Debout, C. 2010. *Je suis décontamineur dans le nucléaire*, Editions Paul Ramand.

Delage, C. & Guigueno, V. 2004. *L'historien et le film*. Paris: Gallimard.

Delcroix, O. 28 August 2013. Grand Central. In *Le Figaro*.

Fayner, E. 9 May 2012. *Nucléaire: la bombe humaine*. France 5.

Ferenczi, A. 19 May 2013. Grand Central ou la fission dangereuse du sentiment. In *Télérama*.

Ferenczi, A. & Strauss, F. 28 August 2013. Grand Central. In *Télérama*.

Ferro, M. 1993. *Cinéma et Histoire*. Paris: Gallimard.

Filhol, E. 2010. *La Centrale*. Paris: POL Editeur.

Fournier, P. 2012. *Travailler dans le nucléaire*. Paris: A. Colin.

Gérard, M. 26 April 2011. A Dampierre, avec les nomades du nucléaire. In *Le Monde*.

Gester, J. 19 May 2013. Rebecca Zlotowski, centrale atomique. In *Libération*.

Grand Central. 28 August 2013. In *Le Parisien*.

Hecht, G. 2004. *Le rayonnement de la France*. Paris: Editions de La Découverte.

Incerti, M. 2013. Press pack. Ad Vitam.

Journot, M.-T. 2002. *Le vocabulaire du cinéma*. Paris: Nathan.

Jullier, L. 2013. *L'analyse de séquences*. Paris: A. Colin.

Kaganski, S. 27 August 2013. Très belle histoire de coeur et de réacteurs. In *Les Inrocks*.

Lacomme, J.-P. 24 August 2013. Sous hot tension. *Le Journal du Dimanche*.

Mannoni, P. 1998. *Les représentations sociales*. Paris: PUF.

Mandelbaum, J. 26 August 2013. Grand Central: une folle chamade sur fond de radioactivité. In *Le Monde*.

Marie, M. 1992. Texte et contexte historique en analyse de films. In *Cinémaction*, n°65: 22–28.

Martin, C. Portelli, A Guarnieri, F. 2013. Myths and Representations in French Nuclear History. *22nd ESREL Conference—Safety, Reliability and Risk Analysis*, Amsterdam.

Martin, C. & Guarnieri, F. 2012. Nuclear decommissioning and organizational reliability, involving subcontractors in collective action. In *SFEN*.

Mayhew, C. & Quinlan, M. 1997. The management of health and safety where sub-contractors are employed. *Journal of Occupational Health and Safety*, Australia.

Nicolas, B. 21 May 2013. *Centrales nucléaires: démantèlement impossible ?* Arte.

Narbonne, C. August 2013. Grand Central. In *Première*.

Nouchi, F. 26 August 2013. Rebecca Zlotowski: Mon film est politique, il n'est pas militant. In *Le Monde*.

Pascariello, P. 28 October 2011. *La sous-traitance dans le nucléaire*. France Inter.

Pinel, V. 2005. *Vocabulaire technique du cinéma*. Paris: A. Colin.

Puiseux, H. 1987. *L'apocalypse nucléaire et son cinéma*. Paris: Les Editions du Cerf.

Raspiengeas, J.-C. 19 May 2013. Le Démantèlement et Grand Central. In *La Croix*.

Sorlin, P. 1977. *Sociologie du cinéma.* Paris: A. Montaigne.

Sotinel, T. 20 May 2013. Grand Central: fission amoureuse à l'ombre de la centrale. In *Le Monde*.

Thébaud-Mony, A. 2000. *Sous-traitance et servitude*. Paris: Inserm.

Topçu, S. 2006. Nucléaire: de l'engagement savant aux contre-expertises associatives. In *Natures Science Sociétés*: 249–266.

Vanoye, F. et al. 2001. *Précis d'analyse filmique*. Paris: Nathan.

Weiler, N. 11 October 2010. Les droits bafoués des sous-traitants du nucléaire. In *Bastamag*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On designing educational aids for users' safety in road tunnels

K. Chatzoglou, E. Rokou & I.P. Tatsiopoulos
Sector of Industrial Management and Operations Research, School of Mechanical Engineering, National Technical University of Athens, Athens, Greece

K. Kirytopoulos
School of Natural and Built Environments, Barbara Hardy Institute, University of South Australia, Adelaide, Australia

ABSTRACT: This paper's goal is to assist in road tunnel safety, providing a set of educational scenarios that incorporate the best practices regarding the use of unidirectional road tunnels. The scenarios point out the basic guidelines of driving behaviour that a tunnel user should maintain and the proper responses of the user in case of an incident. Ten UML diagrams were constructed, in order to depict the basic interactions of the tunnel user within the environment of a road tunnel.

1 INTRODUCTION

Road tunnels are a critical part of the transportation infrastructure because their use is beneficial to almost every national and international highway. The fact that they facilitate highway communication and trade, combined with the decreasing construction cost, which is the outcome of the evolution of the construction technology, has led to the increased use of road tunnels in Europe in the last years.

However, increased use of road tunnels is raising safety concerns. Accidents in road tunnels may result in severe damages to the transportation network and in the loss of human lives. Taking into account the major road tunnel accidents that took place towards the end of the twentieth century there is an on-going effort to improve safety conditions (Kirytopoulos et al., 2010).

In most countries, there are increased safety measures regarding the construction and the operation of road tunnels. Establishing new technical standards that implement more advanced technology and improving the emergency facilities are the most common measures to ensure higher levels of safety in road tunnels.

Despite the efforts made, there still remains the issue of the drivers' behaviour when they have to use a road tunnel, especially when critical conditions exist. Recent studies have shown that there is lack of education among drivers when it comes to road tunnels (PIARC, 2011). The issue is mainly addressed to by professional organizations, while scientific literature is scarce.

Human factor being pivotal to the outcome of an emergency situation, the issue of tunnel users' education demands more attention (Tesson, 2009; PIARC, 2008). The better a tunnel user is informed, the more are the chances to reduce the possibility of an accident, as well as to mitigate the consequences, if the accident eventually occurs.

For the purpose of this study a total of ten educational scenarios were constructed and three of those are presented in this paper. The scenarios were modelled in order to facilitate the development of an educational software application, which is the long term goal of this research.

2 EDUCATING USERS IN ROAD TUNNEL SAFETY

2.1 *Tunnel users*

The need for increasing the effort on educating tunnel users became a central issue of tunnel safety, because a series of events revealed that their behaviour inside road tunnels did not match the expected, as determined by international organizations (Tesson et al., 2012).

Bringing tunnel users' education up to the desired standards is not an easy task. Several attempts have been made in order to study the behaviour of drivers when they are using a road tunnel, and the results show that drivers adopt a negative perception of tunnels. Drivers tend to feel anxious and uncomfortable, a fact that is mainly caused by the confined space but can also be attributed to the drivers being unfamiliar with the road tunnels' environment (Amundsen, 1994; Serrano & Blennemann, 1992; Arias et al., 2008).

The most important part of the education that tunnel users should receive is pointing out the main

differences between road tunnels and open highways and the expected behaviour on their part.

The role of the tunnel operator is a critical factor that many tunnel users do not take into account. The tunnel users should be informed that many of the tunnels' safety systems and signs are controlled by an operator, and they should at any time follow the operator's instructions. When information or instruction are being provided through the tunnel's radio frequency, the tunnel's loudspeakers or there is a change in traffic lights, variable speed limit signs or the tunnel's closure system, the tunnel users should respond without hesitation (Papaioannou & Georgiou, 2003).

Many tunnel users are not informed about the road tunnels infrastructure and equipment. One of the major issues of the tunnel users' education is to make it clear that when driving through a road tunnel the user should pay attention to the location of emergency equipment, emergency exits, emergency phones and emergency stop areas. This behaviour might become extremely important when a tunnel user is involved in a critical incident, because at that point there might not be enough time to locate the necessary equipment. It should be pointed out that all the safety equipment and infrastructure of a road tunnel is highlighted with the corresponding signs (PIARC, 2011; Tesson, 2009).

Furthermore, tunnel users often seem to be unfamiliar with basic traffic rules inside a tunnel. Avoiding U-turns and reverse movement, switching on the headlights and taking off their sunglasses, are some of the most important rules that drivers do not comply with.

The most important issue of tunnel safety is the development of fire inside a road tunnel. Unfortunately, this is one of the most difficult issues to educate tunnel users on. The series of actions when encountering fire in a road tunnel should consist to instructing tunnel users to guide themselves to safety as soon as possible using an emergency exit. There are also several useful actions that a tunnel user should perform in order to assist the operator in case of fire. It would be useful to report the fire to the tunnel operator and enable the tunnel's fire alarm as soon as possible. It would also be critical to try and extinguish the fire if it is possible. These actions should only be performed if the tunnel user is well prepared to manage the fire and only if the fire is at a starting stage (Carvel & Beard, 2005; Gandit et al., 2009; PIARC & ITA, 2004). It should be taken into account that the impact of the psychological factor on the reactions of the tunnel users is pivotal. Although human reaction in stressful situations is uncertain, it is considered that being educated on safety issues, tunnel users can improve their reactions when an unexpected incident occurs (Canter, 1980; Papaioannou & Georgiou, 2003; Reisser-Weston, 1996).

2.2 *Educational scenarios*

With the aim of achieving better results regarding the education of tunnel users, it is essential to provide a theoretical structure of the educational process. Creating an educational scenario requires the specification of the conditions and the activities that have to be performed to enable the learners to acquire the desired knowledge (Koper & Olivier, 2003; Lejeune & Pernin, 2004). The aim of this research is to produce an online educational tool for the education of the users of uni-directional tunnels. The structure of this tool will be based on educational scenarios that incorporate the basic guidelines for proper behaviour inside a road tunnel, as they derive by the existing literature and the existing researches of professional organizations.

In order to create a proper educational scenario, various aspects of the educational process should be taken into account. At first it is essential to determine the main aim of the educational process, along with the set of relevant information. An important part of the educational scenario is the assignment of roles. The role is characterised by the requirements that each participant has to comply with throughout the process, and the set of actions that should be performed. Two other factors that should be taken into account are the stages of the process and the environment in which it takes place. The distinction between the stages of the educational scenario is critical in the manner that as the process advances there are changes on the main scenario, and during the latter stages of the educational process more complicated issues have to be addressed. Describing the educational environment, means providing information on the conditions under which the educational process takes place, and determining the use of educational aids. In some cases, usually when the educational process is interactive, special guidelines are provided to the participants determining the way they should react on specific circumstances. These guidelines should also be part of the educational scenario (Koper, 2005).

Determining and designing the environment in which the educational activities take place is a complex task. In order to support this task the use of modelling languages is proposed. Modelling languages provide the notations that enable the designers to overcome the complexity of educational scenario design and create a visual model of the described process. The use of modelling languages for educational scenarios is gaining more attention in the last few years because of the increasing use

of e-learning and other forms of computer aided education (Derntl & Hummel, 2005).

3 RESEARCH METHOD

In order to create and model the educational scenarios and develop the corresponding diagrams, it was necessary conduct a scientific literature review, as well as explore professional organizations' relevant research. Doing this revealed the basic information about the good practices of unidirectional road tunnel users. This is how the basic aspects of the scenarios were determined.

Furthermore, there was the need to research the field of educational design, for the purpose of acquiring valid information about the structure and the components of an educational scenario. Based on the literature on educational design, it proved to be essential to model the educational scenarios using a standardised modelling language.

The language that was used is UML (Unified Modelling Language), a standardised general purpose, object oriented modelling language. Using UML provided the ability of reviewing the scenarios, to emphasizing on specific elements and components, and focusing on different aspects of the scenarios according to the needs. Taking into account that UML was primarily designed for use in the fields of software engineering, the research aim of creating the design of an educational software application is facilitated (Fowler, 2004; Rumbaugh et al., 1999).

4 EDUCATIONAL SCENARIOS FOR INCREASING SAFETY OF ROAD TUNNEL USERS

In order to describe the basic guidelines that a road tunnel user should follow, a series of scenarios were constructed and represented in the respective UML diagrams. The scenarios provide a description of the proposed course of action when the tunnel user is presented with specific events inside a road tunnel. The scenarios are summarized in ten use cases (Fig. 1):

- Approaching a road tunnel.
- Driving through a road tunnel.
- Immobilising the tunnel user's vehicle.
- Vehicle malfunction or collision.
- Communication with Tunnel Operator.
- Emergency exit.
- Managing fire in tunnel user's vehicle.
- Managing fire in another vehicle.

Due to space limitation, only the sequence diagrams of the "Driving through a road tunnel",

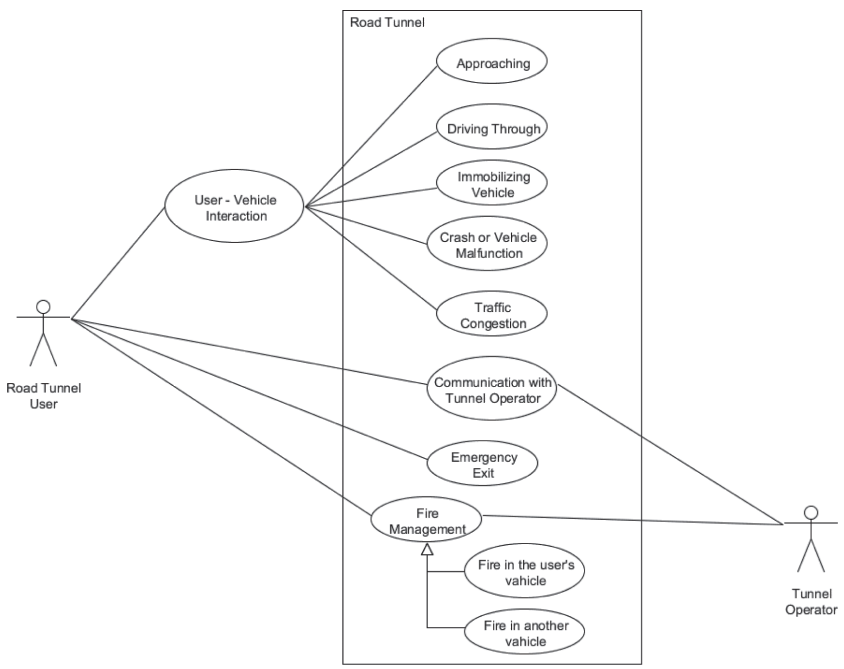


Figure 1. Use case diagram of the tunnel user's interactions.

"Emergency exit" and "Communication with Tunnel Operator" use cases are presented here.

In these use cases the actors are the tunnel user and the tunnel operator. Tunnel user interacts with the use cases either directly or through the interaction of the vehicle, while tunnel operator is in all cases directly interacting. The main focus of the study being the tunnel user, the role of the tunnel operator is secondary and only the interacions of the communication among the operator and the user are depicted.

4.1 *Driving through a road tunnel*

This use case depicts the series of actions that a tunnel user is expected to perform, after entering a road tunnel and until exiting. The sequence diagram developed (Fig. 2) describes

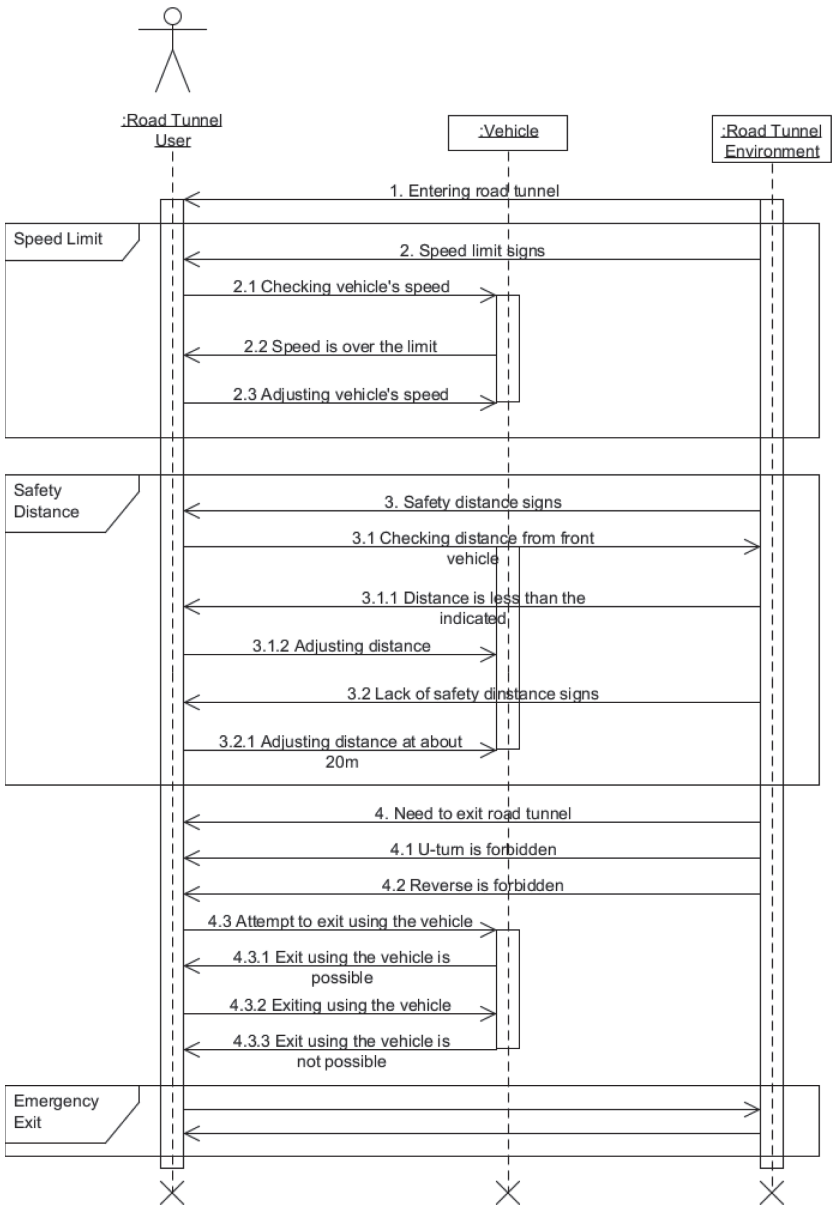


Figure 2. Sequence diagram of "Driving through" use case.

the expected actions, both in normal and critical conditions.

When a tunnel user enters the road tunnel, the priority is to maintain the vehicles speed, under the speed limit that is applied inside the road tunnel. The tunnel user should notice the speed limit signs and make sure that the vehicle's speed is not exceeding this limit. If the limit is indeed exceeded, then the vehicle should be slowed down to the desired speed, making sure that there will not be an abrupt change of the vehicle's speed that could endanger the tunnel users' safety.

The second point of interest is the maintained distance to the preceding vehicle. In road tunnels there might be limitations on the distance between moving vehicles, different than those on a freeway. Tunnel user should notice the corresponding traffic signs, and adjust the distance to at least match the indicated. Even if there are no signs concerning safety distance or the driver fails to locate them, the distance between two vehicles should not be less than twenty meters.

When the need to exit the road tunnel occurs, tunnel users should first attempt to exit using the vehicle. If this is not possible, the tunnel user should leave the vehicle and move to an emergency exit on foot. In all cases tunnel users should keep in mind that U-turns as well as moving in reverse should not be attempted inside a uni-direction road tunnel.

4.2 *Emergency exit*

In the case that the need to immediately exit the tunnel arises, the tunnel user and the tunnel operator are expected to act in a specific manner. The actions they should perform are described by the "Emergency exit" use case (Fig. 3).

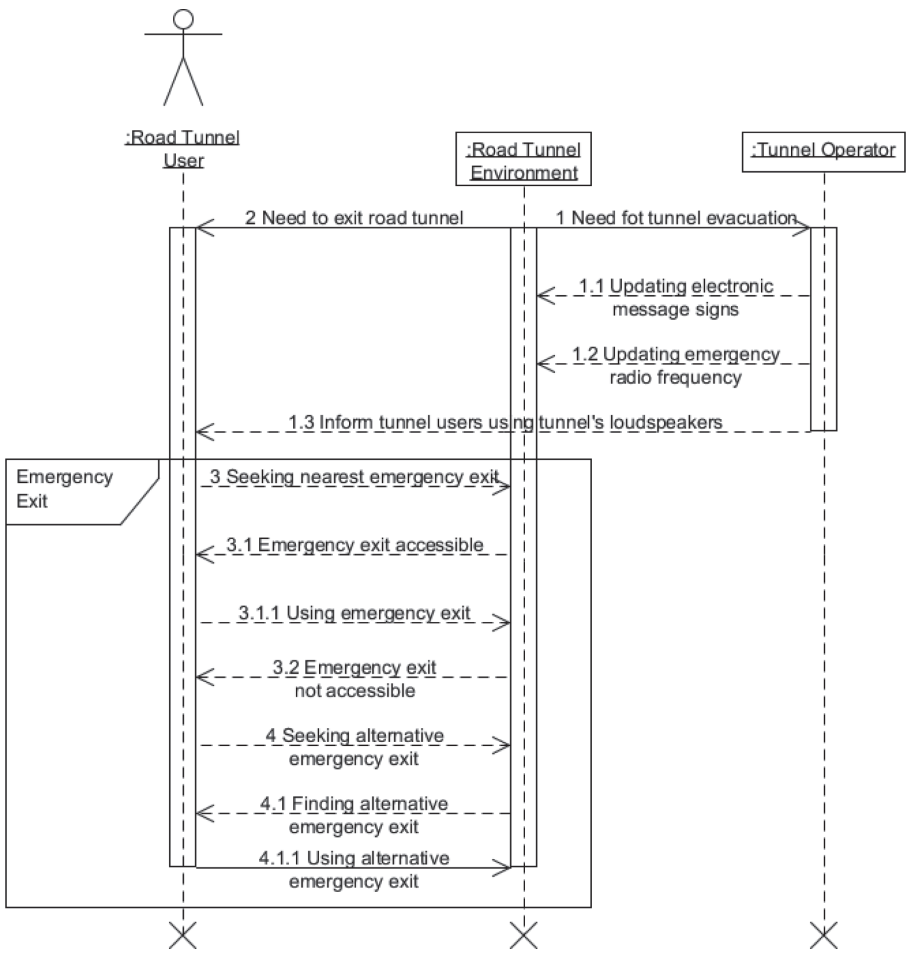


Figure 3. Sequence diagram of "Emergency exit" use case.

When the tunnel operator, based on the situation inside the tunnel, decides that there is the need to evacuate the tunnel, the primary priority is to notify the tunnel users. To achieve that, the tunnel's infrastructure should be used. The messages that are displayed on the electronic message sings and the emergency radio frequency should be updated in accordance to the situation and the tunnel's loudspeakers should provide information and directions to the tunnel users.

As soon as the tunnel user perceives the need to evacuate, the proper reaction is to seek for the nearest emergency exit and use it, if it is accessible. Otherwise, seeking for an accessible emergency

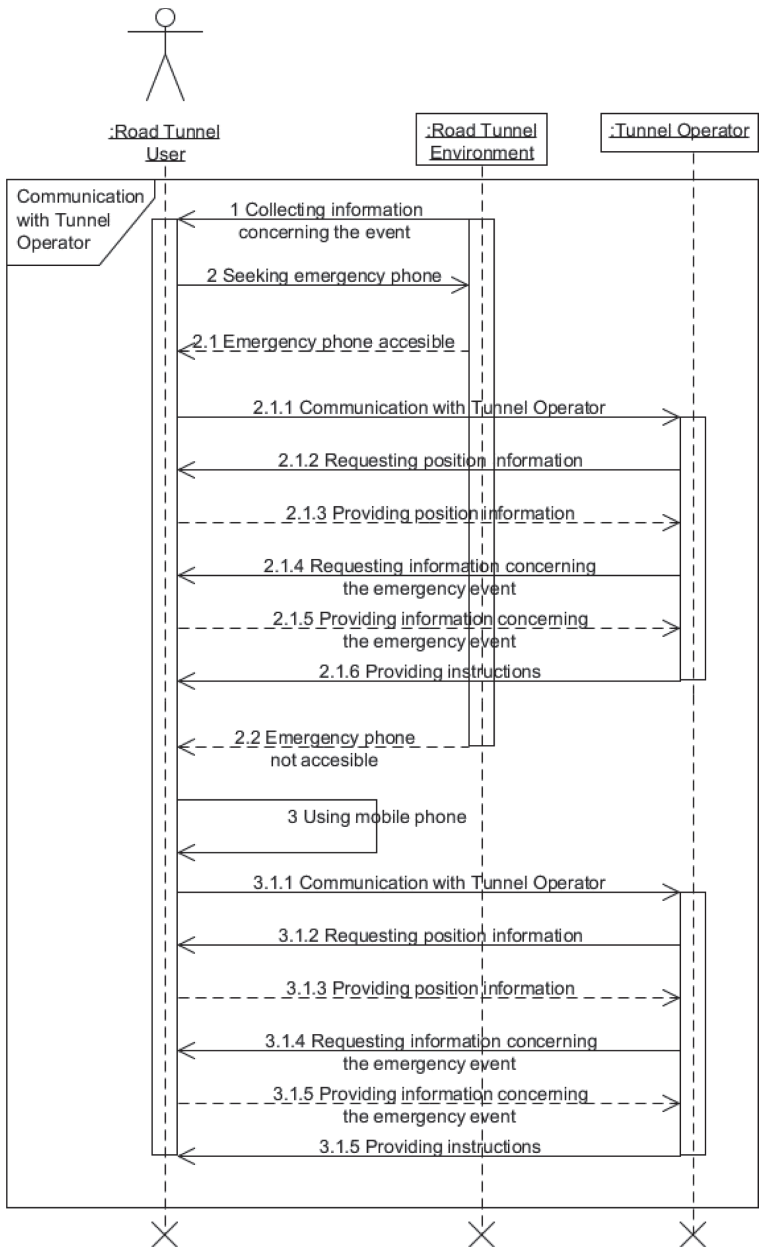


Figure 4. Sequence diagram of "Communication with tunnel operator" use case.

exit, while moving away from danger, is the proper reaction.

4.3 *Communication with tunnel operator*

When a tunnel user observes any irregularity inside a road tunnel, it is necessary to inform the tunnel operator of the situation. For this action to be helpful, there are specific requirements and priorities that the tunnel user should follow. The sequence diagram that describes the use case of "communication with tunnel operator" (Fig. 4), is presenting the course of actions that comply with those requirements.

Before communicating with the tunnel operator, the tunnel user should be prepared by gathering information about the event that needs to be reported. Being able to describe the exact position of the event, the existence of fire or injured people and the involvement of vehicles carrying dangerous goods is significant when reporting an incident.

The tunnel user should use the closest accessible emergency phone and only if this is not an option a mobile phone should be used.

Regardless of the means of communication used, after the tunnel user provides the operator with all the details that are need, the tunnel operator will instruct the user for the appropriate response to that specific situation.

5 CONCLUSIONS

5.1 *Practical implications*

When it comes to road tunnel safety, the human factor is critical. The course of actions that a tunnel user will chose to follow under normal condition may make the difference between avoiding an accident and provoking one. In the same manner the tunnel users' reactions under critical conditions can determine the outcome of the situation. Proper education of drivers for the use of road tunnels is pivotal to their reactions and has a great impact on the safety of themselves and the other users of the tunnel.

For the purpose of minimising the hazards that are results of erroneous human behaviour, a structured educational process is necessary. Although it is known that the human factor is unpredictable in critical situations, the probability of a proper reaction increases if the tunnel users have received better education and training. Throughout the education and training process, tunnel users should familiarise themselves with an otherwise strange environment (i.e. the road tunnel). Apart from basic rules and guidelines, the tunnel user should be able to react in a proper manner even in more complicated circumstances. Recognising the circumstances under which a reaction is called for and being able to remain patient under critical conditions is one of the main goals of the tunnel user's education.

The educational scenarios that were developed as part of this research address this issue. Providing tunnel users with information about events that might occur inside a unidirectional road tunnel and the good practices when confronting such events is of key importance to their education. By being able to identify which course of actions is needed in any incident that might take place inside a road tunnel, a well-trained user will be able to respond safely an also be an example for other users to follow.

In practice, these scenarios can be the base of a complete educational process and assist in the effort of increasing tunnel safety by improving the users' reactions.

5.2 *Further research*

Constructing and modelling educational scenarios that describe the proper behaviour and actions of a tunnel user, is the first step of creating an educational software application. These scenarios will be incorporated into the application, where the user will be asked to follow the provided instructions while interacting with a road tunnel environment. The scenarios will be tested on groups of drivers in order to provide feedback for the improvement and expansion of the educational tool.

Other aspects of further research include the effort to model the physical and environmental processes inside road tunnels with the aim of facilitating the decision making process in emergency situations. The application of these models may result in an online tool for mobile phones that will receive information from the tunnel users and the tunnel environment. This information can then be used as input for the operating centre's decision making system, and allow the operator to guide tunnel users to safety, through an interactive process.

ACKNOWLEDGEMENTS

This research has been co-financed by the European Union and Greek national funds through the Operational Program "Competitiveness and Entrepreneurship" of the National Strategic Reference Framework—Research Funding Program: Support of SME clusters for Research & Technological Development activities.

This research has been undertaken by the companies SIEBEN, Mediacape and SYNERGEIA with the National Technical University of Athens as a scientific consultant-subcontractor.

REFERENCES

Amundsen, F.H. 1994 Studies of driver behaviour in Norwegian road tunnels. *Tunnelling and Underground Space Technology,* 9: 9–15.

Arias, A.V., López, S.M., Fernández, I., Martínez-Rubio, J.L. & Magallares, A. 2008 Psychosocial factors, perceived risk and driving in a hostile environment: Driving through tunnels. *International Journal of Global Environmental Issues,* 8: 165–181.

Canter, D.V. 1980 *Fires and human behaviour*, John Wiley & Sons.

Carvel, R. & Beard, A.N. 2005 *The handbook of tunnel fire safety*, Thomas Telford.

Derntl, M. & Hummel, K.A. 2005 Modeling context-aware e-learning scenarios. *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*. IEEE.

Fowler, M. 2004 *UML Distilled: A Brief Guide to the Standard Object Modeling Languange*, Addison-Wesley Professional.

Gandit, M., Kouabenan, D.R. & Caroly, S. 2009 Road-tunnel fires: Risk perception and management strategies among users. *Safety Science,* 47: 105–114.

Kirytopoulos, K.A., Rentizelas, A.A., Tatsiopoulos, I.P. & Papadopoulos, G. 2010 Quantitative risk analysis for road tunnels complying with EU regulations. *Journal of Risk Research,* 13: 1027–1041.

Koper, R. 2005 Current research in learning design.

Koper, R. & Olivier, B. 2003 Representing the learning design of units of learning.

Lejeune, A. & Pernin, J.-P. 2004 A Taxonomy for Scenario-Based Engineering. *CELDA.*

Papaioannou, P. & Georgiou, G. 2003 Human behaviour in tunnel accidents and incidents: endusers, operators and response teams. UPTUN Deliverable.

Piarc 2008 *Human Factors and Road Tunnel Safety Regarding Users*, World Road Association (PIARC).

Piarc 2011 *Recommendations regarding road tunnel drivers' training and information*, World Road Association (PIARC).

Piarc & Ita 2004 Fire Safety in Tunnels. *Routes-Roads.* World Road Association (PIARC) & International Tunnelling Association (ITA).

Reisser-Weston, E. 1996 Simulating human behaviour in emergency situations. *RINA, International Conference of Escape, Fire, and Rescue.*

Rumbaugh, J., Jacobson, I. & Booch, G. 1999 *The Unified Modeling Language Reference Manual*, Addison-Wesley Professional.

Serrano, J. & Blennemann, F. 1992 Motorist behaviour study for the Gibraltar road tunnel. *Tunnelling and Underground Space Technology,* 7: 9–18.

Tesson, M. 2009 Adapting the road tunnel safety devices to the users. *4th Sysmposium on Human Behaviour in Fire*: 375–386.

Tesson, M., Perrin, B. & Aurand, V. 2012 Road Tunnel Safety: HGV Driver Training in France. *Procedia—Social and Behavioral Sciences*, 48: 473–483.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Public buildings safety: Addressing a pilot evacuation exercise

A. Santos & M. Queirós
Centre for Geographical Studies, Institute of Geography and Spatial Planning, Universidade de Lisboa, Lisbon, Portugal

ABSTRACT: The safety conditions regarding an emergency evacuation of the building of the Faculty of Letters, University of Lisbon, were investigated. Some traps inside the building were found and thus a group of researchers created their own emergency plan. The plan includes escape routes and a meeting point outside of the building. The goals of this experience were to test the emergency plan by conducting a pilot-evacuation exercise and also to analyze the behavior of the participants. In fact, this was the first time such an emergency evacuation exercise was performed at the Lisbon University main campus. The findings of this study raise some questions that may have policy implications: how to communicate the risk and how to include participation in planning escape; is hazard prevention education and training important for people awareness; are risks awareness a priority of public institutions.

1 INTRODUCTION

Recent experiences related to disasters around the world have caused a significant number of casualties, as well as millions of costs in damage. As a consequence, the general population and stakeholders are more aware of the safety procedures and the importance of regular practice of emergency drills in urban areas, including neighborhoods, public buildings and facilities. Even in academic literature, some studies focus on the practical ways that common building users can deal with fires and other hazards (Ramachandran, 1990).

In recent years, a new dimension to emergency preparedness emerged to ensure rapid and safe evacuation of occupants of buildings in the event of a fire: human behavior. The success of fire safety measures depends to a great extent on the behavior of building occupants who are under stress at the time of a fire (Ramachandran, 1990). Moreover, crisis management researchers have becoming more proactive in assessing the safety conditions of their academic institutions by developing and enhancing their disaster response plans (Beggan, 2011). In addition, a study showed that schools that had a disaster plan were more prepared for earthquakes than those that did not have a disaster plan (Ocal, 2011), thus showing the importance of having one. Moreover, the analysis of the survivors' accounts of the 2011 Tohoku Tsunami (Santos & Queirós, 2013) showed that knowledge about emergency plans combined with regular drills and evacuation exercises prepared many people to evacuate safely during the tsunami.

For the above reasons, the authors investigated the safety conditions of the Faculty of Letters building of the University of Lisbon (FLUL), Portugal, located at the main university campus. The authors noticed a chilling reality about the exit doors: most of the doors of the basement are permanently closed, as shown in Figure 1a, b. Although this is a security measure, the locked basement doors do not ensure the safe and quick evacuation of the building in emergencies. In addition, the building itself has several traps. Figure 1c shows a door locked with a chain, which allows access to an interior garden but no possible path to the exterior of the building. Constant building modifications, which include the creation of narrow corridors and the division of wide rooms into smaller ones, full until the roof with books and research objects, also make emergency evacuations from the building challenging.

Therefore, FLUL community should be aware of these aspects of the building, which are a threat and should practice emergency evacuation procedures.

Portuguese Law has several national regulations related to the fire and earthquake safety for educational buildings (ME, 2003, SNBPC-CML, 2005).

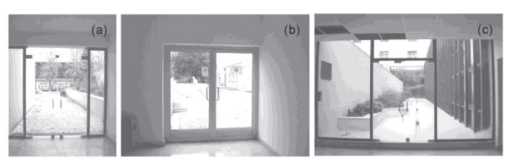


Figure 1. Photos of the exit doors in the basement of the FLUL taken on December 30, 2011: (a) and (b) are permanently locked; (c) is closed with a chain.

Under Portuguese Law, public buildings must have an emergency plan, which in the case of FLUL complies with all of safety guidelines. However, the authors have never had access to or knowledge about such an emergency plan for the FLUL building. The authors have also investigated past events that might have occurred in the building, but did not find records of any previous incident such as a fire, gas leak, or any other type of hazard endangering the building users.

Thus, the members of the Research Group on Environmental Hazard and Risk Assessment and Management (RISKam) decided to create their own emergency plan that includes escape routes and an emergency evacuation meeting point outside of the FLUL building. Thus, the objectives of the study are to test the emergency plan by conducting an evacuation exercise and to observe and discuss the human behavior of the usual occupants of the building during the pilot evacuation exercise.

This was the first time that an emergency evacuation study was conducted at the FLUL building. In fact, it was the first time such an emergency evacuation exercise was performed at the Lisbon University campus. The trigger event of this evacuation exercise was a hypothetical earthquake; also a basic training on how to safely evacuate the building was tested. Portugal is not a country prone to earthquakes. Nevertheless, the concern about earthquakes is related to the fact that in the past there were severe damage and fatalities due to earthquakes (ANPC, 2010).

In several other countries, the impact of extreme weather events motivates a variety of strategies for pre-disaster preparedness (Greenough et al., 2001). An example of the consequences of harsh weather conditions during an emergency evacuation was observed with the 2011 Tohoku Tsunami. The first author participated in the 2012 UNESCO Technical Field Trip to the areas affected by the 2011 Tohoku Tsunami. When the group was visiting Onagawa, it was snowing and it was about 1ºC outside. It was cold, and the weather conditions were similar to the day of the disaster. Because it was snowing on March 11, 2011, some people did not feel the urgency to evacuate, which is one of the many reasons that some people did not evacuate in time to escape the tsunami (Santos, 2011). As a consequence, weather conditions should be taken into consideration when an outdoors exercise is organized.

2 WHY CONDUCT DRILLS?

The increased interest in the study of risk mitigation is due in large measure to the rise of the "risk society", a recent societal and ideological reflexive context (Queirós & Henriques, 2009). However, this concern has resulted in a variety of scientific efforts to determine objective risk (hazard and quantification of human exposure to these hazards) rather than to actually study how risks are assessed and integrated into the practices of everyday life. A good knowledge of human perceptions and actions in response to risks is essential to the implementation of preventive and mitigation measures for increasing the safety level of the population. Buildings contain a variety of people, some who will be able to escape in most circumstances, some who will have extreme difficulty, and some who will not attempt to escape, and others will take the risk of fighting the hazard (Ramachandran, 1990). These facets of behavior were confirmed by the accounts of survivors of the 2011 Tohoku Tsunami (Murakami et al., 2012; Santos & Queirós, 2013). Behavior during an emergency is influenced by psychological, physiological and circumstantial factors (Ramachandran, 1990); it can also be influenced by the severity of threat posed by the hazard, the design of the building in which an emergency takes place, and the protective devices installed in the building. In addition, previous involvement in hazard incidents is also important in the risk perception (Queirós et al., 2007; Momani & Salmi, 2012). The role of risk perception in shaping people's behavior in the face of hazards has long been debated in the disaster research. Slovic's (1987) analysis for years explain that people tend to be intolerant of risks that they perceive as being uncontrollable, having catastrophic potential or bearing an inequitable distribution of risks and benefits. In its view assessments of risk can be more accepting of the role of emotions and cognition in people conceptions of danger, thus it is relevant to aid decision-makers by improving interaction with the public, by better directing educational efforts.

Several studies have been focusing on evacuation procedures based on simulations and models (Xudong et al., 2009). However, the best approach to test such models is to conduct drills and evacuation exercises (Kobes et al., 2010). Considering that regular building users are not safety professionals (like fire-fighters, civil protection agents or first aid experts), practice is the key for a successful emergency evacuation. In fact, the only way people have to practice emergency evacuations and be able to learn about safety procedures is handling with drills and evacuation exercises. For this reason, drills across Japan are made on a persistent basis. For example, Japanese drills are conducted annually on September 1 to mark the anniversary of the 1923 Great Kanto Earthquake (NHK World, 2011, 2012). Furthermore, evacuation drills help

to develop "muscle memory" (Dengler et al., 2011) in individuals to prepare themselves to appropriate responses to the natural warning signals of local tsunamis. Evacuation drills also provide an opportunity to test evacuation routes, and to provide input to officials and stakeholders for improving evacuation models. While drills are organized on regular schedules in Japan, in Portugal the number of evacuation exercises and drills are rare.

3 METHODOLOGY

After investigating about evacuation procedures on public buildings (Rodriguez et al., 2006; ISDR, 2007; Oreta, 2009; Machado, 2011; Penuel & Statler, 2011; Wisner et al., 2012; Handmer & Dovers, 2013) the authors decided to elaborate an evacuation plan. The most challenging part was to choose which path to follow as some offices have only one exit door, while other offices have at least two options of path leading to the street. Therefore, the criterion was to leave the building by using the shortest path, away from windows or narrow corridors. The plan determined indoors evacuation routes according to the location of the offices in the FLUL, and defined the place for the evacuation meeting point outside of the FLUL building. The evacuation plan was executed based on the authors' experience in collaboration with a highly skilled teacher of emergency plans for schools (see Machado, 2011).

In order to test the emergency plan, a pilot-evacuation exercise was organized. The participants agreed in advance that the exercise would start at 16:00 Lisbon Time (16:00 UTC) on March 21, 2012, with a situation of calm and nice weather. The participants had synchronized watches and were on their desks. At 16:00 all participants left their offices by following the evacuation route indicated on the emergency plan to the designated meeting point, outside the FLUL building. Those who were sharing the same office walked in order, others walked alone.

When the participants reached the meeting point, they answered the questionnaire shown in Figure 2, which was prepared by the authors. The participants did not know anything about the contents of the questionnaire until it was administered to ensure that participants would not prepare answers in advance. Some questions given in questionnaire seem to be to some extent naïve (for ex. 2.6, 3.1, 3.5). However, since this was the first time that such an approach was undertaken at the university campus, it was the authors' intention to ask even the most basic and obvious questions to test human ability to sense signs and codes present in the environment related with safety measures.

1. Personal Information
1.1 Sex
1.2 Age
1.3 Classify your motivation to this exercise.
1.4 Classify your health.
1.5 Have you ever participated in a drill?
1.6 Have you ever used a fire extinguisher (drill/real situation)?
1.7 Have you ever participated in a Civil Protection course/workshop?
1.8 Write the following phone numbers:
National Emergency Number/INEM _____
Nearest Fire department _____
Nearest police station _____
Building security _____

2. Drill
2.1 How long did you take to reach the meeting point?
2.2 Did you follow the path initially established?
2.3 During the evacuation did you noticed any exit sign?
If you answered *yes* to question 2.3, go to question 2.4. Otherwise, go to question 2.5.
2.4 Did your path coincide with the observed signs? 2.5 During the evacuation did you see any fire extinguisher?
2.6 During the evacuation did you see any emergency buttons?

3. Evaluation
3.1 Now that you finish the drill, do you feel safer in the building?
3.2 Now that you finish the drill, do you feel more prepared to deal with an emergency situation?
3.3 Now that you finish the drill, do you think the initial emergency plan is adequate?
3.4 Now that you finish the drill, do you recommend that others did it also?
3.5 Would you like to participate in future drills?
If you answered *yes* to question 3.5, go to question 3.6. Otherwise, go to question 3.7.
3.6 What kind of situations would you like to practice?
3.7 Comments and suggestions.

Figure 2. Questionnaire answered by the participants of the evacuation exercise.

Also, to understand if the experience of the exercise provides more self-awareness of how individuals think about and respond to risk (Slovic, 1987).

4 RESULTS

The answers given by the participants to the questionnaire were treated as descriptive statistics. The study population was a sample of sixteen participants who are professors, researchers and PhD students.

The questionnaire's results are shown in Figure 3. The responses to question 1.1 indicate there was a balanced distribution of genders (50% male and 50% female). The average age was 34 years, ranging from 25 (minimum) to 56 (maximum) years old. The most frequent value of ages was 37 years old; 44% of participants in the exercise were in the age range between 30–40 years (44%), and the standard deviation for the ages of the respondents is about 9 years. For 94% of the respondents, the motivation for participation (question 1.3) in the evacuation exercise was high or very high, corresponding to 15 people; only one person answered sufficiently motivated. Regarding the health status of the participants, not all of the participants felt healthy

Question	%
1. Personal Information	
1.1 Sex:	
Male	50
Female	50
1.2 Age:	
Age group 20-30	31.25
Age group 30-40	37.5
Age group 40-50	12.5
Age group 50-60	12.5
No reply	6.25
1.3 Motivation:	
High or very high	93.75
Sufficient	6.25
1.4 Health	
very healthy	31.25
Healthy	56.25
Sufficient	6.25
sick	6.25
1.5 Participation in a drill:	
Yes	25
No	75
1.6 Use of fire extinguisher:	
Yes	12.5
No	87.5
1.7 Participation in course on civil protection:	
Yes	6.25
No	93.75
1.8 Knowledge of emergency phone numbers:	
INEM	100
Others	6.25
2. Drill	
2.1 Evacuation time (minutes):	
3:00-3:30	6.25
3:30-4:00	12.5
4:00-4:30	81.25

Question	%
2.2 Followed the route initially established:	
Yes	100
2.3 Observation of emergency signs:	
No	100
2.5 Observation of fire extinguishers:	
Yes	37.5
No	62.5
2.6 Observation of emergency buttons:	
No	100
3. Evaluation	
3.1 Feel safer after this exercise:	
Yes	25
No	75
3.2 Feel better prepared to act in an emergency situation:	
Yes	81.25
No	18.75
3.3 Initial emergency plan adequate:	
Yes	62.5
No	37.5
3.4 Repetition of the exercise:	
Yes	100
3.5 recommendation that the exercise could be extended to other building users:	
Yes	100
3.6 Situations to practice:	
simple evacuation exercise	37.5
Fire	93.75
Flood	37.5
Gas leak	68.75
Earthquake	50
Other (landslide)	6.25

Figure 3. Results of the questionnaire.

(12.5%). Through their responses to questions 1.5, 1.6 and 1.7, most of the participants revealed that they did not take part of an exercise of this nature (75%). 87% have never used a fire extinguisher, and 94% have never attended a course on civil protection. Question 1.8 was related to emergency phones. Everyone knew the National.

Emergency Number, but nobody was aware of the telephone numbers of the nearest police station and the fire station. Only one participant knew the FLUL building security number.

The results of the Group 2 questions of the questionnaire are as follows: the average evacuation time (question 2.1) was 4′6″. The standard deviation of evacuation was 16″. Only one person left the building in less than 3′ 30″; 2 people took between 3′30″ and 4′ to leave the building, and 81% of the participants took more than 4' to evacuate. All participants followed the route initially established (question 2.2), and nobody noticed the emergency signs and buttons along the building (questions 2.3 and 2.6, respectively). However, 38% observed the fire extinguishers.

In the evaluation of the evacuation exercise (the Group 3 questions of the questionnaire), participants stated they did not feel safer after this exercise (75%), but a majority experienced a feeling of being better prepared to act in an emergency situation, corresponding to 81%. However, a significant percentage of the participants (62%) stated that the initial emergency plan "was adequate". All the participants recommend that the exercise could be extended to other building users. Also, all participants enjoyed the exercise. About 94% of the participants would like to conduct a fire drill.

5 DISCUSSION

Immediately after the pilot evacuation exercise, an indoor inspection was conducted at the FLUL building, and all distances used by the participants were measured (both inside and outside the building) till the meeting point. Figure 4 shows some of the emergency signs and equipment that are spread throughout the building. The inspection shows the FLUL building is very well equipped with all of the necessary emergency signs. All photos shown in Figure 4 were taken in areas where the exercise participants walk every day, several times a day. All the exit signs are located more than 2 m



Figure 4. Emergency signs and equipment: (a) and (b) at floor 1; (c) and (d) floor 0, (e) and (f) basement.

from the floor. However, a recent study shows that low-placed exit signs, rather than high placed signs, appear to have a positive influence on the use of the nearest fire exit (Kobes et al., 2010).

The pilot evacuation exercise shows the weaknesses in the preparation of FLUL building users during an emergency evacuation. The most significant results indicate that 100% of the participants did not see any emergency buttons (question 2.6). Initially, this question looked somehow naïve. However, this paper shows the importance of these types of evacuation exercises because the users did not noticed the existence of the emergency buttons. Although the indoor inspection shows the building is well equipped with emergency buttons, they are useless (Fig. 4c, d, e) if users do not know about the existence of these buttons; also 100% of the participants did not realize any exit signs, showing they were not aware of the signs and equipment. An example is the exit sign at the right hand side of a door that most of participants use every day, several times a day (Fig. 4a). Furthermore, the indoor inspection revealed that in some parts of the evacuation path chosen in the exercise was in the opposite direction of the exit signs. Figure 4a show the exit sign pointing to the left (conducting the users to the main exit door which is located about 390 m from the sign), while the nearest exit to the exterior of the FLUL building is located on the right (at about 50 m distance). 81% of the participants took more than 4' to evacuate. Therefore, for future emergency plans, the estimated evacuation time should be 4'30''. Those participants who used the shorted path (about 230 m) took an average velocity of 0.94 m/s, which is in agreement with the average velocity of 0.9–1.0 m/s, measured by Kobes et al. (2010). However, those participants who took the longest path (about 970 m) had an average velocity of more than 5 m/s. This shows that these last participants evacuated the building running, instead of walking. Therefore, the 2012 pilot-evacuation exercise at the FLUL confirms that more evacuation exercises are essential to avoid future panic, mishaps and human errors, as point out by Woodcok & Au (2013).

Initially, question 3.1 seems too obvious; however, 75% of the participants stated they did not feel safer after this exercise as they realized that they are unprepared to risk situations. On the other hand, question 3.2 shows a majority—corresponding to 81%—that experienced a feeling of being better prepared to act in an emergency situation. A significant number of the participants (62%) stated that the initial emergency plan "was adequate" (Fig. 3). However, the plan needs to be improved. These results show the participants may have been confused by the exercise and therefore need to practice evacuations more often. Finally, the participants were highly motivated to learn about proper emergency evacuation procedures. They would like to continue the emergency preparedness drills and evacuation exercises. They also indicated that would recommend emergency preparedness to others. These findings show that although the evacuation exercises are not incorporated in the university campus practices, the participants understood the importance to continue with these kinds of safety activities.

One of the purposes of the questionnaire was to study the human behavior in an emergency evacuation, and more specifically, to study the perception and the degree of internalization of the concept of risk by the users of the FLUL building. Through this study, the authors tried to ascertain the extent to which the idea of risk is not fully incorporated by the participants (Queirós & Henriques, 2009). After conducting the evacuation exercise, the authors can assert that there is an insufficient internalization of "being at risk" through the preparedness of the users of the building during the evacuation. Moreover, the existence of the correct emergency signs and equipment it is not enough to raise awareness to the buildings' users. Thus, the importance of the evacuation exercises to allow a more practical dissemination of information to the general users (Capel, 1973).

In traditional scientific thought, one cannot generalize on the basis of a single case (Flyvbjerg, 2006), and a case study cannot contribute to scientific development; nevertheless, the author states that this is not completely true because *one can often generalize on the basis of a single case and the case study may be central to scientific development via generalization as a supplement or as an alternative to other methods. However, formal generalization is overvalued as a source of scientific development, whereas "the force of example" is underestimated.* Deferring to conventional wisdom, because of the small size of the group that participated in the exercise and since the evacuation exercise was a single case study, the authors are cautious about generalizing the results. Still, having in mind Flyvbjerg reasons in mind, with the results achieved with this pilot evacuation exercise, the authors are convinced that this kind of research is also essential for the development of social science because this contributes to the understanding of the degree to which certain phenomena are present in a given group. Nevertheless, questionnaires are important tools to assess participant experiences (Ocal, 2011; Murakami et al., 2012), even with a small number of participants.

On the other hand, the initial traps found at the exit doors (Fig. 1) demonstrate that security measures continue to be a barrier to the safe and quick evacuation of the building in an emergency

situation. In addition, there is no exit sign in the vicinity of the doors shown in Figure 1. In fact, Figure 5 shows the emergency plan placed about 1.7 m from the ground floor, near the door shown in Figure 1a. The instructions are difficult to read, and most users are not aware of the sign. Nevertheless, a closer look reveals that the information on the board shows that the exit door shown in Figure 1a is indeed a "regular exit path to the exterior"; however, this door is permanently closed, without any alternative quick escape route nearby. In addition, no emergency plan or sign was found near the door shown in Figure 1b. These situations already have been reported to the safety management staff of the FLUL buildings and are being studied. Regarding earthquakes and fires other safety improvements are already underway such as training courses for the staff as well as measures to improve the emergency plan. However, for potential terrorist attacks the problem of evacuation is more difficult and the evacuation exercises should be supervised by external security experts, and also military and police forces.

The findings of this study have implications for risk prevention education and training on the university campus. For the foregoing reasons, drills and more emergency preparedness training should be extended to all FLUL users. Drills ought to be extended to all of the Lisbon University campuses. In addition, future drills and evacuation plans should be more complex, by informing instructions and cooperating with the rescue units. As Slovic (1987) states risk preparedness, risk management and risk communication efforts may not result in better outcomes unless they are structured as a two way process involving both building users and experts on risk assessment and management.

Finally, the findings of this pilot exercise raise some questions with policy implications: how to communicate the risk and how to include participation in planning "escape routes" in public (University) buildings. Hazard prevention education and training are important measures for people's awareness and preparedness, thus risks perceptions and acquaintance on human behavior in emergency situations should be a priority in higher education institutions.

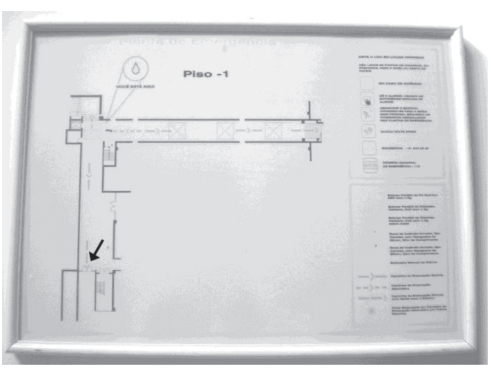


Figure 5. Emergency plan found in the interior of the FLUL building. The arrow indicates the emergency door to the exterior of the FLUL building that is locked.

ACKNOWLEDGEMENT

This research was supported by the TsuRiMa Project—TSUnami RIsk MAnagement for spatial planning and civil protection (PTDC/CSGEO/118992/2010), funded by the Foundation of Science and Technology (FCT), Portugal.

REFERENCES

ANPC—Autoridade Nacional de Protecção Civil. 2010. Estudo do Risco Sísmico e de Tsunamis do Algarve, Techincal Report, 165 pp.

Beggan, D. 2011. Disaster recovery considerations for academic institutions, *Disaster Prevention and Management* 20 (4): 413–422.

Capel, H. 1973. Percepción del medio y comportamiento geográfico. 1973. RACO, Revista de Geografía, Universidad de Barcelona, Vol. VII, nº1, p. 58–150. http://www.raco.cat/index.php/RevistaGeografia/article/view/45873/56665.

Chen, C-Y., Yu, k-H., Chen, M-Y. 2012. Planning of professional teacher-training program for disaster prevention education and executing efficiency evaluation. *Disaster Prevention and Management* 21 (5): 608–623.

Dengler, L., Goltz, J., Fenton, J., Miller, K., Wilson, R. 2011. Building tsunami-resilient communities in the United States: An example from California, *TsuInfo Alert* 13 (2): 1–14.

Flyvbjerg, B. 2006. Five Misunderstandings About Case-Study Research, *Qualitative Inquiry* 12 (2): 219–245.

Greenough, G., McGeehin, M., Bernard, S.M., Trtanj, J., Riad, J., Engelberg, D. 2001. The potential impacts of climate variability and change on health impacts of extreme weather events in the United States, *Environmental Health Perspectives*, 109 (2): 191–198.

Handmer, J. & Dovers, S. 2013. Handbook of Disaster Policies and Institutions Improving Emergency Management and Climate Change Adaptation, Earthscan from Routledge, 224 pp.

ISDR—International Strategy for Disaster Reduction 2007. Towards a Culture of Prevention: Disaster Risk Reduction Begins at School. Good Practices and Lessons Learned, UN, 156 pp.

Kobes, M., Helsloot, I., de Vries, B., Post, J.G., Oberijé, N., Groenewegen, K. 2010. Way finding during fire evacuation; an analysis of unannounced fire drills in a hotel at night. *Building and Environment* 45: 537–548.

Machado, A. 2011. Plano de Segurança, Escola Secundária Eça de Queirós, v1, 62 pp.

ME—Ministério da Educação 2003. Manual de Utilização, Manutenção e Segurança nas Escolas, Ministério da Educação, 84 pp.

Momani, N., Salmi, A. 2012. Preparedness of schools in the Province of Jeddah to deal with earthquakes risks. *Disaster Prevention and Management* 21 (4): 463–473.

Murakami, H., Takimito, K., Pomonis, A. 2012. Tsunami Evacuation Process and Human Loss Distribution in the 2011 Great East Japan Earthquake—A Case Study of Natori City, Miyagi Prefecture. *15 WCEE*, Lisbon, Portugal, 10 pp.

NHK World. 2011 Daily news broadcasted on September 1, 2011, Tokyo drills for major earthquake. NHK World online, http://www3.nhk.or.jp/nhkworld/.

NHK World 2012. Daily news broadcasted on September 1, 2012, Earthquake drills held across Japan. NHK World online, http://www3.nhk.or.jp/nhkworld/.

Ocal, A. 2011. Earthquake preparedness in schools in seismic hazard regions in the South-East of Turkey. *Disaster Prevention and Management* 20 (3): 334–348.

Oreta, A. 2010 Advocacy Guide, one million safe schools and hospitals campaign. UNISDR Asia and Pacific, 48 pp.

Penuel, K.B., Statler, K.B. 2011. Encyclopedia of Disaster Relief, *SAGE Publications, Inc*, 984 pp.

Queirós, M., Henriques, E.B. 2009. (In)seguranças numa Região de Elevada Susceptibilidade: implicações para a Gestão do Risco. In: Guedes Soares C, Jacinto C, Teixeira AP, Antão P, editors. Riscos Industriais e Emergentes, Vol. 1. Lisboa: Edições Salamandra, pp. 181–200., http://riskam.ul.pt/images/pdf/henriquesqueiros_2009%20cpia.pdf.

Queirós, M., Vaz, T., Palma, P. 2007. Uma reflexão a propósito do risco. *Actas do V I Congresso da Geografia Portuguesa,* Lisboa http://riskam.ul.pt/images/pdf/comlivactnac_2007_reflexao_risco.pdf.

Ramachandran, G. 1990. Human Behavior in Fires—A Review of Research in the United Kingdom. *Fire Technology* May: 149–155.

Rodrigues, H., Enrico, Q., Russel, D. 2006. Handbook of Disaster Research, 611pp.

Santos, A. 2011. Análise preliminar do Tsunami de Tohoku de 2011, *VIII Congresso Geografia Portuguesa*, Lisbon, Portugal, 6 p, http://riskam.ul.pt/images/pdf/Risco_69-428-1.pdf.

Santos, A., Queirós, M. 2013. The 2011 Tohoku Tsunami: analyzing the evacuation of the survivors. *IGU Regional Conference,* Kyoto, Japan, http://riskam.ul.pt/images/pdf/igu_abstracts_survivors.pdf.

SNBPC-CML—Serviço Nacional de Bombeiros e Proteção Civil e Câmara Municipal de Lisboa 2005. Plano de Prevenção e Emergência para Estabelecimentos de Ensino, 61 pp.

Slovic, P. 1987. Perception of Risk. Science, New Series, Vol. 236, No. 4799. (Apr. 17, 1987), pp. 280–285 (Stable URL: http://links.jstor.org/sici?sici=0036–8075%2819870417%293%3A236%3A4799%3C280%3APOR%3E2.0.CO%3B2-N).

Timco, G., Wright, B., Barker, A., Poplin, J. 2006. Ice damage zone around the Molikpaq: implications for evacuation systems. *Cold Regions Science and Technology*, 44: 67–85.

Woodcok, B., Au, Z. 2013. Human factors issues in the management of emergency response at high hazard installations. *Journal of Loss Prevention in the Process Industries* 26: 547–557.

Wisner, B, Gillard, J.C., Kelman, I. 2012. Handbook of Hazards and Disaster Risk Reduction, Francis & Taylor, 880 pp.

Xudong, C., Heping, Z., Qiyuan, X., Yong, Z., Hongjiang, Z. and Chenjie, Z. 2009. Study of announced evacuation drill from a retail store. *Building and Environment* 44: 864–870.

This page intentionally left blank

Simulation methods in system safety and reliability

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A safety analysis via minimal path sets detection for object-oriented models

C. Schallert
German Aerospace Centre, Institute of System Dynamics and Control, Wessling, Germany

ABSTRACT: Safety is of prime importance for aircraft and must be considered from the beginning of the design process. Conducting a safety analysis involves considerable effort, particularly if traditional methods, such as manual fault tree analysis, are used. This may explain why analyses are performed usually only once or twice during an entire aircraft development. Furthermore, traditional methods are hardly linked to other tools for system conceptual design.

In the field of modelling and simulation, multi-domain object-oriented languages are increasingly adopted. They enable an intuitive way of modelling, since objects and their interconnections correspond with real components. Thus, large-scale system models can be created and simulated efficiently.

A new method is developed that integrates safety analysis with multi-domain object-oriented modelling. This is the contribution aimed by this paper. In essence, the proposed method automatically detects the minimal path sets of a technical system.

1 INTRODUCTION

This paper describes a method for automated safety analysis of a technical system that is represented as a multi-domain object-oriented model. The proposed method automatically detects the minimal path sets of the modelled system. Then, the probability of system operation or failure is computed from the minimal path sets using component failure rates.

Object-oriented modelling based on differential algebraic equations offers large expressive power for establishing multi-disciplinary engineering tools. In addition, the structure of an Object-Oriented Model (OOM) resembles the functional paths that cause a technical system to operate. This property is exploited by the minimal path sets detection method.

Fault modelling is introduced in addition to the common modelling of normal operation. This forms a basis for the proposed method that belongs to the class of state space simulations. In this context, the state space denotes the set of all possible combinations of intact and failed components of a system. Search algorithms from graph theory are adopted to narrow down the state space, thus preventing unfeasibility of the method due to an exponential increase of the number of combinations and thus simulations to be performed.

The developed modelling approach is not exclusively dedicated to safety analysis. It rather serves several purposes, such as system performance or parameter studies, as usually is the motivation for physical modelling and simulation.

This paper is organised as follows: Section 2 recaps the basics of OOM, describes the selected modelling approach and establishes an example model of a safety relevant aircraft system. Section 3 describes the minimal path sets detection and exemplifies the method by means of the established system model. Section 4 concludes the paper.

2 MULTI-DOMAIN OBJECT-ORIENTED MODELLING OF SAFETY RELEVANT AIRCRAFT SYSTEMS

2.1 *Multi-domain object-oriented modelling*

This section briefly recaps the basic principles of the modelling approach.

The idea of multi-domain object-oriented modelling was formulated by Elmqvist (1978), who proposed a language called Dymola (Dynamic Modelling Language). In object-oriented modelling, objects, their boundaries and interconnections correspond with real existing equipment. Physical equations have to be established or understood only for each object. By connecting objects with each other, further model equations are introduced.

A translator then automatically transforms the model equations into a simulation ready runtime model. This approach has a couple of advantages over block diagrams (e.g., Simulink), as explained by the two corresponding model implementations of a small electronic circuit shown in Figure 1.

As Figure 1 shows, the OOM (a) retains the physical structure of the circuit, whereas the block diagram (b) does not. The OOM is changed intuitively by removing or adding components and connecting them with other components. Different physical domains can be combined in a single model.

The circuit model includes, among others, a resistor, capacitor and inductor. Such component models are available from standard libraries. The model equations are $v = R \cdot i$, $i = C \cdot der(v)$ and $v = L \cdot der(i)$, respectively, where $der(\,)$ denotes the time derivative. Each component has two electric pin interfaces (filled and non-filled blue squares in Figure 1a) that include the voltage v as a potential and current i as a flow variable. Model equations are introduced for connected component (object) interfaces as follows: The potential is the same, whereas the sum of flow equals zero according to Kirchhoff's node rule. For example, in case of the circuit model shown by Figure 1a): $v_1 = v_3 = v_7$ and $i_1 + i_3 + i_7 = 0$.

The system model described in section 2.3 also covers the mechanical (M) and hydraulic (H)

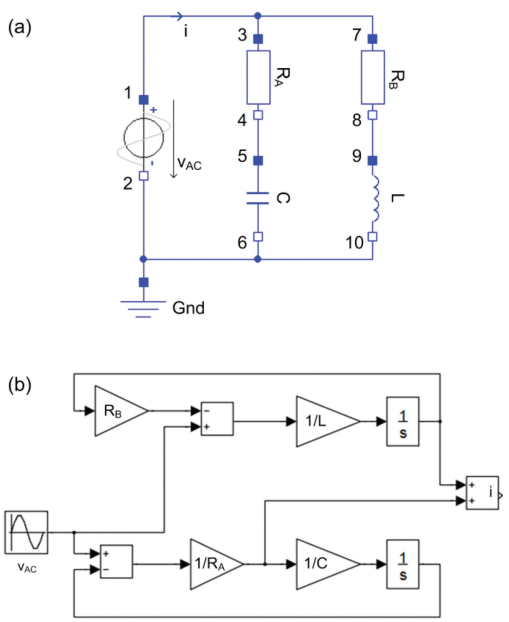


Figure 1. Small electronic circuit (a) and its block diagram representation (b). Taken from The Modelica Association (2000).

Table 1. Model interfaces, icons and domain (dom) identifiers.

connector	potential	flow	icon	dom
electric pin	voltage v	current i	■ □	E
translational flange	position s	force f	■ □	M
rotational flange	angle φ	torque τ	● ○	M
hydraulic port	pressure p	flow rate q	■ □	H
real signal	input u, output y		▶ ▷	S
Boolean signal	dto.		▶ ▷	S

domains, as well as real and Boolean signals (S). Table 1 summarises the according interface definitions and icons. These appear in Figures 1 (a), 3, 4 and 5.

Thus, an OOM consists of the equations of each object and of those imposed by the connections between them. By symbolic processing, this set of equations is translated into a simulation runtime model of the differential algebraic (DAE) form

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A} \cdot \boldsymbol{x}(t) + \boldsymbol{B} \cdot \boldsymbol{u}(t) \\ \boldsymbol{y}(t) &= \boldsymbol{C} \cdot \boldsymbol{x}(t) + \boldsymbol{D} \cdot \boldsymbol{u}(t) \end{aligned} \tag{1}$$

2.2 *Modelling additions for safety analysis*

2.2.1 *Modelling and simulation of failures*

The proposed safety analysis method is based on simulation of failures. Component models that only reflect normal operation have to be enhanced accordingly. At system level, control or reconfiguration logics have to be implemented that define how a system reacts to the occurrence of failures. The pursued modelling approach is structure invariant, i.e. the DAE structure (equation 1) remains always the same. Failures are represented by model parameter (values in matrices $\boldsymbol{A}$, $\boldsymbol{B}$) changes.

Elmqvist et al. (2014) propose and Bouissou et al. (2014) use a structure variant approach that is even more flexible for the modelling of failures. Future work will combine this approach with the minimal path sets detection method described in this paper.

In general, the concept of minimal path sets distinguishes only between operation and failure. Thus, the proposed detection method addresses two states (intact, failed) at component and at system level.

2.2.2 *Indication of system status*

Safety assessment requires the analyst to define criteria that distinguish normal operation from failure of a system. The analysis method proposed by this paper requires implementing these criteria in a system model, such that an output signal indicating the system status is computed. A system model is simulated by the analysis method for various combinations of intact and failed components, and

the resulting system status (operation or failure) is correlated with the respective component states.

2.2.3 *Insertion of component failure rates*

Failure rates λ are stored in each component model that is enhanced with failures. Constant failure rates (exponentially distributed lifetimes) are assumed per default. Since the stress level of a component is known in the simulation, its failure rate can be adapted accordingly. Failure rates are used to compute probability of system operation $R_{sys}(t)$ or failure $F_{sys}(t)$ from the detected minimal path sets.

2.3 *Stabiliser trim system model*

This section describes the multi-domain object-oriented model of a stabiliser trim control and actuation system. This model of a safety relevant aircraft system is based on generally available information (Airbus Training, Boeing B737 NG, Persson et al. 2001). It is established for exemplification of the automated minimal path sets detection method.

2.3.1 *System description*

Longitudinal control of an aircraft is achieved by elevators and a horizontal stabiliser surface. The latter is positioned by a stabiliser trim control and actuation system. A main part of this system is a ballscrew actuator that is equipped with two hydraulic motors to rotate the ballscrew through a reduction gear. If the stabiliser is not moved, it is held in place by the actuator. To this end, an electro-mechanical, power-off engaged brake (POB) is mounted to each motor shaft. The brakes are engaged if the associated motor is shut off or if the system has to be stopped after a failure is detected.

The pilots operate the system via pairs of trim switches that are mounted to each control wheel (or centre pedestal). The trim switches are spring-loaded to the neutral position. To command trimming, the two switches of a pair have to be pushed up or down simultaneously. This causes the active system channel to release the associated brake and energise a hydraulic valve to direct fluid to the motor. The actuator moves the stabiliser until the trim switches are released, the end of the stroke is reached, or a fault is detected. The system is monitored for faults, such as loss of hydraulic pressure, valve or motor failure, by comparing the sensed motor speed and stabiliser motion rate with the actual trim command.

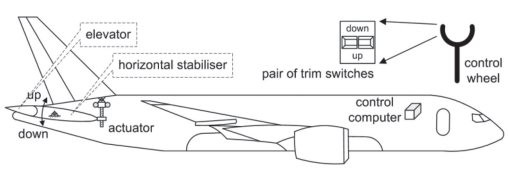


Figure 2. Stabiliser trim control and actuation system.

The minimal path sets detection method reveals those conditions that cause a system to operate. The example system is considered operational if it moves the stabiliser surface according to the actual command and holds it in place if no command is present.

2.3.2 *Component modelling*

The modelling of the stabiliser trim system includes one-dimensional mechanics with elasticity, damping, inertia and friction; hydraulics with bulk modulus, fluid density, turbulent and laminar flow; and resistive electrics. One of the developed component models is explained below.

A spur (reduction) gear is essentially described by the ratio of input and output torques and angles:

$$0 = I_{SG} \cdot \tau_a + \tau_b, \qquad \varphi_a = I_{SG} \cdot \varphi_b \tag{2}$$

The "IdealGear" element introduces these equations to the spur gear model. The "Disconnect" and "Jam" elements are rotational spring-dampers described by:

$$\tau = c \cdot \varphi_{rel} + d \cdot \dot{\varphi}_{rel}, \qquad \tau = \tau_b = -\tau_a,$$
$$\varphi_{rel} = \varphi_b - \varphi_a \tag{3}$$

They are used to represent failures of the spur gear. To this end, the spring and damping coefficients (c and d) are varied as indicated by Table 2. In equations 2 and 3, indices a and b denote the rotational flanges of the spur gear and of the spring-damper elements (shown in Figure 3), respectively.

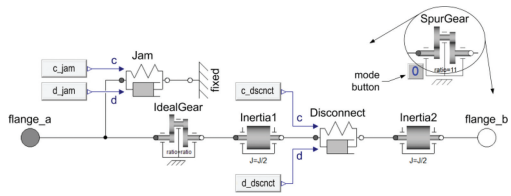


Figure 3. Spur gear model including disconnection and jam.

Table 2. Modelling of spur gear failures by variation of spring and damping coefficients. [c] = *Nm/rad*, [d] = *Nms/rad*

	Mode	C_{dscnct}	d_{dscnct}	d_{jam}
Normal operation	0	10^4	10^4	d_{G-drag}
Disconnection	1	0	0	d_{G-drag}
Jam	2	10^4	10^4	10^4

In normal operation, the "Disconnect" element is quasi-rigid. It is literally broken to represent a disconnection of the spur gear. A jam is modelled by a quasi-rigid connection to the "fixed" element. The coefficient values implicate small relative rotations in the order of $\varphi_{rel} = 10^{-3}$ *rad* for a transferred torque of $10Nm$, which is negligible for the present application. The coefficients have to be adapted for applications of different scale. The "Jam" element also reflects the friction of the intact spur gear, e.g. by $d_{G-drag} = 2 \cdot 10^{-4}$ *Nms/rad*.

Normal operation (*mode* = 0) or disconnection (*mode* = 1) of the spur gear are considered for the detection of minimal path sets.

2.3.3 *System model*

Figure 4 shows an image of the developed stabiliser trim control and actuation system model. It contains two instances of the drive channel model depicted by Figure 5. Each channel consists of a control computer, a hydraulic valve, motor and brake (POB) that are electrically activated. The channels are connected to different electric (DC1, 2) and hydraulic (Pressure1, 2) sources. Each computer is connected to the trim switches (Up1, 2 and Down1, 2), and to the other channel computer for coordination of active or stand-by status. The model interface and connection types are as defined in Table 1.

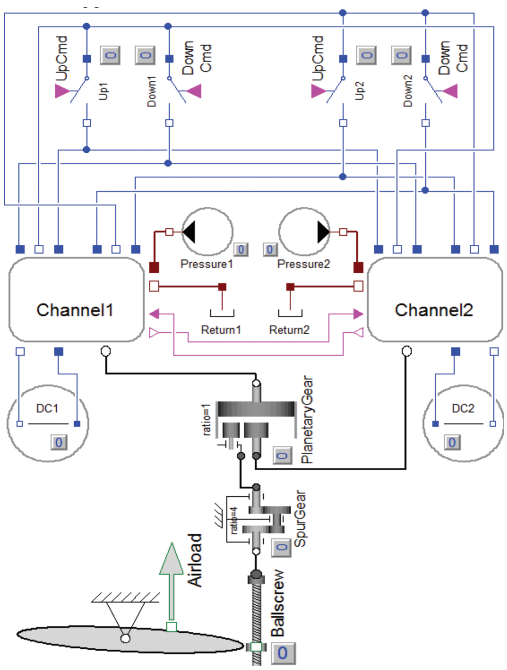


Figure 4. Stabiliser trim control and actuation system model.

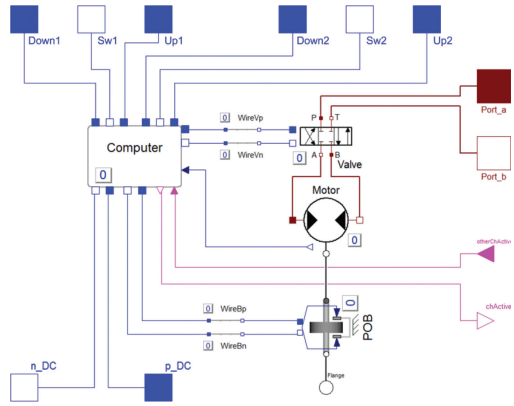


Figure 5. Model of a drive channel of the stabiliser trim system.

As explained in section 2.2.2, a system status output (not shown in the images) is computed for use by the minimal path sets detection (section 3). This output indicates if the system operates normally or if it fails (no motion or uncommanded motion). To this end, the actual motion rate of the stabiliser surface is compared with the command (trim switch inputs).

3 DETECTION OF MINIMAL PATH SETS

This section describes the proposed method for automated detection of the minimal path sets of a technical system. It is based on the idea that the related object-oriented model structure resembles the functional paths that cause the system to operate.

After detection of the minimal path sets, probabilities of system operation $R_{sys}(t)$ or failure $F_{sys}(t)$ are computed from failure rates (section 2.2.3) using the method described by Heidtmann (1989).

3.1 *Definitions*

A *path set* is a set of intact components that causes a system to operate. A *path set* is *minimal* if it contains only as many intact components as are necessary for the system to operate.

A *path* is a sequence of consecutive nodes in a graph, where each two successive nodes are connected via an edge.

A *union* (denoted by ∪) of a collection of *paths* consists of all nodes in the collection of *paths*.

3.2 *Properties of minimal path sets in an object-oriented model*

The structure of an OOM is regarded as a graph. Nodes and edges of the graph represent

components (objects) and connections between them. Nodes that include failure behaviour are indicated by filled circles in Figures 6, 7 (b), 8, 10–15. Non-filled circles indicate nodes that are always intact. Non-filled squares indicate auxiliary nodes.

In such a graph, minimal path sets are not just simple s-t paths. An s-t path connects two nodes "s" and "t" of a graph through an unbranched, open walk:

Minimal path sets are sometimes unbranched, just as s-t paths are. In general, however, a minimal path set includes junctions or circles, as Figure 7 indicates for a part of the stabiliser trim

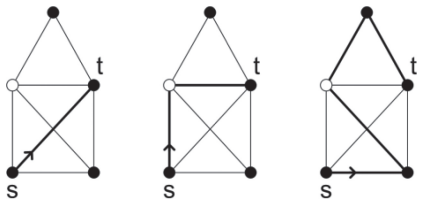


Figure 6. Several s-t paths in a graph.

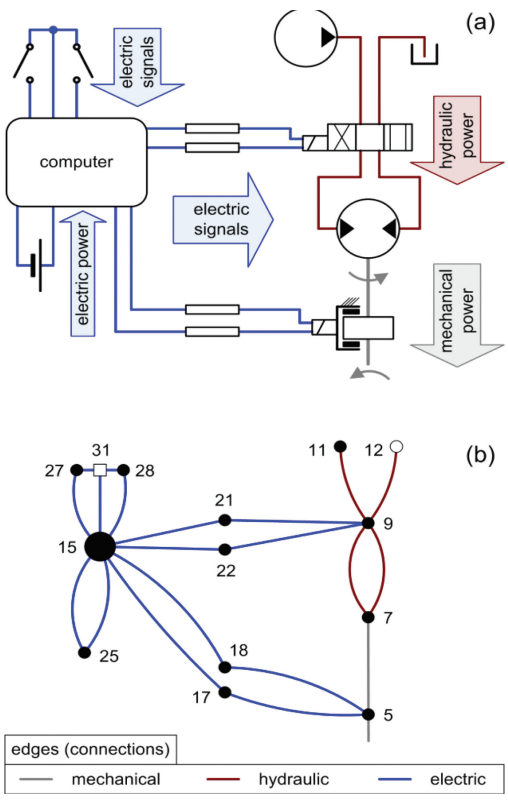


Figure 7. Exchange of power, material and signals across the edges in a coherent set of nodes—Part of OOM of stabiliser trim system (a) and corresponding graph (b).

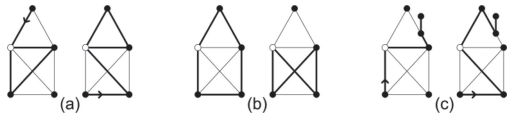


Figure 8. Ties (a), circles (b) and open walks (c) in a graph.

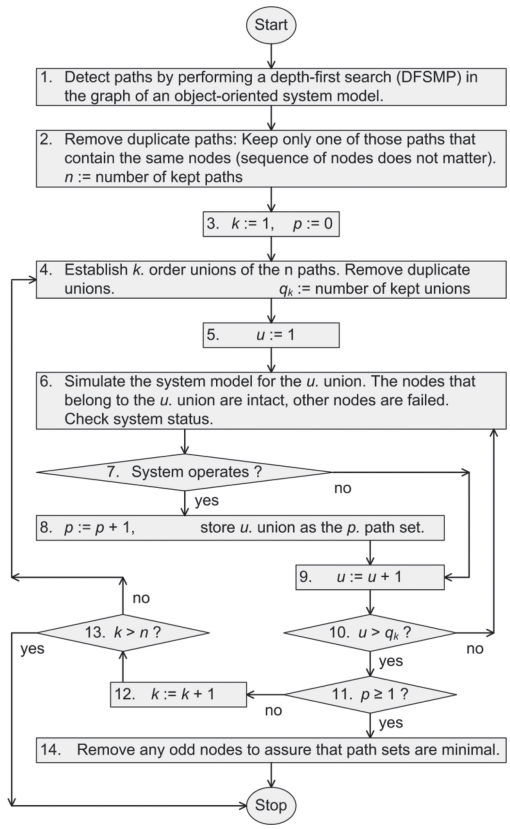


Figure 9. Flow chart of a minimal path sets detection method.

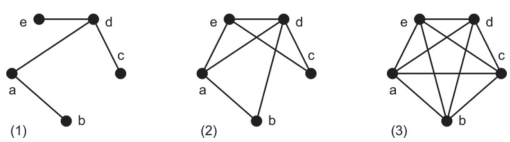


Figure 10. Three graphs of different density.

system model graph. The electric connections between the computer (15), valve (9) and brake (5) introduce such junctions. (The numbering of nodes is consistent with Figures 11–14 and section 3.4.) Since there is more than one junction, circles exist in the graph.

A minimal path set consists of one or more nodes. Power, material or signals are exchanged between neighboured nodes across the connections (edges) between them, as depicted in Figure 7. This causes a technical system to operate. Only neighboured nodes, i.e. coherent sets of nodes, can perform this exchange and render a system operational.

3.3 *Detection method*

The proposed detection method belongs to the class of state space simulations. At first, the system model graph is evaluated to find candidates of minimal path sets. This is achieved by an adapted depth-first search algorithm and establishing of unions of the found paths. Then, the system model is simulated only for the candidates to detect the actual minimal path sets. Figure 9 shows a flow chart of the detection method. Without the prior evaluation of the model graph, the number of simulations would be 2^{nr}, nr being the number of system components.

3.3.1 *An adapted depth-first search*

Due to the described properties of minimal path sets, it is meaningful to use a Depth-First Search (DFS) for detection. This algorithm is known from many references, such as Krumke et al. (2012). It finds sets of consecutive nodes (paths) in a graph. In doing so, it commences at a start node and progresses into depth with one of the neighbours of each visited node. For the purpose of detecting minimal path sets, the algorithm is adapted (→ DFSMP) with a definition of the target nodes. It finds the following types of path:

a. Ties. A tie is a path that ends at a node already contained in the path.
b. Circles. A circle is a special case of a tie.
c. Open walks. An open walk ends at a node that only has one neighbour.

3.3.2 *Unions of paths*

The DFSMP is capable of finding minimal path sets that include a junction or circle. Still, a minimal path set might not be detected if the start node is unfavourably selected, or if more than one junction or circle occur. To accommodate for such formations (present in Figure 7), unions of paths are established. This corresponds with step 4 of Figure 9.

The maximum number of unions is denoted by the binomial

$$\binom{n}{k} = C(n,k) = \frac{n!}{k!\cdot(n-k)!} \tag{4}$$

where n is the number of all paths and k is the number of paths to be merged in a union. The actual number of unions q_k is much lower, dependent on the density d of the graph. d is generally defined, e.g. by Roberts et al. (2007), as

$$d(N,E) = \frac{2\cdot E}{N\cdot(N-1)} \tag{5}$$

For the three graphs depicted in Figure 10, each having $N = 5$ nodes, the number of edges E, density and number of paths n are listed in Table 3. The paths are established starting from node "a" according to the rules defined in section 3.3.1. Since the sequence of nodes in a path or union does not matter, duplicates are removed. n paths or, respectively, q_k unions are kept as summarised in Table 4.

For the complete graph ($d = 1$), q_k is much lower than the corresponding binomial. The reason is that the paths are longer, the higher the density of the graph is. The longer the paths are, the more they cover the graph. Unions of long paths cover

Table 3. Number of edges, density, and number of paths.

Graph	E	d	n
(1)	4	0.4	3
(2)	7	0.7	5
(3)	10	1	11

Table 4. Binomial (n in rows, k in columns) and actual number of unions q_k for the three graphs.

$C(n, k)$	2	3	4	5	q_k	2	3	4	5
3	3	1			3	3	1		
5	10	10	5	1	5	3	2	1	1
11	55	165	330	462	11	5	5	5	1

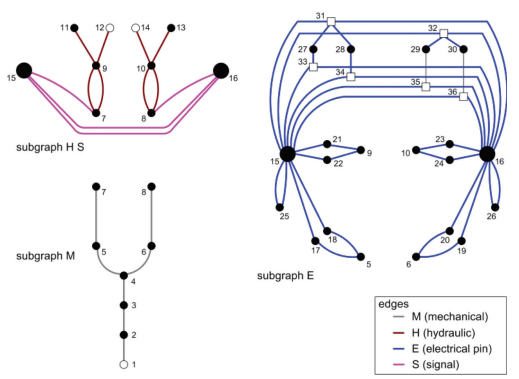


Figure 11. Subgraphs of stabiliser trim system model.

the graph even more, so the number of different unions q_k is relatively low. For a low-density graph, the paths are relatively short, so relatively more different unions (compared to the binomial) occur.

3.3.3 *Removal of odd nodes*

In some cases, the detected path sets are not minimal. This means that more (odd) nodes are contained in a path set than are necessary to cause the system to operate. A path set is minimal only if a failure of any of its nodes (components) causes system failure.

Thus, a check is introduced at the end of the detection method (step 14 in Figure 9): Tracing and removal of odd nodes.

Essentially, the check proceeds by simulating the system model for each path set such that one of its nodes fails, one by one, while the others are intact. If the system still operates, then the respective path set is stored without the failed node. This is repeated until no odd nodes are detected in any path set anymore. Since it is basic trial-and-error, without any evaluation of the model graph, this check is used only to assure that the path sets are minimal by removing a small number of odd nodes, if necessary.

3.3.4 *Separation of physical domains*

The number of paths n in a graph increases strongly with the number of its nodes N and density d, the phenomenon known as combinatorial explosion. This is clarified by an estimation of the number z of s-t paths proposed by Roberts et al. (2007) for graphs of a density $d \in [0.1; 0.9]$. (The DFSMP detects three different kinds of paths. However, estimations exist only of the number of s-t paths.)

$z(N,d) \approx K(N) \cdot d^{N-1+\delta(N,d)}$ where

$$K(N) = \sum_{k=0}^{N-2} \frac{(N-2)!}{k!}, \qquad \delta(N,d) = \frac{3.32}{N} - \frac{5.16}{d \cdot N} \qquad (6)$$

It is proposed to mitigate the growth phenomenon by splitting up the model graph at the boundaries of the physical domains. These are identified by the different types of model interfaces (listed in Table 1). Thus, a model graph split-up algorithm is created that recognises these interface attributes.

Smaller subgraphs are established that are evaluated one by one according to the flow chart of Figure 9. (Due to splitting up the model graph, some additions to the algorithm are needed, as Schallert (2014) describes.) Figure 11 shows the subgraphs established for the stabiliser trim system model. Table 5 lists some of the properties of the model graph before split-up (all-up) and of the subgraphs. n are the actual numbers of paths found in a (sub-)graph.

Table 5. Number of nodes, edges, density, estimated number of s-t paths and actual number of paths in (sub-) graphs.

Subgraph	N	E	d	z	n
all-up	36	54	0.086	1766	1932
M	8	7	0.25	2.4	3
H S	10	9	0.2	2.09	4
E	26	38	0.117	244	91

3.4 *Course of minimal path sets detection algorithm for the stabiliser trim system model*

The minimal path sets detection algorithm is exemplified by means of the stabiliser trim system model.

Subgraph M is evaluated first, starting from node 2 (ballscrew in Figure 4). Figure 12 shows this stage of the algorithm. The DFSMP finds three paths (parentheses indicate nodes that are always intact):

$path_1 = \{2, (1)\}$; $path_2 = \{2, 3, 4, 5, 7\}$;
$path_3 = \{2, 3, 4, 6, 8\}$

The three paths are tested by simulation of the system model (steps 6. - 10. in Figure 9). At the same time, all nodes covered by the shaded area are intact. The result of this first iteration is that the system does not operate for any of the three paths.

Thus, steps 6. - 10. are repeated for $k = 2$, which reveals that the system operates for the union {2, 3, 4, 5, 6, 7, 8}. The removal of odd nodes (step 14. in Figure 9) leads to storing the two, yet incomplete minimal path sets

$MP_1 = \{2, 3, 4, 5, 6, 7\}$; $MP_2 = \{2, 3, 4, 5, 6, 8\}$

These are indicated by the green nodes in Figure 13. After this, the evaluation of subgraph M ends.

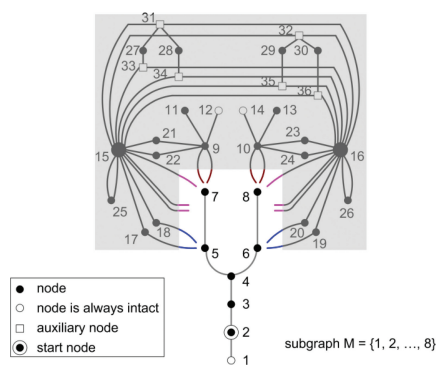


Figure 12. Evaluation of mechanical domain subgraph.

The algorithm continues by evaluating subgraph H S for each of the two incomplete minimal path sets. For MP_1, the DFSMP starts from node 7 (as shown by Figure 13) and finds four paths:

$path_1$ = {7, 9, 11}; $path_2$ = {7, 15, 16, 8, 10, (14)}

$path_3$ = {7, 9, (12)}; $path_4$ = {7, 15, 16, 8, 10, 13}

Next, the paths are tested by simulating the system model (steps 6. - 10. in Figure 9 for k = 1).

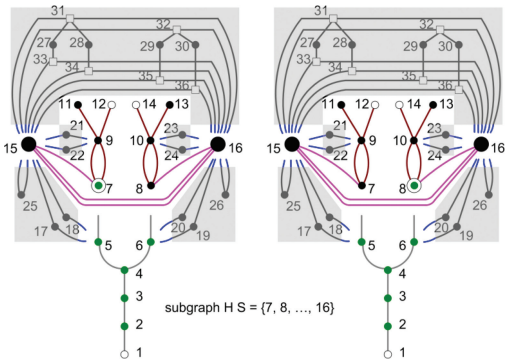


Figure 13. Hydraulic and signal domains subgraph evaluation.

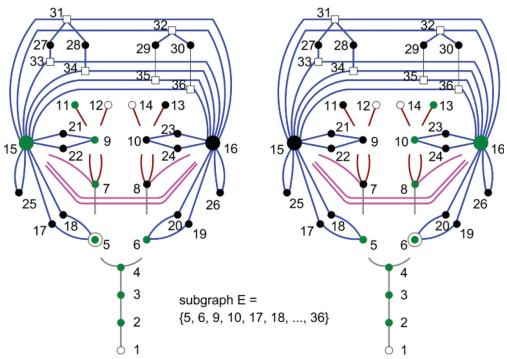


Figure 14. Evaluation of electrical domain subgraph.

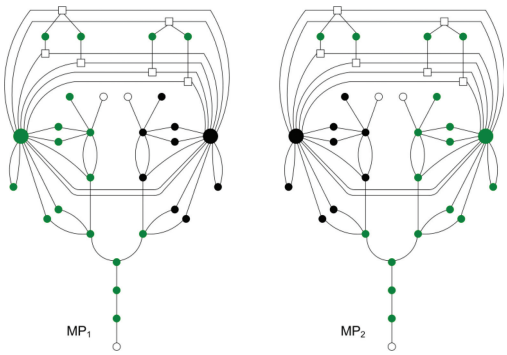


Figure 15. Minimal path set of stabiliser trim system.

In doing so, those nodes are intact that belong to $MP_1 \cup path_j$, $\forall j \in \{1, 2, 3, 4\}$ respectively. Also, all nodes covered by the shaded area are intact. The system does not operate. The next iteration (k = 2) reveals that the system operates for the union $MP_1 \cup path_1 \cup path_2$. The removal of odd nodes leads to storing MP_1 = {2, 3, 4, 5, 6, 7, 9, 11, 15}.

The algorithm proceeds accordingly for the second minimal path set (DFSMP starts from node 8). After the evaluation of subgraph H S is complete, it is stored as MP_2 = {2, 3, 4, 5, 6, 8, 10, 13, 16}. The two minimal path sets developed so far are indicated by the green nodes in Figure 14.

Next, the algorithm evaluates subgraph E to complete the two minimal path sets. For MP_1, the DFSMP starts from node 5 and find 91 paths. Three of them are:

$path_1$ = {5,17,15,25}; $path_2$ = {5, 18, 15, 21, 9, 22};

$path_3$ = {5, 17, 15, (33), 27, (31), 28, (34), 16, (36), 30, (32), 29, (35)}

The loop (steps 6. - 10. in Figure 9) of testing paths and unions by simulating the system model is repeated up to k = 3. Then, the system operates for the union $MP_1 \cup path_1 \cup path_2 \cup path_3$. Odd nodes are removed, and the minimal path set is stored as MP_1 = {2, 3, 4, 5, 6, 7, 9, 11, 15, 17, 18, 21, 22, 25, 27, 28, 29, 30}.

For k = 2, $C(91, 2)$ = 4095 unions were established of which a number of q_k = 634 remained after removal of duplicates. For k = 3, $C(91, 3)$ = 121485 unions were established of which a number of q_k = 1279 remained. As explained, the model is simulated only for the respective q_k unions.

Next, the second minimal path set is completed by starting a DFSMP from node 6. The loop of testing paths and unions in the simulation is run through up to k = 3 with similar computing effort. The result is MP_2 = {2, 3, 4, 5, 6, 8, 10, 13, 16, 19, 20, 23, 24, 26, 27, 28, 29, 30}. Both complete minimal path sets are indicated by the green nodes in Figure 15.

The total number of system model simulations performed is 4129. Most of them are caused by step 6., and a few are due to step 14. of the minimal path sets detection algorithm depicted by Figure 9. If the model graph was not split up (row 1 in Table 5), this would cause a total of > 615000 simulations, which is unfeasible. Without any evaluation of the model graph, the number would even be $2^{27} = 1.34 \cdot 10^8$ due to the system comprising 27 components (nodes) that include failure behaviour.

4 CONCLUSIONS

This paper described and exemplified a method for minimal path sets detection of a technical

system that is represented by a multi-domain object-oriented model. The method is the core of an automatic safety analysis that can be performed throughout the design process of the system, thus keeping the analysis consistent with design iterations. It is meaningful to apply the method if multi-domain object-oriented modelling is used already in systems engineering. The proposed method enhances the scope of application of a system model while permitting all other simulation studies that originally motivated development of the model to be conducted.

The method belongs to the class of state space simulations. A search algorithm from graph theory is adapted to evaluate the object structure of the model, which prevents exponential growth of the state space and thus unfeasibility of the method.

Further detail of the proposed method, estimation of computing effort, as well as modelling and analysis examples are described by Schallert (2014).

It must be beared in mind that all model-based analysis methods capture only those phenomena that are covered in the modelling approach. Then again, the automation ensures that all relevant failure conditions (at least in so far as modelled) are considered, whereas a manually conducted analysis might be errorneous or incomplete.

ACKNOWLEDGEMENTS

This research has received funding from the European Union's 7th Framework Programme (FP7/2007–2013) for the CleanSky Joint Technology Initiative under grant agreement CSJU-GAN-SGO-2008-001.

REFERENCES

Airbus Training, *A320 Flight Crew Operating Manual, section 1.27.00—Flight Controls*. Available at website: http://www.smartcockpit.com/

Boeing B737 NG—*Systems Summary—Flight Controls*. Available at website: http://www.smartcockpit.com/

Bouissou, M. & Elmqvist, H. & Otter, M. & Benveniste, A., 2014. Efficient Monte Carlo simulation of stochastic hybrid systems. *Proceedings of the 10th international Modelica conference,* Lund, Sweden, March 10–12, 2014.

Elmqvist, H., 1978. *A Structured Model Language for Large Continuous Systems*. PhD thesis, Lund Institute of Technology, Lund, Sweden.

Elmqvist, H. & Mattsson, S.E. & Otter, M., 2014. Modelica extensions for Multi-Mode DAE Systems. *Proceedings of the 10th international Modelica conference,* Lund, Sweden, March 10–12, 2014.

Heidtmann K.D., 1989. Smaller Sums of Disjoint Products by Subproduct Inversion. *IEEE Transactions on Reliability* (Vol. 38, No. 3): pp. 305–311.

Krumke, S.O. & Noltemeier, H., 2012. *Graphentheoretische Konzepte und Algorithmen*. Vieweg+Teubner Verlag, 3. Auflage. In German.

The Modelica Association, 2000. *Modelica—A Unified Object-Oriented Language for Physical Systems Modeling*. Available at website: https://modelica.org/documents/ModelicaTutorial14.pdf/

Persson, U. & Schallert, C., 2001. *The 728 JET flight control system*. Deutscher Luft- und Raumfahrtkongress, Hamburg, Germany, September 2001.

Roberts, B. & Kroese, D.P., 2007. Estimating the number of s-t paths in a graph. *Journal of Graph Algorithms and Applications* (Vol. 11, No. 1): pp. 195–214.

Schallert, C., 2014 (to appear). *Integration of Safety and Reliability Analysis Methods with Object-Oriented Modelling*. PhD thesis, Technische Universität Berlin, Germany.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The use of on-board flight recorder in the modeling process of aircraft landing operations

P. Stańczyk & A. Stelmach
Warsaw University of Technology, Warsaw, Poland

ABSTRACT: In recent years the world observed great interest in air transport, which consequently leads to an increase in air traffic. Growing technology forces on air transport to meet the requirements of safety and economics of transport.

That is why it becomes important problem of mathematical modeling of the high degree of precision mapping of actual flights a mathematical model in the form of artificial neural network. In order to obtain a very good accuracy of mapping the actual flight, the studies have used actual data, whose source was the on-board recorder operating the flight.

During the analysis examined data from more than a dozen flights made EMB—170 aircraft on the same route but in different weather conditions. The results were analyzed in terms of qualitative and quantitative evaluation on the quality of the mapping by comparing the results obtained using the model developed with the results obtained from the recorder. Mapping the landing phase of an aircraft by means of an artificial neural network gives positive results.

Model developed based on actual data from on-board flight data recorder, can be used to create a simulation model used in the study of air traffic and to create flight crew training simulators.

1 INTRODUCTION

In the last century, have been increasing interest in air transport, which leads to increased air traffic. Constantly evolving technology forces air transport to meet the requirements of security and transport economics.

Then it becomes essential problem of mathematical modeling of the high degree of precision mapping of actual flights by mathematical model in the form of artificial neural network.

In order to obtain a very good accuracy of mapping the actual flight, studies have used actual data, which originated in the on-board recorder operating the flight.

2 LANDING PHASE

In the literature [5], is described as a landing operation of the aircraft transitions from flight to ground operations. This should be carried out into the wind. This helps reduce the ground speed, shorten the landing run and avoid lateral drift [3].

Landing is the last stage of the flight, which consists in bringing the aircraft to the airport. Approaching the landing is the most complex stage of the aircraft's flight, called Critical phases of flight [1].

At this stage, the aircraft approaches the surface of the earth, and the flight is at a variable height and in variable—speed wind [4].

During the landing phase is distinguished by the following steps: final approach to landing, supply, alignment, endurance, touchdown and roll (Fig. 1).

At presented below figure shows the change in position (value) parameters were determined by which individual segments. The main factors affecting the course of the flight phase include: chassis, flaps position and speed of the aircraft.

For the landing maneuver the aircraft pilot gives a configuration, through a series of operations at specific stages of the flight. Each airport has a personalized procedure for landing on the runway.

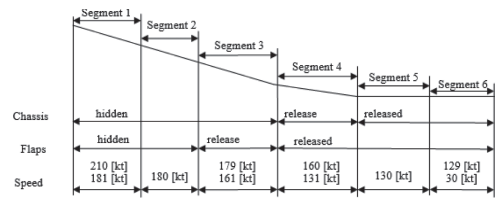


Figure 1. Schematic landing phase of aircraft [own elaboration].

During the study utilized the data from the EMB 170 aircraft landing on the road 11 (RWY 11) at the Chopin airport in Warsaw.

3 FLIGHT DATA RECORDER

Flight recorders are devices that are designed to save and protect the information from the course of the flight, the main parameters include [6]:

- Flight parameters (ex. position, time, attitude, pressure altitude, arte of climb, heading, true air speed, distance above surface),
- Parameters of the drive unit,
- The location of the controls by air,
- The status of individual devices and systems,
- Background sound in the aircraft, including radio communication and internal communications,
- Image from cameras onboard instruments working.

The sources of information for the recorder are:

- On-board systems,
- Transmitters angular displacements,
- Linear encoders,
- Transmitters motion (spatial position, angular velocity, acceleration),
- Transmitters parameters of the environment surrounding the aircraft (the atmosphere).

Most information is processed in block acquisitions. To the recorder provided the following signals:

- Analog,
- Digital transmitted by interfaces (Bus),
- Binary.

Recorders qualifies for flight control objective, making it a priority element having an impact on raising the level of flight safety and prevention of air accidents. They are used, among others, to control the remote piloting techniques.

Thanks to new technologies, the information obtained from the "black boxes" have enabled flight animation, and their simulation, which enables the efficient training of the flight crew. Thus it can be seen that the objective measures of flight control are crucial in the training of pilots.

Recorders on aircraft appeared from the very beginning. Brothers Wilbur and Orville Wright documented its first flight recording engine speed, the distance traveled and the time of flight. The first flight across the Atlantic made by Charles Lindberg in 1927 was registered by the barograph.

The Flight Data Recorder (FDR) has been around for more than 70 years. The first unit was invented in 1939 and slowly developed into a useable flight unit in the late 1940s. It wasn't until 1954 that the Cockpit Voice Recorder (CVR) was invented.

The first FDR systems were rather simplistic because they were entirely electro-mechanical units which utilized specific foil as the recording media which motored between spools, and had five styluses that scratched readings for altitude, heading, vertical accelerations, airspeed and time on one-side of the foil. Soon this system was enhanced by adding three more styluses on the opposite side of the foil, thus adding roll, pitch, and flap information.

The literature distinguishes four basic classification recorders [6]:

1. Flight data recorders FDR (Flight Data Recorder):
   - Catastrophic,
   - Consumables.
2. Special recorders.
3. Image DVR (Digital Video Recorder).
4. Sound CVR (Cocpit Voice Recorder).

With the arrival of the Solid State, the Digital Flight Data Recorder—both the survivability and reliability of this valuable monitoring system leapt, thanks to the elimination of tapes, drive motors, drive belts, and all other moving parts that were necessary with all previous versions. So that they become more popular and used in commercial aircraft.[2]

During the study were used data from flight data recorder FDR.

4 MODELING PROCESS

For the analysis of the landing phase of an aircraft based on data obtained the actual flight recorders. All flights were performed during similar meteorological conditions.

Data obtained from the recorder board included:

CAS - Calibrated Airspeed,

GSPED - Ground Speed - speed relative to the earth's surface,

LAT - Latitude,

LONG - Longitude,

LOACC - Long Acceleration,

MHEAD - Magnetic Heading,

N1 - N1 Engine,

Pitch - Pitch Attitude—the horizontal position,

PRALT - Pressure Altitude,

RALT - Radio Altitude—the height of the radio,

VACC - Normal Acceleration,

AGSW - Air/Ground Sensor—position indicator ground/air,

AT - Auto Throttle Engaged—sensor readings of the recording: the location on the ground or in the air, moments when the crew are broadcast radio messages, signaling the inclusion of auto throttle,

FLAPS - Flaps Position Angle,

GW - Gross Weight—the total weight of the aircraft [kg],

LGPOS_L - Left Main Landing Gear Position—position of the chassis,

TAT - Total Air Temperature,

WND_DIR - Wind Direction,

WND_SPD - Wind Speed,

local time.

The first step was the selection of the data in terms specify only those that described the landing phase, on the basis of the above data.

Then had to extract individual segment of the test flight phase, as presented in Figure 1.

Another important activity for the analysis was conducted of data normalization. The values were normalized according to the formulas presented below:

- mapped parameter flight (flight speed):

$$\overline{y}_i = \frac{y_i - y_{min}}{\Delta y} \tag{1}$$

where:

- i—measurement number,
- $\Delta y = y_{max} - y_{min}$

- mapped flight parameter (time):

$$\overline{t}_l = \frac{t_i - t_{\min}}{\Delta t} \tag{2}$$

where:

- $\Delta t = t_{max} - t_{min}$

If $y_i = y_{min}$ then $\overline{y}_l = \frac{0}{\Delta y} = 0$

If $y_i = y_{max}$ then $\overline{y}_l = 1$.

In this way, the prepared data are implemented to the artificial neural network.

5 OPERATION MODEL

The prototype of all the neural network is the human brain. The neural network is substantially simplified model of the brain. It consists of a large number (several hundred to several thousand) information processing elements, called neurons.

Neurons are linked in a network with connection parameters (weights) modified during the so-called learning process. Topology of connections and their parameters are the program activities of the network, and the signals appearing at its output in response to the output signals are solutions against her tasks.

Most recently built and used in a neural network has a layered structure, during the learning process divided into the following layers:

- the input,
- output,
- hidden layer [7–10].

The paper input signals are stored in vector form (Fig. 2):

$$X^T = [t, s, V_{i-2}, V_{i-1}] \tag{3}$$

where:

- t - time [s],
- s - segment [-],
- V_{i-2} - the speed at the moment of i- 2 [kt]
- V_{i-1} - the speed at the moment of i- 1 [kt].

The output of the airspeed at the time (i) (vi).

In the presented neural network is used neuron as in Figure 3.

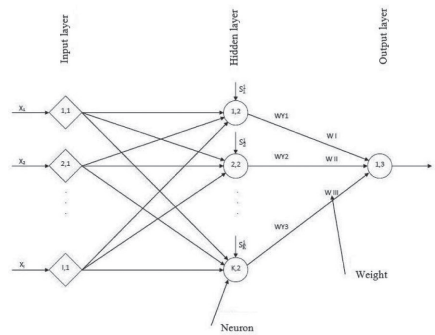


Figure 2. Schematic of a multilayer neural network [own elaboration].

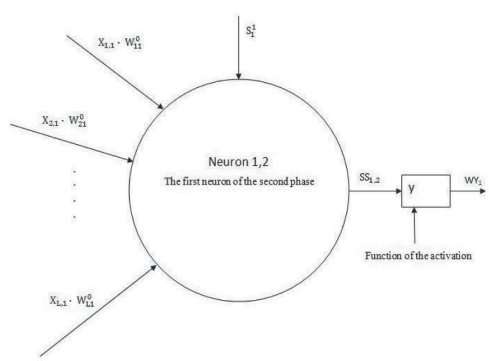


Figure 3. Neuron used in the modeling of neural networks. Function of the activation [own elaboration].

As presented above neuron output of the first neuron is the sum of the input x_{11}, x_{21}, ..., x_{L1}, multiplied by the weight wo_{11}, wo_{21}, ..., wo_{L1} and constant s_{11}.

The output signal $ss_{1,2}$ has the form:

$$SS_{1,2} = x_1(1,1) \cdot w_1(1,1) + s_1^1 \tag{4}$$

where:

$X_1=[x_{1l}, \ldots, x_{Ll}]$;
$W_1=[w^0_{11}, \ldots, w^0_{L1}]$.

Furthermore, the activation function was used in the form of:

$$y = \frac{1}{1+\exp(-2y_w)} \tag{5}$$

The essence of the development of the ANN is to determine the weights and fixed using the results of the registration board flights. For the algorithm used to create the torque back propagation method, in which the variables are constant learning α and η momentum.

Assessment of the accuracy of the mapping is determined by the sum of squared differences between the model and the real object and the number of positive events. The next step is to test the accuracy of the determination or the network compared input and output signals from the network [7].

6 RESULTS

In tests, examined data from more than a dozen flights EMB 170 aircraft. The research shows that the structure of the network, which accurately reproduces the landing phase of an aircraft EMB-170 is a network with four inputs, two hidden layers respectively five and four neurons and one output (4541).

Table 1 lists the results obtained by assessing the accuracy of the mapping model in an artificial network of the actual speed during the landing phase of flight of the EMB 170 aircraft.

The results are shown for different neural network structures. The number of neurons the input and output layer is always the same, respectively 4 and 1, and the change in the number of hidden layers and the number of them occurring in neurons.

The presented network structures shows that the EMB-170 aircraft network with structure 4541 (4 inputs, 1 output and 2 hidden layers with 5 and 4 neurons) generates the lowest value of χ2, which means that the selected structures is this best matches the actual flight. The number of events for the presented flight was 190, as can be seen all the tested structure gave 100% the number of positive events.

Also checked the extent to which a change in the momentum η and constant learning α affects the accuracy of the mapping.

The results obtained clearly define the impact of a constant learning and the momentum mapping accuracy landing speed by ANN.

The following graph shows the results. Figure 4 shows a comparison of the speed of the aircraft with registration and on-board artificial neural network for the EMB 170 aircraft.

V_{lot} course presents the actual speed of the on-board flight recorder, V_{SSN-D} velocities of the ANN with the best degree of mapping and V_{SSN-Z} the speed of the SSN of the worst degree of mapping the actual flight.

From the obtained results it can be concluded that, for the EMB 170 aircraft in the initial landing phase, the neural network very well reproduces the speed of the aircraft. In the final step results in inferior image.

Table 1. Rating accuracy of mapping the actual landing phase by SSN with different structures.

No	No of neurons in the hidden layer		No of positive events [%]	χ^2av
1	2	0	100	$0{,}51060 \cdot 10^{-3}$
2	3	0	100	$0{,}41722 \cdot 10^{-3}$
3	4	0	100	$0{,}29450 \cdot 10^{-3}$
4	5	0	100	$0{,}41122 \cdot 10^{-3}$
5	6	0	100	$0{,}44352 \cdot 10^{-3}$
6	2	2	100	$0{,}53347 \cdot 10^{-3}$
7	3	2	100	$0{,}52562 \cdot 10^{-3}$
8	4	2	100	$0{,}51354 \cdot 10^{-3}$
9	5	2	100	$0{,}51225 \cdot 10^{-3}$
10	2	4	100	$0{,}49822 \cdot 10^{-3}$
11	3	4	100	$0{,}40185 \cdot 10^{-3}$
12	4	4	100	$0{,}39590 \cdot 10^{-3}$
13	5	4	100	$0{,}39959 \cdot 10^{-3}$

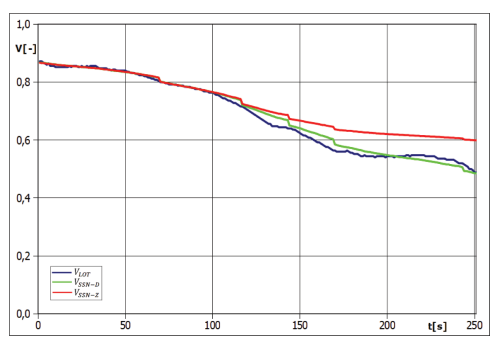


Figure 4. Speed course of the aircraft with registration board and ANN [own elaboration].

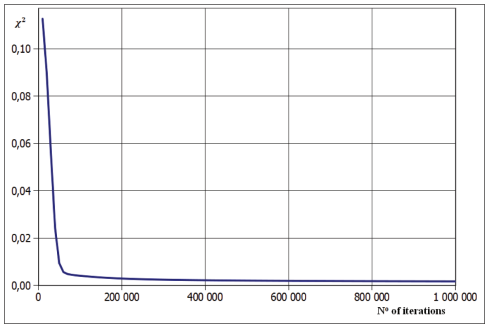


Figure 5. The process of learning artificial neural network with the best structure [own elaboration].

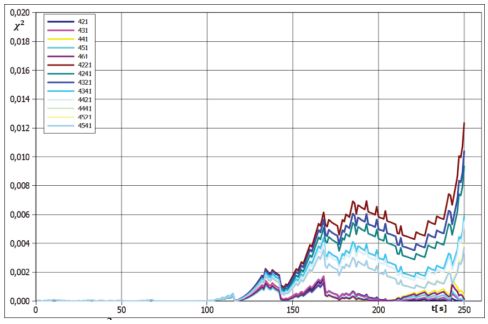


Figure 6. X^2 value as a function of the duration of the landing phase of flight for the various structures [own elaboration].

7 CONCLUSIONS

During the analysis examined data from more than a dozen flights made EMB-170 aircraft on the same route but in different weather conditions. The results were analyzed in terms of qualitative and quantitative evaluation on the quality of the mapping by comparing the results obtained using the model developed with the results obtained from the recorder. Mapping the landing phase of an aircraft by means of an artificial neural network gives positive results.

Yes developed models can be used to create simulation models used to study air traffic, as well as training simulators. Unfortunately drawback of this method is time-consuming very large data associated with the preparation and testing of the network.

REFERENCES

Air OPS, commercial air transport, related EASA decisions (AMC & GM), 2013.

Code of Federal Regulations, Title 14.

Domicz, J., Szutowski, L, 1998. *Podręcznik pilota samolotowego*, wydanie drugie rozszerzone, Technika, Poznań.

Fiedczyn S.S., 1974. *Nawigacja lotnicza*, WKŁ, Warszawa.

Malarski, M., 2006. *Inżynieria ruchu lotniczego*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Polak Z., Rypulak A., 2000. *Awionika, przykłady i systemy pokładowe*, część II, Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych Katedra Techniki Lotniczej, Dęblin.

Stelmach A., Manerowski J., 2011. Identyfikacja modelu matematycznego operacji lądowania samolotu, *Czasopismo Logistyka*, nr 4/2011, Poznań.

Stelmach A., 2014. *Identyfikacja modeli matematycznych faz lotu samolotu*, OWPW, Warszawa.

Stelmach A., 2011. Modeling of the selected aircraft flight phases using data from flight data recorder, *Archives of Transport*, vol. XXIII, no.4, pp. 541–555, Warsaw.

Tadeusiewicz R., 1993. *Sieci neuronowe*, Akademicka Oficyna Wydawnicza, Kraków.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability analysis for Runway Overrun using subset simulation

K. Zwirglmaier
Engineering Risk Analysis Group, Technische Universität München, Germany

L. Drees & F. Holzapfel
Institute of Flight System Dynamics, Technische Universität München, Germany

D. Straub
Engineering Risk Analysis Group, Technische Universität München, Germany

ABSTRACT: Runway overrun is one of the main accident types in airline operations. Nevertheless, due to the high safety levels in the aviation industry, the probability of a runway overrun is small. This motivates the use of structural reliability concepts to estimate this probability. We apply the physically-based model for the landing process of Drees and Holzapfel (2012) in combination with a probabilistic model of the input parameters. Subset simulation is used to estimate the probability of runway overrun for different runway conditions. We also carry out a sensitivity analysis to estimate the influence of each input random variable on the probability of an overrun. Importance measures and parameter sensitivities are estimated based on the samples from subset simulation and concepts of the First-Order Reliability Method (FORM).

1 INTRODUCTION

The airlines organized in the International Air Transport Association (IATA) carried about 3.6 billion passengers in 2012. Among these, 414 where killed in an aviation accident (IATA, 2013). Of the many accident types, runway excursion is the most common one. There are several types of runway excursions; one of the most critical one is runway overrun (RWO) of a landing aircraft, which is investigated in this paper.

The high safety requirements within the civil aviation industry make a quantitative estimation of the probability of a runway excursion important. However, the already high reliability standards within the industry hinder an estimation of accident probabilities with purely statistical methods. In particular, it is difficult to investigate the effect of individual factors on the probability of specific accidents. This motivates the use of structural reliability concepts. This is demonstrated in this paper, where we estimate the probability of runway overrun using a previously proposed physically-based model for the landing process (Drees and Holzapfel, 2012).

A few authors proposed RWO models based on regression e.g. (Kirkland, 2001, Hall et al., 2008, Ayres Jr. et al., 2011). However, to the best of our knowledge, structural reliability methods in combination with a physically-based model have not been applied previously.

In the next section a short outline to structural reliability in general and subset simulation in particular is given. This is followed by a summary of the RWO model and the related probabilistic model. Thereafter, the results of the reliability analysis are presented for different runway conditions. The influence of the individual input random variables on the probability of a RWO is investigated through different importance and sensitivity measures. In this context, FORM is shortly explained, as some of its theory is applied. The paper concludes with a discussion of the results.

2 STRUCTURAL RELIABILITY

In reliability analysis, $\mathbf{X}$ denotes a vector of random variables that are the input to a model; $\mathbf{X}$ has the joint probability density function $f(\mathrm{X})$. The response of the physical model as a function of $\mathbf{X}$ is described by means of Limit State Functions (LSF) $g(\mathbf{X})$. For RWO, $g(\mathbf{X})$ corresponds to the stop margin of the aircraft, i.e. the length of the runway minus the operational landing distance (the distance actually needed to stop the aircraft). A runway overrun corresponds to the event $g(\boldsymbol{X}) \leq 0$ and its probability can be written as:

$$\Pr(RWO) = \int_{g(\mathbf{X})\leq 0} f(\mathbf{X}) d\mathbf{X} \tag{1}$$

This type of problem is well known within the field of structural reliability, which is concerned with estimating probabilities of failure of engineering structures (Rackwitz, 2001). As the integral in Equation (1) can in general not be calculated analytically, a number of methods for efficiently solving this kind of problems have been developed in the field of structural reliability. The most prominent among these are the first—and second-order reliability methods (FORM and SORM) e.g. (Der Kiureghian, 2005), the standard Monte Carlo Simulation (MCS), and advanced sampling methods like importance sampling or subset simulation (SuS) (Au and Beck, 2001).

Both FORM and SORM rely on finding the Most Likely Failure Point (MLFP), i.e. the most likely realization of $\mathbf{X}$ that leads to failure, here RWO. These methods are based on optimization for finding the MLFP. This may be critical if the method is to be applied for the computation of the probability of RWO in near-real time. For this reason, we apply SuS, which is still relatively efficient, but does not necessitate optimization.

2.1 *Subset simulation (SuS)*

The classical MCS approach provides an unbiased estimate $\hat{P}_F$ of Equation (1) by generating n_S samples from the joint distribution $f(\mathbf{X})$ and evaluating $g(\mathbf{X})$ for each of the samples. The estimated probability of failure is then:

$$\hat{P}_F = \frac{1}{n_S}\sum_{i=1}^{n_S} I_{g(\mathbf{X}_i)\le 0}(\mathbf{X}_i) \tag{2}$$

where $I_{g(\mathbf{Xi})\le 0}(\mathbf{X_i})$ is an indicator function, which is 1 for $\mathbf{g}(\mathbf{X_i}) \le 0$ and 0 otherwise. This MCS approach becomes computationally unfeasible for small probabilities of failure. For a desired coefficient of variation of the estimate $\delta_{\hat{P}_F}$ the required number of samples is:

$$n_S = \frac{1-\Pr(F)}{\delta^2_{\hat{P}_F}\Pr(F)} \tag{3}$$

For a small probability of failure of $\Pr(F) = 10^{-8}$ and a desired coefficient of variation of $\delta_{\hat{P}_F} = 0.1$ approximately 10^{10} LSF evaluations would be necessary. SuS proposed by (Au and Beck, 2001) overcomes this problem by expressing the failure event F as a sequence of nested events F_i.

$$F_1 \subset F_2 \subset \cdots \subset F_n = F$$

With these nested events the probability of failure can be rewritten as:

$$\Pr(F) = \Pr(F_1)\prod_{i=2}^{n}\Pr(F_i|F_{i-1}) \tag{4}$$

The probability of the first intermediate event, $\Pr(F_1)$, is not conditional on a previous intermediate event and can therefore be estimated with a standard MCS. All other probabilities $\Pr(F_i|F_{i-1})$ in Equation (4) are conditional on a previous intermediate event, these conditional probabilities are estimated using Markov Chain Monte Carlo (MCMC) simulation procedures. In Figure 1 the MCMC approach is schematically shown for estimating $\Pr(F_2|F_1)$. The grey points represent the samples generated from $f(\mathbf{X})$ in the initial MCS step. Those samples $\mathbf{X}_i$, which are above the LSF (shown here as a black line) are said to be in the failure domain F_1, i.e. for them $\mathbf{X}_i \in F_1$. From each of those m intermediate failure samples, a Markov Chain of length n_S/m is generated (black samples). In these chains a new candidate state is generated conditional on the previous state of the chain. Furthermore if the newly generated candidate state $\mathbf{X}'$ fulfills the condition $\mathbf{X}' \in F_1$ it becomes the new state of the chain otherwise the previous state is repeated. SuS is performed in the uncorrelated standard normal space (U-Space). The component wise Metropolis Hastings algorithm, which was proposed by (Au and Beck, 2001) as a MCMC algorithm for SuS makes use of this by generating the candidate states independently for each dimension. The performance of SuS thus becomes independent of the number of dimensions of the problem.

In this paper we apply a MCMC algorithm proposed by (Papaioannou et al., 2014) for use in SuS. Like the algorithm of (Au and Beck, 2001) this algorithm works in a component-wise fashion and its performance is therefore also independent of the dimensionality of the problem. However, the generation of the pre-candidate states is done, such that every pre-candidate state is accepted.

Typically the intermediate failure events F_i are chosen adaptively, such that $\Pr(F_1) = \Pr(F_2|F_1) = \cdots = \Pr(F_{n-1}|F_{n-2}) = p_0$. Often a value of 0.1 is chosen for p_0. The final failure event $F_n = F$ is fixed and therefore its conditional probability cannot be chosen a priori. Equation (4) is then:

$$\Pr(F) = p_0^{\,n-1}\Pr(F \mid F_{n-1}) \tag{5}$$

As SuS is applied in U-space the random variables $\mathbf{X}$ have to be transformed to U-space. Typically the Nataf or the Rosenblatt transformations are applied for this purpose (Hohenbichler and Rackwitz, 1981). In the problem at hand one of the random variables is defined conditional on other random variables. For that reason the Rosenblatt

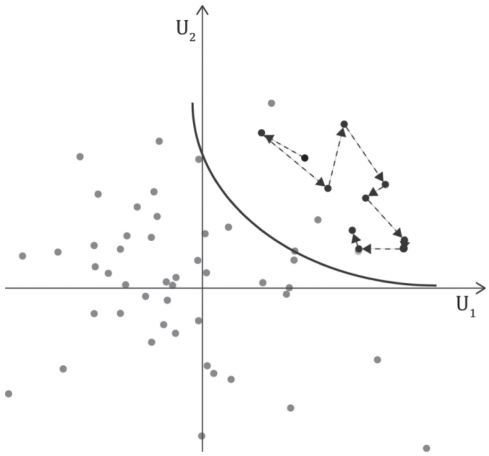


Figure 1. Generation of samples conditional on a first intermediate failure event. The new samples (black) are sampled starting from a seed sample using a MCMC algorithm. The grey samples were obtained by MCS in a previous step.

transformation appears to be suitable. This transformation is based on expressing the distribution of every random variable conditional on the previous random variables.

3 PHYSICAL MODEL OF RUNWAY OVERRUN (RWO)

In this section, we *briefly* present the applied RWO model. For a more detailed description, the reader is referred to the original paper by (Drees and Holzapfel, 2012). The RWO event can be defined as the operational landing distance exceeding the runway length (Fig. 2). The LSF can therefore be written as:

$$g(\mathbf{X}) = \textit{Stop margin}\ (\mathbf{X})$$

The stop margin is the deterministic runway length minus the operational landing distance, which depends on a number of factors that are modeled as random variables. The model is derived from the equations of motion. The acceleration of the aircraft in x-direction is:

$$\dot{V} = \frac{1}{m}[T - D - mg \cdot \sin\gamma - \mu_F(mg \cdot \cos\gamma - L)] \quad (6)$$

where m is the mass of the aircraft, T is the propulsion force from the aircraft engines and D is the aerodynamic drag. The term $mg \cdot \sin\gamma$—with g being the constant of gravitation and γ the flight path angle—represents the contribution of the runway slope to the acceleration. Finally, the last term describes the influence of the friction and brake forces. L denotes the aerodynamic lift and μ_F the friction coefficient, which depends on the runway condition, on the brake force and on the velocity of the aircraft.

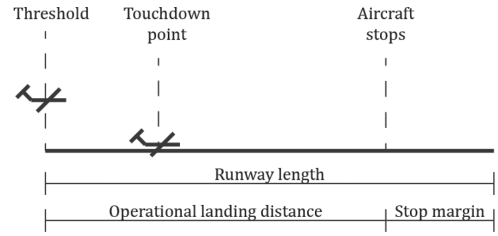


Figure 2. Definitions.

The drag force can be written as:

$$D = \frac{\rho}{2}(V_K - V_W)^2 S \cdot C_D \quad (7)$$

and the lift force as:

$$L = \frac{\rho}{2}(V_K - V_W)^2 S \cdot C_L \quad (8)$$

ρ is the air density, V_K is the speed of the aircraft and V_W the speed of the surrounding air, such that $V_K - V_W$ is the speed of the aircraft relative to the wind speed. Furthermore, S is the reference area of the wings and C_D respectively C_L are the drag and the lift coefficients.

Integrating equation (6) twice with respect to time will yield the operational landing distance. For practical reasons the operational landing distance is split in three parts. First the touchdown distance, which is directly modeled as a random variable; second the distance from the touchdown point to the point where the pilot deactivates the auto-brake system, which, in addition to the environmental and technical factors, depends on a number of human factors, e.g. the point in time until the pilot starts braking and the point in time when the spoiler is deployed. The third part is the distance the aircraft travels from the point of auto-brake deactivation to the final stopping position. During a normal landing, the aircraft will not stop completely on the runway but exit the runway with slow velocity to the taxiways. However, it is assumed that in the case of a critical landing, which is likely to result in a RWO, this distance is traveled with maximum deceleration efforts i.e. maximal braking forces.

Table 1. Random variables of the physical model. The pressure is the air pressure adjusted to the sea level. Approach speed deviation is the deviation from the target approach speed. The mean value of the touchdown point depends on the calculated required landing distance, which again is a function among others of the headwind, the landing weight and the temperature. Abbreviations: weibull distribution (WBL), normal distribution (N) and generalized extreme value distribution (GEV).

Random variable	Distribution model	Mean	Std. dev.
Landing weight [t]	WBL (60.0,44.3)	59.3	1.69
Head wind [kts]	N (5.4,5.8)	5.4	5.8
Temperature [°C]	GEV (–0.26,7.9,6.5)	9.4	8.0
Pressure [hPa]	N (1016,8.1)	1016	8.1
Appr. speed dev. [kts]	GEV (–0.20,4.0,3.0)	4.7	4.2
Rev. deployment [s]	Gamma (9.0,0,55)	5.0	1.7
Start braking [s]	GEV (0.15,3.9,10.2)	13.1	6.4
Splr. Deployment [s]	GEV (0.11,0.89,3.7)	4.3	1.3

3.1 *Technical and human factors*

The quantities in the differential Equation (6) are influenced by environmental factors on the one hand, and technical as well as human factors on the other hand. The technical aspects are captured in the RWO model by allowing certain technical components like the spoiler, the auto-brake system or the engines to be either operative or inoperative with a certain probability. The brake system can be operative, inoperative or degraded. In the scope of this paper we do not consider any technical failures, thus all components are considered to be fully operative. Furthermore, we assumed the flaps and slats to be in configuration full, which is used in 96% of approaches (Drees and Holzapfel, 2012).

The friction coefficient between the tire and the runway μ_F is a major factor influencing the deceleration of the aircraft. This friction coefficient is mainly determined by the runway condition; we differ between a dry and a wet runway in our calculations.

The auto-brake system automatically applies a brake pressure when the landing gear touches ground. The magnitude of the applied pressure depends on the setting of the auto-brake system. For the scope of this paper, we compute RWO probabilities for the auto-brake settings set to medium.

In operational aviation, the times after touchdown at which the spoiler and thrust reversers are deployed and the times at which the braking starts and ends can be obtained from operational data. On the basis of this measured data, distribution models are selected. These models are summarized in. Another factor, whose variability is influenced mainly by human actions, is the touchdown point. A normal distribution, with fixed standard deviation and a mean value (μ_{TDP}) that is a function of the environmental conditions is used for this. It was found from flight operation data that pilots change their touchdown behavior according to the required landing distance estimate, which they calculate during the approach. The required landing distance is thereby calculated from aircraft and runway specific characteristics as well as from the flap setting, the head wind, the temperature and the landing weight.

4 PROBABILITY OF A RWO

As a case study, we calculate the RWO probabilities for an aircraft of type Airbus A320 landing on runway EDDM 26 L at the Munich airport (MUC). The runway is 4000 m long with a concrete surface. We apply subset simulation using the MCMC algorithm proposed in (Papaioannou et al., 2014). The inter-sample correlation is initially chosen as 0.8. The intermediate thresholds were chosen adaptively, such that at each simulation level 10% of the samples would lie in the intermediate failure region. At each of the simulation levels, 1000 samples were generated such that considering the presented results in Table 2 7000 respectively 8000 LSF evaluations were necessary for each simulation run.

The resulting probabilities are in the same order of magnitude for the different runway conditions.

The fact that the RWO probabilities are smaller for a wet runway than for a dry one may be counterintuitive, as a wet runway reduces the friction between the tire and the runway and thus also the effectiveness of the braking procedure.

The explanation for this result is that the pilots calculate the required landing distance according to an approximate formula when approaching an airport and adapt their landing behavior to the

Table 2. Simulation results for different runway conditions (dry and wet). For each simulation 1000 samples were used per simulation level.

Runway condition	$P_r(RWO)$
Dry	1.06E – 7
Wet	7.03E – 8

result. In the model this is accounted for through the mean value of the touchdown point. The inferior grip of the tires is therefore compensated or even overcompensated by an adapted touchdown behavior, at least according to the model.

5 SENSITIVITY ANALYSIS

We conduct a sensitivity analysis to find the influence of the individual random variables on the probability of a RWO. First importance measures based on FORM are calculated. For the most important random variables, parameter sensitivities are then calculated based on the samples from subset simulation. In the following the concepts of FORM, which are of major importance for our purpose are introduced. For a deeper introduction the reader is again referred to the literature e.g. (Der Kiureghian, 2005, Ditlevsen and Madsen, 2007). In a later section parameter sensitivities are calculated using the samples from SuS.

5.1 *Importance measures with FORM*

FORM gives an approximation of Equation (1) by substituting the LSF in U-space with a linear surrogate model $g_L(\mathbf{u})$. The linearization of the LSF is done in the design point i.e. the most likely failure point $\mathbf{u}^*$ in U-space. The probability of failure Pr(F) can then be approximated through the probability of failure corresponding to the linear surrogate model. With Φ being the standard normal CDF and β_{FORM} the reliability index Pr(F) can be approximated as:

$$\hat{P}_F = \Phi(-\beta_{FORM}) \tag{9}$$

With the reliability index being defined as:

$$\beta_{FORM} = |\mathbf{u}^*| \tag{10}$$

The task of calculating the probability of failure reduces thus to finding the design point $\mathbf{u}^*$. In general the convergence of the optimization algorithms, applied to find $\mathbf{u}^*$ is the bottleneck in FORM analysis.

A useful byproduct of the FORM analysis is the normal vector of the linear approximation of the LSF $\boldsymbol{\alpha}$ (Der Kiureghian, 2005). The elements of this vector can be interpreted as importance measures of the standard normal random variables U_i (Figure 1):

$$\alpha_i = \frac{u_i^*}{\beta_{FORM}} \tag{11}$$

If a random variable U_i is the only one influencing $\hat{P}_F$ its corresponding α_i will have an absolute value of 1. If on the other hand U_i has no influence on $\hat{P}_F$ its α_i is 0. We can further distinguish between random variables of load type, which have a positive α_i and those, which are of capacity type that correspond to a negative α_i.

If the random variables in $\mathbf{X}$ are independent the importance measures $\boldsymbol{\alpha}$ of the transformed variables $\mathbf{U}$ are readily valid also in the original space otherwise a transformation as described in (Der Kiureghian, 2005) needs to be applied.

In the scope of this paper the FORM importance measures are determined for a linear LSF fitted to sample points as proposed in (Melchers and Ahammed, 2004). Thus the optimization usually necessary for FORM, which is a bottleneck especially in near-real time applications, is circumvented. Fitting a linear hyper-plane to a set of points is a robust way to estimate the design point according to (Melchers and Ahammed, 2004). As the linear LSF $g_L(\mathbf{u})$ should approximate the actual LSF as accurately as possible mainly in the proximity of the design point/limit state surface it is suggested to only use those sample points $\mathbf{u}$, for which $g_L(\mathbf{u}) \approx 0$ or $g_L(\mathbf{u}) \leq 0$.

The sensitivity analysis is done in this paper for a dry runway. A simulation run with 1000 samples per simulation level was done to this end and the samples from the last simulation step were used to fit the linear LSF with the method of least squares.

In Table 3 the FORM importance measures for the problem at hand are summarized. The numbers in brackets give the values for a linear LSF that was fitted to sample points from a different simulation run.

'Head wind', 'Start braking', 'Touchdown point', Approach speed deviation' and 'Landing weight' appear to be the random variable, having the most influence. All of them are of load type except head wind, which is of capacity type meaning that a large head wind velocity reduces the probability of a RWO.

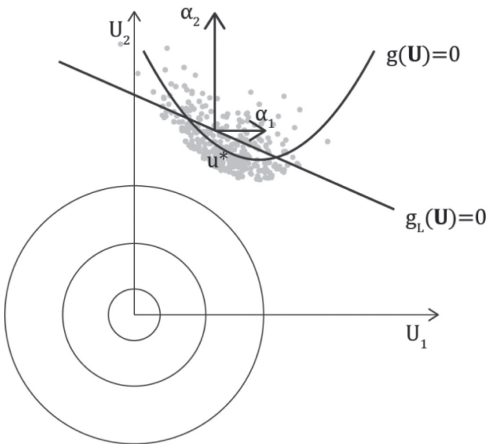


Figure 3. Importance measures α of linear LSF approximation fitted to samples from a SuS run.

Table 3. FORM importance measures for the dry runway conditions and a flap setting medium.

Random variable	FORM	Measures
Landing weight [t]	0.116	(0.138)
Head wind [kts]	–0.693	(–0.663)
Temperature [°C]	0.020	(0.010)
Pressure [hPa]	0.010	(0.002)
Appr. speed dev. [kts]	0.202	(0.179)
Rev. deployment [s]	0.037	(0.042)
Start braking [s]	0.650	(0.680)
Splr. Deployment [s]	0.019	(–0.013)
End braking [s]	0.004	(0.013)
Touchdown point [m]	0.204	(0.213)

From Table 3 it becomes obvious that the linear LSF depends on the points used for fitting. However the results show that the measures for the variables with a large influence (i.e. > |0.1|) are fairly similar in both runs while the variables that have only a minor influence are in one case even of different type (i.e. load or capacity) in the two runs.

Although the 'Touchdown point' is one of the main influencing factors according to the FORM measures one may expect it to have an even larger influence. The reason for that is, that it was modeled as a function with fairly low variability and a mean, which is shifted according to the outcome of other random variables.

In general it should be noted that the FORM importance measures in Table 3 are dependent on the distributions of the random variables. For example from the fact that the pressure appears to have only a minor influence in the case study at hand it cannot be concluded that the pressure may not be an important factor if one considers different airports, where some of them are located at high altitudes.

5.2 *Sensitivity measures*

For the random variables, which were found to be important according to the FORM importance measures, parameter sensitivities are calculated. We calculate sensitivities of the probability of failure with respect to the parameters of $f(\mathbf{X})$, $\boldsymbol{\theta}$. These sensitivities can be defined as:

$$\frac{\partial \hat{P}_F}{\partial \theta_i} = \int_{g(\mathbf{X})\leq 0} \frac{\partial f_{\mathbf{X}}(\mathbf{X},\boldsymbol{\theta})}{\partial \boldsymbol{\theta}_i} d\mathbf{X} \tag{12}$$

where $f_{\mathbf{X}}(\mathbf{X}, \boldsymbol{\theta})$ is the probability density function of X with the parameters $\boldsymbol{\theta}$. $\boldsymbol{\theta}_i$ denotes the parameter with respect to which the sensitivity is calculated. In the scope of this paper we consider sensitivities with respect to the means μ_i and standard deviations σ_i of the random variables X_i.

Based on the calculated FORM approximation of the LSF, sensitivities of the form $\partial \Pr(F)/\partial \boldsymbol{\theta}$ can be calculated as described in (Der Kiureghian, 2005). These approximate sensitivities can be calculated based on a design point, which was obtained using an optimization algorithm. In a near real-time context, where convergence of the optimization algorithms may be critical this can be done also based on a linear LSF fitted to samples, as already described. Here we calculate the sensitivities with respect to the mean values μ_i and standard deviations σ_i directly from the samples obtained from SuS. The parameter sensitivities can be written as:

$$\frac{\partial \hat{P}_F}{\partial \theta} = \sum_{i=1}^{n} \frac{\hat{P}_F}{P_i} \frac{\partial P_i}{\partial \theta} \tag{13}$$

where P_i are the (un)conditional failure probabilities corresponding to the intermediate failure events i.e. $P_1 = \Pr(F_1)$ and $P_i = \Pr(F_i|F_{i-1})$ for $i > 1$. The derivative of the intermediate failure probabilities can be estimated using the samples obtained in subset simulation (Song et al., 2009):

$$\frac{\partial P_i}{\partial \theta} \approx \frac{1}{N} \sum_{k=1}^{N} \left[I_{F_i}(\mathbf{X}_k) \left(\frac{1}{f_{\mathbf{X}}(\mathbf{X}_k)} \frac{\partial f_{\mathbf{X}}(\mathbf{X}_k)}{\partial \theta} - \sum_{j=1}^{i-1} \frac{1}{P_i} \frac{\partial P_j}{\partial \theta} \right) \right] \tag{14}$$

where $I_{F_i}(\mathbf{X}_k)$ denotes the indicator function, which is 1 if $\mathbf{X}_k \in F_i$ and 0 otherwise.

Table 4. Elasticities of $\hat{P}_F$ with respect to μ_i and σ_i, calculated following Equation (13) and (15).

Random variable	$(\mu_i/\hat{P}_F)(\partial\hat{P}_F/\partial\mu_i)$	$(\sigma_i/\hat{P}_F)(\partial\hat{P}_F/\partial\sigma_i)$
Landing weight [t]	53,4	1.4
Head wind [kts]	–3.2	10.6
Appr. speed dev. [kts]	0.8	0.04
Start breaking [s]	1.1	56.0
Touchdown point [m]	–	1.0

In Table 4 the elasticities $\varepsilon_{\hat{P}_F,\theta}$ are shown for the five most important random variables according to the FORM importance measures from Table 3. Elasticities are defined as:

$$\varepsilon_{\hat{P}_F,\theta} = \frac{\theta}{\hat{P}_F}\frac{\partial\hat{P}_F}{\partial\theta} \tag{15}$$

They describe the relative change of probability of failure due to a relative change in the parameter θ and are in general easier to interpret than sensitivities.

6 CONCLUDING REMARKS

Structural reliability methods have been applied to estimate runway-overrun probabilities and were shown to be suitable for this purpose. In particular, the calculated sensitivities and FORM importance measures support the interpretation and further development of the model. With the help of the FORM importance measures, one can simplify the model by modeling the quantities of minor importance deterministically. We have found that the parameters 'Temperature', 'Pressure', 'Reverser deployment', 'Spoiler deployment' and 'End breaking' may be modeled deterministically without inducing a large error. This does, however, not imply that the influence of these quantities is small. It can only be concluded that the uncertainty associated with the quantity is not significant. The parameter sensitivities were in this paper calculated based on the samples obtained with subset simulation. These parameter sensitivities describe the effect of a change of the mean or standard deviation on the probability of failure. We presented the parameter sensitivities in the form of elasticities, which are typically easier to interpret. From the results it can be seen that the variables, which are of main importance according to the FORM importance measures, are the most sensitive ones with respect to a change in the standard deviation (i.e. the variability).

A physically-based RWO model in combination with robust methods for reliability analysis could be applied in real time or near-real time risk assessment. A possible scenario would be an aircraft approaching an airport and getting gradually better information on uncertain factors like landing weight, head wind at the destination airport etc. Based on the calculated RWO probabilities a pilot could decide on whether it is save to land at the destination airport or to approach an alternate airport.

REFERENCES

Au, S.-K. & Beck, J.L. 2001. Estimation of small failure probabilities in high dimensions by subset simulation. Probabilistic Engineering Mechanics, 16, 263–277.

Ayres JR., M., Shirazi, H., Carvalho, R., Hall, J., Speir, R., Arambula, E., David, R., Wong, D. & Gadzinski, J. 2011. Improved Models for Risk Assessment of Runway Safety Areas. ACRP Report 50, Washington D.C.

Der Kiureghian, A. 2005. First- and Second-Order Reliability Methods. In: Nikolaidis, E., Ghiocel, D.M. & Singhal, S. (eds.) Engineering Design Reliability: Handbook. CRC PressINC.

Ditlevsen, O. & Madsen, H.O. 2007. Structural Reliability Methods. John Wiley & Sons.

Drees, L. & Holzapfel, F. 2012. Determining and Quantifying Hazard Chains and their Contribution to Incident Probabilities in Flight Operation. AIAA Modeling and Simulation Technologies Conference. American Institute of Aeronautics and Astronautics.

Hall, J., Ayres Jr., M., Wong, D., Eddowes, M., Shirazi, H., Speir, R., Pitfield, D., Caves, R., Selezneva, O. & Puzin, T. 2008. Analysis of Aircraft Overruns and Undershoots for Runway Safety Areas. ACRP Report 3, Washington D.C.

Hohenbichler, M. & Rackwitz, R. 1981. Nonnormal dependent vectors in structural safety. Journal of Engineering Mechanics, Trans. ASCE, 107(6), 1227–1238.

IATA 2013. Safety report 2012. International Air Transport Association (IATA).

Kirkland, I.D.L. 2001. The risk assessment of aircraft runway overrun accidents and incidents. PhD-Thesis, Loughborough University.

Melchers, R.E. & Ahammed, M. 2004. A fast approximate method for parameter sensitivity estimation in Monte Carlo structural reliability. Computers & Structures, 82, 55–61.

Papaioannou, I., Betz, W., Zwirglmaier, K. & Straub, D. 2014. MCMC algorithms for subset simulation. Manuscript

Rackwitz, R. 2001. Reliability analysis—a review and some perspectives. Structural Safety, 23, 365–395.

Song, S., Lu, Z. & Qiao, H. 2009. Subset simulation for structural reliability sensitivity analysis. Reliability Engineering & System Safety, 94, 658–665.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A meta model framework for risk analysis, diagnosis and simulation

H. Kanj & J.-M. Flaus
Université Grenoble Alpes, G-SCOP, Grenoble, France
CNRS, G-SCOP, Grenoble, France

ABSTRACT: This document represents an overview of the Function Interaction Structure (FIS) modeling, where the goal is to represent a system and the risk analysis that is made, and to obtain a simulation model from the risk analysis. This model is able to show the results of risk analysis. This model is supplemented by information on its behavior, in order to generate the dynamic model in degraded mode. Our proposed meta model is also used to analyze the risk associated with a system such as: evacuation system, transport of dangerous goods, ...

1 INTRODUCTION

The goal of risk analysis is to identify events that may have one or several undesirable consequences on a system, and to assess the likelihood and severity of these consequences. A lot of methods can be used to conduct risk analysis (Flaus, 2013a) such as Preliminary Hazard Analysis (PHA) and Failure Mode Effects Analysis (FMEA) (Papadopoulos et al., 2004). In most of these methods, the obtained information may be used to build a risk model. The next step after risk analysis is to study the behavior of the system, when the undesirable events occur, in order to evaluate its performance in degraded conditions, and its robustness or resilience. An approach to allow integrated risk analysis and simulation has been proposed for business process management (Tjoa et al., 2011).

The aim of this paper is to present a meta model, suitable to socio-technical systems. This model allows describing the system to analyze, the result of the risk analysis, and the required aspects of dynamical system behavior, in order to automatically perform simulation under degraded conditions. The model is an extension of the FIS model presented in (Flaus, 2011, Negrichi et al., 2012). The meta model may also be used for fault diagnosis, as it can be used to generate redundancy relation and to perform root cause search (Flaus et al., 2011).

The remainder of this paper is organized as follows. Section 2 represents the first part of the FIS model, defines the architecture of the analyzed system, and describes the characteristics the system and the material entities used. This is the basic view. Section 3 represents the second part of the FIS model. It is built when we realize the risk analysis (Karagiannis et al., 2010). Section 4 displays the last part of the FIS model. It is assembled when we describe the behavior of the system in normal or degraded mode. An illustration of this method on transporting hazardous material by road is presented and discussed in Section 5. Finally, Section 6 concludes this paper.

2 SYSFIS VIEW

This part describes the structure of the equipment or the analyzed object, in a relatively simple manner by showing the various systems interactions, and specifying, if necessary their functions and the material components (human, technical or informational) that compose them (see Figure 1). This part also allows describing the links between these elements. The purpose of this view is to provide a frame structure for the dysfunctional or for behavioral view (Flaus, 2008).

2.1 *Elements of the model*

The basic element of the representation is the *process* or *system*, composed of functions, physical

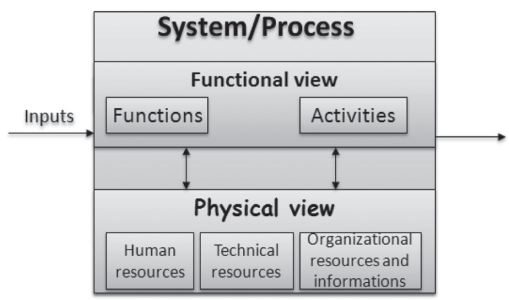


Figure 1. SysFis model.

resources and input/output ports. A process or system is seen as an organized set of activities that uses resources (personnel, device, equipment andmachinery, raw material and information) to transform inputs into output elements. Each process or system is described internally by:

- The *Structural Elements* (SE), known as *resources* or *entities*, which consist of hardware (machinery and materials), informational, human and organizational activities to conduct the process activities. We distinguish machines, materials and processed parts, human actors, methods represented by procedures, software, The physical context characterized by variables such as temperature, the concentration of various products, the noise level ...
- The *Functional Elements* (FE), called *functions* or *system activities*, are defined as the role played by a set of resources in terms of purpose. It is a kind of dematerialization of a set of entities specifying what the system can do. This represents a specification of the system behavior. A function can be active or not active at a given time. Its behavior is characterized by a set of variables, and eventually by a performance model describing the temporal evolution.

It is possible to define for each system a structural element and a main functional components. A system is decomposed of subsystems, which themselves can be described by structural elements and/or functional components.

The advantages of this model for risk analysis are:

- on the one hand: it allows a description of the installation or the object analyzed, in an organized and hierarchical way. This description may be systemic, functional or structural where the different parts of the model are managed simultaneously.
- and on the other hand, it helps at the identification of risks, based on the category of the different elements of the model. For example, a risk of explosion types can be identified for the element "gas pressure".

Note: When modeling a complex reality, it is necessary to decompose it in several systems, and eventually subsystems.

2.2 *Links between model elements*

Relationships may be defined between the structural and functional elements of the model (Figure 2). To perform a function or activity:

- a number of incoming items may be necessary, they are consumed or brought using information, there are inputs for the function. This is the case of a raw material, a part to be assembled or a sensor;
- other elements are generated where there state is modified, resources are then "outputs" for the function. This is the case of a material produced from an assembled or machined object;
- finally, some *structural elements* may be used, they are "supports" for the function. For example, this is the case of a machine or an operator used to perform a function.

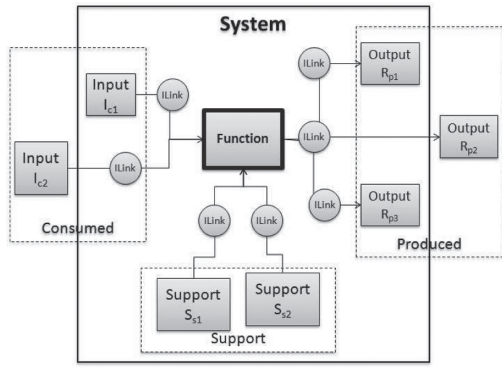


Figure 2. Relations.

When the links are given at the systems level, they represent a broader point of view, because they do not detail the relationships within a system. Links between elements of the model may contain information, such as coefficients or properties.

Remark *Resources include both items that are processed, items products and components used for processing. The terminology used in the context of flow simulation, is to call entity, produced and consumed resources and resources, used ressources.*

2.3 *Details of model elements*

Before describing in detail the elements of the model, we may define:

- A *variable*, which corresponds to a magnitude that can be represented by an integer, a real, ...
- An *attribute*, that can describe any property given by: $a =< name, value >$, where value is any value representable by a structured string character following the ECMA-404 JSON Data Interchange Standard syntax.

A *variable* can be used to evaluate system behavior, values are the possible values of a state variable of a hybrid dynamical system. An *attribute* is of a different nature. Its aim is to represent one of the properties of a meta element. Its values can be generally represented by an object, the chosen format is JSON.

Formally, a structural view of a model is defined by $M =< S, L >$ where:

- S is a set of systems, $S = \{s_i \mid 0 \le i \le n\}$ with $s =< F(s), R(s), Sub(s), V(s), A(s) >$ is a system defined by a set of functions F, a set of resources R, a set of subsystems Sub, a set of variables $V(s)$ and a set of attributes $A(s)$.
- L is a set of links defined as follows $L =< me_s, me_t, nature, A(l), nature, direction, M_s \times M_t >$

A model element, me may be a system, a functional element or a structural element. The set of model elements connected to a model element is denoted by $N_s(me)$.

Remark *The function $O(x)$ defines the owner(s) of x. This function is denied for variables $O(v)$, attributes$O(a)$, functions, structural element $O(r)$, ...*

3 DYSFIS VIEW

3.1 *Elements of the model*

The dysfunctional view (Figure 3) is used to describe the risk analysis or malfunction. This analysis consists in identifying, for each element of a system, states in which this element may cause a damage, or might be unable to answer correctly with the expected level of performance. The principle of this analysis with the view DysFis is as follows:

- each fact that may occur is represented by an event;
- the nature of the fact is described by the type of events: there are such events characterizing hazards, failure modes or deviations of variables;
- each event is associated with the element of the model view SysFIS to which is related. For example, a failure mode can be associated with a given resource;
- the causal links between events can describe the sequence of malfunctions. It is possible to associate properties to these links and barriers that affect the propagation.

The list of event types proposed by the model is the following: events representing the degraded dangerous phenomena (*dp*), events representing the failure modes (*fm*), events representing the deviations of variables (*vdev*), events representing degradation events (*dam*), intermediate events (*gen*), events characterizing the hazardous situations (*hs*), central unwanted events characterizing the loss of control (*uce*).

Each event is associated with a Boolean value. For a model element, the OK mode is defined as true if no event model dysfunction is true.

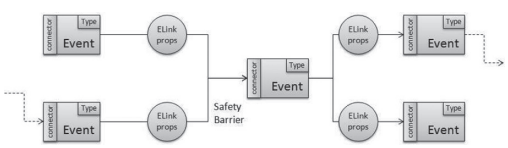


Figure 3. Events graph.

3.2 *Links between model elements*

Events are related to each other by links representing causal relationships: the causes of an event are connected to the input of the resulting event. Different types of connectors exist, such as AND and OR connectors. Links between events may occur with a certain probability, in particular an influence coefficient. Each link may relate to the input or the output of an event a barrier characterized by a reduction coefficient of the likelihood or severity.

The events are connected depending on the causal links. The model allows then to generate the fault tree relating to an event. Furthermore, the links between events can be weighted and it is possible to associate them with security gates.

3.3 *Details of model elements*

Figure 4 illustrates the relationship between the views SysFis and DysFis: events are associated with different elements. Links between the elements of SysFis model can guide the analysis of the propagation of dysfunctions for causal links between events.

Formally, the dysfunctional view is defined by a set of events $E = \{e_i\}$, and a graph G. The events are defined as

$$e =< N, P(e), S(e), O(e), g, \mu, \nu, A(e), V(e) >$$

where

- N is the set of the nature of events. Most often, $N \subset \{dp, fm, vdev, hs, uce, dam, gen\}$;

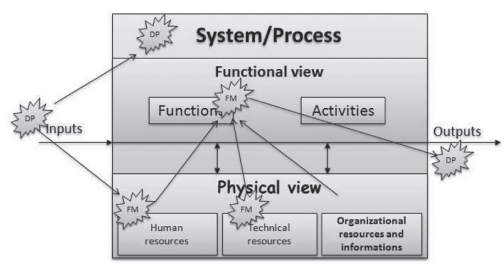


Figure 4. Links between system element, function, resources and events.

- $P(e)$ and $S(e)$ are sets of predecessors and successors of the event;
- $O(e)$ is the owner of event;
- $g_i(e)$ is the input gate;
- μ is a function that defines the likelihood of the event, and v is the severity of the event.

The event graph G is defined with the sets $P(e)$ and $S(e)$ for each event; $\rho(e_i,e_j)$ is a partially defined function which describes a weight related to the edge between two events; $M(e_i,e_j)$ a partially defined function which associates modifiers to the relation between e_i and e_j. An example of modifier is a safety barrier. The failure mode of a model element is denoted by $fmode_i$ (failuremode). The normal of a model element is defined as:

$$ok = \bigwedge_i \neg dfmode_i$$

4 SIMFIS VIEW

The SimFis view describes the dynamic behavior of the system. It is not necessary to construct this view to perform a simple risk analysis or even to build a fault tree or node bow tie diagram. However, when we have this view, it is possible to simulate the operation of the system, including degraded mode. In addition, some elements of this view can be exploited for diagnostic or prognostic (Flaus, 2013b, Giap et al., 2009).

The behavior is described by several complementary aspects. Each model element (*System*, *Functional element* or *Structural element*), which is desired to describe the evolution, has one or more behavior modes. Usually, at least one mode of behavior is defined for the *OK* mode of, and a mode of behavior is associated with each failure mode that could be interesting to simulate. A model element may be active or inactive, which means that it is not used in a given configuration.

At each mode of behavior is associated with one or more activities, which can be of the following types:

- a simple modification activity of the informational state, described by a mathematical relationship and an execution duration (may be null);
- an activity of transformation element, which can be seen as an entity processor (Figure 5) and used to represent the flow diagrams of processing: a *System*, a *Functional element* or a *Structural element* can be seen as a processor which transforms into output, member elements, or that performs actions on elements. A processor can be active or not;
- a macro-type activity described by a diagram of subset of BPMN Type (Figure 6).

When an element becomes active for a given mode, the corresponding activities to this mode become active and can describe the behavior of this element. When it changes its operation mode, i.e from a normal mode OK to a dysfunctional mode DM1, the current activity is interrupted and the dynamic behavior changes. More precisely, a simple activity is defined by $a =< name, x \leftarrow f_a(x), \delta >$ where x is a vector of variables defined in the model element or the set of model elements via a structural link english $N_s(me)$, and δ is a positive integer representing the time english $t = \delta.T_s$.

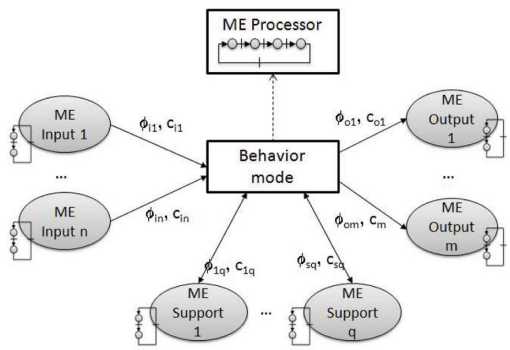


Figure 5. Process.

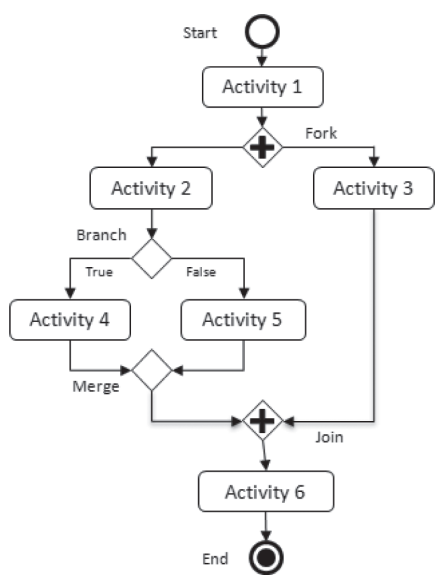


Figure 6. Activity diagram.

A transformation activity is defined by:

- a transformation relation defined as follow:

$$\sum n_i me_i \mid \varphi_i .. \rightarrow \overset{n_s me_s \mid \varphi_s}{\longrightarrow} \sum n_o me_o \mid \varphi_o \{m_i\}$$

where me_i is an input model element, required in number n_i and which must satisfy the condition φ , which a logical relation expressed with respect to the variables, the attributes and the events available in the scope. me_o is an output and me_s is a model element representing a support;
- a positive integer duration δ representing the time english $t = \delta.T_s$, and/or a set of final conditions;
- a priority p;
- a set of input actions defined as mathematical relation on variables in the scope $\{me\} \cup N_s(me)$.

$$x_c(k) \leftarrow f_{input}(x_c(k)) \cup \{m_i\};$$

- a set of output actions defined in a similar way

$$x_c(k) \leftarrow f_{ourtput}(x_c(k)) \cup \{m_i\};$$

- a set of evolution equations, computed at each sampling time

$$x_c(k+1) = f(x_c(k)) \cup \{m_i\}.$$

This set of elements allows to model the system behavior as follows:

1. A model element, when it is active, evolves according to the diagram in Figure 7:
   (a) block 1 is activated: this step consists of searching input elements satisfying the conditions in adequate numbers. If all items are not available, the block 1 is still active;
   (b) else, block 2 becomes active. The input actions are performed;
   (c) block 3 becomes active and evolution calculation is performed, if the equations are defined;
   (d) while the execution time mode is less then max time and the final condition is false, the block will be executed;
   (e) the final actions are executed, the inputs are destroyed and the support and outputs are released.

Remark • *An operating mode can be defined for each phase of life in OK mode, phases of life taking values in the set OM : Normal Operating Mode, DW : Shutdown, MA : Maintenance, UP : Startup, DW : Shutdown;*

- *model elements have a variable defining the number of modes of behavior that use and an attribute defining the max number (generally 1);*
- *the dynamic model is only valid for a given mode. In this mode, the connection variables are carried out during the activation step, and they are disconnected during the desactivation phase.*

Remark. *Changing the functional mode for an transforming activity type. When a change mode occurs, if the transformation relationship is not valid for this mode, this one is interrupted and the elements being processed (inputs and outputs) are destroyed. If we desire specifying a simple abnormal transformation of inputs, it is sufficient to define the activity as being valid for this mode, and to specify in the dysfunctional model, that the defects of the support element or the defects associated with the function behavior pattern, lead to a output default. For example, a default in a machine may product a defective part, while maintaining the same behavior in terms of machining.*

4.1 *Use for the simulation and diagnosis*

The proposed meta model may be used to structure the risk analysis, and to allow the exploitation of the obtained information for system simulation and diagnosis (Chittaro and Ranon, 2004). For space reasons, we can not give details here. A simulation approach which uses the transformation of the FIS meta model into High level Petri net may be found in (Negrichi et al., 2012).

5 EXAMPLE OF APPLICATION

In this section, we will illustrate the behavior of the system for transporting hazardous materials by road. This system consists of five functions: *Loading* of hazardous materials in a truck; *Moving* of the truck along a given route; *Waiting* for the truck at various points: parking, waiting for unloading at customer or waiting for loading at supplier; truck *Unloading* at customer; *Storage* at customer or supplier. We will detail the *Loading* function. We will construct the structural, the dysfunctional and the evolution views. This function presents the *Loading* of hazardous materials (which is simulated in the form of blocks) in a truck. To achieve such a load, many entry attributes are required such as a deposit, a machine, a worker and a truck, and it needs as attributes outputs: a deposit, truck and materials. The deposit and materials are seen as modified resources. *Loading* will decrease the amount of materials contained in the deposit and will change the positions of contents. Deposit, truck, workman are seen as supports for the *Loading* function, they are reserved prior to

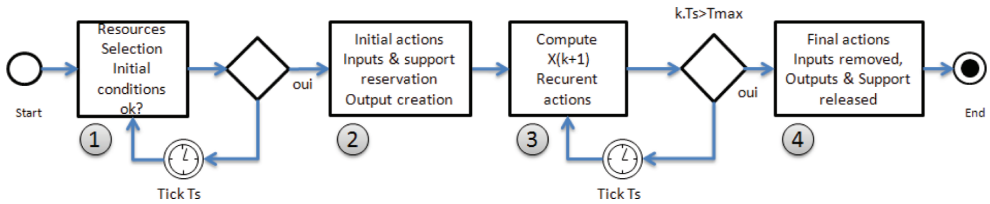


Figure 7. Activity diagram.

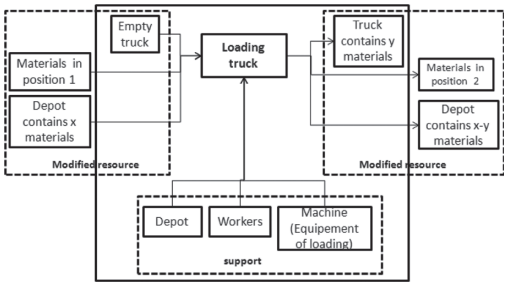


Figure 8. Relations for Loading.

loading and released at the end. Figure 8 shows relations of *Loading* describing before.

To have a good load, we should take note about time loading and the quality of loaded products, and eliminate any incompatibilities of products in the same expedition. A *Load* failure may come from four cases (Flaus and Granddamas, 2002) (Wirth et al., 1996):

- delay of loading (unavailability of a deposit, truck, worker or machine);
- delay during loading (in case of unavailability of the machine, materials can be loaded manually but it may take much time);
- a collision during loading which can affect the quality of contents;
- and finally a bad loading represented by an expedition of incompatible two products in the same truck.

Figure 9 shows the various failure modes of loading describing a Fault tree (Karagiannis et al., 2010).

Table 1 illustrates the evolution mode of each situations. Our simulation allows the system to evolve the basic events (basic events Fault tree), and it describes the failure mode of the function. This failure mode helps to obtain the behavior mode related to each failure (Table 1), where each Fault tree (Delay during loading, delay of loading, bad loading and Accident) is carried by a behavior mode evaluating the level of risk related to each situation.

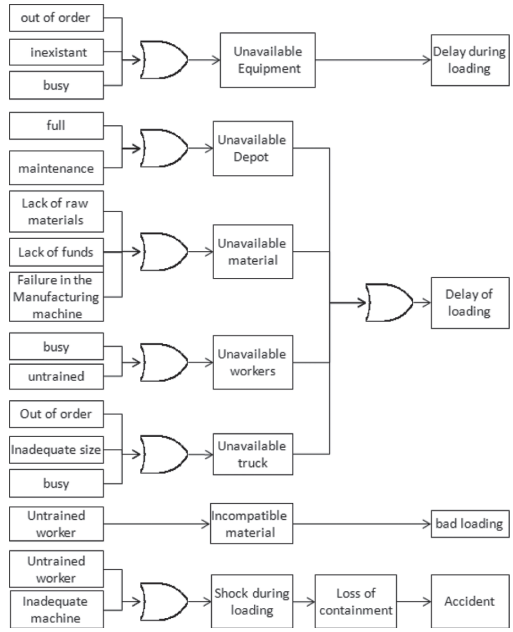


Figure 9. Fault tree for loading.

6 CONCLUSION

In this paper, we have presented a method for risk analysis including a specification of the general process and her functions. For each function, we have precised the inputs, the outputs, the required resources, a dysfunctional model, and a model of evolution. The main interest of this meta model is that it allows the representation of risk analysis and dynamical behavior in a coherent manner, which can be used to perform various related tasks: risk evaluation, diagnosis, simulation under degraded conditions, prognostics ...This was illustrated through an example of loading hazardous materials in a truck. One of our future goals is to to simulate several times a complex phenomenon of transportation of dangerous goods, by using multi-agent based simulation and to generate randomly risks via the Monte Carlo simulation.

Table 1. Evolution mode of load function.

Model element	Behavior mode	Related fault tree event	Equations
Loading	Normal		$T = f(q,d) = \frac{q}{d}$ where T is the loading time, q is the quantity to be loaded, and d is the loading flow;
Loading	Abnormal1	Delay of loading	$T = f(q,d) = \frac{q}{d} + T_1$ where $T1$ time of unavailability of machine, workers, depot, material or truck;
Loading	Abnormal2	Delay during loading	$T = f(q_1,d_1) = \frac{q_1}{d_1 \times n}$ where q_1 is the quantity to be loaded, d_1 is the loading flow for one workers, and n is the number of workers;
Loading	Abnormal3	Bad loading	$\frac{\Delta T}{\Delta t} = F(T,c_a,c_b)$ where c_a is the concentration of product A, c_b is the concentration of product B, and T is the environmental temperature;
Loading	Abnormal4	Accident	$D = f(M,t)$ where M is the material to be loaded, and t is the temperature.

REFERENCES

Chittaro, L. and Ranon, R. (2004). Hierarchical model-based diagnosis based on structural abstraction. *Artificial Intelligence*, 1–2:147–182.

Flaus, J. and Granddamas, O. (2002). Towards a formalisation of mads, system failure analysis model, in lambda-mu 13. ESREL.

Flaus, J. M. (2008). A model-based approach for systematic risk analysis. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 222(1):79–83.

Flaus, J.-M. (2011). A modelling framework for model based risk analysis. *Safety and Reliability for Managing Risk ESREL'11*.

Flaus, J.-M. (2013a). *Risk Analysis: Socio-technical and Industrial Systems*. John Wiley & Sons.

Flaus, J.-M. (2013b). *Risk Analysis: Socio-technical and Industrial Systems*.

Flaus, J.-M., Adrot, O., Ngo, Q.D., et al. (2011). A first step toward a model driven diagnosis algorithm design methodology. *Safety and Reliability for Managing Risk ESREL'11*.

Giap, Q.H., Ploix, S., and Flaus, J.-M. (2009). Managing diagnosis processes with interative decompositions. 296:407–415.

Karagiannis, G., Piatyszek, E., and Flaus, J. (2010). Industrial emergency planning modeling: A first step towards a robustness analysis. *Journal of Hazardous Materials*, 181:324–334.

Negrichi, K., Di Mascolo, M., Flaus, J.-M., et al. (2012). Risk analysis in sterilization services: A first step towards a generic model of risk. *Proceedings GISEH'2012*.

Papadopoulos, Y., Parker, D., and Grante, C. (2004). A method and tool support for model-based semiautomated failure modes and effects analysis (fmea) of engineering designs. *Research and Practice in Information Technology, ACM, ISSN 1445-1336*, 47:89–95.

Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., and Quirchmayr, G. (2011). A formal approach enabling risk-aware business process modeling and simulation. *Services Computing, IEEE Transactions on*, 4(2):153–166.

Wirth, R., Berthold, B., Krämer, A., and Peter, G. (1996). Knowledge-based support of system analysis for the analysis of failure modes and effects. *Engineering Applications of Artificial Intelligence*, 9(3):219–229.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Proposing a multi-layer modeling framework for complex infrastructure systems

C. Nan & G. Sansavini
Reliability and Risk Engineering Group, ETH Zürich, Switzerland

ABSTRACT: The heterogeneity and tight coupling of modern infrastructure systems makes a tractable description of their emergent behaviors a challenging task. Classic analytical methods lack the capability to provide sufficient insights into system behaviors and fully capture the complexity of these systems. In this paper, a multi-layer modeling framework is proposed, targeting toward an in-depth understanding and holistic analysis of infrastructure systems. Within this framework, an infrastructure system is viewed as three interrelated subsystems in corresponding layers, i.e., System Under Control (SUC), Operational Control System (OCS), and Social System (SS). Subsystem 1-SUC (layer 1) and subsystem 2-OCS represent the technical parts of infrastructure systems. In general, the SUC is a time-based, while the OCS is an event-driven and service-oriented. Subsystem 3-SS (layer 3) represents the non-technical part of infrastructure systems, which is generally related to social factors that intend to have influences on the overall system performance. In order to demonstrate the capability the proposed modeling framework, a feasibility experiment is developed using Swiss electricity supply system as an exemplary system.

1 INTRODUCTION

The welfare and security of each nation rely on a continuous flow of essential goods (e.g., energy, food, water, data) and services (e.g., banking, health care, public administration). Infrastructure systems are those systems so vital to any country that their incapacity or destruction would have a debilitating impact on the health, safety, security, economics and social well-being, including the effective functioning of governments (Kröger and Zio, 2011). Infrastructure systems have always been "complicated", but in recent years, they have witnessed growing integration and interconnectedness, which have turned them into complex systems (Eusgeld et al., 2009, Kröger, 2008). According to its definition, inherent characteristics of a complex system include having a large number of dimensions, nonlinear and adaptive behaviors, strong internal and external interactions, uncertain rules of interaction among its components (may change over time time), etc (Kröger and Nan, 2014). Besides inherent complexities of these systems, one important aspect is their interconnections, which made them grow into a so-called "Systems-of-Systems" (SoS). These unforeseen interdependencies could become an important factor providing the tolerance to attacks and failures if well managed (positive impact). For instance, technical failures such as abnormal disconnection of a transmission line (a component of electricity power supply system) can be detected by devices remotely installed at substation and corresponding alarm can be transmitted to a control centre via services provided by coupled telecommunication systems in order to prevent further failure propagations. However, on another side, these interdependencies might also be a source of threat generating new uncertain risks, especially the risk of cascading failures, which made them more vulnerable (negative impact). For instance, a failure within one infrastructure system or loss of its continuous service may be damaging enough to society and economy, while cascading across system-boundaries has the potential for multi-infrastructural collapse and unprecedented consequences (e.g., the August 14, 2003 blackout in North America affected 50 million people and led to 3 billion USD insurance claims).

Modern societies have become embedded in an increasingly dense and intricate web of interconnected infrastructure systems (Vespignani, 2010). Addressing the significance of infrastructure systems is a challenge due to the complexity and perpetual nature of these systems, the lack of sufficient information clearly characterizing failure propagations, and the lack of modelling/simulation tools by which their interactions can be comprehensively analysed. All this makes clear that it is vital to develop an over-arching and cross disciplinary vision of integrated risk management, e.g., horizontal approach using the advanced modelling and simulation techniques.

2 RESEARCH STREAMS AND PROPOSED FRAMEWORK

2.1 *Available methods and approaches*

Research work related to modeling infrastructure systems is still at an early stage and is challenged by their inherent characteristics, e.g., dynamic/nonlinear behaviors, intricate rules of interactions as the results of their openness and high degree of interconnectedness (Griot, 2010, Pederson et al., 2006). Developing a comprehensive modeling framework with the capabilities of achieving a closer representation of behaviors of these systems and gaining insights into interactions within and among them seems promising and is vital for improving our understanding and identifying means to design, maintain, and protect SoS in the long run. Currently a broad scale of modeling approaches/techniques have been developed and applied, e.g., Input-output Inoperability Modeling (IIM), Complex Network Theory (CNT), Agent-based Modeling (ABM), System Dynamic (SD), PetriNet(PN)-based, Bayesian Network (BN), etc (see (Zio and Sansavini, 2011b) and (Ouyang, 2014) for more details about these approaches). The capability and applicability of these approaches in terms of analyzing infrastructure system behaviors vary. Each of these approaches can be used to deal with a specific topic and has the ability to represent characteristic properties of a type of infrastructure system, e.g. physical, social, informational, or cyber. Some approaches are only capable of analyzing infrastructure systems at the structure/topology level, e.g., CNT approach, while some approaches are capable of capturing and analyzing dynamic behaviors of studied systems at the functional level, e.g., ABM approach.

2.2 *Proposing a multi-layer modeling framework*

Modern infrastructure systems, e.g., power supply, telecommunication, and rail transport systems, are all large-scale, complex, highly integrated and particularly interconnected. The operators of these systems must continuously monitor and control them to ensure their proper operation (Igure et al., 2006). These industrial monitor and control functions are generally implemented using an operational control system, e.g., Supervisory Control and Data Acquisition (SCADA) system. The fundamental purpose of this type of systems is to allow a user (operator) to collect data from one or more remote facilities and send control instructions back to those facilities (Boyer, 2004). Moreover, the primary focus of modeling/simulating an infrastructure system has been on technical part, almost ignoring non-technical parts, e.g., organizational factors, human factors, etc (Ferscha et al., 2011, Baxter and Sommerville, 2011). A number of studies have shown that human and organizational factors are major causes for accidents occurred in electric power, railway, aviation and maritime infrastructure sectors (Johnson and Holloway, 2007, Kröger and Nan, 2014, Wreathall et al., 2003), highlighting the importance of these factors.

In practice, there is still no a "one-fits-all" approach for analyzing the full spectrum of characteristics and dimensions of a SoS. The lack of coherent modeling approaches hinders the possibilities of analyzing/assessing dynamic system behaviors comprehensively in a heterogeneous network of interdependent infrastructure systems. Therefore, there is a need to develop a comprehensive modeling framework with the capabilities of achieving a closer representation of their behaviors. The framework should also be capable of considering social factors in order to better understand how these factors affect the performance of infrastructure systems. Furthermore, modeling entire infrastructure system as a whole is usually impractical (Ring, 2012, Bloomfield et al., 2009, Filippini and Silva, 2012). Choosing relevant subsystems and modeling them efficiently for the intended purposes seem more promising. For each subsystem, appropriate modeling approaches/methods can be determined to fully represent its behavior and functionalities. Based on this concept, a multi-layer modeling framework is proposed. Within this framework, infrastructure systems are viewed as three interrelated subsystems in corresponding layers, i.e., System Under Control (SUC), Operational Control System (OCS), and Social System (SS).

Subsystem 1-SUC (layer 1) represents the technical part of infrastructure systems, which is generally time-based. In order to fully model this type of systems, both functionality (physical laws) and structure (topology) need to be considered. Therefore, the approaches of ABM and CNT seem promising. Subsystem 2-OCS (layer 2) also represents the technical part of infrastructure systems, which is generally event-driven and service-oriented. The major responsibility of this type of systems is to control and monitor corresponding SUC. The developed model needs to be able to process messages among components efficiently and to represent the functionality of the system. Compared to all the approaches introduced above, the approach of ABM seems more promising. Subsystem 3-SS (layer 3) represents the non-technical part of infrastructure systems, which is generally related to social factors that have influences on the overall system performance. The developed model needs to be able to evaluate and quantify the effects of social factors such as human

performance, organizational behaviors, etc. For example, the approach of HRA (Human Reliability Analysis) seems promising for the evaluation of human performance.

2.3 *Modeling the layers of a complex infrastructure system*

The key idea of the proposed multi-layer modeling framework is to develop different types of modeling approaches for each subsystem, to search solutions to integrate these approaches and finally to be able to represent behaviors of the studied system including interconnections among components in different layers. In this section, the framework will be further introduced and explained in detail, using the Swiss Electricity Power Supply System (EPSS) as an exemplary system to demonstrate its feasibility and applicability.

2.4 *Representing EPSS by multi-layer modeling framework*

The three subsystems of the EPSS are:

- **Subsystem 1-SUC:** electricity transmission network is used as an exemplary system of the SUC within the EPSS, which is controlled and monitored by a SCADA system. Components of this system include transmission lines, generators, busbars, etc (see (Brand et al., 2003) for more detail).
- **Subsystem 2-OCS:** a SCADA system is used as an exemplary system of the OCS within the EPSS. Components of this system include (1) field instrumentation and control devices, i.e. FIDs and FCDs respectively (sensors and actuators), (2) Remote Terminal Unit (RTU), a standard stand-alone data acquisition and control unit with the capabilities of acquiring data from monitored processes, transferring data back to the control centre, and controlling locally installed equipment, (3) Communication Unit (CU), providing a pathway for communications between a control centre and RTUs, and (4) Master Terminal Unit (MTU), which is the "host computer" issuing commands, collecting data, storing information, and interacting with operator(s) (see (Boyer, 2004) for more details).
- **Subsystem 3-SS:** the human operators in the control center of the SCADA system is used as an exemplary element of SS within the EPSS. It should be noted that in this paper only human performance is considered and other social factors such as organizational behavior are ignored. Generally, their responsibilities include monitoring/processing generated alarms, switching off components located at remote substations, sending commands to remote substations, etc. Although these responsibilities are mainly related to system functionalities of monitoring and remote control and may not appear to have significant impacts on system performance, examining the reliability of the human operator remains crucial.

Figure 1 shows a simplified multi-layer representation of the EPSS with various interacting subsystems and associated components: parallel planes represent different subsystems in corresponding layers while nodes represent various components together with some of interconnections among them. The elements of the various layers depend on each other, depicted by various horizontal (inside a layer) and vertical (between layers) links. These links demonstrate (inter)links among components of different layers and a failure of a component may cascade to other layers and impacts functionality of the infrastructure system.

2.5 *Modeling SUC and OCS*

Several modeling approaches have been briefly introduced in Section 2.1. Among these approaches, the CNT and ABM turned out to be promising for modeling infrastructure systems, especially their technical parts. Both approaches intend to represent a whole system by dividing it into many smaller interacting entities, i.e. nodes (CNT) or agents (ABM). Within the CNT, the SoS is mapped into a graph G(V,E) composed by a set of nodes V and the set of connections E between them. Each node (or vertex) represents an element of the system, while a link (or edge) represents the relation between corresponding elements. A number of

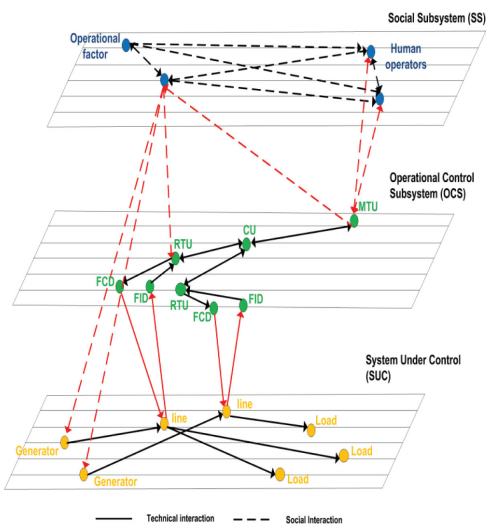


Figure 1. Representing EPSS in three subsystems (layers).

modeling efforts have been made to adopt this approach for the development of infrastructure system models demonstrating its capability of modeling relation established through connections among technical components (Crucitti et al., 2004, Bompard et al., 2009, Duenas-Osorio and Vemuru, 2009, Zio and Sansavini, 2011a). This approach is based on the network model mapping physical configuration of the components of infrastructure systems and their physical interconnections. However, it lacks the ability to capture uncertain and dynamic characteristics of infrastructure systems, which can be overcome by replacing nodes/links with agents in the ABM approach.

Using the ABM approach, each agent is capable of modifying its internal data, behaviors and adapts itself to environmental changes. ABM can be regarded as a bottom-up approach and each component can be modeled as an agent; different agents interact with each other directly or indirectly (Schläpfer et al., 2008, Sanford Bernhardt and Mcneil, 2008, Chappin and Dijkema, 2008). Compared to CNT, ABM is able to provide an integrated environment where a more comprehensive analysis of dynamic system behaviors can be performed by "looking-into" the component level of studied systems. Motivated by the advantages of this approach, a two-layer agent-based modeling approach (Fig. 2) has been developed and applied for the purpose of the vulnerability assessment of the electric power system (Schläpfer et al., 2008). Within this approach, the lower layer represents the separate modeling of the physical components by means of conventional, deterministic techniques such as power flow calculations, whereas the upper layer represents the abstraction of the electric power system with all its components as individual agents.

The SCADA system (an example of OCS) is event-driven and service-oriented. Normally it is used to monitor and control very large industrial process facilities such as electricity transmission

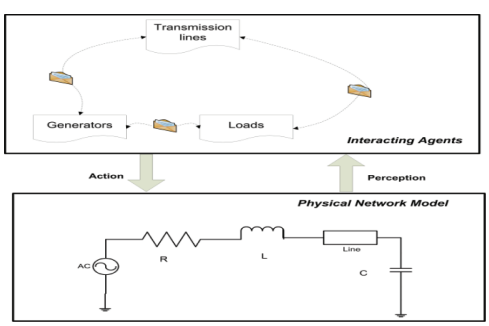


Figure 2. Two-layer agent-based modeling approach (illustration using SUC of EPSS as an example).

facilities and oil and gas production facilities (Boyer, 2004). In general, it comprises remotely located field level devices, which are connected to a control center through a variety of communication devices. Modeling a SCADA system is not just a challenge from a theoretical point of view but of great practical importance (Balducelli et al., 2007) (Bobbio et al., 2010). It is not applicable to use graph-based (e.g., CNT) or analytical (e.g., IIM) approaches. Motivated by the results of applying two-layer agent-based modeling approach to model the SUC, a failure-oriented two-layer agent-based modeling approach is also developed to model the SCADA system. Compared to the approach applied for modeling the SUC, device modes are introduced as parts of agent development. Within this approach, the "agent state" is defined as a location of control with a particular set of reactions to conditions and/or events of its related agent, while the "device mode" is defined as the hardware status of corresponding simulated hardware devices. The transition of various device modes can affect corresponding agent state. It should be noted that this type of approach mainly focuses on the negative effects due to technical failure of components (see (Nan and Eusgeld, 2011b) for more details).

2.6 *Modeling SS*

Social factors play an important role in the operations of infrastructure systems. The lack of careful consideration of influences of these "non-technical" parts of infrastructure systems often results in poor system performance and high costs. Their roles and impacts need to be strengthened by developing advanced approaches that take these factors into consideration and focus more on the ways to analyse their effects efficiently in varying contexts. Over the years, many HRA methods have been widely developed and improved in order to provide a more applicable way to assess these factors, especially human performance. However, these methods are challenged by their inherent limitations, e.g., the lack of objectivity, inability to take other social factors (e.g., organizational/political factors) and contexts (e.g., emotion, learning ability, and experience) into consideration. Furthermore, most of these works are based on the implementation of classical analytical approaches and seem not sufficient to represent the complexity of social factors, which is the most critical shortcoming compared to research works focused on technical parts of infrastructure systems. The full mapping of the complexity of infrastructure systems depends on the continued development/improvement of social factor models. Motivated by these challenges, a hierarchy modeling approach to model the SS is proposed, illustrated in Figure 3. Within this model, it is assumed that the

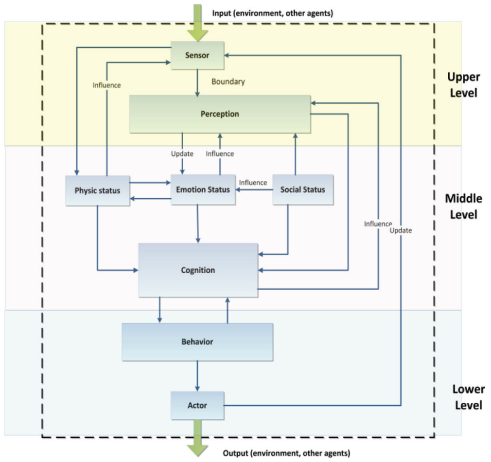


Figure 3. The structure of the proposed hierarchy modeling approach.

human factor is the key factor and all other factors such as organizational behaviors and cultures eventually have influences on it.

The model consists of three levels. The upper level includes the components sensor and perception, which can be regarded as the input of the model. The information such as interactions with other agents, influence of environment, predefined goals, is first processed by the sensor component. After that, the information will be further interpreted by the perception component. For example, if an alarm is received by the operators in the control room, it needs to be first received by the sensor and then interpreted by the perception in order to extract more detailed information, such as the severity of the alarm, etc. The middle level includes four components: physic status, emotion status, social status and cognition. These components contain parameters, state variables, states, rules, which can be used to determine states and behaviors of the human agent. The social status is one of most important components for determining the behavior and state of the agent. Similar to the physic and emotion status, this component also includes different internal states. The interaction among agents, which is mainly represented in this component, potentially can be used to model/represent trusts between agents. The influences of other social factors such as organizational factor can be included in the three status components. The lower level includes the components of behavior and actor, which can be regarded as the output of the model. The order of executing agent action/behavior is determined by the component behavior, while the execution is carried out by the component actor. The information that has influence potentially on other agents/objects will be sent out by the component actor.

2.7 *Experimental simulation platform*

All the developed models (three subsystems) are integrated in an HLA (High Level Architecture)-compliant experimental simulation platform. The platform consists of four components: the SUC model, the SCADA and SS model, the RTI (Run Time Infrastructure) server, and the simulation monitor. RTI is the core element of the HLA standard providing common services (e.g., joining into and resigning from the federation, specification of interfaces, etc) to all the participating components (models). These components are connected over a Local Area Network (LAN). The RTI server acts as the center of the experimental platform and is responsible for synchronizing the simulation and routing communications among all components. The RTI server interacts with each model through corresponding local RTI interface. The simulation monitor is a real-time tool, through which the simulation of three models can be observed. The standard of HLA 1516 (IEEE, 2000) is used to implement this platform (see (Nan and Eusgeld, 2011a) for more details about this platform).

3 CASE STUDY

Electric power systems are among the most prominent representatives of infrastructure systems and the need for their reliable and resilient performance during disruptive events is essential (Zio and Sansavini, 2013, Bilis et al., 2013). In this section, the Swiss EPSS is selected as an exemplary system to demonstrate the feasibility and applicability of the proposed modeling framework. It is assumed that this system is a stand-alone and the energy exchange with the neighboring countries is regarded as independent positive and negative power injections at the respective boundary substations.

The modeling approaches proposed for each subsystem (i.e. SUC, OCS, and SS), introduced in section 3, have been further applied to model the exemplary system. Based on the two-layer modeling approach, an agent-based model is developed to represent the SUC within the EPSS using the software Anylogic 5.5. In total, 585 agents are created to represent its components, i.e., transmission lines, generators, busbars, and loads. The SCADA system within the EPSS is modeled by applying the proposed failure-oriented two-layer modeling approach using the software Anylogic 6.6. In total, 587 agents are created to represent its components, i.e., FCDs, FIDs, and RTUs (see (Nan et al., 2013) for more details about SCADA model). Based on the hierarchy modeling

approach, an agent-based model is developed to model the SS of the EPSS using the software Anylogic 6.6. The focus of this model is mainly related to the evaluation of the performance of human operators (examples of human factors), therefore, the effects of other social factors (e.g., organizational factor) are ignored. The second generation HRA (Human Reliability Analysis) method CREAM (Cognitive Reliability Error Analysis Method) is applied to implement the perception component of the SS model (see (Hollnagel, 1998) for more details about CREAM). Using this method, Performance Shaping Factors (PSFs) can be assessed dynamically based on current simulation environment, e.g., time of day, simultaneous goals, etc, and corresponding Human Error Probability (HEP) ([0,1]) will then be calculated. The lower HEP value indicates better performance. To decide whether or not there is an error by human operators, it is necessary to set a threshold value (HEP_A) representing the maximum acceptable HEP value. If a calculated HEP is more than HEP_A, then it is assumed that a human error occurs (the human is not successful). The higher HEP_A indicates fewer changes of human errors (see (Nan and Kröger, 2014) for more details).

In order to demonstrate the applicability of the proposed modeling framework, a feasibility experiment has been designed and developed. The purpose of this experiment is to study the capability of the proposed modeling framework as an approach to represent behaviors of infrastructure systems in a comprehensive way. In this experiment, it is assumed that a certain number of components of the EPSS fail to function at same time, i.e. the related failure modes are triggered simultaneously. Among all the failure modes that have been considered for the EPSS, the SCADA FRH (Failure to run (too high)) is selected to be triggered due to its significant negative effects to the performance of whole system (see (Nan et al., 2013) for more details). The FRH failure mode can be described as the failure of a FID (Field Instrumentation Device) to indicate the actual value of its monitored variable and indicates a larger than actual value. The causes could be personnel performance error during maintenance and other activities, insufficient attention to the aging of piece parts of FID, etc. For example, personnel apply outdated procedures for adjusting FIDs, mistakes during calibrating setpoint values, or erroneously not accounting for technical modifications of the field when calculating setpoint values. In this experiment, it is assumed that the number of FID devices that are in FRH failure modes is 30. The reason to set the number of failed FIDs as 30 is based on several trial tests before starting the experiment. Results obtained from these tests show that likelihood of the occurring of cascading failures after failures of 30 FIDs becomes high. To evaluate the performance of the three subsystems, following MOPs (measurement of performance) are developed.

$$\mathrm{MOP}_{\mathrm{SUC}} = \frac{\text{Number of available transmission lines}}{\text{Number of total transmission lines}} \in [0,1]$$

$$\mathrm{MOP}_{\mathrm{SCADA}} = \frac{\text{Number of available RTU devices}}{\text{Number of total RTU devices}} \in [0,1]$$

$$\mathrm{MOP}_{\mathrm{SS}} = \mathrm{HEP}(\text{Human Error Probability})$$

Figure 4 shows the MOPs of those three subsystems during the experiment. The simulation starts at the $t = 0$ h, which is the time used by the simulation platform to synchronize the communication among platform components. The failure modes of corresponding FIDs are triggered at time 3 h, meaning that the calibration value of the FID devices is modified to a larger value. Therefore, the lines monitored by these FIDs become overloaded although they should not. Normally, whenever a transmission line is overloaded, an overload alarm will be generated and sent to the operator in the control centre (MTU) by the RTU of the SCADA system. If, after a certain period, the operator fails to react to the overload alarm, then the protection devices such as disconnectors (an example of FCD) will automatically disconnect the overloaded transmission lines to minimize the negative consequence of the problem. As shown in Figure 4, MOP_{SS} increases (from 0 to 0.036), indicating that the likelihood of the operators in control room making errors also increases. This might be caused by the sudden increase of the number of alarms received in the control center. Due to the assumed poor performance of the operators (in this experiment, it is assumed that the HEP_A equals to 0.03), the overload alarms can not be handled appropriately and transmission lines start to be disconnected. The MOP_{SUC} starts to drop at time 3.3 h, meaning that the number of disconnected transmission lines increases. As a consequence, the

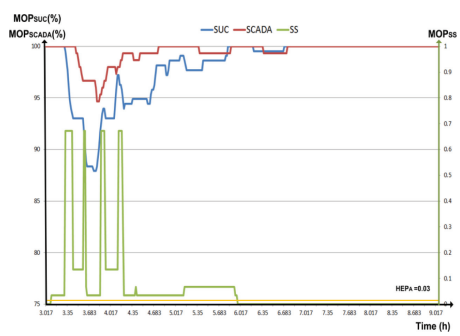


Figure 4. The performance of three subsystems measured by appropriate MOPs ($HEP_A = 0.03$).

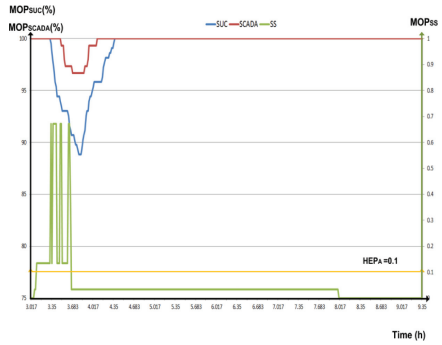


Figure 5. The performance of three subsystems measured by appropriate MOPs ($HEP_A = 0.1$).

MOP_{SCADA} value drops after a certain period. In total, 48 overload alarms are triggered, 30 of which are caused by the triggering of the FRH failure modes of initially selected FID devices (the size of the disconnection cascade is 18 FID devices).

Figure 5 shows simulation results when HEP_A is set to 0.1 (i.e. human performance is improved). As seen from this figure, after triggering initial disruptive events, both MOP_{SUC} and MOP_{SCADA} drop due to human performance errors ($HEP = 0.672$), which is similar to the previous test. However, in this case, it takes less time for the MOP value of both systems to reach 100% due to the improvement of human performance ($HEP_A = 0.1$), although the triggering of overload alarms continues (MOP_{SS} returns to zero after time 8 h).

The results from the feasibility experiment demonstrate how three subsystems interact with each other. The failures are initially triggered in components (FIDs) of the SCADA system, which causes the overloads of transmission lines. Due to sudden increase of the number of overload alarms, the operator might become overwhelmed and the MOP_{SS} rises, increasing the possibility that the human operators can make a mistake. As the consequence, transmission lines start to be disconnected, increasing the number of impacted components of the SCADA system (more RTUs start to lose power). In this experiment, the importance of human operators is also demonstrated. If the human operator is able to respond to overload alarms adequately and send commands to corresponding RTUs for further corrective functions, failures might not propagate and negative consequences can be significantly minimized.

4 CONCLUSIONS

In recent years, infrastructure systems have become increasingly intricate and interdependent, which have dramatically increased their overall complexity, turning them to so-called "systems-of-systems" and causing the emergence of unpredictable behaviors and negative impacts. Our society should face the fact that these systems will continue to become more integrated and their behaviors may become more complex. Understanding and characterizing them is a real challenge; research in this area is still at an early stage. It is essential to get a clearer understanding of their cascading behaviors by applying appropriate techniques. Consequently, modeling/simulating those systems will remain as a field of active research. Although progress has been made in advanced modeling and simulation, more efforts are needed to further improve the methods/tools, to validate them and to scale them up to the level of SoS.

This paper proposes a multi-layer modeling framework in order to achieve a closer representation of system behaviors and getting in-depth insights of infrastructure systems. The framework is mainly focused on the engineered infrastructure systems. Within this framework, each infrastructure system is viewed as three interrelated subsystems in corresponding layers, i.e., System Under Control (SUC), Operational Control System (OCS), and Social System (SS). The proposed modeling framework provides a more efficient and comprehensive way to analyze behaviors of infrastructure systems. For each subsystem, appropriate modeling approaches and methods can be determined which fully utilize advantages of each approach and optimize the performance of the overall simulation. Furthermore, not only technical parts of infrastructure systems, non-technical parts (i.e. social factors) are also considered by the framework.

The first results from the application seem promising, demonstrating the feasibility of the proposed framework, not just due to its capability for representing the complexity of infrastructure systems, but also its modeling flexibility and adaptability. They demonstrate how the three subsystems interlink with each other. For example, the operator performance degrades when a burst of false overload alarms occur due to faulty calibration of sensors and its impact on the overall system performance. Currently, more experiments are under development such as the experiment targeting the analysis of behaviors of socio-technical systems and the experiment to evaluate the resilience related behaviors of infrastructure systems.

REFERENCES

Balducelli, C., Bologna, S., Lavalle, L. & Vicoli, G. 2007. Safeguarding information intensive critical infrastructures against novel types of emerging failures. *Reliability Engineering and System Safety,* Vol.92, p.1218–1229.

Baxter, G. & Sommerville, I. 2011. Socio-technical systems: From design methods to systems engineering. *Interacting with Computers,* Vol. 23, p.4–17.

Bilis, E.I., Kroger, W. & Nan, C. 2013. Performance of Electric Power Systems Under Physical Malicious Attacks. *Systems Journal, IEEE,* Vol.7, p.854–865.

Bloomfield, R., Chozos, N. & Nobles, P. 2009. Infrastructure interdependency analysis: Requirements, capabilities and strategy.

Bobbio, A., Bonanni, G., Ciancamerla, E., Clemente, R., Iacomini, A., Minichino, M., Scarlatti, A., Terruggia, R. & Zendri, E. 2010. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. *Reliability Engineering and System Safety,* Vol.95, p.1345–1357.

Bompard, E., Napoli, R. & Xue, F. 2009. Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection,* Vol.2, p.5–12.

Boyer, S.A. 2004. *SCADA supervisory control and data acquisition*, Research Triangle Park, ISA.

Brand, K.-P., Lohmann, V. & Wimmer, W. 2003. *Substation automation handbook*, Utility Automation Consulting Lohmann.

Chappin, E.J.L. & Dijkema, G.P.J. 2008. Agent-based modeling of energy infrastructure transitions. *In:* Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), 2008 First International Conference on, 10–12 Nov. 2008.

Crucitti, P., Latora, V. & Marchiori, M. 2004. Model for cascading failures in complex networks. *Physical Review E,* Vol.69, 045104.

Duenas-Osorio, L. & Vemuru, S.M. 2009. Cascading failures in complex infrastructure systems. *Structural Safety,* Vol.31, p.157–167.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M. & Zio, E. 2009. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering and System Safety,* Vol.94, p.954–963.

Ferscha, A., Zia, K., Riener, A. & Sharpanskykh, A. 2011. Potential of Social Modelling in Socio-Technical Systems. *Procedia Computer Science,* Vol.7, p.235–237.

Filippini, R. & Silva, A. 2012. Resilience analysis of networked systems-of-systems based on structural and dynamic interdependencies. *PSAM 11 & ESREL 2012.* Helsinki (Finland), p.10.

Griot, C. 2010. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. *International Journal of Critical Infrastructure,* Vol. 6, p.363–379.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method CREAM*, Elsevier.

IEEE 2000. IEEE Standard for Modeling and Simulation High Level Architecture (HLA)—Framework and Rules. *IEEE Std. 1516-2000*, i–22.

Igure, V.M., Laughter, S.A. & Williams, R.D. 2006. Security Issues in SCADA Networks. *Journal of Computers and Security,* Vol.25, p.498–506.

Johnson, C.W. & Holloway, C.M. 2007. A Longitudinal Analysis of the Causal Factors in Major Maritime Accidents in the USA and Canada (1996–2006). *In:* Redmill, F. & Anderson, T. (eds.) *The Safety of Systems.* Springer London.

Kröger, W. 2008. Critical infrastructure at risk: A Need For A New Conceptual Approach and Extended Analytical Tools. *Reliability Engineering and System Safety,* Vol.93, p.1781–1787.

Kröger, W. & Nan, C. 2014. Addressing Interdependencies of Complex Technical Networks. *In:* D'Agostino, G. & Scala, A. (eds.) *Networks of Networks: The Last Frontier of Complexity.* Springer International Publishing.

Kröger, W. & Zio, E. 2011. *Vulnerable Systems*, Springer.

Nan, C. & Eusgeld, I. 2011a. Adopting HLA standard for interdependency study. *Reliability Engineering & System Safety,* Vol.96, p.149–159.

Nan, C. & Eusgeld, I. 2011b. Exploring impacts of single failure propagation between SCADA and SUC. *In:* IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2011b. p.1564–1568.

Nan, C., Eusgeld, I. & Kröger, W. 2013. Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. *Reliability Engineering and System Safety,* Vol.113, p.76–93.

Nan, C. & Kröger, W. 2014. Toward Modelling of Human Performance of Infrastructure Systems. *In:* 12th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM12), 22–27 June 2014, Honolulu, USA.

Ouyang, M. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety,* Vol.121, p.43–60.

Pederson, P., Dudenhoeffer, D., Hartly, S. & Permann, M. 2006. Critical Infrastructure Interdependency Modeling: A Survey of U.S and International Research. Idaho National Laboratory.

Ring, J. 2012. Systems of the Third Kind: Distinctions, Implications, and Initiatives. *INCOSE INSIGHT,* Vol.15, p.9–12.

Sanford Bernhardt, K. & Mcneil, S. 2008. Agent-Based Modeling: Approach for Improving Infrastructure Management. *Journal of Infrastructure Systems,* Vol.14, p.253–261.

Schläpfer, M., Kessler, T. & Kröger, W. 2008. Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach. 1*6th power systems computation conference.* Glasgow.

Vespignani, A. 2010. Complex networks: The fragility of interdependency. *Nature,* Vol.464, p.984–985.

Wreathall, J., Roth, E., Bley, D. & Multer, J. 2003. Human reliability analysis in support of risk assessment for positive train control.

Zio, E. & Sansavini, G. 2011a. Component Criticality in Failure Cascade Processes of Network Systems. *Risk Analysis,* Vol.31, p.1196–1210.

Zio, E. & Sansavini, G. 2011b. Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. *Reliability, IEEE Transactions on,* Vol.60, p.94–101.

Zio, E. & Sansavini, G. 2013. Vulnerability of Smart Grids With Variable Generation and Consumption: A System of Systems Perspective. *Systems, Man, and Cybernetics: Systems, IEEE Transactions on,* Vol.43, p.477–487.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Hybrid modeling and simulation approach selection to the reliability and vulnerability analysis of Critical Infrastructures

G. Sansavini
Reliability and Risk Engineering Laboratory, ETH Zürich, Switzerland
Risk Center, ETH Zürich, Switzerland

C. Nan
Reliability and Risk Engineering Laboratory, ETH Zürich, Switzerland
Land Using Group, ETH Zürich, Switzerland

W. Kröger
Risk Center, ETH Zürich, Switzerland

ABSTRACT: Challenges to the modeling and simulation of engineered Critical Infrastructures (CI) lie in the multiple levels of interdependencies and lack of fixed boundaries, in the diversity of the underlying physics of the provided service, in the coexistence of multiple time scales, and in the level of resolution required to fulfill the objectives of the analysis. Such challenges impact the selection of the most suitable modeling approach or integration of different approaches for the reliability and vulnerability analysis of CI. This paper suggests a framework for selecting the hybrid modeling and simulation approach which is more suitable to analyze specific types of CI. The focus steps consider the system characteristics, e.g. interdependencies between CI, identification of the host system, and the objectives of system analysis. The framework is exemplified with reference to CI of different types.

1 INTRODUCTION

Decades of massive system integration and scarce investments have caused large-scale/wide-area technical networks, such as engineered Critical Infrastructures (CI), to become increasingly interdependent on each other and to operate in the proximity of system limits. Emerging "Systems-of-Systems" (SoS) have shown the emergence of unprecedented complex behaviors with negative impacts, e.g. vulnerability to cascading failures with widespread consequences. Understanding and characterizing such complex systems is vital for thorough reliability and vulnerability analysis and for capturing emergent behaviors and failure cascades, especially when strong interdependencies exist.

Research on this topic is characterized by two key aspects: *i*) it is not feasible to build lab-scale experimental setups to reproduce systemic failures (i.e., involving the entire system) of large-scale technical networks; *ii*) empirical observations of systemic failures in large-scale technical networks are available but sparse because these systems are designed and operated to minimize such occurrences. Therefore, we have to resort to models and simulations which can capture the system behavior and reproduce the consequences of the disruptive event, taking advantage of the few empirical observations of events in CI (Luiijf et al., 2009). The challenge is the development of adequate modeling/simulation approaches capable to represent characteristics and underlying physics specific to different types of infrastructures with high fidelity. These approaches must be balanced; on the one hand, avoid the danger of creating artifacts which postulates systemic hazards which do not occur in real-world infrastructures, while on the other hand, oversimplification may fail in capturing the actual system behavior and misrepresent or underestimate potential severe consequences at the system level.

The modeling and simulation of CI and SoS is challenged by the key characteristics of these systems: *i*) coexistence of multiple time scales, from infrastructure evolution to real-time contingencies; *ii*) multiple levels of interdependencies and lack of fixed boundaries, i.e. CIs are made of multiple layers (management, information & control, energy, physical infrastructure); *iii*) broad spectrum of hazards and threats; *iv*) different types of physical flows, i.e. mass, information, power,

vehicles. An additional challenge lies in the level of resolution required to fulfill the objectives of the analysis, which guides the level of abstraction and aggregation in the models and simulations.

Currently, a broad scale of modeling approaches has been developed and applied and two main directions have been followed, namely, knowledge-based and model-based approaches. Knowledge-based approaches are based on empirical investigations and brainstorming aimed at analyzing past events to improve the understanding of the dimensions and types of interdependencies in CI. Model-based approaches aim at analyzing interdependent infrastructure systems comprehensively by using advanced modeling/simulation techniques, capable of providing both quantitative and qualitative information. A variety of models have been applied, e.g. Input-output Inoperability Modeling (IIM), Complex Network (CN) Theory, Agent-Based Modeling (ABM), System Dynamic (SD), Petri Nets (PN), Bayesian Networks (BN) and Dynamic Control System Theory (DCST).

These modeling approaches vary in their applicability and capability of analyzing behaviors of CI. The most suitable approach or integration of different approaches (a hybrid modeling and simulation approach) must be identified in connection to specific system characteristics and objectives of system analysis.

This paper proposes a framework for selecting the hybrid modeling and simulation approach which is more suitable to the analysis of a specific type of SoS, and which can be integrated into existing frameworks for the vulnerability analysis of CI (Kröger and Zio 2011). The focus steps will consider the system characteristics, e.g. interdependencies between infrastructures, identification of the host systems, and the objectives of system analysis. Taking advantage on the literature about existing approaches to the model of CI (Satumtira and Dueñas-Osorio 2010; Kröger and Nan 2014), the framework is exemplified with reference to infrastructures of different types, i.e. energy supply (electricity, gas), information and communication and transport (rail, road).

2 CONCEPTUAL FRAMEWORKS FOR VULNERABILITY ASSESSMENT

A conceptual framework for vulnerability analysis of CI was proposed in Kröger and Zio (2011) to bring all system aspects and attributes together and to take advantage of the diverse capabilities of the available model and simulation approaches. Vulnerability analysis address several system issues: the end states of interest for the given systems; the boundary definition; the threats and hazards of relevance and the susceptibility of the system; the resulting cascades; system interdependencies and their impact; the uncertainties involved; the obvious and non-obvious ("hidden") vulnerabilities to be reduced and managed.

The conceptual framework for vulnerability analysis follows a stepwise, problem-driven approach tailored to the needs of the analysis, and distinguishes five steps, several decision points and feedback loops (Figure 1).

The first step, the preparatory phase, integrates the task framing and definitions (step 1.1) into the process of familiarization with the system. It is also important to decide on the spectrum of hazards and threats to be included into the analysis. Furthermore, it is necessary to deeply understand failure models and effects on each of the components of the CI. For a more effective screening of the system vulnerability some reasonable simplifications should be made. These assumptions need re-visiting in a later phase of the assessment (step 3.2). After key information is collected and pre-assessment is done, the knowledge base should be checked with respect to the availability of methods suitable for the defined tasks.

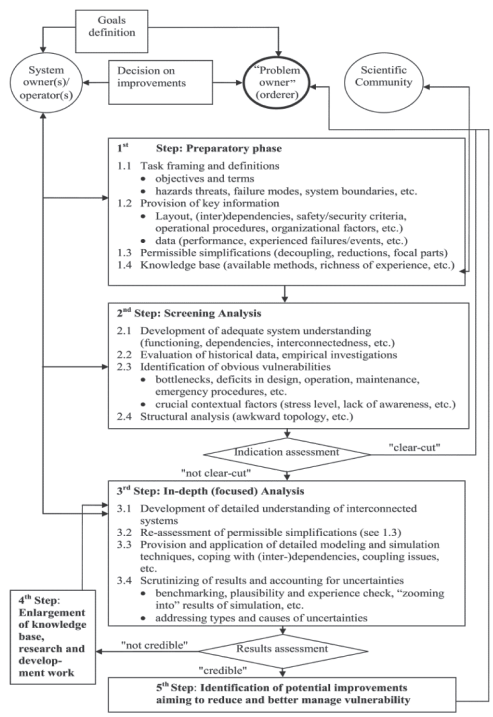


Figure 1. Conceptual framework for the vulnerability analysis of interconnected infrastructures (Kröger and Zio 2011).

The purpose and goals of the analysis affects the degree of detail, e.g. the assessment of interdependencies and cascading failures, or the width of system boundaries. It is assumed that the vulnerability analysis should evolve in two steps where appropriate. A screening-type of analysis might be efficient and sufficient to identify eye-catching, obvious weak points, e.g., awkward topology, spatial proximity of interconnected systems or bottlenecks, and further actions should focus on eliminating or reducing them. The screening analysis could also prepare the ground for and give steer to the in-depth analysis which may turn out necessary. The screening analysis leads off with development of adequate system understanding; we assume that information provided from system owners/operators (step 1.2) allows for general understanding of main functionalities, states of relevance, interfaces, interdependencies. In this phase, the main emphasis is placed on experts' opinions, brainstorming, etc., rather than on application of detailed models. If the results and insights gained by screening analysis are not satisfying (not "clear-cut") and major hidden vulnerabilities are still feared, a more sophisticated in-depth analysis (step 3) has to be launched. To achieve a higher degree of accuracy in the vulnerability evaluation, system understanding has to be further developed on the basis of additional information about the system and its operating environment. Special attention should be placed on interdependencies within or among systems. The re-assessment of simplifications made earlier may call for more sophisticated methods of analysis, e.g., following a system or even a system-of-systems approach, and integrating a comprehensive spectrum of different phenomena. While full validation and verification of models and methods, as well as of results, seem infeasible, benchmarking against other similar analyses, plausibility checks and checks against experienced events, if available, may help to support the credibility of the vulnerability assessment and build confidence in the decision making which follows.

System improvements (step 5) may be proposed to further reduce and better manage vulnerabilities by all means of provisions.

3 APPROACHES FOR INTERDEPENDENCY ANALYSIS

Applied modeling/simulations approaches, have different viewpoints, e.g., functional or structural, different levels of abstraction, different focus, objectives and metrics, different degrees of maturity and are based on different levels of available information and knowledge. None of the available methods alone is capable to address and tackle the variety of issues of vulnerability assessment including the impact of interdependencies. It is commonly agreed that a universal, all-encompassing approach or model which accounts for all issues does not exist. In recent years, two main directions can be distinguished, i.e., knowledge-based and model-based approaches.

3.1 *Knowledge-based approaches*

Knowledge-based approaches, e.g., empirical investigations or brainstorming, intend to use data collected by interviewing experts and/or analyzing past events to acquire information and improve the understanding of the dimensions and types of interdependencies (Zimmerman 2004; Luiijf et al., 2009). This approach is straightforward and easy to understand. It is capable of providing a qualitative assessment on the severity of interdependencies and can be considered as an efficient screening method. However, it is a purely data-driven approach, meaning that the accuracy of results depends on the quality and the interpretation of the collected information.

3.2 *Model-based approaches*

Various advanced modeling approaches are available and have been applied, e.g., Input-output Inoperability Modeling (IIM), Complex Network (CN) Theory, PetriNet (PN)-based modeling, Agent-Based Modeling (ABM), System Dynamic (SD), Bayesian Network (BN), Dynamic Control System Theory (DCST).

The IIM approach captures interdependencies among infrastructure systems via mathematical models. This approach is originally a framework for studying the equilibrium behavior of an economy by describing the degree of interconnectedness among various economic sectors. It assumes that each system can be modeled as an atomic entity whose level of operability depends on other systems and propagation between them can be described mathematically based on the basic Leontief high order mathematical model. The IIM approach is capable of analyzing cascading failures and providing a mechanism for dependency measurement (Haimes et al., 2005).

The PN-based approach is a mathematical modeling language for the description of distributed systems which has also been used to represent/assess interdependencies among infrastructure systems. In this approach, components (subsystems) of infrastructure systems and their states are modeled using basic PN elements such as places, transitions, etc. This approach alone has difficulties representing infrastructure systems quantitatively

and needs to be combined with other methods (Klein et al., 2007).

Fundamental elements of the CN theory approach are originally formed by graph theory. It captures the coupling among systems as a set of nodes connected by a set of links and by this characterizing their topology. A number of modeling efforts have been made to adopt this approach for the development of infrastructure system models and interdependency-related assessments, demonstrating its capability of representing relationships established through connections among system components (Eusgeld et al., 2009; Buldyrev 2010). The CN theory approach is based on the network model mapping physical configuration of the components (elements) of studied infrastructure systems and their (physical or logical) interconnections. The analysis of the topological properties of the network is able to reveal useful information about the structural properties, topological vulnerability, and the level of functionality demanded for its components. However, this approach lacks the ability to capture uncertain and dynamic characteristics of infrastructure systems and system properties when dynamical processes, acting on the network, occur. For instance, the underlying physics of voltage collapse or frequency instability in electric power grids is overlooked by CN theory models.

In ABM approach, each agent is characterized by internal data, its behavior and environment, and adapts itself to environmental changes (Eusgeld et al., 2009). An agent can be used to model both a technical component (e.g., a transmission line), and a non-technical component (e.g., a human operator). The rules of behaviors of each agent are represented by using Finite State Machines (FSMs) and include both deterministic and stochastic time-dependent, discrete events. The ABM approach achieves a closer representation of system behaviors by integrating the spectrum of different phenomena that may occur, e.g., generating a multitude of representative stochastic, time-dependent event chains. However, this approach demands a large number of parameters defined for each agent, requiring thorough knowledge of the studied systems.

SD is a mathematical modeling technique for framing, understanding, and managing complex feedback systems. Stocks, flows, and feedbacks are central concepts of this approach, which are used to describe the system behaviors. The approach assumes that the behaviors of infrastructure systems are the results of interrelationships among various system variables (Min et al., 2007). It is possible to use this approach to perform CI interdependency analysis by representing a system or a system component as a node and an influence among systems or components as a link. In general, SD based models developed for CI interdependency study intend to explore system behaviors by studying high-level services provided by each infrastructure system. Differential equations are developed to evaluate relationships between different nodes. SD is capable of modeling the interdependencies among CIs only a relatively abstract level, and lacks modeling flexibility, e.g. probabilistic relationships are not modeled.

BN is a probabilistic approach that can be used for modeling behaviors of a system, based on observed stochastic events. A BN is a model representing the interactions among components in a system from a probabilistic perspective (Di Giorgio & Liberati 2011). One of major disadvantages of this approach is its difficulty of taking time into account. Therefore, an improved approach, Dynamic Bayesian Network (DBN), has been developed. In order to analyze CI interdependencies, the general BN and DBN represent system components as variables and interactions between variables as directed probabilistic links. BN or even DBN approach is not suitable to analyze dynamic, often non-linear, behaviors of infrastructure systems.

DCST (Casalicchio et al., 2011) can be applied to assess the interdependencies using transfer functions and corresponding frequency responses. Each studied infrastructure needs to be assumed as a linear time invariant dynamic system. The input/output relationship among components or infrastructure systems can be represented and quantified by transfer functions. Based on the overall transfer function and its corresponding frequency responses, the stability of interdependencies between infrastructures can be evaluated using Bode and Nyquist diagrams. In DCST, all the links between components and infrastructures are determined during the transfer function development. Therefore, hidden vulnerabilities caused by interdependencies cannot be captured.

4 HYBRID MODELING AND SIMULATION APPROACH

Due to inherent complexity of interdependencies among infrastructure systems, there is still no "silver-bullet" approach. The knowledge-based approaches are straightforward and easy to understand, while the model-based approaches are more comprehensive and promise to gain a deeper understanding of behaviors of studied systems. The level of this "deeper understanding" also varies: some approaches are only capable of analyzing the structure/topology level, which can be considered as appropriate approaches for the screening

analysis, e.g., CN theory, PN and BN modeling approaches, while some approaches are capable of capturing and analyzing dynamic behaviors of studied systems, e.g., ABM and IIM approach.

Therefore, it has proven necessary to integrate different types of modeling approaches into one simulation tool in order to fully utilize advantages of each approach and to optimize the efficiency of the overall simulation. One of the key challenges for developing such type of simulation tool is the required ability to create multiple-domain models, e.g., discrete and continuous time models, time-based and frequency-based models, and to effectively exchange data among them (Bloomfield et al., 2009). One solution for meeting these challenges and handling these technical difficulties is to distribute different simulation components by adopting the concept of modular design. The overall simulation platform can be divided into different simulation modules and distributed across one simulation platform.

This hybrid modeling/simulation approach intends to integrate different modeling and simulation techniques for the analysis of interdependent infrastructures (Rome et al., 2014). Different simulation components are developed interacting with each other over a real-time simulation platform. Each distributed component represents specific system characteristics by the appropriate modeling approaches. The information and control commands exchanged among simulation components are interpreted and processed over the network connection, allowing quick assembly of independently developed components without full knowledge of their peer simulation components.

Integrated hybrid simulation approaches provide a high-fidelity representation of the infrastructure under analysis. They are very expedient to run scenarios and case studies. On the other hand, it is difficult to draw general conclusions regarding system operations and management based on their application because they rely on the tuning of many parameters which have competing effects on the system behavior. As a countermeasure to that, reduced-order models can be developed and validated based on the results of high-fidelity simulation and used as a surrogate approximated model in the hybrid modeling/simulation approach. The use of reduced-order model alleviates the computational burden of the distributed simulation and enables general insights on system behavior.

4.1 *Objectives of the analysis*

The hybrid modeling and simulation approach may be aimed at the quantification of different objectives, which has an impact on the selection of the most suitable combination of approaches:

- Reliability: the probability that the system is operational or that it meets the target performance throughout the mission time.
- Vulnerability: specific components of the system subjected to expected adverse events whose occurrence causes loss in functionality of the system (Linkov et al., 2014). Vulnerability analysis helps the system prepare and plan for adverse events.
- Resilience: the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events (Linkov et al., 2014). Resilience management further integrates temporal patterns of the capacity of a system to absorb and recover from adverse events, then adapt.
- Optimization of system planning (design phase).
- Optimization of operations.

Any of the modeling/simulation approach can be used in the reliability analysis when the stochastic nature of the system components is represented and when the target system state is identified and assessed. Vulnerability analysis and system planning rely on the characterization of system functionality; hybridization of CN theory, SD, DS, IIM and ABM approaches is suitable in this step. Resilience analysis and optimization of the operations require modeling time-dynamics, transitions between discrete states, adaptation and recovery in the systems; hybridization of CN theory, IIM and ABM approaches is suitable in this step.

4.2 *Identification of the host system*

The quantification of system performance in presence of interdependent networks may vary depending on the presence of clear host system. It is sometimes not clear whether there is one system (host system) which profits from the services of a dedicated network (dedicated guest/support system), in which the system under control and the control system can be clearly distinguished, or whether interdependent infrastructures are at an equal level. In the first case, the system performance level should characterize the host system, while in the second case, the different performance levels of the interdependent networks have to be considered.

Example of host system and dedicated support system is a power distribution network monitored and controlled by a dedicated SCADA; on the other hand, a power distribution network and a monitoring and controlling communication infrastructure, e.g. the public IP network, are examples of two comparable systems. By the same token, the functionality of the power distribution network

may have an impact on the urban freshwater supply (host system), while the contrary may not be true.

The proposed models should be built through a process by which a system consisting of a network requiring the input of another network for normal or exceptional operations is represented by the two networks, where the first network is the behaving net and the second is the auxiliary net.

4.3 *System behavior*

The selection of the approaches to integrate in modeling interdependent infrastructures must be tuned on the required ability to capture specific system features and behaviors:

1. Structure/topology level, abstract level vs. dynamic behavior at the functional level. Among all approaches, IIM is the least adaptable in mapping the system structure because it describes the system through a lumped operability value. CN theory, SD, DCST and ABM can capture time dynamics in the system. Among them, CN theory requires a certain level of abstraction of system functionality and is less capable of integrating physical laws.
2. Intensity and system performance levels. PN and BN can assess the probability that a system operates at a given performance level but cannot adapt to varying performance levels.
3. Cascading failures. As in 2), PN and BN are not suitable for this task.
4. Specific characteristics of a type of infrastructure system, e.g. physical, social, informational, or cyber. SD, DCST and ABM can integrate physical laws and model different infrastructure characteristics.

4.4 *Interdependency characteristics*

The selection of the approaches to integrate in modeling interdependent infrastructures must be tuned on the required ability to capture specific characteristics of the interdependencies:

1. Dynamics, time delays and failure repair rates (event-driven interdependencies). ABM can include event-driven processes in the interdependency modeling. SD and DCST also model dynamics taking place through the interdependencies using analytical functions, but do not capture event-driven processes. PN and BN can account for probabilistic dependencies (transition rates).
2. Explicitly model of the independencies vs. simulating the behavior of the CI interconnected within the SoS and assess the strength of interdependencies as an emerging system property. The former is a top-down model which assumes the existence of interdependencies. The latter is bottom-up system description which maps the functional relations among components in different systems. ABM can be regarded as the bottom-up approach; CN, SD, and DCST can represent system functionality as bottom-up approaches; PN, BN and IIM require the identification of system dependencies and are top-down approaches.
3. Local physical/logical/functional interdependencies among system components vs. macroeconomic sector interdependencies based on expert knowledge. IIM is not suitable to model interdependencies at the atomic component level.

Table 1 offers an overview of the capabilities of different approaches to capture specific characteristics of the interdependencies.

5 APPLICATION TO CRITICAL INFRASTRUCTURES

For different CI, we suggest the approaches which seem to be more promising for their use in hybrid integrated modeling and simulation approaches.

5.1 *Energy supply (electricity, gas)*

Power supply systems have been modeled using CN theory (Bompard et al., 2009; Hernandez-Fajardo

Table 1. Capabilities of different approaches to capture specific system features and behaviors and interdependencies characteristics. √ and × indicate capable and incapable approaches, respectively.

			Structure	Component level	Functional links (delays, repair)	Non linear, time dynamics of system behavior	Integrate physical laws	Bottom-up modeling of interdependencies	Cascade representation	Reliability analysis	Vulnerability analysis & System planning	Resilience analysis & Operations optimization
Knowledge -based	Empirical Investigation, Brain Storming		x	√	x	x	x	x	x	x	x	x
Model-based	Graph Theory	CN	√	√	x	√	x	√	√	√	√	√
	Probabilistic	PN	√	√	x	x	x	x	x	√	x	x
		BN	√	√	x	x	x	x	x	√	x	x
	Dynamic System Theory based	SD	√	√ (abstract)	√	√	√	√ (abstract)	√ (abstract)	√	√	x
		DCST	√	√ (abstract)	√	√	√	√ (abstract)	√ (abstract)	√	√	x
	Mathematic	IIM	x	x	√	x	√	x (abstract)	√ (abstract)	√	√	√
	Object Oriented	ABM	√	√	√	√	√	√	√	√	√	√

& Dueñas-Osorio 2013; Schneider et al., 2011). Thanks to their level of abstraction, CN models have relatively few parameters and their behavior can be explored somewhat comprehensively. General considerations and behaviors can be easily inferred. By contrast, physical models of real systems can have many parameters which are even difficult to measure in the real infrastructure. Thus, the interesting behavior of the CN models, i.e. power law distributions of cascade size, optimal interconnectivity and systemic risk, has served as hypotheses to test and refine in more realistic models (D'Souza et al., 2014). On the other hand, CN topological approaches do not seem to correctly model and represent the power grid (Eusgeld et al., 2009; Hines et al., 2010) because they model failure propagation in power grids as an epidemic spreading with local propagation effects. In fact, the failure of a component in the power grid causes an almost instantaneous rerouting of the power flow following Kirchhoff laws with distant non-local effects.

Physic-based models embedding power flow equations complement the information on the topological structure of the system with physical parameter and represent non-local cascading effects. Physic-based models are used in the energy hub concept (Geidl & Andersson 2007). Energy hubs are considered as interconnection points among energy-carrier networks (electricity, gas and heat) which are modeled within a power flow approach. In contrast to CN and network flow models (Quelhas et al., 2007), power flow models incorporate constitutional physical laws, such as the relation between voltage and current, pressure and flow, etc. These relations are system specific and have to be adapted to represent the individual types of energy flows.

Thanks to the great computer power available nowadays, CN theory models are outperformed by reduced-order physical models, e.g. DC power flow in power grids. Nonetheless, power-flow models alone lack the capability of capturing time-varying interdependencies and discrete processes, e.g. cascading failures, therefore, it is advisable to integrate them into approaches such as ABM to represent discrete event-driven processes (Schläpfer et al., 2008; Nan et al., 2013).

Nonetheless, when the boundaries of the analyzed CI are pushed forward to embrace the continental scale, e.g. in Carvalho et al., (2014) for the gas supply network, CN approaches may be only solution for a feasible analysis.

5.2 *Information and communication*

High-fidelity simulation of communication networks based on ABM is employed for the analysis of network problems and validation of models of communication networks (Riley et al., 2004). These high-fidelity simulations require high computational demand, which can be overcome either by distributing the simulation across multiple networked processors, which results in faster simulation, or by setting up the distributed simulation as a federation of several simulators, which allows simulating larger networks.

Simulators for such discrete-event systems have the capability of accommodating physical processes in communication networks, i.e. MAC addresses, but they may fail in integrating with other models for interdependent infrastructures due to their computational burden which hinders their interfacing.

Interdependencies between communication networks and other infrastructures can be assessed by analytical approaches based on DCST (Casalicchio et al., 2011). Transfer functions of the system and its components are defined and characterized to couple them and interdependent infrastructures. In order to create high-fidelity DCST models, ABM simulation of the communication networks must be used to validate the analytical models before their inclusion in a hybrid model/simulation approach for interdependent infrastructures.

5.3 *Transport (rail, road)*

The ABM approach is employed in the modeling of car traffic because it is able to capture individual drivers' preferences (Galus et al., 2012). In particular for electric car mobility, ABM takes advantage of high resolution road network maps and allows for an accurate mapping between the transportation network and the electricity infrastructure. However, in order to evaluate interdependencies between road and electricity network, detailed data on the electric equipment, drivers' behavior, and power demand are needed.

When such detailed data are missing or when the knowledge of individual driver's behavior is not needed, the transportation infrastructure and vehicle traffic can be modeled using CN and network flow model (Lee et al., 2007). PN have been employed when the objective of the analysis is the estimation of delays in the rail system (Trantopoulos 2011).

ABM was also proposed to assess the impact of electric blackout on the railway infrastructure, and the interdependencies between the latter and alternative transportation networks through the customers' behavior (Balducelli et al., 2005).

SD is suggested to assess the impact of the railway infrastructure on the stability of the electric infrastructure (Genge et al., 2013).

Table 2 summarizes the suggestions of specific modeling and simulation approaches for their use

Table 2. Suggestions of specific modeling and simulation approaches for their use in the hybrid modeling/simulation approach which encompasses multiple interdependent CI.

	Electricity	Gas	ICT	Rail	Road
Electricity		ABM + physical CN (network flow)	DCST ABM BN	ABM	SD
Gas	ABM + physical				
ICT	ABM DCST				
Rail	SD				ABM
Road	ABM				

in hybrid modeling/simulation approaches which encompass multiple interdependent CI. Each cell (*i*, *j*) of Table 2 contains the approaches that are suggested when we want to assess the impact of the infrastructure *i* on infrastructure *j*. Interdependencies between the electric infrastructure and other infrastructures are better understood as it appears from the first row and column which are fully populated. The electric infrastructure is indeed the major coupling point between the other multi-energy energy networks and infrastructures.

On the other hand, empty cells identify interdependencies between infrastructures that are not well understood or for which data are scarce. When this is the case, approaches that model the entire infrastructure as an individual element, i.e. IIM, SD and DCST, can be tailored on the basis of economic data, empirical observations and expert judgment. As an example, IIM can be used to model the infrastructure as a whole entity and the magnitude of the interdependencies can be approximated by the flow of value between them.

6 CONCLUSIONS

This paper proposes a framework for selecting the hybrid modeling and simulation approach which is more suitable to the analysis of a specific type of SoS, and which can be integrated into existing frameworks for the vulnerability analysis of CI. Although the selection is CI-specific, general conclusions can be drawn.

Approaches that can embed physical laws are promising, i.e. ABM has capability of representing the complexity of CI through bottom-up modeling of its elements and does not explicitly assume interdependencies. ABM can be integrated with many other modeling/simulation techniques including physical laws and can be applied to reliability, vulnerability and resilience analysis, as well as to CI planning and operations optimization.

The selection of hybrid approaches strongly depends on the required level of the detail of the analysis, on the granularity in system representation and on data availability. Nonetheless, there are approaches that are outperformed irrespective of the required level of detail. In the electricity infrastructure, DC power flow is a valid alternative to CN theory.

Reduced-order models, i.e. CN, SD and DSCT, can enhance the feasibility of hybrid modeling and simulation approaches but the adherence to real system behavior must be validated by high-fidelity simulations.

REFERENCES

Balducelli C., Bologna S., Di Pietro A. et al., 2005. Analyzing interdependencies of critical infrastructures using agent discrete event simulation. *International Journal of Emergency Management* 2(4): 306–18.

Bloomfield R., Chozos N. & Nobles P. 2009. Infrastructure interdependency analysis: Introductory research review.

Bompard E., Napoli R., Xue F. 2009. Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection* 2: 5–12.

Buldyrev S.V, Parshani R, Paul G. et al., 2010. Catastrophic cascade of failures in interdependent networks. *Nature* 464: 1025–8.

Carvalho R., Buzna L., Bono F. et al., 2014. Resilience of Natural Gas Networks during Conflicts, Crises and Disruptions. *PLoS ONE* 9(3): e90265.

Casalicchio E. Bologna S. Brasca L. et al., 2011. Interdependency Assessment in the ICT-PS Network: The MIA Project Results. *Critical Information Infrastructures Security*. 6712: 1–12.

D'Souza R.M., Brummitt C.D. & Leicht E.A. 2014. Modeling Interdependent Networks as Random Graphs: Connectivity and Systemic Risk. *Networks of Networks: The Last Frontier of Complexity*. 73–94.

Di Giorgio A. & Liberati F. 2011. Interdependency modeling and analysis of critical infrastructures based on Dynamic Bayesian Networks. *19th Mediterranean Conference on Control & Automation (MED)*: 791–7.

Eusgeld I., Kröger W., Sansavini G. et al., 2009. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering and System Safety* 94: 954–63.

Galus M.D., Waraich R.A., Noembrini F. 2012. Integrating Power Systems, Transport Systems and Vehicle Technology for Electric Mobility Impact Assessment and Efficient Control. *IEEE Transactions on Smart Grid* 3(2): 934–49.

Geidl M. & Andersson G. 2007. Optimal power flow of multiple energy carriers. *IEEE Transactions on Power Systems* 22(1): 145–55.

Genge B., Siaterlis C. & Hohenadel M. 2013. AMICI: An Assessment Platform for Multi-domain Security Experimentation on Critical Infrastructures. *Critical Information Infrastructures Security*. 7722: 228–39.

Haimes Y.Y., Horowitz B.M., Lambert J.H. et al., 2005. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. *Journal of Infrastructure Systems* 11: 67–79.

Hernandez-Fajardo I. & Dueñas-Osorio L. 2013. Probabilistic study of cascading failures in complex interdependent lifeline systems. Reliability Engineering & System Safety, 111: 260–272

Hines P., Cotilla-Sanchez E. & Blumsack S. 2010. Do topological models provide good information about electricity infrastructure vulnerability?. *Chaos* 20(033122).

Klein R., Rome E., Beyel C. et al., 2007. Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS. *IRRIS Report*.

Kröger W. & Nan C. 2014. Addressing Interdependencies of Complex Technical Networks. *Networks of Networks: The Last Frontier of Complexity*, 279–309.

Kröger W. & Zio E. 2011. *Vulnerable Systems*. London: Springer-Verlag.

Lee E.E., Mitchell J.E., Wallace W.A. 2007. Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach. Systems. *IEEE Transactions on Man, and Cybernetics, Part C: Applications and Reviews* 37: 1303–17.

Linkov I. et al., 2014. Changing the resilience paradigm. *Nature Climate Change* 4: 407–9.

Luiijf E., Nieuwenhuijs A., Klaver M. et al., 2009. Empirical Findings on Critical Infrastructure Dependencies in Europe. *Critical Information Infrastructures Security*. 5508: 302–10.

Min H.-S.J., Beyeler W., Brown T. et al., 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions* 39: 57–71.

Nan C, Eusgeld I, Kröger W. 2013. Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. *Reliability Engineering and System Safety* 113: 76–93.

Quelhas A., Gil E., McCalley J.D. et al., 2007. A Multiperiod Generalized Network Flow Model of the U.S. Integrated Energy System: Part I—Model Description. *IEEE Transactions on Power Systems*, 22(2): 829–36.

Riley G.F., Ammar M.H., Fujimoto R.M. et al., 2004. A federated approach to distributed network simulation. ACM Trans. Modeling and Computer Simulation 14(2):116–48.

Rome E., Langeslag P. & Usov A. 2014. Federated Modeling and Simulation for Critical Infrastructure Protection. Networks of Networks: The Last Frontier of Complexity: 225–53

Satumtira G., Dueñas-Osorio L. 2010. Synthesis of modeling and simulation methods on critical infrastructure interdependencies. *Sustainable Resilient Critical Infrastructure Systems*. 1–51.

Schläpfer M, Kessler T, Kröger W. 2008. Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach. 1*6th power systems computation conference*. Glasgow.

Schneider C.E., Moreira A.A., Andrade Jr. J.S. et al., 2011. Mitigation of malicious attacks on networks, *Proc. Nat. Acad. Sci.* 108: 3838–41.

Trantopoulos K. 2011. Focal Report: Methods for the Vulnerability Assessment of Multi-layer Infrastructure Networks-The Swiss Rail System. BABS Report: Lab for Safety Analysis, ETH Zurich.

Zimmerman R. 2004. Decision-making and the vulnerability of interdependent critical infrastructure. *IEEE International Conference on Systems, Man and Cybernetics* 4059–63.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Time dependent gas transmission network probabilistic simulator: Focus on storage discharge modeling

V. Kopustinskas & P. Praks
European Commission, DG Joint Research Centre, Institute for Energy and Transport
Energy Security Unit, Ispra, VA, Italy

ABSTRACT: The overall aim of the ProGasNet (Probabilistic Gas Network Simulator) project is to develop the European gas transmission network probabilistic model capable to analyse reliability and risk aspects of the network under normal load and extreme crisis situations. The paper presents extension of the existing probabilistic Monte-Carlo based gas network model of 1-day to longer periods of up to 30 days when storage supply might be important to overcome crisis or network equipment failures. The study test case represents a country transmission network model and impact of storage supply under various crisis situations is presented and various network management options are discussed.

1 INTRODUCTION

Recent gas supply crisis in Europe (Russian-Ukrainian gas disputes in 2006, 2008, 2009; Libyan crisis in 2011) affected many consumers and challenged security of gas supply to Europe. The gas dispute in January 2009 between Russia and Ukraine resulted in gas supply disruptions to many EU countries. This event stimulated to look at security of gas supply issue from political, technological and research perspectives. The EU Regulation (2010) which appeared after the 2009 crisis highlights importance of security of gas supply in Europe and proposes a number of measures by improving network resilience and encouraging EU countries to cooperate more by sharing infrastructure and building interconnections.

The overall aim of the ProGasNet (Probabilistic Gas Network Simulator) project is to develop the European gas transmission network probabilistic model capable to analyse reliability and risk aspects of the network under normal load and extreme crisis situations. The paper presents extension from 1-day simulation model (Praks & Kopustinskas, 2014) to longer periods of up to 30 days when storage supply might have an important role to overcome crisis situations.

Computational studies of energy networks and infrastructures are increasingly important in the current world of challenging crisis and disruptions. Risk, reliability, vulnerability, resilience issues in various networks have been analysed by many researchers (Ball et al., 1992; Johansson et al., 2013). The most recent focus is however on security of supply aspects in the infrastructure networks (E. Zio et al., 2012).

Reliability analysis of energy infrastructure networks present a number of challenges as many network analysis algorithms (optimal distribution of capacity, rerouting of flows etc.) originally developed for telecommunication networks are not directly applicable. The main reason for this is physical properties of energy transport when the flows can be exchanged from the nearest source and do not necessarily need to be transport through the whole network as is the case in case of information transmission.

2 METHODOLOGY

The gas transmission network model is based on maximum flow algorithm well known in graph theory (Deo, 2008). The algorithm was modified to reflect gas transport property to have lower pressure at the points far from the supply source. This means that in case of disruption and lack of gas in the network, consumers that are closer to the source have better chances to be served rather than those that are located far away. Therefore, the maximum flow algorithm was modified to distribute gas first to the consuming nodes close to the supply source and distance from the nearest source was used as a priority criteria.

Let f represent the amount of flow in the network from node 1, called the source, to node m, called the sink. With each arc (i, j) a non-negative flow is associated having an upper bound of u_{ij}. Then

the maximal flow problem may be mathematically formulated as an optimization problem with constrains:

Maximize f subject to

$$\sum_{j=1}^{m} x_{ij} - \sum_{k=1}^{m} x_{ki} = \begin{cases} f & if\ i = 1 \\ 0 & if\ i \neq 1\ or\ m \\ -f & if\ i = m \end{cases} \qquad (1)$$
$$x_{ij} \leq u_{ij},\ i, j = 1,\ldots,m$$
$$x_{ij} \geq 0, \quad i, j = 1,\ldots,m,$$

where the sums and inequalities are taken over existing arcs in the network. Here the symbol x_{ij} represents the flow from node i to node j. This is called the node-arc formulation of the MF problem since the constraint matrix is a node-arc incidence matrix (Bazaraa, 2010).

The aim of this optimization problem (1) is to masximize the value of f which represents the amount of flow passing from the source node to the sink node. The first constrain represents a conservation of flows: the sum of the flows entering a node must equal the sum of the flows exiting a node, except for the source node and the sink node. The second constrain represents capacity: the flow of an edge is non-negative and cannot exceed its capacity.

The optimization problem of the MF problem can be solved by various approaches, for example by linear programming or by Ford–Fulkerson algorithm, which finds directed paths from the source node to the sink node with available capacity on edges in this path. In the algorithm, this path-searching process is repeated until no additional flow can be added to this directed path. The algorithm uses the concept of so called residual networks (Ahuja et al., 1988), which represents the maximum additional flow that can be sent from any node i to any node j using the arcs (i, j) and (j, i).

The case of multiple sources and sinks, involving several source nodes $s_1, s_2, \ldots, s_k$ and several sink nodes $t_1, t_2, \ldots, t_r$, and where the flow from any source can be sent to any sink, it is known as Multiple Sources and Sinks problem, and can be straightforwardly converted into a one-source and one-sink problem by introducing a supersource s (virtual source node) with edges (of unlimited capacity) directed from this supersourse s to all source nodes $s_1, s_2, \ldots, s_k$. Furthermore, a supersink node t (virtual source node) is introduced with edges (also of unlimited capacity) directed from all sink nodes $t_1, t_2, \ldots, t_r$ to t. Then the problem of maximizing the total value of the flow from all sources is then the same as that of maximizing the value of the flow from s to t.

In order to concurrently model both reliability and capacity constraints of the gas transmission network, stochastic network representation is used, where each node and edge of the flow network can randomly fail, according to a predefined probabilistic model. The component failures in the network are modelled by the Monte-Carlo simulation technique.

The algorithm has these inputs:

- The capacity matrix C that provides information about capacity constraints of the network elements including input source nodes, demand nodes and information about connected pipeline capacities;
- The length matrix L that provides information about length of the edges between nodes. This matrix is used to generate pipeline failures in the network;
- Component failure probabilities and failure consequences to the network operation;
- Supply and demand data for each node in the network.

The output of the algorithm is an optimal flow matrix F satisfying for each Monte-Carlo step the relation (1) and the distance based supply pattern, in which the nodes closer to the source are served first. In order to correctly model the priority supply pattern based on the distance from the source node for the case of tasks with multiple sources and sinks, additional conditions has to be introduced. For a task with multiple sources, the links between the virtual source node s and the source nodes $s_1, s_2, \ldots, s_k$ are assumed to be unidirectional. It also means that the virtual source node cannot be reached from source nodes. This condition is expressed in the length matrix by adding further constrains: infinite distance. The same is valid in case of multiple sinks.

At the initial stage of the computational process, for each Monte Carlo simulation run, network configuration is generated by using failure probability matrix P. This step defines which network components are operating and which are failed. The total failure of the network element causes the component inaccessibility, which can be coded in the algorithm by an infinity distance penalty. The length matrix must be updated accordingly. The algorithm can be also used for modelling the partial failure of a multi-state component, which can be expressed by a partial reduction of the component capacity. In the next step distance vector is computed. It contains the distance of the shortest paths between the virtual source node and all remaining non-virtual nodes. For this purpose, Matlab tool Bctnet (Rubinov and Sporns, 2010) based on Dijkstra's algorithm was used. Contrary to the classical Dijkstra's algorithm, it is not necessary to compute the full distance matrix, as only the distance from the virtual source node is used

in the developed algorithm. The distance vector is used to prioritise the supply in case of lack of available gas in the network due to disruption scenarios or component failures. At the last step flow matrix F of the Maximum flow algorithm is computed. The aim is to maximize the flow from the virtual source node 1 to the virtual sink node t, according to given constrains by using Ford–Fulkerson algorithm. The resulting flow matrix F is ready for further exploration by statistical methods in order to estimate lack of gas probability and determine the weakest nodes in the network.

3 TEST CASE

Figure 1 shows topology of the test case gas transmission network. It is based on a real country network topology and data, however geographical locations are not displayed.

Table 1 shows types of nodes used in the test network. The virtual supersource node 1, virtual supersink sink node 47 and other virtual nodes (used for computational purposes only) are not shown in the Table 1. The test case network contains major elements of the gas transmission network. The network is supplied by pipelines and no LNG terminal is available. Table 2 shows maximum capacities of input supply nodes in millions of cubic meters (mcm) per day. It should be noted that maximum shown UGS supply capacity decreases with time.

The total maximum supply capacity is 24.7 mcm per day. The total network demand (Node 47) is 16.8 mcm/d, so the network has certain degree of spare capacity to compensate supply disruptions.

The probability failure matrix P is based on the following annual failure rates:

- Compressor Station (CS) failure: 2.5E-01/yr;
- UnderGround Storage (UGS) failure: 2.5E-01/yr,
- Pipeline failure: 3.5E-05 /km/yr.

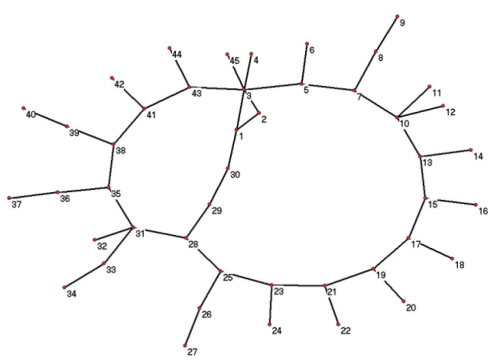


Figure 1. Topological layout of the test case network.

Table 1. Types of network nodes: CS—Compressor station; UGS—underground storage; D—demand nodes (millions of cubic meters per day).

Node type	Node no.	Demand, mcm/day	Node type	Node no.	Demand, mcm/day
CS	2	0	D	24	0.022
CS	3	0	D	26	6.319
CS	35	0	D	27	0.445
UGS	30	0	D	29	0.132
D	4	0.348	D	32	0.930
D	6	1.183	D	33	0.051
D	8	0.052	D	34	0.177
D	9	1.594	D	36	0.142
D	11	0.060	D	37	0.104
D	12	0.048	D	39	0.209
D	14	0.003	D	40	0.178
D	16	2.109	D	42	0.6
D	18	1.158	D	44	0.258
D	20	0.089	D	45	0.072
D	22	0.532			

Table 2. Maximum supply capacity.

Node	Capacity, mcm/day
1->2	19.2
1->30	4.3
1->3	1.2

The CS failure rate was computed using a typical model of CS station and industrial reliability data. The UGS failure is modelled assuming the same probability of failure as a compressor station which is an assumption due to lack of reliable data. The pipeline failure rate was taken from EGIG (2011) incident database and assuming that rupture occurs 10 less frequently as incident.

As a consequence due to a CS failure, capacity reduction by 20% of the inlet pipelines and also the outlet pipelines until the next connection node is assumed. This assumption is based on physical flow models, however is not accurate in all cases and also multiple CS failures will have more severe effects on the network operation. Further research is planned in order to estimate the effect of CS failures more accurately.

4 STORAGE DISCHARGE MODELING

A number of studies have already been completed by using probabilistic gas network model (Praks & Kopustinskas, 2014) for 1-day duration. The present study case includes storage facility and 1-day model cannot capture the effect of reduced

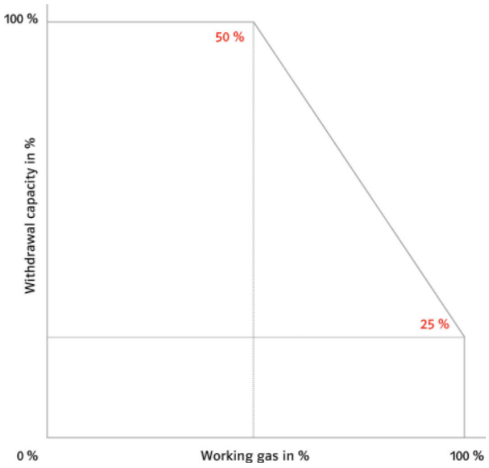


Figure 2. Typical storage withdrawal curve.

Table 3. Time steps and possible duration at lower discharge levels.

Time step	Duration, days	Discharge, mcm/d
1	15	4.3
2	45	3.0–4.2
3	40	2.0–3.0
4	40	1.0–2.0
5	–	0

flow from storages if disruption continues for a long period. The model was extended to be able to model disruptions in a time dependent manner for many days.

Figure 2 shows typical storage withdrawal pattern. In fact, maximum withdrawal capacity (Node 30 in Table 2) can be maintained only until 50% of the total storage capacity is reached and then linearly decreases. The minimum discharge capacity is about 25% of the maximum discharge capacity.

Assuming 70% level of the UGS in the present case study at the moment of disruption, maximum discharge level can be maintained for 15 days. Duration for lower supply levels are shown in Table 3. The model simulations in a time-dependent manner can be performed for each day, however due to memory limitations, 4 time steps were used, assuming minimum flow available. Time step 5 was also used reflecting empty storage situation.

5 DISRUPTION SCENARIOS

The probabilistic model takes into account internal component failures: pipelines, compressor stations and other facilities (storages, LNG terminals if present). However, external import supply by pipeline is not probabilistically modeled because of a number of reasons:

– Lack of upstream pipeline system model;
– Difficult to estimate numerically possible political/social origin of the disruption (e.g., Libyan war or Russian-Ukraine gas dispute);

The focus of the current study is on storage importance to address supply crisis, therefore only 3 scenarios were analysed in detail:

Scenario A: all facilities and input sources operate as expected;

Scenario B: storage facility is unavailable.

The storage discharge is modeled in Scenario A with 4 time steps (see Table 3).

The model results are obtained by running 1 million Monte Carlo simulations.

6 MODELING RESULTS

The modeling results for 1-day are shown in Table 4 (Scenario A) and Table 5 (Scenario B). The time-dependent storage discharge effects are modeled by additional simulations and results are reported

Table 4. Probabilistic results of Scenario A for 1-day for demand D as shown in Table 1.

No	P(X = 0)	P(X < 0.5D)	P(X < 0.8D)	P(X < D)
4	0.00038	0.00038	0.00038	0.00038
6	9.00E-06	9.00E-06	0.000697	0.000698
8	0.000704	0.000704	0.000704	0.000704
9	0.000705	0.000723	0.000723	0.000723
11	0.0007	0.0007	0.0007	0.0007
12	0.000699	0.000699	0.000699	0.000699
14	0.000721	0.000721	0.000721	0.000721
16	0.000731	0.00081	0.001116	0.001181
18	0.000876	0.000878	0.000878	0.000878
20	0.01637	0.01637	0.01637	0.01637
22	0.01663	0.01663	0.1101	0.1101
24	0.01647	0.01647	0.01647	0.01647
26	0.000198	0.000275	0.01646	0.01648
27	0.01648	0.01648	0.01648	0.01648
29	0.000193	0.000193	0.000193	0.000193
32	0.000702	0.000702	0.000702	0.000702
33	0.000702	0.000702	0.000702	0.000702
34	0.000714	0.000714	0.000714	0.000714
36	0.001194	0.001194	0.001194	0.001194
37	0.001196	0.001196	0.001196	0.001196
39	0.000697	0.000697	0.000697	0.000697
40	0.000703	0.000703	0.000703	0.000703
42	0.000697	0.000697	0.000697	0.000699
44	0.000693	0.000693	0.000693	0.000693
45	0.000305	0.000305	0.000305	0.000305
47	0	0.000697	0.000885	0.1114

Table 5. Probabilistic results of Scenario B for 1-day for demand D as shown in Table 1.

No	P(X = 0)	P(X < 0.5D)	P(X < 0.8D)	P(X < D)
4	0.000378	0.000378	0.000378	0.000378
6	6.00E-06	6.00E-06	0.000639	0.000639
8	0.000641	0.000641	0.000641	0.000641
9	0.000643	0.000701	0.000701	0.000701
11	0.000639	0.000639	0.000639	0.000639
12	0.000639	0.000639	0.000639	0.000639
14	0.000697	0.000697	0.000697	0.000697
16	0.000699	0.000879	0.00088	0.000881
18	0.000882	0.000883	0.000883	0.000883
20	0.06335	0.06335	0.06335	0.06335
22	0.06425	0.06425	0.4366	0.4368
24	0.064	0.064	0.064	0.064
26	0.000644	0.00085	0.064	0.06401
27	0.06401	0.06401	0.06401	0.06401
29	0.000644	0.000644	0.000644	0.000644
32	0.000641	0.000641	0.000641	0.000641
33	0.000641	0.000641	0.000641	0.000641
34	0.000642	0.000642	0.000642	0.000642
36	0.001148	0.001148	0.001148	0.001148
37	0.001148	0.001148	0.001148	0.001148
39	0.000637	0.000637	0.000637	0.000637
40	0.000637	0.000637	0.000637	0.000637
42	0.000634	0.000634	0.000634	0.000638
44	0.000633	0.000633	0.000633	0.000633
45	0.000304	0.000304	0.000304	0.000304
47	0	0.000642	0.0012	0.4374

below in this section. By interpreting the results, the following model features should be considered:

- Failures are simulated on annual basis;
- No more failures nor repairs can occur during time-dependent phase of the simulation;
- Demands are assumed to be maximum peak demands throughout the year.

Under scenario A the overall network reliability is good enough, as probability to supply less than required maximum demand (D) is 1.1E-01 per year and probability to supply less than 80% of demand is only 8.8E-04 per year, see Figure 3 for details. Looking at the specific locations, Node 22 seems to be the weakest point of the network but its demand is low. Probability to supply less than demanded volume is 1.1E-01 per year, in fact very close to overall network non-supply probability. The other nodes with the highest probability of non-supply are 20, 24,26 and 27, but their corresponding probability is much lower: 1.6E-02 per year of having less than demanded gas. In case of Node 26 (high demand node) the probability to have no gas at all is very low: 2E-04 per year, and less than 50% of maximum demand: 2.7E-04 per year. The model allows quantification of the obvious advantage of ring gas network structure against the tree structure (Praks & Kopustinskas, 2014). Other network nodes have lower non-supply probabilities and indicate relatively reliable supply situation.

Under Scenario B (UGS is not available) the network is affected, but at rather moderate levels in terms of severity. Nodes 22 remains the weakest link (complete annual loss of supply probability is 4.368E-01) and Nodes 20, 24, 26 and 27 are second weakest points (complete annual loss of supply probability is 6.4E-02) of the network as they are geographically situated far from the single supply source. However, Node 26 (high demand node) supply situation is much better compared to other weakest points as its complete loss of supply probability differs significantly (6.4E-04 per year). The total network probability of supply less than demanded is 4.374E-01 per year and Node 22 is the major contributor to this probability. Probability to have less than 50% of demanded gas in the network is significantly lower: 6.4E-04 per year. Figure 4 provides more details on CDF of the total loss of supply probability.

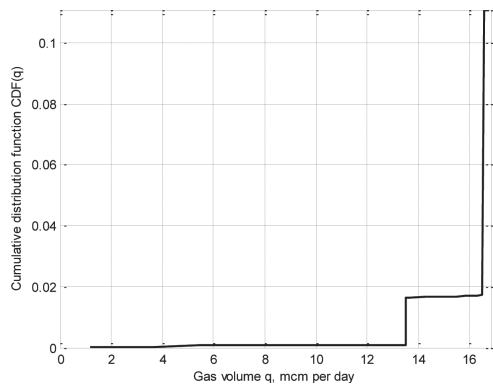


Figure 3. Cumulative distribution function of the total network supply under scenario A.

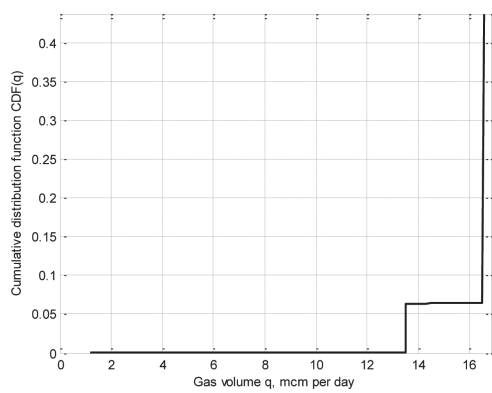


Figure 4. Cumulative distribution function of the total network supply under scenario B.

The next set of computations was performed for different time steps as presented in Table 3. The results show the effect of storage discharge volumes available for the consumers, see Table 6.

Figure 5 shows CDF at different time steps and the effect of storage supply can be quantified. Computations were performed for different supply levels at the main pipeline connection (Node 2), having maximum capacity of 19.2 mcm per day (Table 2). The following hypothetical supply capacity of Node 2 was analysed:

15 mcm per day (Figure 6);

13 mcm per day (Figure 7);

10 mcm per day (Figure 8).

The effect of storage supply is well visible in these CDF plots and can be quantified. For example, when full input capacity is available, probability to get less than 80% of demanded gas is rather low and is estimated to be 1.2E-03 per year even if storage is unavailable (Table 6). However, if Node 32 supply capacity is reduced to 10 mcm per day (almost 50% reduction) then probability to get less than 66% of the demanded gas reaches one at time step 3 (after 60 days). The results are available for each node, however they are most interesting at the total network level.

Using the probabilistic network model, many hypothetical scenarios can be tested in order to

Table 6. Estimated probabilities of the total available gas in the network at different Time steps (Ts).

Ts	P(X = 0)	P(X < 0.5D)	P(X < 0.8D)	P(X < D)
1	0	0.0007	0.00089	0.11
2	0	0.0007	0.00089	0.16
3	0	0.0007	0.00089	0.16
4	0	0.0007	0.0011	0.16
5	0	0.00064	0.0012	0.44

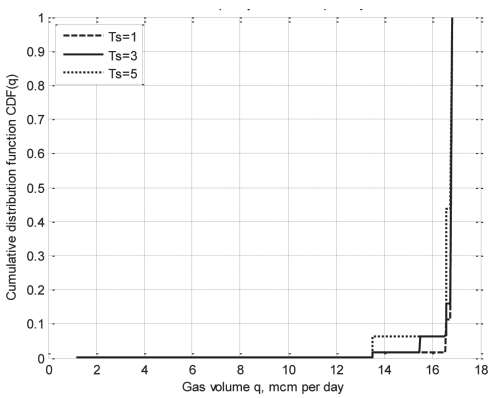


Figure 5. Cumulative distribution function at time steps 1, 3 and 5. Pipeline supply in Node 2 is fully available.

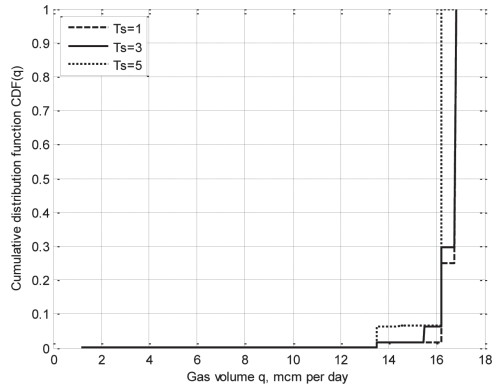


Figure 6. Cumulative distribution function at time steps 1, 3 and 5. Pipeline supply in Node 2 is reduced to 15 mcm per day.

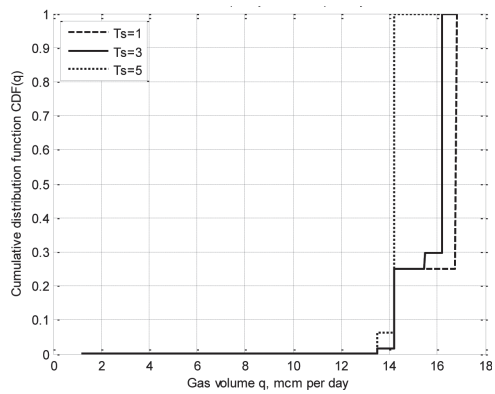


Figure 7. Cumulative distribution function at time steps 1, 3 and 5. Pipeline supply in Node 2 is reduced to 13 mcm per day.

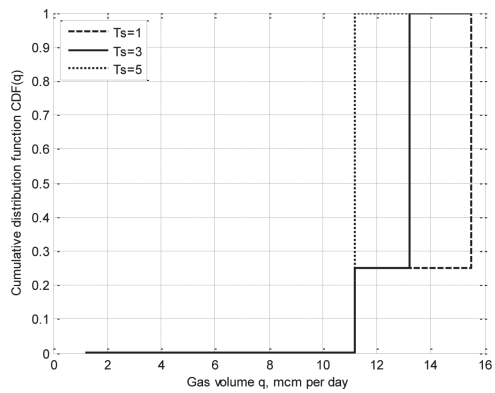


Figure 8. Cumulative distribution function at time steps 1, 3 and 5. Pipeline supply in Node 2 is reduced to 10 mcm per day.

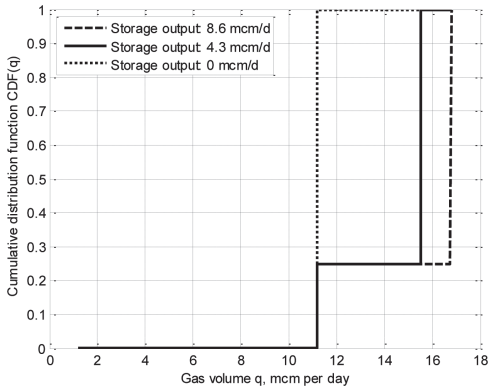


Figure 9. Comparison of the storage effect with double maximum discharge volume.

investigate network response and find optimum configuration. For example, storage maximum discharge volume can be increased and the effect to the network can be quantified.

Figure 9 effectively shows the results of the double maximum storage discharge volume effect on the total gas volume availability in the network. Similar "what-if" type of analysis can be done for any element and parameter in the network in order to effectively plan network modifications and quantify various options in terms of security of supply.

7 CONCLUSIONS AND DISCUSSION

The probabilistic gas network model has been developed and tested on a number of scenarios including time-dependent storage discharge scenario. The testing network is a real one country gas transmission network, but its geographical location is not provided. The model has a number of advantages and limitations that must be considered by interpreting the results. The model at this stage cannot model adequately consequences of failures of compressor stations. Currently, it is assumed that pipeline capacity is reduced by 20% in the nearest section, however this assumption needs to be validated by physical flow computations. Failures of two nearby compressor stations would have severe effect on the network capacity, but this event is not considered in the current version of the probabilistic model.

The model currently computes time-dependent storage discharge in a simplified step-wise manner. These limitations will be eliminated or reduced in the future versions of the model.

Despite the limitations, the model provides an indication of the worst networks nodes in terms of security of supply and provides their numerical ranking. It is recommended to use the results of the model in a qualitative (comparative) way rather than interpret numerical values directly. The model is very powerful to compare and evaluate different supply options, new network development plans and analyse potential crisis situations.

REFERENCES

Ahuja R, Magnanti T. & Orlin J. 1988. Network flows. MIT.

Ball M., Colbourn C. & Provan J. 1992. *Network Reliability*. University of Maryland. http.//hdl.handle.net/1903/5255.

Bazaraa M., Jarvis J. & Sherali D. 2010. Linear Programming and Network Flows, John Wiley & Sons.

Deo N. 2008. Graph Theory with Applications to Engineering with Computer Science. Prentice Hall.

EGIG, 2011. 8th Report of the European Gas Pipeline Incident Data Group. Groningen, Netherlands.

EU Regulation. 2010. Regulation No.994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC. Official Journal of the European Union, L295. 53:1–22.

Johansson J., Hassel H. & Zio E. 2013. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliability Engineering & System Safety* 120: 27–38.

Praks P. & Kopustinskas V. 2014. Development of a gas transmission network reliability model: A case study. In Steenbergen et al. (Eds), Safety, Reliability and Risk Analysis: Beyond the Horizon; Proc. ESREL 2013, Amsterdam, 29 Sept—2 Oct 2013. CRC Press, pp. 2177–2183.

Rubinov M. & Sporns O. 2010. Complex network measures of brain connectivity: Uses and interpretations. *NeuroImage* 52:1059–69.

Zio E., Golea L. & Sansavini G. 2012. Optimizing protections against cascades in network systems: A modified binary differential evolution algorithm. *Reliability Engineering & System Safety*, 103:72–83.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Weekly availability changes of web applications implemented in virtualized environment

T. Walkowiak
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT: Paper presents a numerical method for determining changes of availability of web applications implemented in virtual environment. It takes into account the reliability and performance aspects of software and hardware elements of the web system. The revenue process model takes into account working hours of administrators and a time of repair (or reconfiguration) for each type of failures. The described method was a basis for the development of a Monte-Carlo simulator that allows calculating variability of web application availability over a week. The paper contains the numerical results for a test case web application implemented in virtualised environment.

1 INTRODUCTION

Over the last decade we observe not only rapidly increase in a number of web page users but also significant amount of new web applications, that became available every day. As modern web applications are complex systems with wide range of features and access to many external services, meeting expectations of nowadays user is a challenging task for websites providers.

The formal service's requirements are defined in a negotiated agreement between a customer and a website provider which is called SLA (service-level agreement). One of the most significant problems that web site providers have to face is how they can provide the QoS (quality-of-service) required by their clients, having in mind that the web traffic is highly dynamic and volatile (Liu et al. 2006). A given web server configuration may meet requirements under some traffic load while under other workload its performance may not be satisfying.

Many aspects like hardware features, software characteristic, a multilayer architecture and network aspects make the problem of analyzing, projecting and reconfiguration of the web service not a trivial one. One of important techniques in implementing web application is virtualization. It supports the backups and rollback feature, which allows recovering virtual machine after security breaches (Hoopes 2009) and performing reconfiguration (Walkowiak & Caban 2014) very fast.

One of quality metrics used for web systems is availability, defined as the probability that a user will be properly serviced by a system at a specific time.

In the paper we propose to analyze the availability of web systems implemented in virtualized environment. The analysis takes into consideration functional aspects (like changes in workload) and reliability aspects of the system on which the application is deployed. The reliability aspects includes virtualization environment, reconfiguration as a method of preserving continuity of services in case of failures (Caban & Walkowiak 2012) and working hours of system administrator (Walkowiak 2014).

The organization of the paper is as follows. We start with short analysis of related works, next virtualization and its reliability aspects are presented. In the section 4 the availability of a web application is defined including reliability and functional aspects. It is followed by a detail model of assessing the web application availability by computer simulation. Finally, a test case system is presented and its availability calculated as it varies in time (over a week). We conclude with a short summary.

2 RELATED WORKS

There are a large number of studies examining the reliability of websites or web applications. However, in most cases the reliability analysis is based on Markov processes (Barlow & Proschan 1996) and the analyzed system is modelled as a simple serial one (Lipinski 2006). The Markov or Semi-Markov approach have significant limitations (Malinowski 2012) which includes the limited distributions (mostly exponential), narrow applicability (only to a special class of systems) and poor compliance with reality. That is why computer simulation (Juan et al. 2012) is used for availability analysis of complex systems.

The administration hour's model presented in the paper aims to create a detail model of repair time. Whereas due to the popularity of the Markov approach the most common assumption done by researches is a usage of exponential distribution for a repair time (Aven & Uve 1999). In fewer cases researches are using other distributions (Jia & Wu 2009) or compose the repair time of two periods: waiting and real repair (Zhang & Wu 2009). The last one approach is related to presented here.

The paper addresses some issues connected with relocating services as a reaction to hardware failures and security incidents, so called reconfiguration. This is a well-documented concept and a review of which is given in (Lent 2012). The analysis of the system availability under reconfiguration could be found in (Walkowiak & Caban 2014).

Methods of availability analysis of web systems that are described in the literature are based on the analytical models (Gokhale & Jijun 2006) on real system monitoring (Banerjee et al. 2010) or computer simulation (Rahmawan & Gondokaryono 2009).

The approach presented in this paper is an extension to work (Walkowiak 2014). The extension includes:

– modelling failure results not only by as an inoperability of a component but also by a degradation of component performance,
– modelling the reconfiguration process as a reaction to failures,
– analysis of web application deployed in virtual environment resulting in a hierarchy of failures (virtual machines and physical servers) and less importance of hardware failures.

3 VIRTUALIZATION

3.1 *Introduction*

IT industry is nowadays affected by virtualization trend. Increasing popularity of virtualization was born since it became clear that virtualization is supposed to help companies to save money on IT costs. Virtualization advantages encourage business owners to invest in it. However, they should also take in consideration the risks, dangers and weaknesses of this technology (Stanclik & Walkowiak 2013).

The term virtualization refers to methodology of dividing the computer (or server) resources (the CPU, memory, disk drives, network interface cards and so forth) in to multiple separate execution environmental achieving by many mechanisms such as hardware partitioning, time-sharing, partial or complete machine simulation, emulation and others. The resulting environments which are called virtual machines should ensure efficiency as high as possible (Smith & Nair 2005).

3.2 *Reliability aspects of virtualization*

Moving business into virtualization brings undoubtedly many benefits. First, server consolidation allows increasing the utilization of physical servers. Many servers use only 10 to 15% of hardware re-sources (Portnoy 2012), thus other resources are wasted. Such a solution is very unprofitable. Virtualization gives the way to better utilization of resources. Moving processing environments to virtual machines decreases the number of physical machines with utilization ratio up to 90% (Portnoy 2012). Fewer servers also reduce the costs of power consumption as well as money spends on hardware maintenance.

Each guest operating system deployed on the server running in isolation manner, which is crucial for a secure and reliable environment. Any guest's fault appearing in the virtual system cannot be spread on the others while virtual machines' operations are separated from each other. This feature keeps virtual environment safer. Additionally to increase security level, during configuration security settings can be assigned to virtual machines rather than to the server. It relates especially to the access privileges. In standard operating system each application in general runs with administrator access. However under virtualization applications can be run on the designated virtual machines, each may be configured with different credentials and different privilege access.

Hardware management is one of the biggest challenges that organizations are faced with. Each failure or hardware upgrade can take hours to restore server operability. Virtualization makes the virtual infra-structure management more convenient and efficient. Since operating systems are independent from the hardware they can be easily moved to another server. This is a key feature when server's memory capacity gets low especially it takes only a few minutes. A storage virtualization gives also better way for data management. Data centralization makes data access much easier when it can be assigned as a single logical entity instead of being separated along several individual physical servers.

To protect business continuity virtualization provides also disaster recovery mechanism. Disaster recovery ensure that when virtualized system crash, it will be restored as quick as possible. With system allows to take snapshots of current state of system each virtual machine can be backup from any time, for example from last week. What is more such mechanism is used for data replication

keeping data consistent and up to date. (Stanclik & Walkowiak 2013)

4 AVAILABILITY OF WEB APPLCIATION

4.1 *Reliability analysis*

The faults occurring in the web based systems can have multiple causes. Hardware faults, most commonly considered in reliability analysis, occur relatively rarely due to the advances in manufacturing technology. However, they require long time to repair. (Walkowiak & Caban 2014)

Most failures in contemporary computer systems are caused by exploitation of software faults, which can have consequences ranging from decreased availability to complete blockage of an application. Intentional attempts at exploitation of software vulnerabilities constitute the most widespread type of threats to a web application. Human mistakes can have effects similar to vulnerability exploitation, even if they are less likely than the intentional attacks. (Caban & Walkowiak 2012)

Whenever a fault manifests itself in a web system, whether it is a hardware failure, a software error or a security attack, an administrator is faced with a difficult problem to maintain the continuity of business services. Isolation of the affected hardware and software is usually the first reaction (to prevent propagation of the problem to yet unaffected parts of the system). It then follows that the most important components of the application have to be moved from the affected hosts/servers to those that are still operational. This process of reconfiguration is easily achieved nowadays in virtualization environment.

Therefore, the web system from the reliability point of view is a repairable system. Faults occur in the system randomly, usually with a predictable distribution. Then the system for some time operates in a degraded state or becomes inoperational in a failure state until maintenance procedures start. It is firstly based on partly restoring the system operability by redeployment of virtual machines so for some time the system operates in degraded state and finally is restored to full operability. The performance of the application is different at each level of degradation. (Walkowiak & Caban 2014)

Summarizing, the application is operating in one of $0...L$ levels of degradation (including normal operations—without any failure). Since the process of changes of degradation levels is ruled by a random distribution let assume, that we could describe each level of degradation be its probability. Let $P(t,l)$ be a probability that the web application is in the l-level of degradation at time t [s], i.e.:

$$P(t,l) = \Pr(S_{l,t}), \tag{1}$$

where $S_{l,t}$ is an event that the application is in the the l-the level of degradation at time t.

4.2 *Availability analysis*

The paper focuses on assessing the availability defined as the probability that a user will be properly serviced by a web application at a specific time, i.e.:

$$A(t) = \Pr(U_t), \tag{2}$$

where U_t is an event that the application provides correct responses. It the previous section we have distinguished a set of levels at which the application is operating. Therefore, taking into consideration the conditional probabilities and Bayes' law the (2) could be calculated as:

$$A(t) = \sum_{l=0}^{L} \Pr(U_t \mid S_{l,t}) P(t,l). \tag{3}$$

It has been proven (Nielsen 1994) that if user will not receive answer for the service in less than 10 seconds he/she will probably resign from active interaction with the service and will be distracted by other ones. Therefore, the user is not properly serviced if there are too long responses of the web application. It could be caused by the system overload or/and the working of the system in the degradation state as a result of some failure. The response time in web systems depends also on the intensity of user request (Goseva-Popstojanova et al. 2010) that is changing in time—$\Lambda(t)$ [1/s]. Let's mark the availability of the web application at the l-level of degradation and under the intensity of user requests Λ as $Af(\Lambda,l)$, so:

$$\Pr(U_t \mid S_{l,t}) = Af(\Lambda(t),l). \tag{4}$$

Therefore, based on (3) and (4), the web application availability could be calculated as the expected value of functional availability over all degradation levels, i.e.:

$$A(t) = \sum_{l=0}^{L} Af\left(\Lambda(t),l\right) P\left(t,l\right). \tag{5}$$

The number of degradation levels could raise technical problems. For example if we assume that

the system consist of n independent components which could be failed and we consider two types of failures (distinguished based on its results) it results in 2^{2n} reliability states. It does not directly define the number of degradation states since several reliability states could be classified to one of L+1 degradation levels. But still L could be quite large and we have to assess the functional availability for each level of degradation.

The problem could be solved in a similar way as presented in (Walkowiak & Michalska 2011) by limiting the sum in (5) to the most probable levels and skipping less probable ones. It could be done by sorting all levels by its cumulative probability (calculated for the analyzed period T) starting with the most probable, and then by selecting N—levels that represent more than 99.99% of cases, i.e.:

$$0.9999 < \sum_{n=1}^{N} \int_{t=0}^{T} P(t,n)dt \tag{6}$$

5 AVAILABILITY ASSESSMENT

5.1 *Reliability model*

As it was stated in the introduction we are analyzing web applications that are deployed in the virtualized environment. Therefore, we could distinguish two groups of components that failure could result in the application inoperability or in the degradation of its performance: virtual machines and physical servers.

Let's assume that one technical service (like databases, web servers, application servers) is deployed on one virtual machine. This is a typical situation in case of virtualization. That is why we don't have to analyze additional levels in the reliability structure (i.e. technical services). A failure of one of servers results in a failure of all virtual machines deployed on that server and therefore of all technical services deployed on affected virtual machines.

The reliability analysis requires to model failures occurrence, their results and the repair time.

Let's assume that component failures could be modelled by a set of independent failures. Each component could fail in two different ways resulting in the component inoperability or in the degradation of its performance. The time to failure is modelled by the exponential distribution like in the Markov approach. The failure result is modelled by assigning each set of virtual machines (the lowest level of the hierarchy of components) failures to one of the degradation levels of the web application (including the level of the inoperability of the whole application). It seems that this is not a simple process. Since it has to take into consideration a large number of possible combination of failures, but, as noticed in section 4.2, it could be simplified by selecting only the most probable combinations. Moreover inoperability of one of virtual machines mostly results in inoperability of the web application. So cases with at least one inoperability failure exists are assigned to one degradation level. This is not true in case of the performance degradation failure.

Next step in the reliability analysis is the repair model. As it was stated in section 4.1 it is a three phase approach since at first the failed component is isolated and moved to other server or other virtual machine instance, secondly the component is repaired and finally the normal operation is restored. We need to describe the process of reconfiguration and to model duration of each phase.

We propose to model the repair time taking into consideration administrator working hours, i.e. a reconfiguration or repair could start only if the administrator is available. We assume that the administration staff works within a given time limit each day (defined by work start and finish hour) as well as on given days (working days) within a week. So the working hours of administration are periodic over a week time.

Let assume that the repair time consists of following phases:

1. time to failure discovery—equal to zero if a failure happens during working hours, in other cases it is a time to next working period;
2. failure analysis time—a time needed to discover a failure reason and to make a decision of how to reconfigure the system, we propose to model it by a random variable with a truncated normal distribution, it is a short period time so we assume that the administrator is finishing it even if it overlaps with a not working period;
3. component replace time—time required to replace a failed hardware component or to reinstall failed software component, it is modelled by a random variable with the truncated normal distribution plus an extra value in case of overlapping with not working hours; in case of hardware failures a repair time starts on the next working day, it models the delivery of a new system component by courier (Walkowiak 2014).

During a time to failure discovery and failure analysis time the web application is working on degraded level of performance defined by a failure type (like discussed above). After the failure analysis time system is reconfigured and the web application is working on degraded level of performance till the end of a repair time, when the application returns to normal operation. We assume that repairs of each component could be done independently

on each other, but degradation levels for each of repair time phases have to be analyzed.

5.2 *Degradation levels probability*

The described reliability model is based on a stochastic state-transition process, in which the states are described by the vectors of operability states of all the components in the system. The transitions between states are caused by incident occurrence and by renewal.

The state-transition model can be analyzed using a number of approaches: as a Markov chains, using semi-Markov processes or using Monte Carlo simulation (Fishman 1996). The applicability of each method depends on the assumptions that can be made regarding faults occurrence and a repair time. In case of the Markov approach, it is necessary to assume that both the faults and renewals occur with constant intensities (i.e. exponential distribution). Also the large number of states makes Markov or semi-Markov method more difficult to use. Presented in the previous section reliability model includes random values with exponential, truncated normal and discrete distributions as well as some periodic relations (staff working time), so it is hard to be solved by analytical methods.

Therefore, authors developed the reliability simulator for calculation of the probability of each degradation level. It was implemented in C++ within the Scalable Simulation Framework (SSF) (Liu 2006). Operation of the simulator is based on repetition of the failure and repair process simulation. Following simulations differ in the values of random variables occurring in the analyzed system. Knowing the distribution of these variables (input data for simulation), one can get information about the behavior of the system in the most probable cases. By observing changes of some metric values, the information about their distributions and any other statistics could be easily gathered. A single simulation last for a fixed length (in the analyzed case a multiplication of a week).

5.3 *Functional analysis*

The availability calculation method defined by (4) requires a way to assess the functional availability, i.e. the probability that a user will be properly serviced within a time less than a limit. It is a function of the degradation level and the intensity of user requests. The functional availability can be determined experimentally by performing load tests of real systems (using tools as: Funkload, Apache JMeter, Rational Performance Tester or Developer Tools from Microsoft), estimated by analytical models (Gokhale & Jijun 2006) or by simulation techniques (Walkowiak 2009). Due to fact that in case of virtualized environment it is easy to modify the system configuration, authors performed tests on the real system using self-developed load test tool. The tests were performed only for the most probable degradation levels (see section 4.2).

6 AVAILABILITY ANALYSIS OF A CASE SYSTEM

6.1 *Testbed overview*

The infrastructure of analyzed web system consists of six servers. From a pool of physical servers six virtual machines are created, on which Windows Servers are installed. All six servers are connected in a VMware cluster, under control of VMware ESXi hypervisor. The purpose of this solution is unbreakable high availability of the system, regardless of the efficiency of each server. The use of such a solution results from VMware policy, which assumes that if all servers are available, is best to keep each virtual machine separate on the server, which delivers high performance. The advantage is that if a server failure occurs, hosted virtual machine is moved up and running on the server that is the least loaded at the time. Servers and virtual machines are managed in fact from another virtual machine, VMware vCenter Server installed on one of hosts (we a copy on each of others).

In case of any failure in the system D2D2T (disk-to-disk-to-tape) backups are generated. It is the most popular backup strategy based on storing of the same data simultaneously on disk array and tape. This type of backup assumes that a backup is stored on the disk, and then stored on a magnetic tape media. As a result two backup copies are created. It is a protection in case something goes wrong during the data restoring. Then a second equivalent of a copy, stored on the tape, can be used.

6.2 *Reliability model parameters*

Since, today's computer devices are characterized by high reliability parameters, the intensity of server failure was set to one per three years. In case of hardware failures (assigned only to servers) the component replace time takes into consideration the time needed to delivery of a new system component by courier. The software components failure (with intensity set to one per year) with probability 0.2 results in the component inoperability, in other cases in the component performance degradation.

The repair model parameters were set as follows:

- mean failure analysis time—15 minutes,
- mean component replacement time—2 hours for inoperability failure, 15 minutes for performance degradation failure,

– working hours of administrator—8 am to 16 pm, Monday to Friday,
– standard deviation of truncated normal distributions—20% of its mean values.

6.3 *Simulation results*

Due to symmetrical structure of the system (identical servers, only one virtual machine per server, only one technical server on each virtual machine) and rule given by formula (6), only five levels of degradation were analyzed. The achieved results for simulating 3,000 weeks 5,000 times are presented in Figure 1. The changes of degradation level probability within a week could be noticed. The lowest value is achieved on Monday morning. It is caused by the fact that the administrator is not working during weekends and failures that occurred during that time are maintained on the next working day (Walkowiak 2014).

As it was stated in section 5.3 the functional availability was assessed by workload test on the real system. The results for analyzed degradation levels are presented in Figure 2.

It is obvious that the intensity of user requests varies in time. It depends on a type of provided service. But usually on weekends, there are fewer users then on weekdays. Also one could notice changes in traffic during a day with a peak load in a middle of day, and minimum load at night. For the analyzed case we have used the variations of intensity of user requests as presented in Figure 3.

And finally the web application availability could be calculated according to (4). The results are presented in Figure 4. It could be noticed that availability varies in time, following changes of user requests intensities and system reliability (due to a fact that the system administrator is not working 24 hours per day).

6.4 *Expected value of not properly serviced requests*

The web application availability plot from Figure 4 shows how the rate of properly serviced requests changes in time.

Since the intensity of users requests is also changing in time a more practical metric should show how many requests are rejected in a given moment of time. We propose to name it as expected intensity of rejected requests and define as:

$$Irr(t) = A(t) \cdot \Lambda(t) = \Lambda(t) \sum_{l=0}^{L} Af\left(\Lambda(t), l\right) P\left(t, l\right) \tag{7}$$

The value of this metric is presented in Figure 5.

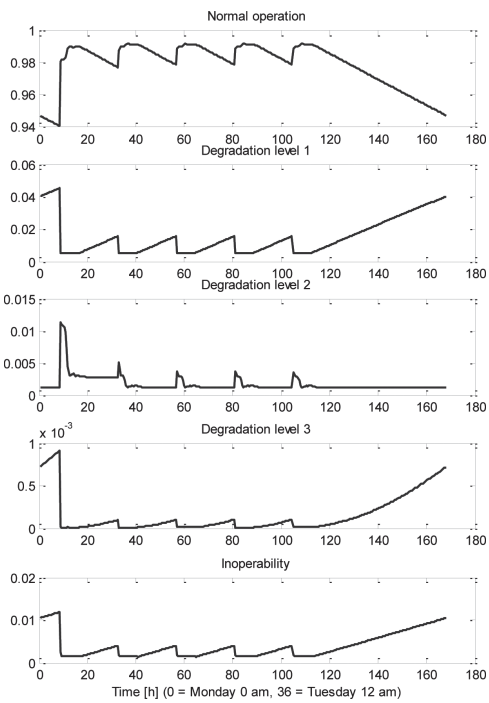


Figure 1. Probability of each degradation level as it varies over a week.

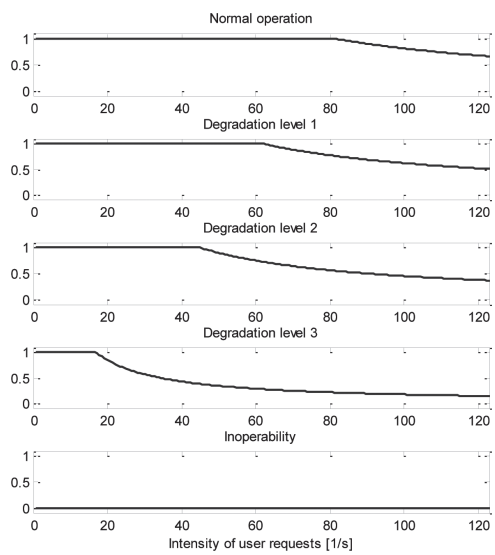


Figure 2. Functional availability for all analyzed level of degradation as a function of user requests intensity.

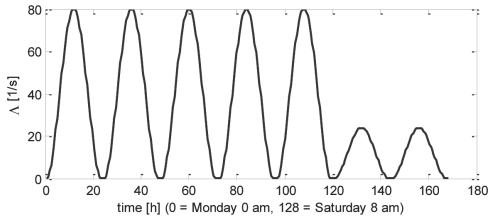


Figure 3. Assumed changes in user request intensity over a week.

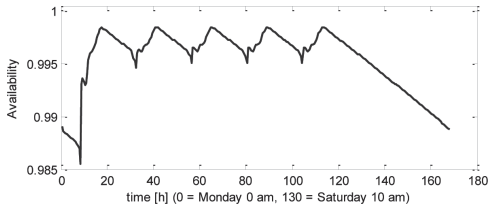


Figure 4. Web application availability changes over a week.

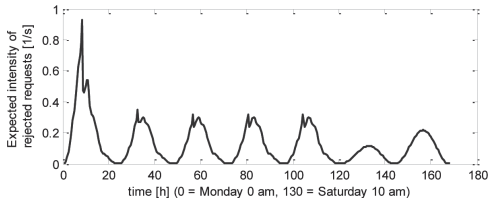


Figure 5. Expected value of not properly serviced requests changes over a week.

7 CONCLUSIONS

We have presented a method for assessing the availability of the web application based on modelling and analysis approach. It allows to:

- analyse the web application deployed in virtual environment
- analyse failures that results in an inoperability of or performance degradation of the system,
- model the reconfiguration process,
- model the repair time by three phases and to take into account working hours of administrators within a week,
- model the changes in user request intensity over a week.

The described method was a basis for the development of a Monte-Carlo simulator that calculates the variability of the web application availability over a week.

The reliability model contains some arbitrary assumptions, such as working hours of administrator. However, the proposed method allows changing the assumptions and thus different maintenance scenarios could be simulated. However, it could require changes in the source code of the simulator.

The presented method and developed tool allow to explore the impact of changes in the system maintenance (such as number of shifts or working hours of administrator) on the web application deployed in virtual environment availability. This is why the proposed solution may become the essential tool for operators of web systems.

Due to a fact that failures occur very rare in modern web systems and that the web system life is relatively short it is almost impossible to establish reliability parameters required to calculate the availability based on historical data. That is why these parameters are fixed based on experts' experience. To model the uncertainty introduced by experts we plan to use fuzzy sets, for example following methodology proposed in (Chongshan 2009), to model the web system availability.

The presented work was supported by the Polish National Science Centre under grant number N N516 475940.

REFERENCES

Aven, T., Uwe, J. Stochastic Models in Reliability. New York: Springer, 1999.

Banerjee, S., Srikanth, H. & Cukic B. 2010. Log-based reliability analysis of Software as a Service (SaaS). Proceedings of the 21st International Symposium on Software Reliability Engineering 1: 239–248.

Barlow, R. & Proschan, F. 1996. Mathematical Theory of Reliability. Philadelphia: Society for Industrial and Applied Mathematics.

Caban, D. & Walkowiak, T. 2012. Preserving continuity of services exposed to security incidents. In: Proc. The Sixth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE, 72–78.

Chongshan, G. 2009. Fuzzy availability analysis of a repairable consecutive-2-out-of-3: F System. In: Grey Systems and Intelligent Services, GSIS, 434–437.

Fishman, G. 1996. Monte Carlo: Concepts, Algorithms, and Applications, Springer-Verlag.

Goseva-Popstojanova, K., Singh, A.D., Mazimdar, S. & Li, F. 2006. Empirical characterization of session-based workload and reliability for Web servers. Empirical Software Engineering; 11(1): 71–117.

Gokhale, S.S. & Jijun L. 2006. Performance and Availability Analysis of an E-Commerce Site. Computer Software and Applications Conference, 1: 495–502.

Hoopes, J. 2009. Virtualization for security: including sandboxing, disaster recovery, high availability. Waltham: Syngress. 10, 20–25.

Jia, J & Wu, S. 2009. A replacement policy for a repairable system with its repairman having multiple vacations. Computers & Industrial Engineering,; 57(1): 156–160

Juan, A.A., Faulin, J., Ramirez-Marquez, J.E. & Martorell Alsina, S.S. 2012. Simulation Methods for Reliability and Availability of Complex Systems, Springer.

Lent, R. (2012). Evaluating a migration-based response to DoS attacks in a system of distributed auctions. *Computers & Security* 31(3), 327–343.

Lipinski, Z. 2006. State Model of Service Reliability. International Conference on Dependability of Computer Systems. IEEE Computer Society, 35–42.

Liu, J. 2006. Parallel Real-time Immersive Modelling Environment (PRIME), Scalable Simulation Framework (SSF), User's manual, Colorado School of Mines Department of Mathematical and Computer Sciences. [Available online: http://prime.mines.edu/]

Liu, X., Heo J. & Sha, L. 2006. Adaptive Control of Multi-Tiered Web Application Using Queueing Predictor. In IEEE/IFIP Network Operations and Management Symposium 5(3). Vancouver, BC, 106–114.

Malinowski, J. 2012. A simulation model for complex repairable systems with inter-component dependencies and three types of component failures. Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011, 128.

Nielsen, J. 1994. Usability Engineering. Morgan Kaufmann, San Francisco.

Portnoy, M. 2012. *Virtualization Essentials*. Indianapolis: Sybex. 9, 20–27.

Rahmawan, H. & Gondokaryono, Y.S. 2009. The simulation of static load balancing algorithms. International Conference on Electrical Engineering and Informatics, 640–645.

Smith, J.E. & Nair, R., 2005. The Architecture of Virtual Machines. In: Computer 5, 38. 32–38

Stanclik, M. & Walkowiak, T. 2013. Risk in systems with virtualization—test case analysis. *Journal of Polish Safety and Reliability Association* 4(2), 249–257.

Walkowiak, T. 2009. Information systems performance analysis using task-level simulator.. DepCoS—RELCOMEX, IEEE Computer Society Press, 218–225.

Walkowiak, T. 2014. Simulation based availability assessment of services provided by web applications with realistic repair time. *Eksploatacja i Niezawodnosc—Maintenance and Reliability* 16 (2), 341–346.

Walkowiak, T. & Caban, D. 2014. The impact of reconfiguration time on the dependability of complex web based systems. DepCoS—RELCOMEX, Springer, To appear.

Walkowiak, T. & Michalska, K. 2011. Functional based reliability analysis of Web based information systems. Dependable computer systems / Wojciech Zamojski [et al.] (eds.). Berlin; Heidelberg: Springer, 257–269.

Zhang, Y.L. & Wu, S. 2009. Reliability analysis for a k/n(F) system with repairable repair-equipment, Appl. Math. Model. 33(7): 3052–3067.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Dynamic approach to modeling MTBF/MTTR in industrial and logistics systems

P. Hoffa & P. Pawlewski
Poznan University of Technology, Poznań, Poland

ABSTRACT: Safety and reliability is very important in every system. Depends on characteristics of system and its specifics different maintenance strategy can be distinguished. Currently, companies seek to reduce operating costs (whether production costs or the provision of services). One of area in which they are looking for savings is maintenance of machines and equipment. That way companies look for suitable strategy. Looking for appropriate way of keeping devices able to work, with a view to lowering costs generated by that economy, can not forget about maintaining an appropriate level of safety and reliability of the study area. In this article authors focus on one aspect, which is simulation modeling of failure of individual elements in an analyzed transport system. Subject of interest of authors is a dynamic method of mapping a failure and damage in a transport system. Authors represent possibilities of modeling aspects of reliability within an area of logistics, which are analyzed, using a variety of approaches to modeling, like using MTBF/MTTR mechanism (MTBF—mean time between next failure, MTTR—mean time to repair) and sending messages by flow item to itself.

1 INTRODUCTION

An article presents results of authors research, relating to a safety and reliability of systems. The general maintenance strategies are shown with their brief characteristics. Attention was drawn to need for selection of an appropriate strategy depending on analyzed system and its specifics. In this paper, authors limited their work to area of logistics—saying more specifically to an issue of maintenance in a field of transport and road infrastructure. Authors focus on one aspect, which is simulation modeling of failure of individual elements in an analyzed transport system. Simulation modeling is a modern method allows a simulation, experimentation, analysis and optimization of an investigated process. Subject of interest of authors is a dynamic method of mapping a failure and damage in a transport system.

Article shows the following aspects:

- a possibility of using, available on a world market, simulation software to analyze a maintenance of a specific area of logistics;
- a need to integrate an approach of Discrete Event Simulation (DES) with simulation based on agent (ABS) in order to modeling a maintenance of an exemplary model of logistics area;
- technique of modeling a disruption/failure of objects, which "are flowing" through a process.

Main purpose of this article is to present possibilities of modeling aspects of reliability within an area of logistics, which are analyzed, using a variety of approaches to modeling.

Main contribution is: the fact that an object is created dynamically, and labels describing the MTBF and MTTR (MTBF—mean time between next failure, MTTR—mean time to repair) definitions are defined when the object is created during a simulation experiment—it make different approach from standard solutions, used in traditional simulation programs.

An article consists of five parts. Section 2 and 3, respectively, contains a description for maintenance issues and a traditional modeling of damage and failure, that is modeling using MTBF/MTTR. A section 4 presents way of modeling failure of selected elements with using agent-based technology. An article ends with conclusions and plans for further work.

2 SYSTEM SAFETY AND RELIABILITY—GENERAL APPROACH

Currently, due to the large availability of any goods or services on the market, the main competitive factors are price and quality of offered goods or services. Companies seek to reduce operating costs (whether production costs or the provision of services), operating costs. One of areas in

which savings are sought is an area of maintenance of machines and equipment. Through look for (define) a suitable method of maintenance for an area of logistics is possible to reduce costs related to a maintenance of equipment and infrastructure (included in a given area) at an appropriate level of action.

Looking for appropriate way of keeping devices able to work, with a view to lowering costs generated by that economy, can not forget about maintaining an appropriate level of safety and reliability of the study area. Neglect of maintain an adequate efficiency levels of machines and devices (related to cuts spending on operations) may involve a complete destruction of the machine or an accident involving humans.

Speaking of issue of safety and reliability of the system, we should pay attention to a very broad aspect of this issue. We can consider production systems, distribution systems, civil infrastructure (such as transportation, water supply, sewers, telecommunications, and electrical and gasnetworks) and the other. In the literature many articles can be found refering to a safety and reliability of various systems (Braglia et al., 2012), (Kim & Kang, 2013), (Zhou et al., 2013), (Barone & Frangopol, 2014), (Aven & Pedersen, 2014). Each system is characterized by specific properties, therefore, for each of them an appropriate method of maintenance should be selected.

Activities related to a maintenance of machinery and equipment at an appropriate level of functionality are considered as unavoidable source of cost. Depending on specifications of the system, these costs range from several to several tens of percent of a total cost. The effect of damage, besides failure of machine for work, can also become a problem with a safety and protection of an environment, which can lead to deterioration of an image of the company (Jasiulewicz-Kaczmarek, 2009a). Therefore, maintenance strategies have a special meaning in the industry (Swanson, 2003); (Vatn & Aven, 2010); (Jia & Cui, 2011); (Tan et al., 2011).

We can distinguish different maintenance strategies (Jasiulewicz-Kaczmarek, 2009b)—two extremes are: preventive maintenance and actions taken only by the occurrence of damage. Costs associated with maintenance depend on a chosen strategy. In that way, companies are looking for solutions to reduce costs while keeping service maintenance on the assumed level.

In the literature we can find many articles about maintenance and strategy of maintenance. Relying on Pawlewski and Jasiulewicz-Kaczmarek (where review of the older, classical methods was presented), several strategies depended on a viewpoint of the goal of a strategy can be distinguished (Pawlewski & Jasiulewicz-Kaczmarek, 2011):

- "Profit oriented strategies; their aim is to plan actions in a profit-maximizing manner, which means, for instance, phasing out technical devices that bring no profit, and reducing investment expenditure to the level that is absolutely essential to sustain economic activity of a company.
- Cost minimization oriented strategies; their aim is to plan actions that will lead to a maximal reduction of costs, e.g. by liquidating supportive departments and the implementation of outsourcing.
- Strategies oriented towards working time maximization; their aim is to maintain technical availability of machinery and technical devices according to the scheduled period of time by means of increasing expenditure on maintaining the efficiency and technical availability of the company's own technological potential, which results from the appointed operational policy." (Jasiulewicz-Kaczmarek, 2009b).

Simulation is one of the methods enable companies to analyze the operation and maintenance services and a financial investment related to this services. New methods for selecting maintenance strategy are created. They are based on use of simulation and optimization experiments. The traditional approach based on the use of a process approach and DES simulation (discrete event simulation). Specificity of maintenance problems, research issues of maintaining system components able to work, mapping failure events and process of their removal also require consideration of other approaches.

The following article focuses on ways of failures and components damages modeling for chosen by authors logistics area. This area includes a supply chain, more specifically a transport of goods from point A to point B. Very often problems of failures of machines and devices involved in the manufacturing process are described. But, to deliver this product to a customer, a transport operation is necessary. Therefore, authors decided to focus on ways of modeling failures and damage components (which are involved in transport)—more specifically on means of transport engaged in the carriage and the other participants in the road.

On the route of goods delivery it can be distinguished a number of possible disruptions. Authors, based on their own experience and observations, distinguished following interferences under this area:

1. Related with means of transport
   - Failures of the means of transport—a failure is random; based on historical data you can predict the probability of such situation; this failure is associated with the time of waiting

for help, and the time required to repair a fault;
- Not providing a vehicle on time (e.g. due to theft)—a disturbance is random; it is necessary to determine the probability of this situation; it results in significant delay in order execution (associated with the search for a replacement car), or failure in order execution;

2. Related with the route
   - Traffic congestion—random factor; based on historical data it is possible to determine the volume of traffic in a changeable geographical/spatial area; it shortens or extends the duration of the transport order;
   - Road traffic accidents (so-called "black spots")—random aspect; based on historical data it is possible to determine the probability of an accident in so-called "Black spots"; vehicle accident without participation of the vehicle executing the transport order: it is associated with a stoppage at the accident site; an accident involving a vehicle performing a transport order: it is associated with longer duration of order execution due to the need to provide roadside assistance, as a result of damages it may impossible to execute the order;
   - Weather conditions (sudden bad weather)—this disturbance is random in nature; based on historical data and weather maps it is possible to determine points of weather breaks; an area of this disturbances will be changeable—depending on strength of this phenomenon; results of this disturbance is time extension of realization order (associated with a lower traveling speed);
   - Toll-collection points on toll roads (in case of toll road)—a time of paying the fee should be determined as a variable (depending on the number of cars waiting to pay the toll and the individual characteristics of particular drivers);
   - Natural disasters (hurricanes, floods, etc.) and other situations that slow down traffic on the road (e.g. strikes)—a disturbance is completely random in nature, it involves a changeable geographical/spatial area affected by the disturbance; it results in significant lengthening of order execution (associated with a slower traveling speed), or failure in order execution;

Authors, later in an article, focus on way of modeling of failure means of transport. They describe in details two ways of modeling a vehicle breakdown, depending on whether we focus on one vehicle or group of vehicles (which creates a traffic on a route).

3 MODELING DAMAGE WITH MTBF/MTTR (DES)

Shown approach to modeling failure of means of transport is presented for simulation model, which use MTBF and MTTR mechanism. The main purpose of this chapter is to show the way of modeling damage with MTBF/MTTR mechanism, not to show exactly a simulation program. MTBF and MTTR mechanism is offered in different simulation softwares. Authors uses Flexsim programme to show this approach. It is possible to define MTBF (time between the occurrence of the next failure) and MTTR (the time required to repair the damage) for almost all objects occurring in the system (Fig. 1). Using this mechanism it is possible to determine an occurrence of any failure of vehicles involved in the analyzed area. In addition, it is possible to model a damage of point on the route—in this way you can map disturbance for exactly a point of road.

Figure 1 presents pre-established times for analyzed operations. Of course it is possible to edit them, depending on user needs. It can be set any statistical distribution with the specified values or other rules of occurrence (Fig. 2).

Presented MTBF/MTTR tool provides a simple and quick way to model a failure of mean of transport or reproduction in some way interference in some points (network in route). However, this approach is limited—allows to modeling failure for static objects, which have been defined at time of creation of model (before performing a simulation experiment) permanently assigned to a model (resources which are not changing position

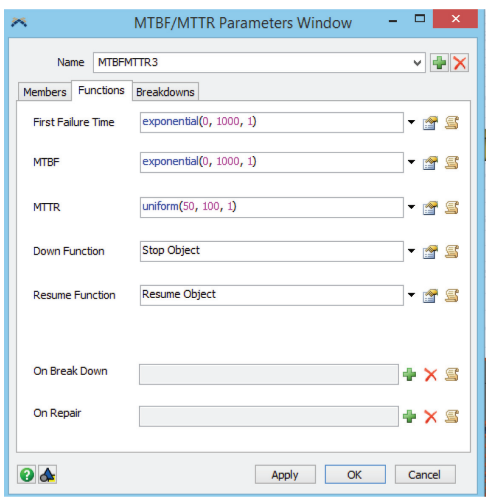


Figure 1. MTBF/MTTR Parameters Window (Source: Flexsim model).

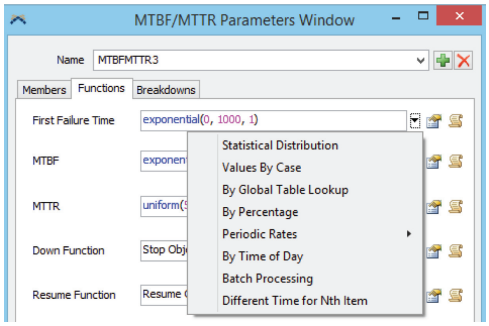


Figure 2. Additional parameters (Source: Flexsim model).

(fixed resource) and resources which are moving (mobile resource)). However, all these elements must be introduced into a model before starting a simulation experiment. This means that in a case of modeling a route with defined traffic volume, these vehicles must be made permanent to a model. They are not generated in a dynamic way. This is a significant limitation. When a situation in which the number of means of transport is unknown, vehicles are dynamically generated during an execution of simulation experiment. In this situation presented approach can not be applied. Authors propose for such cases, a different way of modeling interference/failure, which is described in the next section.

4 FLOW ITEMS DEMAGE MODELING (ABS + MESSAGES)

Authors, in order to model disturbances/failures of objects created dynamically during execution of simulation experiment, suggest use of modeling ABS (called Agent-Based Simulation) with a mechanism for sending messages between objects. To create other transport means in the model in dynamically way, it was decided to map vehicles by using flow items. Flow items are elements flowing through a process. They are not a static resource, they are created and destroyed during the simulation experiment. Creating means an input flow item into the system, manufacturing process, and a destruction means an output flow item of the analyzed system. For these items a failure by MTBF/MTTR can not be modeled. A failure of these components is a random event that affects whole transportation process. Therefore, for flow item authors suggest use an agent-based approach, specifically mechanism of messaging between objects.

To realized such a defined task FlexSim program was used. It is a simulation software, in which tools are both powerful and user-friendly. Analysis and optimization any system in any industry is possible with using FlexSim. Flexsim allows:

– a creation flow items as task executors,
– sending messages between objects.

A simulation based on ABS (Agent-Based Simulation) helps to better understand real-world systems, in which individual entities with their autonomous behavior are presented or modeled. ABS approach is characterized by (Siebers et al., 2010): approach from bottom to top, focus on modeling a behavior of entities and interactions between them, having by entities ability to make decisions and others factors.

These attributes do not describe the manufacturing processes but provide a description of many aspects of management. They can be used to make decisions concerning the choice of maintenance strategy and modeling of failure, repair, preventive maintenance.

Proposed by authors approach is that a flow item is modeled by an object, in which labels describing the two statistical distributions are defined. The first statistical distribution defines MTBF (time between the occurrence of the next failure) and the second MTTR (the time required to repair the damage). These labels are defined and set at the moment of creation of an item flow (entrance to the analyzed system). The fact that an object is created dynamically, and labels describing the MTBF and MTTR definitions are defined when the object is created during a simulation experiment—it make different approach from standard solutions, used in traditional simulation programs.

Figure 3 represents a set labels with MTBF and MTTR.

An essence of modeling an event is sending a message by a flow item object to itself. The first message is sent at time of entry into the system—it is sent with a delay, which is set in accordance with a defined distribution of MTBF. The second message is sent when the first message was received. It is also sent with a delay, which is set in accordance with a defined distribution of MTTR. A cycle can be repeated if a damage is repairable. If it is not, this means the end of a life cycle of an flow item. Figure 4 shows state when object is able to work or not. Depend on ability to work it has state 1 or –1.

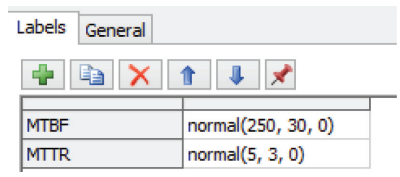


Figure 3. MTBF and MTTR labels (Source: Flexsim model).

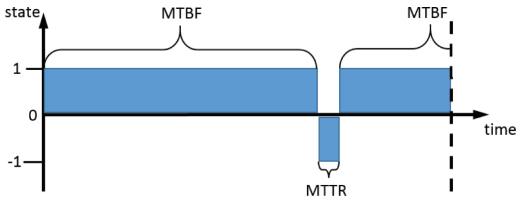


Figure 4. Object states graph (Source: own study based on Braglia et al., 2012).

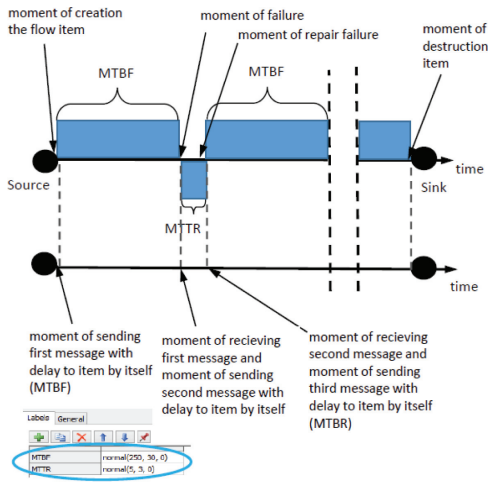


Figure 5. Life cycle of an dynamically created object (Source: own study).

Figure 5 shows a life cycle of an object, which is created dynamically in the model. It shows a general method for modeling dynamic objects and failures of them. It takes into account an occurrence of failure at a certain time and the time required to removing a distortion that has occurred.

It is worth mentioning that in order to make sending and receiving messages by means of transport for himself possible, item flow should be created by using TaskExecuterFlowItem. These elements have additional features compared to the basic, inter alia, Triggers tab, so that it is possible to include receiving messages.

5 CONCLUSIONS

Building flow items using agent-based modeling and messaging element to itself, creates huge opportunities for the modeling of damage elements involved in the analyzed process. This allows a different perspective on the process and modeling of failure of individual 'participants'. In addition, combining it with a built-in mechanism for modeling MTBF/MTTR makes it possible to build a complete model, taking into account the number of failures and damages occurring in the process. With the model, which maps the actual system, it is possible to observe and analyze the behavior of the system depending on the conditions. In addition, simulation of a failure allows for an observation and evaluation of activities undertaken within a selected maintenance strategy.

ACKNOWLEDGEMENTS

Presented research are carried out under the LOGOS project (Model of coordination of virtual supply chains meeting the requirements of corporate social responsibility) under grant agreement number PBS1/B9/17/2013.

REFERENCES

Aven, T., Pedersen, L.M. 2014. On how to understand and present the uncertainties in production assurance analyses, with a case study related to a subsea production system, Reliability Engineering and System Safety 124, 165–170.

Barone, G., Frangopol, D.M. 2014. Reliability, risk and lifetime distributions as performance indicators for life-cycle maintenance of deteriorating structures, Reliability Engineering and System Safety 123, 21–37.

Braglia, M., Carmignani, G., Frosolini, M., Zammori, F. 2012. Data classification and MTBF prediction with a multivariate analysis approach, Reliability Engineering and System Safety 97, 27–35.

Jasiulewicz-Kaczmarek M., 2009a, Participatory Ergonomics as a Method of Quality Improvement in Maintenance B.-T. Karsh (Ed.): Ergonomics and Health Aspects, HCII 2009,.© Springer-Verlag Berlin Heidelberg, LNCS 5624, pp. 153–161

Jasiulewicz—Kaczmarek, M. 2009b. Maintenance strategies and how the methods of maintenance strategies definition—state of the art. [In]: Lewandowski, J., Jałmużna, I. (Ed.): Contemporary problems in managing production and services supporting manufacturing processes, Publishing House of Technical University in Lodz,, 144–154, ISBN: 978-83-7283-322-8.

Jia, X., Cui, L. 2011. Optimization of joint maintenance strategy for safety-critical systems with different reliability degrees Expert Systems, Vol. 28 (3), 199–208.

Kim, Y., Kang, W.-H. 2013. Network reliability analysis of complex systems using a non-simulation-based method, Reliability Engineering and System Safety 110, 80–88.

Pawlewski, P., Jasiulewicz-Kaczmarek, M. 2011. Simulation of Maintenance Strategy on the basis of simulation experiment, [In]: Grzybowska, K., Pawlewski, P. (Eds.): Solutions for supporting the processes of administration, logistics and manufacturing—Selected aspects, Publishing House of Poznan University of Technology, 97–112, ISBN: 978-83-7775-067-4.

Siebers, P.O., Macal, C.M., Garnett, J., Buxton, D. Pidd, M. 2010. Discrete-Event Simulation is Dead, Long Live Agent-Based Simulation!. Journal of Simulation, 4(3), 204–210.

Swanson, L. 2003. An information-processing model of maintenance management. International Journal of Production Economics, Vol.83 No.1, 45–64.

Tan, Z., Li, J., Wu, Z., Zheng, J., He, W. 2011. An evaluation of maintenance strategy using risk based inspection Safety Science, Vol.49 (6), 852–860.

Vatn, J., Aven, T. 2010. An approach to maintenance optimization where safety issues are important Reliability Engineering and System Safety, Vol.95, 58–63.

Zhou, Y., Zhang, Z., Lin, T.R., Ma, L. 2013. Maintenance optimisation of a multi-state series–parallel system considering economic dependence and state-dependent inspection intervals, Reliability Engineering and System Safety 111, 248–259.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A new Monte Carlo method for environmental contour estimation

Arne B. Huseby
University of Oslo, Norway

Erik Vanem
DNV—GL, Norway

Bent Natvig
University of Oslo, Norway

ABSTRACT: Environmental contour estimation is an efficient and widely used method for identifying extreme conditions as a basis for e.g., ship design. Monte Carlo simulation is a flexible method for estimating such contours. A main challenge with this approach, however, is that extreme conditions typically correspond to events with low probabilities. Thus, in order to obtain satisfactory estimates, large numbers of simulations are needed. While these simulations can be carried out very fast, the analysis of the resulting data can be very time-consuming. In the present paper we propose a new Monte Carlo method where only the extreme simulation results are stored and analyzed. This method utilizes the fact that an unbiased estimate of an environmental contour does not depend on the exact values of the non-extreme results. It is sufficient to know the number of such results. Probabilistic structural reliability analysis is performed to ensure that mechanical structures can withstand certain design loads. Obtaining precise environmental contours has become an important part of this analysis. The proposed method improves precision and speeds up calculations.

1 INTRODUCTION

Probabilistic structural reliability analysis is performed to ensure that a structure is able to withstand the required design loads. A realistic description of the environmental loads and structural response is a crucial prerequisite for structural reliability analysis of structures exposed to environmental forces. The concept of environmental contours is an efficient method of estimating extreme conditions as basis for design. See (Winterstein et al., 1993) and (Haver & Winterstein 2009). It is widely used in marine structural design. See e.g., (Baarholm et al., 2010), (Fontaine et al., 2013), (Jonathan et al., 2011), (Moan 2009) and (Ditlevsen 2002). The traditional approach is to use the well-known *Rosenblatt transformation* introduced in (Rosenblatt 1952) to transform the environmental variables into independent standard normal variables and identify a sphere with desired radius in the transformed space. Environmental contours are then found by re-transforming the sphere back to the original space. This approach is closely related to the FORM-approximation (First Order Reliability Method), where the failure boundary in the transformed space is approximated by a hyperplane at the design point.

However, a supporting hyperplane in the transformed space will generally not correspond to a supporting hyperplane in the original space, and this may introduce biases in the failure probability estimates in either direction. See (Huseby et al., 2013). To avoid such biases, contours in the original space can be constructed by using Monte Carlo simulations on the joint environmental model. The resulting environmental contours would then have supporting hyperplanes with the desired failure probability. This yields a more straightforward interpretation of the contours. Another advantage of this approach is a more flexible framework for establishing environmental contours, which for example simplifies the inclusion of effects such as future projections of the wave climate related to climatic change. See (Vanem & Bitner-Gregersen 2012).

In Section 2 we review the basic definitions of environmental contours and the fundamental existence theorem proved in (Huseby et al., 2014). Moreover, we show how this contour can be expressed in terms of a certain percentile function. In Section 3 we explain briefly how to estimate the contour using direct Monte Carlo simulations. More details on this are given in (Huseby et al., 2013) and (Huseby et al., 2014). We then

propose a new Monte Carlo method where only the extreme simulation results are stored and analyzed. This method utilizes the fact that an unbiased estimate of an environmental contour does not depend on the exact values of the non-extreme results. Knowing the number of such results is sufficient. An important part of this approach is how to choose the set of non-extreme results which can be discarded. This isssue is discussed in Section 4. Finally the suggested method is demonstrated on a few numerical examples in Section 5.

2 BASIC CONCEPTS AND RESULTS

Environmental contours are defined in various ways in the literature. See e.g., (Leira 2008), (Moan et al., 2005) and (Haver 1987). In this paper, however, we apply the same definition of environmental contours as used in (Huseby et al. 2013). Let $\mathbf{X}$ be a vector of environmental variables with possible values in the set $\mathcal{X} \subseteq \mathbb{R}^n$ and assume that the distribution of $\mathbf{X}$ is absolutely continuous with respect to the Lebesgues measure in $\mathbb{R}^n$. Moreover, let $P_e \in (0,0.5)$ be a given exceedance probability. The objective is to identify a convex set $\mathcal{B} \subset X$ such that for every supporting hyperplane[1] Π of $\mathcal{B}$, we have $P[\mathbf{X} \in \Pi^+] = P_e$, where Π^+ denotes the halfspace bounded by the hyperplane Π and not containing $\mathcal{B}$. We also introduce Π^- which denotes the halfspace complementary to Π^+. Thus, $\mathcal{B} \subseteq \Pi^-$. The resulting environmental contour is the boundary of the set $\mathcal{B}$ and denoted $\partial\mathcal{B}$. Whenever such a set $\mathcal{B}$ can be found, safely designed structures can easily be identified by considering the points in $\partial\mathcal{B}$.

The properties of the set $\mathcal{B}$ depends on the probability distribution of the vector $\mathbf{X}$. If $\mathcal{B}$ has the property mentioned above, we say that $\mathbf{X}$ admits a P_e-contour. From the above definition we see that the construction of $\mathcal{B}$ is strongly linked to hyperplanes Π with the property that $P[\mathbf{X} \in \Pi^+] = P_e$. We will refer to such hyperplanes as P_e-exceedance hyperplanes, and we denote by $\mathcal{P}(P_e)$ the family of all P_e-exceedance hyperplanes. In (Huseby et al., 2014) necessary and sufficient conditions for the existence of P_e-contours are given. In particular it is shown that in the general case $\mathcal{B}$ can be defined as follows:

$$\mathcal{B} = \bigcap_{\Pi \in P(P_e)} \Pi^-. \tag{1}$$

[1] A hyperplane Π is a supporting hyperplane of a convex set B if B is entirely contained in one of the two closed half-spaces determined by Π and B has at least one boundary-point on Π.

Note that all the halfspaces $\Pi^- \in \mathcal{P}(P_e)$ are convex sets. Hence, the definition of $\mathcal{B}$ given in (1) implies that the set $\mathcal{B}$ is indeed a *convex set* as well since it is an intersection of convex sets.

In the remaining part of the paper we consider the two-dimensional case where $\mathbf{X} = (T, H)$. In this case it is convenient to introduce a function $C(\theta)$ defined for $\theta \in [0, 2\pi)$ as:

$$C(\theta) = \inf\{C : P[T\cos(\theta) + H\sin(\theta) > C] = P_e\}. \tag{2}$$

Thus, $C(\theta)$ is the $(1-P_e)$-percentile in the distribution of the random variable $Y(\theta) = T\cos(\theta) + H\sin(\theta)$. We also introduce:

$$\Pi(\theta) = \{(t,h) : t\cos(\theta) + h\sin(\theta) = C(\theta)\}$$
$$\Pi^+(\theta) = \{(t,h) : t\cos(\theta) + h\sin(\theta) > C(\theta)\},$$
$$\Pi^-(\theta) = \{(t,h) : t\cos(\theta) + h\sin(\theta) \le C(\theta)\}.$$

In (Huseby et al., 2014) it is shown that the expression for $\mathcal{B}$ given in (1) can be simplified to:

$$\mathcal{B} = \bigcap_{\theta \in [0,2\pi)} \Pi(\theta)^-. \tag{3}$$

Existence of P_e-contours can then be expressed as a condition on the function C:

Theorem 2.1. $\mathbf{X}$ admits a P_e-contour if and only if for any $\theta \in [0, 2\pi)$ and $\delta \in (0, \pi/2)$, we have:

$$\frac{1}{2}[C(\theta - \delta) + C(\theta + \delta)] > \cos(\delta)C(\theta). \tag{4}$$

We observe that if C is convex in $[\theta - \delta, \theta + \delta]$, then the condition (4) holds for this particular q and δ. If C is everywhere convex, then (4) will be satisfied for every $\theta \in [0, 2\pi)$ and $\delta > 0$. However, since C typically will have the property that $\lim_{\theta \to 2\pi} C(\theta) = C(0)$, C cannot be strictly convex everywhere. Thus, unless C is constant, this function will have parts where it is concave as well. Intuitively, Theorem 2.1 states that C in its concave parts should behave locally like the cosine function around zero. On the other hand, if C has parts with a more dramatically concave shape, the condition (4) may not hold, and in such cases $\mathbf{X}$ does *not* admit a P_e-contour.

The function $C(\theta)$ can be used to identify the boundary of the set $\mathcal{B}$. In order to show this, we assume that $C(\theta)$ is differentiable. For a given angle $\theta \in [0, 2\pi)$ and a small number $\delta > 0$ we consider the intersection between the two P_e-exceedance hyperplanes $\Pi(\theta)$ and $\Pi(\theta + \delta)$. This point can be found by solving the following linear equations:

$$\begin{aligned} t\cos(\theta) + h\sin(\theta) &= C(\theta), \\ t\cos(\theta + \delta) + h\sin(\theta + \delta) &= C(\theta + \delta), \end{aligned} \tag{5}$$

with the solution:

$$t = \frac{\sin(\theta+\delta)C(\theta) - \sin(\theta)C(\theta+\delta)}{\sin(\delta)} \tag{6}$$

$$h = \frac{-\cos(\theta+\delta)C(\theta) + \cos(\theta)C(\theta+\delta)}{\sin(\delta)}$$

As $\delta \to 0$ the intersection point (t,h) will converge to a point in $\Pi(\theta)$ which we denote by $(t(\theta),h(\theta))$. Using l'Hôpital's rule it is easy to see that $(t(\theta),h(\theta))$ is given by:

$$\begin{pmatrix} t(\theta) \\ h(\theta) \end{pmatrix} = \begin{bmatrix} C(\theta) & -C'(\theta)(8) \\ C'(\theta) & C(\theta) \end{bmatrix} \cdot \begin{pmatrix} \cos(\theta)(9) \\ \sin(\theta) \end{pmatrix}, \tag{7}$$

where $C'(\theta)$ denotes the derivative of $C(\theta)$.

As θ runs through all angles in $[0,2\pi)$, the point $(t(\theta),h(\theta))$ will move along the boundary of the set $\mathcal{B}$. Thus, the environmental contour can be expressed as:

$$\partial\mathcal{B} = \{(t(\theta),h(\theta)) : \theta \in [0,2\pi)\}. \tag{8}$$

In the next section we shall see how the function C and hence also the environmental contour $\partial\mathcal{B}$ can be estimated using Monte Carlo simulation.

3 ESTIMATING ENVIRONMENTAL CONTOURS USING MONTE CARLO SIMULATION

In this section we show how to estimate environmental contours using Monte Carlo simulation. More specifically, we use Monte Carlo simulations in order to estimate the set $\mathcal{B}$ introduced in the previous section, and then use its boundary $\partial\mathcal{B}$ as the desired contour. As in the previous section a two-dimensional environmental space is assumed, and we let T and H denote the two environmental variables. Moreover, for any $\theta \in [0,2\pi)$ we introduce the random variable $Y(\theta) = T\cos(\theta) + H\sin(\theta)$ and its cumulative distribution function $F_\theta(y) = P(Y(\theta) \le y)$.

We start out by performing a Monte Carlo simulation on the joint environmental model (or alternatively on an empirical distribution) producing a total of n sample points:

$$(T_1,H_1),\ldots,(T_n,H_n) \tag{9}$$

For a given angle $\theta \in [0,2\pi)$ we calculate the projections of these points onto the unit vector $(\cos(\theta),\sin(\theta))$, i.e.:

$$Y_i(\theta) = T_i\cos(\theta) + H_i\sin(\theta), i = 1,\ldots,n \tag{10}$$

These projections are then sorted in ascending order:

$$Y_{(1)}(\theta) \le Y_{(2)}(\theta) \le \cdots \le Y_{(n)}(\theta). \tag{11}$$

Using the sampled values $Y_1(\theta),\ldots,Y_n(\theta)$ the cumulative distribution function F_θ can be estimated by the well-known empirical cumulative distribution function:

$$\hat{F}_\theta(y) = \frac{1}{n}\sum_{i=1}^{n} I(Y_i(\theta) \le y). \tag{12}$$

Now, for a given exceedance probability P_e, we recall that $C(\theta)$ is the $(1-P_e)$-percentile in the distribution of $Y(\theta)$. Thus, in order to estimate $C(\theta)$, we look for a value y such that $\hat{F}_\theta(y) = (1-P_e)$. We then note that for $k = 1,\ldots,n$ we have $\hat{F}_\theta(Y_{(k)}(\theta)) = k/n$. Hence, we proceed by identifying an integer k such that:

$$\frac{k}{n} \approx 1 - P_e. \tag{13}$$

That is[2], $k \approx n(1-P_e)$. Having determined k, an unbiased estimate for $C(\theta)$ is:

$$\hat{C}(\theta) = Y_{(k)}(\theta). \tag{14}$$

Furthermore, using standard numerical methods we estimate $C'(\theta)$ by $\hat{C}'(\theta)$. Using these estimates in combination with (7) we obtain the contour estimate. Further details and a couple of alternative methods are given in (Huseby et al., 2013).

For moderately small exceedance probabilities this method works very well. However, in many typical applications P_e can be very small, i.e., less than 0.1%. In such cases a large number of simulations are needed in order to obtain stable estimates. At the same time most of the simulations yield results close to the central area of the joint distribution, and thus very few results provide information about the contour area.

While Monte Carlo simulation on a bivariate distribution can be done extremely fast on modern computers, processing the results in order to obtain the contours can be much more time consuming. In fact, even storing a large number of simulation results in the computer memory can represent a challenge.

In order to address these issues, we propose an alternative sampling scheme. Assume that we can

[2] Assuming that $P_e \in (0,1)$ is a *rational number*, we can in fact ensure that $k = n(1-P_e)$ by choosing n sufficiently large.

find a subset e of the set $\mathcal{B}$. Although the set $\mathcal{B}$ is yet to be estimated, finding such a subset is usually not difficult using e.g., a crude preliminary estimate of the set $\mathcal{B}$. We will return to the problem of choosing a suitable set e later. Since e is a subset of $\mathcal{B}$, it follows that for any supporting hyperplane $\Pi(\theta)$ of $\mathcal{B}$ we will have that $\varepsilon \subset \mathcal{B} \subset \Pi^{-}(\theta)$. See Figure 1.

Hence, for any sampling point $(T_i, H_i) \in \varepsilon$ we have that $Y_i(\theta) \leq C(\theta)$. Thus, in order to estimate $C(\theta)$, we do not need to know the exact values of the sampling points in e. It is sufficient to know the *phnumber of sampling points inside this set.*

In order to explain this idea further, we assume that we have performed another Monte Carlo simulation on the joint environmental model producing a total of n points. However, in this case only the sample points outside of the set e are stored while the sample points inside the set e are discarded. We assume that the number of stored points is d, while the number of discarded points is e, where $d + e = n$. The stored points are denoted:

$$(T_1, H_1), \ldots, (T_d, H_d). \tag{15}$$

As before we also calculate the projections of these points onto the vector $(\cos(\theta), \sin(\theta))$:

$$Y_i(\theta) = T_i \cos(\theta) + H_i \sin(\theta), i = 1, \ldots, d, \tag{16}$$

and sort the projections in ascending order:

$$Y_{(1)}(\theta) \leq Y_{(2)}(\theta) \leq \cdots \leq Y_{(d)}(\theta). \tag{17}$$

Assuming that y is greater than the projections of all the discarded points, we can still estimate the cumulative distribution function $F_\theta(y)$ by $\hat{F}_\theta(y)$ which in this case can be written as:

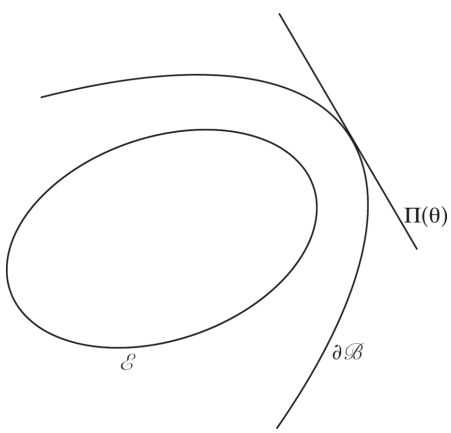


Figure 1. The set ε, part of the environmental contour $\partial\mathcal{B}$ and the supporting hyperplane $\Pi(\theta)$.

$$\hat{F}_\theta(y) = \frac{1}{n} \sum_{i=1}^{d} I(Y_i(\theta) \leq y) + \frac{e}{n}. \tag{18}$$

Again we look for a value y satisfying the following condition $\hat{F}_\theta(y) = (1 - P_e)$. Using (21) it is easy to see that this condition can be expressed as:

$$\tilde{F}_\theta(y) = \frac{1}{d} \sum_{i=1}^{d} I(Y_i(\theta) \leq y) = \frac{n(1 - P_e) - e}{d}, \tag{19}$$

where we have introduced $\tilde{F}_\theta(y)$ denoting the empirical distribution function based on the stored sample points only. Noting that for $k = 1, \ldots, d$ we have $\tilde{F}_\theta(Y_{(k)}(\theta)) = k/d$, we proceed by identifying an integer k such that:

$$\frac{k}{d} \approx \frac{n(1 - P_e) - e}{d}. \tag{20}$$

That is, $k \approx n(1 - P_e) - e$, and an unbiased estimate for $C(\theta)$ is:

$$\tilde{C}(\theta) = Y_{(k)}(\theta). \tag{21}$$

By using the right-hand side of (23) we introduce the following quantity:

$$P'_e = 1 - \frac{n(1 - P_e) - e}{d}. \tag{22}$$

This quantity may be interpreted as an *adjusted* exceedance probability which applies to the reduced sample. When $e > 0$ it is easy to see that we always have $P'_e > P_e$. A consequence of this is that the percentile estimates becomes more stable as the exceedance events occur much more frequent within the reduced sample. Working with this adjusted exceedance probability also has the technical advantage that we may use exactly the same algorithm for the reduced sample as we use for the full sample except that we replace P_e by P'_e as input to the calculations.

Note that if $\tilde{C}(\theta)$ and $\hat{C}(\theta)$ are computed using the same n sample points, the two estimates will in fact be equal. The advantage of $\tilde{C}(\theta)$, however, is that this estimate can be calculated using only a small fraction of the full sample. Hence, we can easily increase the number n substantially without running into memory problems or long processing time.

4 CHOOSING THE SET ε

In this section we return to the problem of choosing the set ε. There are obviously many ways of doing this. In order to explain our approach we

start out by considering a very simple example where the environmental contour can be calculated analytically. This is the case when the environmental variables are independent standard normally distributed. This joint distribution is rotationally symmetric, and the exact environmental contour is a circle centered in the origin. See Figure 2. The radius of this circle can easily be calculated e.g., by considering the supporting hyperplane $\Pi(0)$. In this case the projection of (T,H) is simply:

$$Y(0) = T\cos(0) + H\sin(0) = T. \tag{23}$$

Thus, $Y(0)$ is standard normally distributed, and $C(0)$ is simply the $(1-P_e)$-percentile of this distribution. In fact, due to the rotational symmetry of the joint distribution, $Y(\theta)$ is standard normally distributed for all $\theta \in [0, 2\pi)$. Hence, $C(\theta)$ is constant, which implies that the environmental contour is indeed a circle with radius R equal to the $(1-P_e)$-percentile. Thus, if e.g., $P_e = 0.001$, then $R = 3.09$.

Having found the environmental contour, there is of course no need to perform any simulations in this case. However, it may still be of interest to explore possible choices for the set $\mathcal{E}$. In Figure 2 we have chosen this set to be a circle inside the set $\mathcal{B}$ with radius $r < R$ and centered in the origin. With this choice it is easy to calculate the probability that a sample point is discarded, i.e., $P((T,H) \in \mathcal{E})$. This probability can be expressed as:

$$P((T,H) \in \mathcal{E}) = P(T^2 + H^2 \le r^2). \tag{24}$$

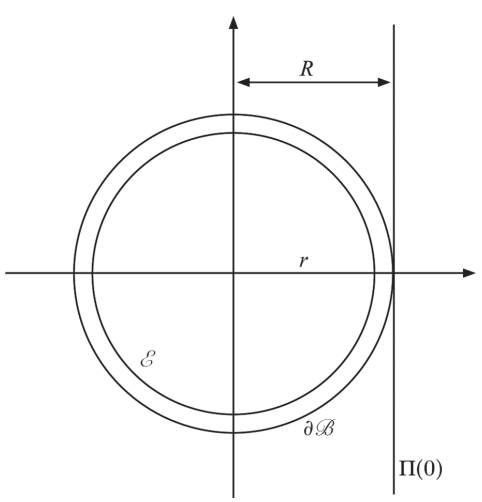


Figure 2. The environmental contour, $\partial\mathcal{B}$, in the case where the variables are independent standard normally distributed.

Furthermore, since T and H are independent standard normally distributed, it follows that $T^2 + H^2$ is χ^2-distributed with 2 degrees of freedom. Hence, it is easy to see that:

$$P((T,H)\mathcal{E}) = 1 - \exp(-r^2/2). \tag{25}$$

Thus, if e.g., $r = 3.0$ we get that $P((T,H) \in \mathcal{E}) = 0.988891$. Hence, if we e.g., perform $n = 1000000$ simulations, then the expected number of stored points is $d = 11109$, while the expected number of discarded points is $e = 988891$. If we plug these numbers along with the exceedance probability $P_e = 0.001$ into (25) we get the following adjusted exceedance probability:

$$P'_e = 1 - \frac{1000000 \cdot (1 - 0.001) - 988891}{11109} = 0.09. \tag{26}$$

We observe that in this case P'_e is as much as 90 times greater than P_e.

We now proceed by extending the methodology to general joint distributions. As mentioned in the introduction it is always possible to transform any pair of random variables into a pair of independent standard normal variables using the Rosenblatt transformation. As before we denote the environmental variables by T and H. The Rosenblatt transformation is a transformation Ψ such that if $(T', H') = \Psi(T,H)$, then T' and H' are independent standard normal variables. As explained above for these transformed variables we can easily find the environmental contour, which we denote $\partial\mathcal{B}'$ and a suitable circular set within the contour, which we denote by $\mathcal{E}'$. Unless the Rosenblatt transformation is linear, which happensonly when (T,H) has a bivariate normal distribution, we cannot simply obtain the environmental contour for T and H by using the inverse Rosenblatt transformation. That is, except for the linear case, we typically have that $\Psi^{-1}(\partial\mathcal{B}') \neq \partial\mathcal{B}$. See (Huseby et al., 2013). However, provided that $\mathcal{E}'$ is not too close to $\partial\mathcal{B}'$, we may still have that $\Psi^{-1}(\mathcal{E}') \subset \mathcal{B}$. Thus, we propose to simply choose $\mathcal{E}$ as $\Psi^{-1}(\mathcal{E}')$. See Figure 3. That is, we let:

$$\mathcal{E} = \{(t,h) : \Psi(t,h) \in \mathcal{E}'\}. \tag{27}$$

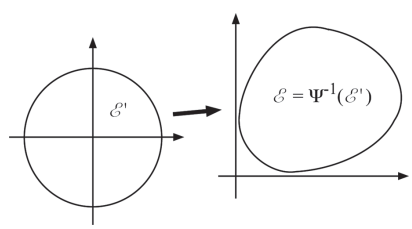


Figure 3. Obtaining the set $\mathcal{E}$ by using the inverse Rosenblatt transformation Ψ^{-1}.

5 NUMERICAL EXAMPLES

In this section we illustrate the proposed method with two numerical examples. In both cases we let $P_e = 0.001$. Moreover, in every plot, the variables T and H are represented by respectively the horizontal and vertical axes.

In the first example we assume that T and H are bivariate lognormally distributed with:

$$\begin{aligned} &\mathrm{E}[\ln(T)] = \mathrm{E}[\ln(H)] = 1.0, \\ &\mathrm{SD}[\ln(T)] = \mathrm{SD}[\ln(H)] = 1.0, \\ &\mathrm{Cov}[\ln(T), \ln(H)] = 0.7. \end{aligned}$$

We start out by running $n = 50000$ simulations where all results are used in the estimation of the environmental contour. The resulting contour is shown in Figure 4. While the overall shape of the contour is fairly well captured, we see some noticable numerical instabilities in the form of loops along the curve. This is a typical phenomenon indicating that the data is insufficient for the exceedance probability.

In Figure 5 the same contour curve is shown along with a scatter representing the simulation results. We see that there are only a few points in the area of the contour. This fact accounts for both numerical and statistical instabilities.

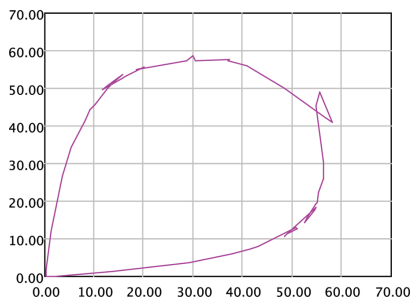


Figure 4. Environmental contour plot obtained using all 50000 points from a simulation run.

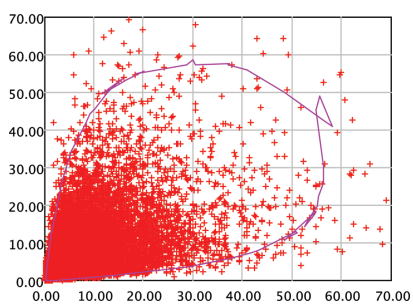


Figure 5. Environmental contour plot and scatter obtained using all 50000 points from a simulation run.

We then proceed by running simulations where a point (t,h) is discarded if $\Psi(t,h) \in \mathcal{E}'$, where the set $\mathcal{E}'$ is a circle with radius 3. This is less than 3.09, which is the $(1-P_e)$-percentile of the normal distribution.

The simulation is run until we end up with $d = 50000$ stored points. The number of discarded points in this case is $e = 4452434$. Thus, the total number of simulations in this case is $n = 4502434$. Since this number is much larger than the total numberof simulations in the case where all results where used, the latter simulation run takes a little bit longer time to finish. However, on a standard PC both runs can be completed in a few seconds anyway. Inserting P_e, n, d and e into (22) we obtain the adjusted exceedance probability $P'_e = 0.09$. Using this as input to the contour plot algorithm we obtain the environmental contour shown in Figure 6.

In this case we get a nice and smooth stable contour. In Figure 7 the same contour is shown along with a scatter representing the simulation results. The area around the contour is now surrounded by a large number of sample points. Thus, with this sampling scheme we get a numerically and statistically stable estimate of the environmental contour.

It is of interest to compare this contour with the corresponding contour obtained by the

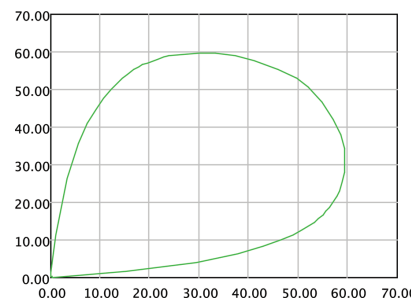


Figure 6. Environmental contour plot obtained using a reduced set of 50000 points from a simulation run.

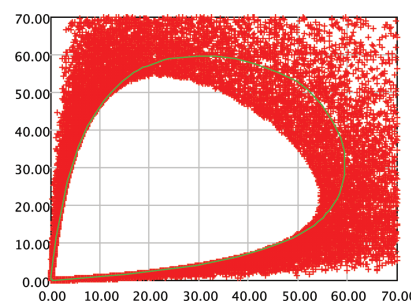


Figure 7. Environmental contour plot and scatter obtained using a reduced set of 50000 points from a simulation run.

transformation method. Denoting as before the contour in the transformed space by $\partial\mathcal{B}'$, the transformed contour is obtained by using the inverse Rosenblatt transformation: $\Psi^{-1}(\partial\mathcal{B}')$. In Figure 8 we have plotted the two curves in the same diagram. We see that the two contours deviate from each other quite noticable due to the bias resulting from the non-linear transformation Ψ^{-1}. In particular in the area around the point $(50,50)$, the transformation method produces a much more optimistic contour than the Monte Carlo method, Thus, in this area the exceedance probability is underestimated if the transformation method is used.

In the second example we again assume that T and H are bivariate lognormally distributed with the same logarithmic means and standard deviations. However, in this case we let $\mathrm{COV}[\ln(T),\ln(H)] = 0.0$.

As in the previous example we start out by running $n = 50000$ simulations where all results are used in the estimation of the environmental contour. The resulting contour is shown in Figure 9. We observe that there are several numerical instabilities in the form of loops along the curve in this case as well.

In Figure 10 the same contour curve is shown along with a scatter representing the simulation results. We see that there are only a few points in the area of the contour. Hence, both numerical and statistical instabilities are to be expected.

As before, we proceed by running simulations where a point (t,h) is discarded if $\Psi(t,h) \in \mathcal{E}$, where the set $\mathcal{E}$ is a circle with radius 3. The resulting contour is shown in Figure 11 and with a scatter in Figure 12.

In this case we also get a very smooth contour. We observe that there is a part of the contour where the scatter is less dense compared to the scatter in the previous example. Still there are more than enough points to obtain satisfactory

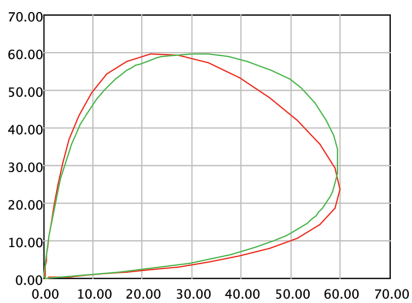


Figure 8. The environmental contour obtained using Monte Carlo simulation (green curve) compared to the contour obtained by the transformation method (red curve).

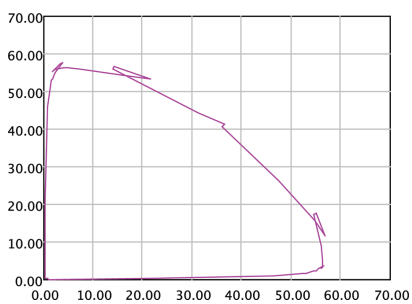


Figure 9. Environmental contour plot obtained using all 50000 points from a simulation run.

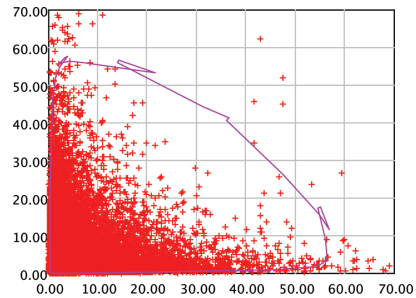


Figure 10. Environmental contour plot and scatter obtained using all 50000 points from a simulation run.

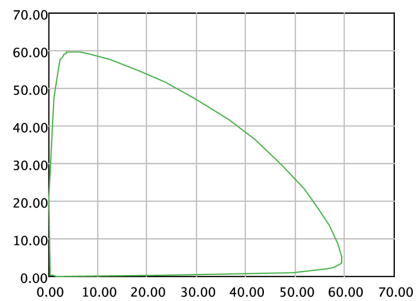


Figure 11. Environmental contour plot obtained using a reduced set of 50000 points from a simulation run.

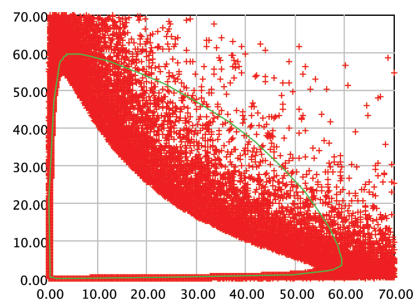


Figure 12. Environmental contour plot and scatter obtained using a reduced set of 50000 points from a simulation run.

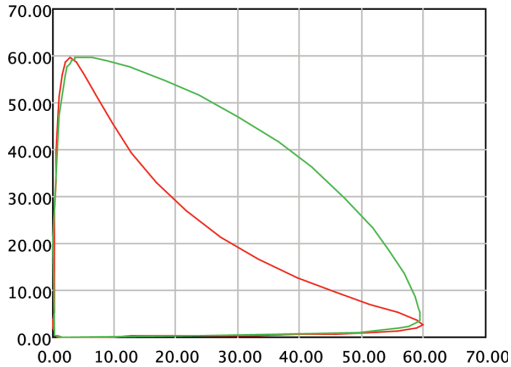


Figure 13. The environmental contour obtained using Monte Carlo simulation (green curve) compared to the contour obtained by the transformation method (red curve).

results from a statistical perspective. It should also be pointed out that the scatter in fact reaches far outside the area included in the figures. Thus, there are in fact a lot of points being used in the calculations even though they do no show up in the scatter.

We close this section by comparing the environmental curve obtained by Monte Carlo estimation to the corresponding contour obtained by the transformation method. Both contours are shown in Figure 13. For this somewhat more extreme joint distribution we observe that the transformation method does not even produce a convex contour. Thus, this contour does not have the required properties. Moreover, most of the contour is biased in the sense that the exceedance probability is underestimated.

6 CONCLUSIONS

In the present paper we have presented a new Monte Carlo method where only the extreme simulation results are stored and analyzed. In the numerical examples the exceedance probability was chosen to be 0.001, and the condition for discarding sampled points were chosen accordingly. For even smaller exceedance probabilities this condition can easily be adjusted so that we always have sufficient data in the area of the contour. Using this new method it becomes very easy to obtain numerically as well as statistically stable results even for very low exceedance probabilities without having to store and analyze millions of simulation results. Contrary to the transformation method the Monte Carlo method avoids bias resulting from non-linear transformations. As seen from the examples this bias can be substantial.

ACKNOWLEDGEMENTS

This paper has been written with support from the Research Council of Norway (RCN) through the project ExWaCli Extreme Waves and Climate Change.

REFERENCES

Baarholm, G.S., Haver, S. and Økland, O.D. Combining contours of significant wave height and peak period with platform response distributions for predicting design response. *Marine Structures* (23): 147–163, 2010.

Ditlevsen, O. Stochastic model for joint wave and wind loads on offshore structures. *Structural Safety* (24): 139–163, 2002.

Fontaine, E., Orsero, P., Ledoux, A., Nerzic, R., Prevesto, M. and Quiniou, V. Reliability analysis and response based design of a moored FPSO in West Africa. *Structural Safety* (41): 82–96, 2013.

Haver, S. On the joint distribution of heights and periods of sea waves. *Ocean Engineering* (14): 359–376, 1987.

Haver, S. and Winterstein, S. Environmental contour lines: A method for estimating long term extremes by a short term analysis. *Transactions of the Society of Naval Architects and Marine Engineers* (116): 116–127, 2009.

Huseby, A.B., Vanem, E. and Natvig, B.A new approach to environmental contours for ocean engineering applications based on direct Monte Carlo simulations. *Ocean Engineering*, (60): 124–135, 2013.

Huseby, A.B., Natvig and B., Vanem, E. Alternative environmental contours for structural reliability analysis. Submitted to *Structural Safety*.

Jonathan, P., Ewans, K. and Flynn, J. On the estimation of ocean engineering design contours. In: *Proc. 30th International Conference on Offshore Mechanics and Arctic Engineering (OMAE 2011)* American Society of Mechanical Engineers (ASME), 2011.

Leira, B.J.A. Comparison of stochastic process models for definition of design contours. *Structural Safety* (30): 493–505, 2008.

Moan, T. Development of accidental collapse limit state criteria for offshore structures. *Structural Safety* (31): 124–135, 2009.

Moan, T., Gao, Z. and Ayala-Uraga, E. Uncertainty of wave-induced response of marine structures due to long-term variation of extra-tropical wave conditions. *Marine Structures* (18): 359–382, 2005.

Rosenblatt, M. Remarks on a Multivariate Transformation. *The Annals of Mathematical Statistics* (23): No 3, 470–472, 1952.

Vanem, E. and Bitner-Gregersen, E. Stochastic modelling of long-term trends in wave climate and its potential impact on ship structural loads. *Applied Ocean Research,* (37): 235–248, 2012.

Winterstein, S., Ude, T., Cornell, C., Bjerager, P. and Haver, S. Environmental parameters for extreme response: Inverse FORM with omission factors. In: *Proc. 6th International Conference on Structural Safety and Reliability, 1993*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On multistate technical system operation process influence on its reliability

K. Kołowrocki, E. Kuligowska & J. Soszyńska-Budny
Maritime University of Gdynia, Poland

ABSTRACT: The paper presents analytical and Monte Carlo simulation methods applied to the reliability evaluation of a complex multistate system. A semi-Markov process is applied to construct the multistate model of the system operation process and its main characteristics are determined. Analytical linking of the system operation process model with the system multistate reliability model is proposed to get a general reliability model of the complex system operating at varying in time operation conditions and to find its reliability characteristics. The application of Monte Carlo simulation based on the constructed general reliability model of the complex system is proposed to reliability evaluation of a port grain transportation system and the results of this application are illustrated and compared with the results obtained by analytical method.

1 INTRODUCTION

The reliability analysis of a system subjected to varying in time its operation process very often leads to complicated calculations and therefore it is difficult to implement its analytical modeling, prediction and optimization, especially in the case when we assume the system multistate reliability model and the multistate model of its operation process (Grabski & Jaźwiński 2009, Grabski 2002, Kołowrocki 2014, Kołowrocki, Kuligowska & Soszyńska-Budny 2012, Kołowrocki & Soszyńska-Budny 2011, 2014). On the other hand, the complexity of the systems' operation processes and their influence on changing in time the systems' reliability parameters are very often met in real practice (Kołowrocki & Kuligowska 2013, Kuligowska 2012, Soszyńska 2007, 2010). Thus, the practical importance of an approach linking the system reliability models and the system operation processes models into an integrated general model in reliability assessment of real technical systems is evident. The Monte Carlo simulation method (Kołowrocki & Kuligowska 2013, Kuligowska 2013, Zio & Marseguerra 2002) is a tool that sometimes allows to simplify solving this problem. All cited here publications presents general results obtained under a strong assumption that the system components have exponential conditional reliability functions at different operation states. To omit this assumption that narrows the investigation down and to get wider a Monte Carlo simulation method is proposed to test the possibility of finding more general solutions better convergent to real technical problems. The analytical approach to the reliability analysis of multistate systems subjected to multistate operation processes is presented and next the computer simulation modeling method for such systems reliability assessment is proposed and practically applied.

2 SYSTEM OPERATION PROCESS

We assume that a system during its operation at the fixed moment t, $t\in\langle 0,\infty)$ may be at one of v, $v \geq 2$, operations states z_b, $b = 1,2, \ldots, v$. Consequently, we mark by $Z(t)$, $t\in\langle 0,\infty)$, the system operation process, that is a function of a continuous variable t, taking discrete values at the set $\{z_1,z_2, \ldots, z_v\}$ of the system operation states. We assume a semi-Markov model (Grabski 2002, Kołowrocki 2014) of the system operation process $Z(t)$ and we mark by Θ_{bl} its random conditional sojourn times at the operation states z_b, when its next operation state is z_l, $b,l = 1,2,\ldots, v$, $b\neq l$.

Consequently, the operation process may be described by the following parameters (Kołowrocki & Soszyńska-Budny 2011):

- the vector $[p_b(0)]_{1\times v}$, $b,l = 1,2, \ldots, v$, of the initial probabilities of the system operation process $Z(t)$ staying at the particular operation states at the moment $t = 0$;
- the matrix $[p_{bl}]_{v\times v}$, $b,l = 1,2, \ldots, v$, of the probabilities of the system operation process $Z(t)$ transitions between the operation states z_b and z_l, $b,l = 1,2, \ldots, v$, $b\neq l$;
- the matrix $[H_{bl}(t)]_{v\times v}$, $b,l = 1,2, \ldots, v$, of the conditional distribution functions of the system

operation process $Z(t)$ conditional sojourn times Θ_{bl}, $b,l = 1,2, \ldots, v$, $b \neq l$, at the operation states.

From the formula for total probability, it follows that the unconditional distribution functions of the sojourn times Θ_b, $b = 1,2, \ldots, v$, of the system operation process $Z(t)$ at the operation states z_b, $b = 1,2, \ldots, v$, are given by (Kołowrocki & Soszyńska-Budny 2011).

$$H_b(t) = \sum_{l=1}^{v} p_{bl} H_{bl}(t), \; b = 1,2,\ldots,v. \tag{1}$$

The limit values of the system operation process $Z(t)$ transient probabilities at the particular operation states $p_b(t) = P(Z(t) = z_b)$, $t \in \langle 0,\infty)$ $b = 1,2, \ldots, v$, are given by (Grabski 2002, Kołowrocki & Soszyńska-Budny 2011, Kołowrocki 2006, Soszyńska 2007)

$$p_b = \lim_{t\to\infty} p_b(t) = \frac{\pi_b M_b}{\sum_{l=1}^{v} \pi_l M_l}, \; b = 1,2,\ldots,v, \tag{1}$$

where M_b, $b = 1,2, \ldots, v$, are given in (Kołowrocki & Soszyńska 2011), while the steady probabilities π_b of the vector $[\pi_b]_{1xv}$ satisfy the system of equations

$$\begin{cases} [\pi_b] = [\pi_b][p_{bl}] \\ \sum_{l=1}^{v} \pi_l = 1. \end{cases}$$

3 RELIABILITY OF MULTISTATE SYSTEM

In the multistate reliability analysis to define the system with degrading components, we assume that:

- n is the number of the system components,
- E_i, $i = 1,2, \ldots, n$, are components of a system,
- all components and a system under consideration have the reliability state set $\{0,1, \ldots, z\}$, $z \geq 1$,
- the reliability states are ordered, the reliability state 0 is the worst and the reliability state z is the best,
- $T_i(u)$, $i = 1,2, \ldots, n$, are independent random variables representing the lifetimes of components E_i in the reliability state subset $\{u,u+1, \ldots, z\}$, while they were in the reliability state z at the moment $t = 0$,
- $T(u)$ is a random variable representing the lifetime of a system in the reliability state subset $\{u,u+1, \ldots, z\}$ while it was in the reliability state z at the moment $t = 0$,
- the system states degrades with time t,
- $E_i(t)$ is a component E_i reliability state at the moment t, $t \in \langle 0,\infty)$ given that it was in the reliability state z at the moment $t = 0$,
- $S(t)$ is a system S reliability state at the moment t, $t \in \langle 0,\infty)$ given that it was in the reliability state z at the moment $t = 0$.

Under the above assumptions, we denote the component E_i, $i = 1,2, \ldots, n$, reliability function by the vector

$$R_i(t,\cdot) = [1, R_i(t,1), \ldots, R_i(t,z)],$$

with the coordinates defined by

$$R_i(t,u) = P(T_i(u) > t) \text{ for } t \in \langle 0,\infty), \; u = 1,2, \ldots, z,$$

Similarly, we denote the system reliability function by the vector

$$\boldsymbol{R}(t,\cdot) = [1, \boldsymbol{R}(t,1), \ldots, \boldsymbol{R}(t,z)],$$

with the coordinates defined by

$$\boldsymbol{R}(t,u) = P(T(u) > t) \text{ for } t \in \langle 0,\infty) \; u = 1,2, \ldots, z, \tag{2}$$

Further, we assume that the changes of the operation states of the system operation process $Z(t)$ have an influence on the system multistate components E_i, $i = 1,2, \ldots, n$, reliability and the system reliability structure as well. Consequently, we denote the system multistate component E_i, $i = 1,2, \ldots, n$, conditional lifetime in the reliability state subset $\{u,u+1, \ldots, z\}$ while the system is at the operation state z_b, $b = 1,2, \ldots, v$, by $[T_i(u)]^{(b)}$ and its conditional reliability function by the vector

$$[R_i(t,\cdot)]^{(b)} = [1, [R_i(t,1)]^{(b)}, \ldots, [R_i(t,z)]^{(b)}],$$

with the coordinates defined by

$$[R_i(t,u)]^{(b)} = P(T_i^{(b)}(u) > t | Z(t) = z_b) \text{ for } t \in \langle 0,\infty), \; u = 1,2, \ldots, z, \; b = 1,2, \ldots, v, \tag{3}$$

The reliability function $[R_i(t,u)]^{(b)}$ is the conditional probability that the component E_i lifetime $[T_i(u)]^{(b)}$ in the reliability state subset $\{u,u+1, \ldots, z\}$ is greater than t, while the system operation process $Z(t)$ is at the operation state z_b.

Similarly, we denote the system conditional lifetime in the reliability state subset $\{u,u+1, \ldots, z\}$ while the system is at the operation state z_b, $b = 1,2, \ldots, v$, by $T^{(b)}(u)$ and the conditional reliability function of the system by the vector

$$[\boldsymbol{R}(t,\cdot)]^{(b)} = [1, [\boldsymbol{R}(t,1)]^{(b)}, \ldots, [\boldsymbol{R}(t,z)]^{(b)}],$$

with the coordinates defined by

$$[\boldsymbol{R}(t,u)]^{(b)} = P(T^{(b)}(u) > t | Z(t) = z_b) \text{ for } t \in \langle 0,\infty), \; u = 1,2, \ldots, z, \; b = 1,2, \ldots, v, \tag{4}$$

The reliability function $[\boldsymbol{R}(t,u)]^{(b)}$ is the conditional probability that the system lifetime $T^{(b)}(u)$ in the reliability state subset $\{u,u+1, \ldots, z\}$ is greater than t, while the system operation process $Z(t)$ is at the operation state z_b.

In the case when the system operation time θ is large enough, the coordinates of the unconditional reliability function of the system defined by (2) are given by

$$R(t,u) \cong \sum_{b=1}^{v} p_b [R(t,u)]^{(b)} \ for\, t \in \langle 0,\infty), u = 1,2,\ldots,z, \qquad (5)$$

where $[\boldsymbol{R}(t,u)]^{(b)}$, $u = 1,2, \ldots, z$, $b = 1,2, \ldots, v$, are the coordinates of the system conditional reliability functions defined by (4) and p_b, $b = 1,2, \ldots, v$, are the system operation process limit transient probabilities given by (1).

Hence, the mean value $\mu(u) = E[T(u)]$ of the system unconditional lifetime $T(u)$ in the reliability state subset $\{u,u+1, \ldots, z\}$ is given by (Kołowrocki 2011, 2014)

$$\mu(u) \cong \sum_{b=1}^{v} p_b \mu_b(u), \quad u = 1,2,\ldots,z, \qquad (6)$$

where $\mu_b(u) = E[T^{(b)}(u)]$ are the mean values of the system conditional lifetimes $T^{(b)}(u)$ in the reliability state subset $\{u,u+1, \ldots, z\}$ at the operation state z_b, $b = 1,2, \ldots, v$, given by

$$\mu_b(u) = \int_0^{\infty} [R(t,u)]^{(b)} dt, \quad u = 1,2,\ldots,z, \qquad (7)$$

where $[\boldsymbol{R}(t,u)]^{(b)}$, $u = 1,2, \ldots, z$, $b = 1,2, \ldots, v$, are defined by (4) and p_b are limit probabilities of the system particular operation states given by (1). Since the relationships between the system unconditional lifetimes $\overline{T}(u)$ in the particular reliability states and the system unconditional lifetimes $T(u)$ in the reliability state subsets can be expressed by

$$\overline{T}(u) = T(u) - T(u+1), u = 0,1,\ldots,z-1, \overline{T}(z) = T(z),$$

then we get the following formulae for the mean values of the unconditional lifetimes of the system in particular reliability states

$$\begin{aligned} &\overline{\mu}(u) = \mu(u) - \mu(u+1), u = 0,1,\ldots,z-1, \\ &\overline{\mu}(z) = \mu(z), \end{aligned} \qquad (8)$$

where $\mu(u)$ $u = 0,1, \ldots, z$ are given by (7).

4 MONTE CARLO SIMULATION APPROACH TO RELIABILITY EVALUATION OF MULTI-STATE SYSTEM

4.1 *Generating system operation process*

We denote by $\theta_{bl}^{(i)}$, $b,l = 1,2, \ldots, v$, $i = 1,2, \ldots, n_{bl}$, $b \neq l$, the realizations of the conditional sojourn time θ_{bl} of the system operation process generated from the distribution H_{bl}, where n_{bl} is the number of those sojourn time realizations during the experiment time $\tilde{\theta}$. Those realizations are generated according to the formulae

$$\theta_{bl}^{(i)} = H_{bl}^{-1}(h), b,l = 1,2,\ldots,v,$$

where $H_{bl}^{-1}(h)$ is the inverse function of the distribution function $H_{bl}(t)$ and h is a randomly generated number from the uniform distribution on the interval $\langle 0,1 \rangle$.

Having the realizations of the conditional sojourn times of the system operation process

$$\theta_{bl}^{(1)}, \theta_{bl}^{(2)}, \ldots, \theta_{bl}^{(n_{bl})}, b,l = 1,2,\ldots,v, b \neq 1,$$

it is possible to determine approximately the total sojourn time at the operation state z_b, during the time of the experiment $\tilde{\theta}$ applying the formula

$$\tilde{\theta}_b = \sum_{\substack{l=1 \\ l \neq b}}^{v} \sum_{j=1}^{n_{bl}} \theta_{bl}^{(i)}.$$

Further, the limit transient probabilities $p_b(t)$ can be approximately obtained using the formula

$$p_b = \frac{\tilde{\theta}_b}{\tilde{\theta}},$$

where

$$\tilde{\theta} = \sum_{b=1}^{v} \tilde{\theta}_b, b = 1,2,\ldots,v.$$

4.2 *Generating system reliability state changing process*

The realizations $[t_i(u)]^{(b)}$, of the components E_i, $i = 1,2, \ldots, n$, conditional lifetimes $[T_i(u)]^{(b)}$, $i = 1,2, \ldots, n$, $u = 1,2, \ldots, z$, $b = 1,2, \ldots, v$, are generated according to the distribution (3), i.e. they are generated by the sampling formula

$$[t_i(u)]^{(b)} = \left([F_i(f,u)]^{(b)} \right)^{-1} = \left(1 - [R_i(f,u)]^{(b)} \right)^{-1},$$

where $\left([F_i(f,u)]^{(b)} \right)^{-1}$ is the inverse function of the distribution function

$$[F_i(t,u)]^{(b)} = 1 - [R_i(t,u)]^{(b)}$$

of the component conditional lifetime $[T_i(u)]^{(b)}$ and $[R_i(t,u)]^{(b)}$ is defined by (3) which in the case of exponential distribution takes the following form

$$[F_i(t,u)]^{(b)} = 1 - \exp[-[\lambda_i(u)]^{(b)} t], \quad for\, t \in \langle 0,\infty),$$

$i = 1,2, \ldots, n$, $u = 1,2, \ldots, z$, $b = 1,2, \ldots, v$.

In the case of the above exponential distribution the realizations of the system component conditional lifetimes take the following form

$$[t_i(u)]^{(b)} = -\frac{1}{[\lambda_i(u)]^{(b)}}\ln(1-f),\ i=1,2,\ldots,n,\quad b=1,2,\ldots,v, \tag{9}$$

The realizations $t(u)$, $u = 1,2, \ldots, z$, of the system unconditional lifetime $T(u)$, $u = 1,2, \ldots, z$, in the reliability state subset $\{u,u+1, \ldots, z\}$ depend on the realizations $[t_i(u)]^{(b)}$, $i = 1,2, \ldots, n$, $b = 1,2, \ldots, v$, of the system component conditional lifetimes $[T_i(u)]^{(b)}$, $i = 1,2, \ldots, n$, $u = 1,2, \ldots, z$, $b = 1,2, \ldots, v$, and are calculated from the expression

$$t(u) = t([t_i(u)]^{(b)},\ i = 1,2, \ldots, n,\ b = 1,2, \ldots, v),$$

for $u = 1,2, \ldots, z$,

taking suitable explicit form dependent of the system structure.

The procedure of Monte Carlo simulation is repeated N times. The approximate mean value of the system lifetimes is an arithmetic mean of all system lifetime realizations for N iterations

$$[\mathrm{t}(u)]_k^{(b)},\ k=1,2,\ldots,N,\ b=1,2,\ldots,v,\ u=1,2,\ldots,z,$$

i.e.

$$[\overline{t}(u)]^{(b)} = \frac{1}{N}\sum_{k=1}^{N}[t(u)]_k^{(b)},\ b=1,2,\ldots,v,\ u=1,2,\ldots,z,$$

Using the procedure of Monte Carlo simulation (Kołowrocki & Kuligowska 2013, Kuligowska 2012, 2013), the histogram of the system unconditional lifetime can be found and the empirical mean value of the system unconditional lifetime can be calculated according to the formulae

$$\mu(u) = \frac{1}{N}\sum_{k=1}^{N} t_k(u), \tag{10}$$

on the basis of system unconditional lifetime realizations for N iterations

$$[t(u)]_k,\ k = 1,2, \ldots, N,\ u = 1,2, \ldots, z.$$

5 PORT GRAIN TRANSPORTATION SYSTEM RELIABILITY EVALUATION

5.1 *Port grain transportation system operation process*

We consider the port grain transportation system, presented in Figure 1, assigned to handle the clearing of exported and imported grain.

The port grain transportation system function is loading railway trucks with grain. The railway truck loading is performed in the following successive grain transportation system steps:

- gravitational passing of grain from the storage placed on the 8th elevator floor through 45 hall to horizontal conveyors placed in the elevator basement,
- transport of grain through horizontal conveyors to vertical bucket elevators transporting grain to the main distribution station placed on the 9th floor,
- gravitational dumping of grain through the main distribution station to the balance placed on the 6th floor,
- dumping weighed grain through the complex of flaps placed on the 4th floor to horizontal conveyors placed on the 2nd floor,
- dumping of grain from horizontal conveyors to worm conveyors,
- dumping of grain from worm conveyors to railway trucks.

In loading the railway trucks with grain the following presented in Figures 1–3 transportation subsystems take part:

S_1 – horizontal conveyors of the first type,
S_2 – vertical bucket elevators,
S_3 – horizontal conveyors of the second type,
S_4 – worm conveyors.

Taking into account the operation process of the considered transportation system, described by its operators, we distinguish its following $v = 3$ operation states:

- z_1– the system operation with the largest efficiency when all components of subsystems S_1, S_2, S_3, and S_4 are used (Figure 1),
- z_2– the system operation with less efficiency system when the first conveyor of subsystem S_1, the first and second elevators of subsystem S_2, the first conveyor of subsystem S_3 and the first

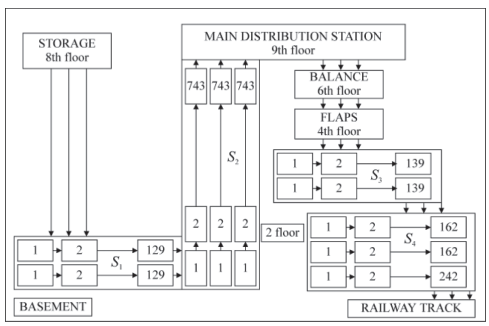


Figure 1. The scheme of the port grain transportation system structure at the operation state z_1.

and second conveyors of subsystem S_4 are used (Figure 2),

– z_3– the system operation with least efficiency when only the first conveyor of subsystem S_1, the first elevator of subsystem S_2, the first conveyor of subsystem S_3 and the first conveyor of subsystem S_4 are used (Figure 3).

At all system operation states, subsystems S_1, S_2, S_3 and S_4 become either non-homogeneous series-parallel systems or non-homogeneous series systems.

This way, the changes of the grain transportation system reliability structure at different operation states are defined.

Considering the system operators opinion, we assume the vector of approximate values of the initial probabilities $p_b(0)$, $b = 1,2,3$,

$$[p_b(0)]_{1x3} = \left[\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right]$$

of the system operation process staying at the particular states z_b at the time $t = 0$ and the matrix of the probabilities of transitions between the states are given by

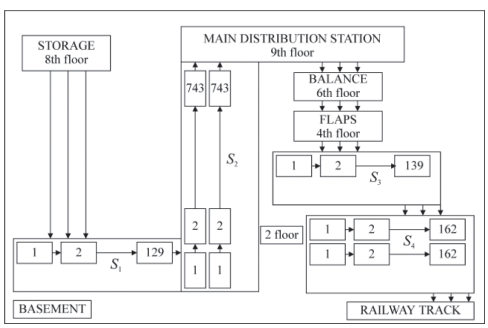


Figure 2. The scheme of the port grain transportation system structure at the operation state z_2.

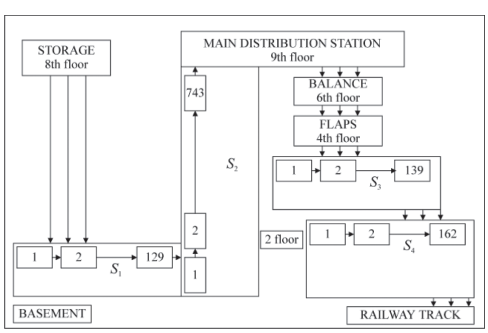


Figure 3. The scheme of the port grain transportation system structure at the operation state z_3.

$$[p_{bl}]_{3x3} = \begin{bmatrix} 0 & \frac{1}{3} & \frac{2}{3} \\ \frac{4}{9} & 0 & \frac{5}{9} \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix}.$$

Moreover, we assume the following matrix of the conditional distribution functions of the system sojourn times θ_{bl}, $b,l = 1,2,3$,

$$[H_{bl}(t)]_{3x3} = \begin{bmatrix} 0 & 1-e^{-5t} & 1-e^{-10t} \\ 1-e^{-40t} & 0 & 1-e^{-50t} \\ 1-e^{-10t} & 1-e^{-20t} & 0 \end{bmatrix}.$$

In (Kołowrocki & Soszyńska-Budny 2014), after considering the above data and applying (1), the following limit values of the system operation process transient probabilities at the operation states are determined

$$p_1 \cong 0.530,\ p_2 \cong 0.109,\ p_3 \cong 0.361. \tag{11}$$

5.2 *Port grain transportation system reliability parameters*

Taking into account the efficiency of the considered in Section 2 port grain transportation system we distinguish the following three reliability states of the systems and its components:

– state 2—the state ensuring the largest efficiency of the system and its conveyors,
– state 1—the state ensuring less efficiency of the system caused by throwing grain off the system conveyors,
– state 0—the state involving failure of the system.

The considered here transportation system reliability analysis at the constant operation conditions is performed in (Kołowrocki 2014). It is assumed that the system reliability structure and its subsystems and components reliability depend on its changing in time operation states. Considering the assumptions and agreements of these sections, we assume that its subsystems S_υ, $\upsilon = 1,2,3,4$, are composed of three-state, i.e. $z = 3$, components $E_{ij}^{(\upsilon)}$, $\upsilon = 1,2,3,4$, having the conditional lifetimes $[T_{ij}^{(\upsilon)}(1)]^{(b)}$ and $[T_{ij}^{(\upsilon)}(2)]^{(b)}$ in the reliability states $\{1,2\}$ and $\{2\}$ respectively the conditional reliability functions given by the vector

$$[R_{ij}^{(\upsilon)}(t,\cdot)]^{(b)} = [1,[R_{ij}^{(\upsilon)}(t,1)]^{(b)},[R_{ij}^{(\upsilon)}(t,1)]^{(b)}],$$
$$b = 1,2,3,$$

with the exponential coordinates

$$[R_{ij}^{(\upsilon)}(t,1)]^{(b)} = P([T_{ij}^{(\upsilon)}(1)]^{(b)} > t) = \exp[-[\lambda_{ij}^{(\upsilon)}(1)]^{(b)}t],$$

$$[R_{ij}^{(\upsilon)}(t,1)]^{(b)} = P([T_{ij}^{(\upsilon)}(1)]^{(b)} > t) = \exp[-[\lambda_{ij}^{(\upsilon)}(1)]^{(b)}t],$$

different at various operation states z_b, $b = 1,2,3$, and with the intensities of departure from the reliability state subsets {1,2}, {2}, respectively

$$[\lambda_{ij}^{(\upsilon)}(1)]^{(b)}, [\lambda_{ij}^{(\upsilon)}(2)]^{(b)},\ \upsilon = 1,2,3,4,\ i = 1,2,\ldots,[i^{(\upsilon)}]^{(b)},$$

$$j = 1,2,\ldots,[j^{(\upsilon)}]^{(b)},\ b = 1,2,3,$$

given in (Kołowrocki 2014) and presented in Tables 1–3.

At all the operational states, subsystems S_1, S_2, S_3 and S_4 are non-homogeneous regular either series-parallel or series systems. The influence of the system operation states changing on the changes of the system reliability structure and its components reliability functions is presented in Tables 1–3.

5.3 *Port grain transportation system reliability characteristics*

5.3.1 *Analytical evaluation*

Analytical evaluation of the system unconditional three-state reliability function is performed in (Kołowrocki & Soszyńska-Budny 2014) and according to (5), (11) it is given by the vector

Table 1. List of system components and intensities of departure at the operation state z_1.

Sub-system	Components	Intensity of departure	
S_1	2 identical belt conveyors (the 1st type)		
	1 belt	0.0125	0.015
	2 drums	0.0015	0.002
	117 channelled rollers	0.005	0.010
	9 supporting rollers	0.004	0.008
S_2	3 identical vertical bucket elevators		
	1 belt	0.025	0.030
	2 drums	0.0015	0.002
	740 buckets	0.030	0.035
S_3	2 identical belt conveyors (the 2nd type)		
	1 belt	0.0125	0.015
	2 drums	0.0015	0.002
	117 channelled rollers	0.005	0.010
	19 supporting rollers	0.004	0.008
S_4	3 chain worm conveyors		
	2 conveyors of the 1st type		
	2 driving wheels	0.005	0.006
	160 links	0.012	0.014
	1 conveyor of the 2nd type		
	2 driving wheels	0.022	0.024
	240 links	0.034	0.040

Table 2. List of system components and intensities of departure at the operation state z_2.

Sub-system	Components	Intensity of departure	
S_1	1 belt conveyor (the 1st type)		
	1 belt	0.011	0.012
	2 drums	0.001	0.0012
	117 channelled rollers	0.003	0.006
	9 supporting rollers	0.002	0.003
S_2	2 identical vertical bucket elevators		
	1 belt	0.020	0.024
	2 drums	0.0012	0.0014
	740 buckets	0.022	0.025
S_3	1 belt conveyor (the 2nd type)		
	1 belt	0.011	0.012
	2 drums	0.001	0.0012
	117 channelled rollers	0.003	0.006
	19 supporting rollers	0.002	0.003
S_4	2 chain worm conveyors (the 1st type)		
	2 driving wheels	0.002	0.004
	160 links	0.008	0.010

Table 3. List of system components and intensities of departure at the operation state z_3.

Sub-system	Components	Intensity of departure	
S_1	1 belt conveyor (the 1st type)		
	1 belt	0.010	0.0105
	2 drums	0.0009	0.0011
	117 channelled rollers	0.002	0.004
	9 supporting rollers	0.001	0.002
S_2	1 vertical bucket elevator		
	1 belt	0.018	0.022
	2 drums	0.0011	0.0013
	740 buckets	0.020	0.024
S_3	1 belt conveyor (the 2nd type)		
	1 belt	0.010	0.0105
	2 drums	0.0009	0.0011
	117 channelled rollers	0.002	0.004
	19 supporting rollers	0.001	0.002
S_4	1 chain worm conveyor (the 1st type)		
	2 driving wheels	0.001	0.003
	160 links	0.007	0.009

$$\boldsymbol{R}(t,\cdot) = [1, \boldsymbol{R}(t,1), \boldsymbol{R}(t,2)],\ t \in \langle 0,\infty), \tag{12}$$

with the co-ordinates

$$\begin{aligned}\boldsymbol{R}(t,1) &= 0.530[\boldsymbol{R}(t,1)]^{(1)} + 0.109[\boldsymbol{R}(t,1)]^{(2)} \\ &\quad + 0.361\,[\boldsymbol{R}(t,1)]^{(3)},\ \text{for } t \in \langle 0,\infty), \\ \boldsymbol{R}(t,2) &= 0.530[\boldsymbol{R}(t,2)]^{(1)} + 0.109[\boldsymbol{R}(t,2)]^{(2)} \\ &\quad + 0.361\,[\boldsymbol{R}(t,2)]^{(3)},\ \text{for } t \in \langle 0,\infty),\end{aligned} \tag{13}$$

where the reliability functions $[\boldsymbol{R}(t,1)]^{(1)}$, $[\boldsymbol{R}(t,1)]^{(2)}$, $[\boldsymbol{R}(t,1)]^{(3)}$, $[\boldsymbol{R}(t,2)]^{(1)}$, $[\boldsymbol{R}(t,2)]^{(2)}$, $[\boldsymbol{R}(t,2)]^{(3)}$ are given in (Kołowrocki & Soszyńska-Budny 2014).

The expected value of the system unconditional lifetime in the reliability state subsets {1,2}, {2}, calculated according to (6)-(7) from the results given by (12)-(13), are

$$\mu(1) \cong 0.0744 \text{ month}, \ \mu(2) \cong 0.0624 \text{ month}. \quad (14)$$

Further, considering (14) and (8), the mean values of the system unconditional lifetimes in the particular reliability states 1, 2, respectively are:

$$\overline{\mu}(1) \cong 0.0120 \text{ month}, \ \overline{\mu}(2) \cong 0.0624 \text{ month}.$$

5.3.2 *Monte Carlo evaluation*

The realizations of the port grain transportation system components lifetimes $[t_{ij}^{(\upsilon)}(u)]_k^{(b)}$, $k = 1,2,...,N$, $\upsilon = 1,2,3,4$, $u = 1,2$, $b = 1,2,3$, $i = 1,2,...,[i^{(\upsilon)}]^{(b)}$, $j = 1,2,...,[j^{(\upsilon)}]^{(b)}$, are generated from the exponential distribution according to (13) and Tables 1–3. The realizations $[t(u)]_k$, $k = 1,2,...,N$, $u = 1,2$, of the system unconditional lifetime depend on the realizations of the system component conditional lifetimes and are calculated taking suitable explicit form dependent of the system operation process and system structure. Namely:

– at the operation state z_1, we use the formula

$$[t(u)]_k^{(1)} = \min\{\max_{1\le i\le 2}\{\min_{1\le j\le 129}\{[t_{ij}^{(1)}(u)]_k^{(1)}\}\},$$
$$\max_{1\le i\le 3}\{\min_{1\le j\le 743}\{[t_{ij}^{(2)}(u)]_k^{(1)}\}\}, \max_{1\le i\le 2}\{\min_{1\le j\le 139}\{[t_{ij}^{(3)}(u)]_k^{(1)}\}\},$$
$$\max_{1\le i\le 3}\{\min_{1\le j\le 242}\{[t_{ij}^{(4)}(u)]_k^{(1)}\}\}\}, k = 1,2,\ldots,N, u = 1,2;$$

– at the operation state z_2, we use the formula

$$[t(u)]_k^{(2)} = \min\{\min_{1\le j\le 129}\{[t_{ij}^{(1)}(u)]_k^{(2)}\},$$
$$\min_{1\le j\le 139}\{[t_{ij}^{(3)}(u)]_k^{(2)}\}, \max_{1\le i\le 2}\{\min_{1\le j\le 743}\{[t_{ij}^{(2)}(u)]_k^{(2)}\}\},$$
$$\max_{1\le i\le 2}\{\min_{1\le j\le 242}\{[t_{ij}^{(4)}(u)]_k^{(2)}\}\}\}, k = 1,2,\ldots,N, u = 1,2;$$

– at the operation state z_3, we use the formula

$$[t(u)]_k^{(3)} = \min\{\min_{1\le \upsilon\le 4}\{\min_{1\le j\le 129}\{[t_{ij}^{(1)}(u)]_k^{(3)}\},$$
$$\min_{1\le j\le 743}\{[t_{ij}^{(2)}(u)]_k^{(3)}\}, \min_{1\le j\le 139}\{[t_{ij}^{(3)}(u)]_k^{(1)}\},$$
$$\min_{1\le j\le 242}\{[t_{ij}^{(4)}(u)]_k^{(3)}\}\}, k = 1,2,\ldots,N, u = 1,2.$$

The simulation was made with N = 1 000 000 runs. The realizations $[t(u)]_k$, $k = 1,2, \ldots, N$, $u = 1,2$, of the system unconditional lifetimes are illustrated in the form of the histograms in Figure 4.

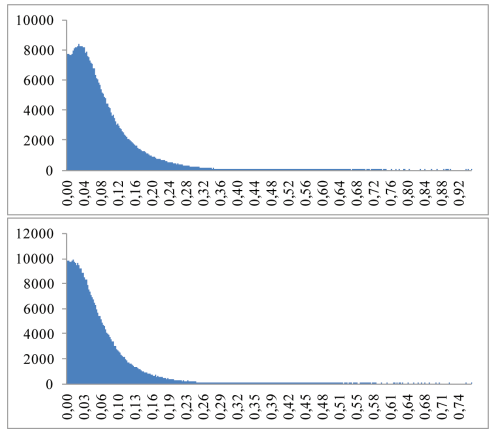


Figure 4. The graph of the histogram of port grain transportation system unconditional lifetime in the reliability state subsets {1,2},{2}.

After analyzing the histograms, we formulate the hypotheses that the system unconditional lifetimes in the reliability state subsets {1,2},{2}, have Weibull distributions. Those hypotheses testing result in the conclusion that the approximate system unconditional reliability function is given by the vector

$$\mathbf{R}(t,\cdot) = [1, \mathbf{R}(t,1), \mathbf{R}(t,2)], \ t \in \langle 0,\infty),$$

with the co-ordinates

$$\boldsymbol{R}(t,1) = \exp[-17.3150 t^{1.1526}],$$
$$\boldsymbol{R}(t,2) = \exp[-23.0851 t^{1.1052}] \text{ for } t \in \langle 0,\infty).$$

Hence, the expected value of the system unconditional lifetime in the reliability state subsets {1,2},{2}, according to (7) are

$$\mu_s(1) \cong 0{,}0801 \text{ month}, \ \mu_s(2) \cong 0.0563 \text{ month}.$$

Consequently, according to (8), the system unconditional lifetimes in the particular reliability states 1, 2, respectively are:

$$\overline{\mu}(1) \cong 0.0238 \text{ month}, \ \overline{\mu}(2) \cong 0.0563 \text{ month}.$$

6 CONCLUSIONS

The Monte Carlo simulation algorithm based on the integrated general model of a complex multistate system reliability, linking its reliability model and its operation process model and considering variable at different operation states its

reliability structure and its components reliability parameters is applied to the reliability evaluation of the port grain transportation system. The predicted reliability characteristics of this system differ not much from those determined for this system by approximate analytical method presented in (Kołowrocki & Soszyńska-Budny 2014). This fact justifies the sensibility of using Monte Carlo simulation approach to reliability evaluation of a very wide class of real complex technical systems changing their reliability structures and reliability parameters at their variable operation processes.

REFERENCES

Grabski, F. and Jaźwiński, J. 2009. Funkcje o losowych argumentach w zagadnieniach niezawodności, bezpieczeństwa i logistyki. Wydawnictwa Komunikacji i Łączności, Warszawa.

Grabski, F. 2002. Semi-Markowskie modele niezawodności i eksploatacji. System Research Institute, Polish Academy of Science, Warsaw.

Kołowrocki, K. 2014. Reliability of Large and Complex Systems, 2nd Edition. Elsevier Science & Technology, Oxford.

Kołowrocki, K. and Kuligowska E. 2013. Monte Carlo simulation application to reliability evaluation of port grain transportation system operating at variable conditions. *Journal of Polish Safety and Reliability Association, Summer Safety & Reliability Seminars* 4(1): 73–81.

Kołowrocki, K., Kuligowska, E. and Soszyńska-Budny, J. 2012. Monte Carlo Simulation for optimization of object operation process and reliability. *Journal of KONBiN* 4(24): 79–92.

Kołowrocki, K. and Soszyńska-Budny, J. 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling—Identification—Prediction—Optimization. Springer, London-Dordrecht-Heidelberg-New York.

Kołowrocki, K. and Soszyńska-Budny, J. 2014. Modeling reliability of complex transportation system. *Proc. Europen Safety and Reliability Conference-ESREL*, Wrocław.

Kuligowska, E. 2013. Monte Carlo simulation for reliability assessment and optimization of an system to varying operation conditions. *Journal of Polish Safety and Reliability Association, Summer Safety & Reliability Seminars* 4(2): 205–218.

Kuligowska, E. 2012. Preliminary Monte Carlo approach to complex system reliability analysis. *Journal of Polish Safety and Reliability Association, Summer Safety & Reliability Seminars* 3(1): 59–71.

Kuligowska, E. 2013. Reliability analysis of a system subjected to two-state operation process. *Scientific Journals Maritime University of Szczecin* 1(36): 100–104.

Soszyńska, J. 2010. Reliability and risk evaluation of a port oil pipeline transportation system in variable operation conditions. *International Journal of Pressure Vessels and Piping* 87(2–3): 81–87.

Soszyńska, J. 2007. Systems reliability analysis in variable operation conditions. International Journal of Reliability, Quality and Safety Engineering. Special Issue: System Reliability and Safety 14(6): 617–634.

Zio, E. and Marseguerra, M. 2002. Basics of the Monte Carlo Method with Application to System Reliability. LiLoLe, Hagen.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Uncertainty improving in importance sampling: An integrated approach with fuzzy-cluster sampling

M. Nadjafi & M.A. Farsi
Aerospace Research Institute, Tehran, Iran

A. Najafi
Computer Science, Ardebil, Iran

ABSTRACT: Modeling and improving uncertainty during importance sampling is a vital component for effective decision making. In real world and examples, elements may be belong to any groups or uncertain. Unfortunately, most of the random numbers sampling studies suffer from uncertainty analysis. The development of tools and techniques for capturing uncertainty in sampling is ongoing and with the set of given numbers or elements or objects in the statistical approaches we can select the elements in a random way to compute values of many subjects like mean, variance and etc. There are some sampling methods in this way that argued in many publications. In this article, the cross-disciplinary approaches for uncertainty analyses are identified and a modified approach suitable for random number generation is proposed by using fuzzy set theory and cluster sampling. The proposed method is applied to improving the sampling efficiency in the (probabilistic and possibilistic) uncertainties. In argued methods each element just belongs to one category, but in our approach each element include in all groups with one exception that membership values are different. In this paper we introduce new approach base on fuzzy theory combined with sampling methods. The case study results show that the proposed method provides better measure of uncertainty than the existing methods as unlike traditional sampling method.

1 INTRODUCTION

Modeling, improving and handling uncertainty the sampling is a vital component for effective decision making. Uncertainty is insufficiently, explicitly communicated to random sampling methods. The quantification and propagation of uncertainty become essential in precisely those situations where quantitative modeling cannot draw upon extensive historical, statistical or measurement data (Kurowicka and Cooke 2006). Fuzzy logic systems constitute a powerful tool for coping with ubiquitous uncertainty in many engineering applications (Ondrej Linda and Manic 2010). The most important point in assessing uncertainty of gained population via sampling is to recognize that all uncertainties are not quantifiable, and therefore they should be separated from the sampling characteristics (Verdonck, Souren et al. 2007). In sampling methods, if we are willing to give up some features of random sampling, notably serial independence, then variance reduction techniques may be invoked (Kwakernaak 1978). A suitable mathematical model for random variables which assume fuzzy values are so-called fuzzy random variables (L. Zadeh 1978). In standard statistics the combination of observations into an element of the sample space is trivial. But for fuzzy data this is not (Viertl 2011). Since Zadeh first introduced the concept of a fuzzy set (Zadeh 1975), Fuzzy principles have been applied to a huge and diverse range of sciences (Garibaldi and John 2003). Now we want use advantages of fuzzy model to improve sampling and solve the problems that occur in probability sampling. In stratified and cluster sampling it is hard and time-consuming to separate data into categories, however after do this it is not precise. For example one element can be belonging to some categories near to that element (Fig. 2). As a result although these methods have many benefits in sampling versus of other methods, unfortunately category based methods have many problems, because of unsuitable clustering results are not precise. A basic problem, at the present stage of the sampling methods, is how to manage the variance of sample process while taking into account its intrinsic features of uncertainty, including imprecision and vagueness.

2 SAMPLING METHODS

Once a choice is made to use a probability sample design, one must choose the type of probability

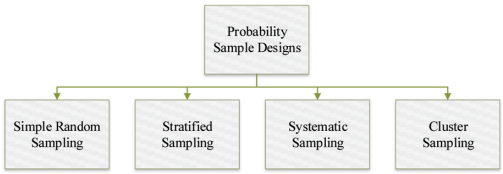


Figure 1. Major types of probability sampling (Levy and Lemeshow 2009).

sampling to use. There are four major types of probability sample designs: simple random sampling, stratified sampling, systematic sampling, and cluster sampling. Simple random sampling is the most recognized probability sampling procedure(Cochran 2007). Stratified sampling offers significant improvement to simple random sampling. Systematic sampling is probably the easiest one to use, and cluster sampling is most practical for large national surveys. Figure 1 shows major types of probability sampling methods (Levy and Lemeshow 2013). These methods have Main weaknesses. For example, simple random sampling requires frame, does not take advantage of knowledge of population, larger errors and less precision, and for widely dispersed population, and data collection costs might be higher. Stratified random sampling requires information that belongs to each stratum, more expensive, time-consuming, complicated, and need to select at least two elements in each stratum. In systematic sampling, combinations of elements have different probabilities of being selected, technically, only the selection of the first element is a probability, principle of independence is violated (selection of first element), and estimating variances is more complex. Cluster sampling may not be as representative, variances tend be much higher, introduces more complexity in analyzing data and interpreting results, and yields larger sampling errors for samples of comparable size than other probability samples.

3 SOURCES OF UNCERTAINTY

The main purpose of most measurements is to enable decisions to be made. The credibility of these decisions depends on knowledge about the uncertainty of the measurement results. Uncertainty in measurement can be defined as being made up of two components: uncertainty derived from sampling a matrix and using those samples to represent the whole sampled mass; and the uncertainty derived from the analytical process. If the uncertainty of measurements is underestimated, for example because the sampling is not taken into account, then erroneous decisions may be made that can have large financial, health and environmental consequences. For this reason it is essential that effective procedures are available for estimating the uncertainties arising from all parts of the measurement process. The uncertainty arises from a variety of sources, and these can be categorized in different ways. The sources of uncertainty from analyses are well studied, but less focus has been upon uncertainty from sampling. In Table 1, some sources of uncertainty in sampling and sample preparation are listed (Grøn, Hansen et al. 2007). Both sampling and analysis contribute to measurement uncertainty. The uncertainty contribution due to physical sample preparation, transport, sample storage etc. is either included in the uncertainty of the sampling or of the analysis. The random part of the uncertainty is described by the standard deviation. The standard deviation of the measurement, $S_{measurement}$, is given by the following equation:

$$S^2_{measurement} = S^2_{sampling} + S^2_{analysis} \quad (1)$$

$$S_{sampling} = \sqrt{S^2_{measurement} - S^2_{analysis}} \quad (2)$$

The cross-disciplinary approaches for uncertainty analyses are identified and a modified approach suitable for random number generation is proposed by using fuzzy set theory and cluster sampling. The proposed method is applied to improving the sampling efficiency in the (Probabilistic and Possibilistic) uncertainties. The relative uncertainty itself can also be used without the subsequent statistical testing particularly if enough is known about the parameter being evaluated. This value of relative uncertainty is given by (Billinton and Allan 1983):

$$Relative\ \ uncertainty = \frac{s}{\overline{x}\sqrt{n}} \quad (3)$$

where
$\overline{x}$ = mean value of parameter
s = standard deviation of parameter
n = number of sample.

In this paper, in order to decrease the uncertainty of sampling, the variance reduction techniques have been used. Variance reduction techniques are methods that attempt to reduce the variance, i.e., the dispersion associated with the variations, of the parameter being evaluated.

Table 1. Some sources of uncertainty in sampling and sample preparation (Grøn, Hansen et al. 2007).

Sampling	Sample preparation
Heterogeneity (or inhomogeneity)	Homogenization and/or sub-sampling effects
Effects of specific sampling strategy (e.g. random, stratified random, proportional etc.)	Milling, drying, dissolution
Physical state of bulk (solid, liquid, gas)	(Pre-)Concentration, dilution errors
Effect of sampling process on composition (e.g. differential adsorption in sampling system).	Control of speciation effects.

4 FUZZY SAMPLING

Now we want use advantages of fuzzy model to improve sampling and solve the problems that occur in probability sampling. In stratified and cluster sampling it is hard and time-consuming to separate data into categories, however after do this it is not precise. For example one element can be belonging to some categories near to that element (see Fig. 2). As a result although these methods have many benefits in sampling versus of other methods, unfortunately category based methods have many problems, because of unsuitable clustering results are not precise. In probability methods there are some problems and weaknesses that we can solve them with our new approach namely fuzzy sampling. Here after review of these methods and their properties, we show that how we can fix their problems with fuzzy approach.

In argued methods each element just belongs to one category, but in our approach each element include in all groups with one exception that membership values are different. For example consider age ranges. (Fig. 3) i.e. a man with 30 years old belongs to five groups by blow membership values:

When we categories such samples with stratified and clustering methods, some errors raised for computing values like variance, mean, etc. in fuzzy approach these types of errors can be eliminated. In fact each element is member of every category with a probability between 0 and 1. Our new approach is a combination of fuzzy and clustering. In this approach we assume that linguistic variables comprised as three parts and modeled in triangular. When we categories such samples with stratified and clustering methods, some errors raised for computing values like variance, mean, etc. in fuzzy approach these types of errors can be eliminated. In fact each element is member of every category with a probability between 0 and 1. Our new approach is a combination of fuzzy and clustering.

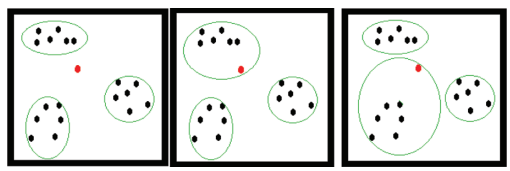


Figure 2. Methods of element categorizing in clusters.

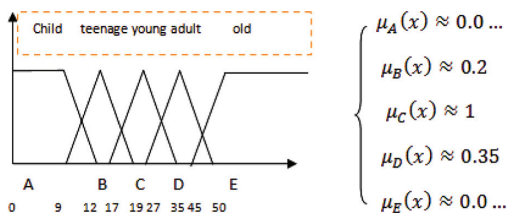


Figure 3. Demonstration of fuzzy membership function for age example.

5 PROPOSED ALGORITHM

Like cluster method we choose some random clusters for sampling, and then we identify the neighborhood of clusters to modeling fuzzy. Let $n_1, n_2 \ldots, n_m$ be the number of elements in each of the m sampled clusters. Let $\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_m$ be the means of the sampled clusters. The relative uncertainty itself can also be used without the subsequent statistical testing particularly if enough is known about the parameter being evaluated. Variance reduction techniques are methods that attempt to reduce the variance, i.e., the dispersion associated with the variations, of the parameter being evaluated. This can result in one of two outcomes. Either the variance is reduced for the same number of sampling or the number of sampling can be reduced for the same variance, the comparison of both being made when no variance reduction techniques are used. This therefore either increases the confidence in the

results or reduces the computational burden. There are many forms of variance reduction techniques and a specialized text should be consulted if full details of all techniques are needed. This algorithm provides reduced variances and standard errors comparison with other traditional methods. Schematic of proposed method is shown in Figure 4. Steps that are used for programming with use of fuzzy-clustering method that are mentioned in below algorithm consist of below classified steps:

1. Select m random clusters
2. Determine neighbors of each selected cluster
3. Calculate membership values for these clusters
4. Calculate mean value, variance, max confidence and min confidence from formulas

Formulations and relations that are used for computing the parameters such as Mean, Variance,

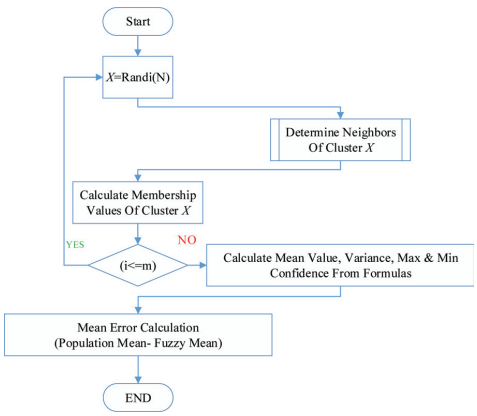


Figure 4. Flowchart of proposed sampling method.

Maximum and Minimum Confidence intervals are the same as cluster sampling formulations, in addition with fuzzy membership functions. Hence, for Mean estimator of this method we have:

$$Mean = \frac{\sum_{i=1}^{m}\left(\bar{X}_i n_i + \mu_{i+1}\bar{X}_{i+1}n_{i+1} + \mu_{i-1}\bar{X}_{i-1}n_{i-1}\right)}{\sum_{i=1}^{m} n_i} \tag{4}$$

where $\bar{X}_i$ and n_i are the mean and the number of elements for ith cluster respectively. And μ_{i+1} and μ_{i-1} are membership values of two neighboring clusters.

An estimator of samples variance is given by:

$$Variance = \frac{M-q}{Mq\bar{n}^2}\frac{\sum_{i=1}^{m} n_i^2\left(\bar{X}_i - mean\right)^2}{q-1} \tag{5}$$

where

$$\bar{n} = \left(\sum_{i=1}^{m} n_i\right)\Big/ q \quad \text{and} \quad q = m^*(\mu_{i+1} + \mu_{i-1}) \tag{6}$$

Using the preceding information, we construct a 95% confidence interval for Mean as follows:

$$\text{Confidence interval} = \text{mean} \pm 1.96\sqrt{variance} \tag{7}$$

For example consider Transport Company that contains trucks is based in N centers (clusters), assume that measure of the weekly average fuel saving for each of the centers is given. We modeled this method, cluster sampling and exhaustive method (real mean and variance) in a system

Table 2. Sampling parameter results.

	No. of iterations	1000	5000	10000
Population (exhaustive)	Run times (s)	0.0156	0.1404	0.2496
	Mean value	15.8781	15.8781	15.8781
	Variance	0.33719	0.33719	0.33719
	Confidence interval	[14.74, 17.016]	[14.74, 17.016]	[14.74, 17.016]
	Error value	0	0	0
Cluster	Run times (s)	0.0624	0.2964	0.5304
	Mean value	15.4939	15.4681	15.4897
	Variance	0.37591	0.3741	0.37508
	Confidence interval	[14.302, 16.685]	[14.276, 16.659]	[14.295, 16.6835]
	Error value	0.63211	0.65154	0.63143
Fuzzy	Run times (s)	0.0156	0.1092	0.234
	Mean value	15.5226	15.4896	15.4914
	Variance	0.29896	0.29754	0.29649
	Confidence interval	[14.461, 16.583]	[14.429, 16.550]	[14.434, 16.5481]
	Error value	0.58528	0.59778	0.59765

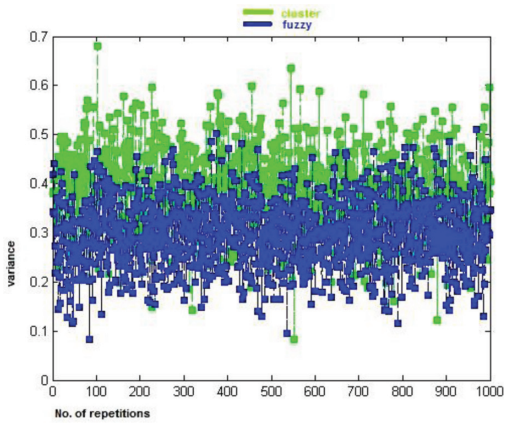


Figure 5. Variance deviations on difference run for fuzzy and cluster sampling.

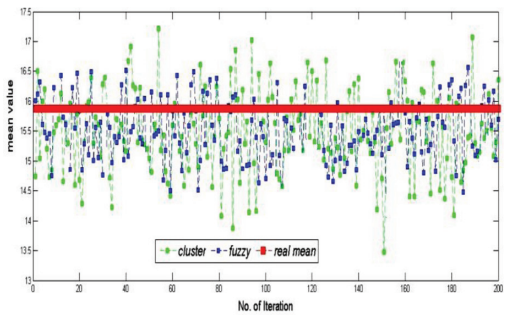


Figure 6. Mean deviations of sampling.

(win 7, mat lab R2010a, 2.30 GHz, 2 GB), and then compared results are given in Table 2.

Results show that significantly error values for fuzzy method is less than clustering and also approximation of mean value for fuzzy is close to population mean. Fuzzy method has less differences variance than cluster method (Fig. 5), as results in statistical approaches we can conclude that this method is an effective way to compute statistical values.

Also, Figure 6 shows the Mean values for exact, cluster sampling, and fuzzy sampling. As obviously, the fuzzy-clustering method has less deviation from the mean exact solution rather than simple clustering method. So, this method shows less error values from the exact solve.

6 CONCLUSION

With the set of given numbers, elements or objects in the statistical approaches we can select the elements in a random way to compute values of many subjects like mean, variance and etc. There are some sampling methods in this way that argued in many publications. In the whole of these methods we assumed that the input data is precise, i.e. each data belongs to a set. For example in stratified sampling we assume that the population of N units may be divided into m groups and the m strata are no overlapping, and then samples select from within each groups. However, in real world, examples and elements may be belong to any groups or not precise. Even in simple random sampling or systematic way we can see some errors lead to equal probabilities of elements. In this paper we introduce new approach base on fuzzy theory combined with sampling methods. The process is to calculate the relative error or uncertainty as the simulation proceeds and, using appropriate statistical tests generally based on the fuzzy theory, calculate the confidence interval after each sampling. This is compared with the pre-specified example. In this paper we introduce new approach base on fuzzy theory combined with sampling methods.

The case study results show that the proposed method provides better measure of uncertainty than the existing methods as unlike traditional sampling method. In this paper, in order to decrease the uncertainty of sampling, the variance reduction techniques have been used. Variance reduction techniques are methods that attempt to reduce the variance, i.e., the dispersion associated with the variations, of the parameter being evaluated. Results show that significantly error values for fuzzy method is less than clustering and also approximation of mean value for fuzzy is close to population mean. Fuzzy method has less differences variance than cluster method (Fig. 5), as results in statistical approaches we can conclude that this method is an effective way to compute statistical values. Also, the fuzzy-clustering method has less deviation from the mean exact solution rather than simple clustering method.

Like cluster method we choose some random clusters for sampling, and then we identify the neighborhood of clusters to modeling fuzzy. Now we want use advantages of fuzzy model to improve sampling and solve the problems that occur in probability sampling.

REFERENCES

Billinton, R. and R.N. Allan (1983). Reliability evaluation of engineering systems: concepts and techniques, Plenum Press New York, NY.

Cochran, W.G. (2007). Sampling techniques, John Wiley & Sons.

Garibaldi, J.M. and R.I. John (2003). Choosing membership functions of linguistic terms. Fuzzy Systems, 2003. FUZZ'03. The 12th IEEE International Conference on, IEEE.

Grøn, C., J. Hansen, B. Magnusson, A. Nordbotten, M. Krysell, K. Jebjerg Andersen and U. Lund (2007). "Uncertainty from sampling—A Nordtest handbook for sampling planners on sampling quality assurance and uncertainty estimation." Nordtest Report TR 604.

Kurowicka, D. and R.M. Cooke (2006). Uncertainty analysis with high dimensional dependence modelling, John Wiley & Sons.

Kwakernaak, H. (1978). "Fuzzy random variables—I. Definitions and theorems." Information Sciences 15(1): 1–29.

Levy, P.S. and S. Lemeshow (2009). Sampling of Populations: Methods and Applications: Solutions Manual, Wiley-Blackwell.

Levy, P.S. and S. Lemeshow (2013). Sampling of populations: methods and applications, John Wiley & Sons.

Ondrej Linda and M. Manic "Importance Sampling Based Defuzzification for General Type-2 Fuzzy Sets', WCCI 2010 IEEE World Congress on Computational Intelligence, July, 18–23, 2010—CCIB, Barcelona, Spain."

Verdonck, F.A., A. Souren, M. van Asselt, P.A. Van Sprang and P.A. Vanrolleghem (2007). "Improving uncertainty analysis in European Union risk assessment of chemicals." Integrated environmental assessment and management 3(3): 333–343.

Viertl, R. (2011). Statistical methods for fuzzy data, Wiley. com.

Zadeh, L.A. (1975). "The concept of a linguistic variable and its application to approximate reasoning—I." Information sciences 8(3): 199–249.

Zadeh L. "Fuzzy sets as a basis for a theory of possibility, Fuzzy Sets Syst. 1 (1978) 3–28.".

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Conversion of a based risk model into a simulation model for simulation and analysis

K. Negrichi, J.-M. Flaus & M. Di Mascolo
Université Grenoble Alpes, G-SCOP, Grenoble, France
CNRS, G-SCOP, Grenoble, France

ABSTRACT: For production systems, risks may have serious effects that may threaten their performance. Nevertheless, we cannot estimate the degradation that a risk may cause to system performance, since risk analysis methods found in the literature do notallow simulating the behavior of the system in degraded mode. In this paper, we propose a translation method that helps to convert a model based risk analysis framework, which is the Function, Interaction, Structure (FIS) model, into an executable model based on Predicate-Transition, Prioritized, Synchronous (PTPS) Petri Net, which is a new class of Petri Net (PN)s that we defined for simulationpurposes. Using the proposed conversion method, we will be able to obtain a model capable of simulating the behavior of a production system in degraded mode. Furthermore, quantitative indicators can be generated to help risk analyst to quantify the performance degradation. To obtain degraded mode simulation model, we start by performing risk analysis of the system using FIS framework. Then, the obtained model from this risk analysis is translated automatically using algorithms into a PTPS Petri Net model. Finally, using a simulator, the PTPS PN model is executed in order to visualize the behavior of the system in degraded mode.

1 INTRODUCTION

Nowadays production systems are asked to perform their activities in a high uncertainty environment and to guarantee their performance in this environment. Therefore they are asked to master risks, that are part of their daily activities, to maintain the performance which is considered their key success factor.

Risk analysis is the discipline used to identify, assess, and prioritize risks according to the criticality of their effects. Their effects on production system performance may vary from simple perturbation to the total system loss.

Today many risk management methods are available and widely used in order to assist production systems in their process of mastering risks. Among these methods we can find classic methods (Villemeur 1992) such as Preliminary Hazard Analysis (PHA), Failure Mode, Effects and Criticality Analysis (FMECA) and HAZard and OPerability (HAZOP) and model driven methods as FIS (Flaus 2008) and CORAS (Lund, Solhaug, & Stølen 2011). By examining from closer view these methods, we can conclude that their risk ranking methods are based on quantitative indicators that depend only of the perception of the person performing the analysis. This kind of risk ranking method can lead to errors especially for risk causing performance degradation to since no quantitative performance indicators are used.

Based on this observation, we propose in this paper a method enabling to convert a risk analysis model into a simulation model. This simulation model is used to perform simulation in degraded mode in order to obtain quantitative performance indicators that can represent the degradation of the system performance in risk situation.

This paper is structured as follows: The next section deals with the risk model used in our proposed approach. Section 3 gives a presentation of the model used to perform degraded mode simulation. Section 4 presents the set of conversion algorithms used to convert risk model to a simulation model. Section 5 presents some of the performance indicators that can be obtained using the simulation model.

2 PRESENTATION OF THE RISK MODEL USED TO PERFORM THE ANALYSIS

There are several methods that exist to perform risk analysis. These methods can be divided to two types:

- Classical methods as PHA, FMECA and HAZOP
- Model driven methods such as FIS and CORAS.

Classical methods have been used for some time now to perform risk analysis. Generally their results consist in a table in which we

include elements of risk (as Hazard, contact event, failure mode…) and the assessment of the risk severity and the necessary corrective measures.

For simulation purposes, classical methods are not suitable to use. In fact, these methods do not offer a sufficient view of the system to perform simulation. For example, in classical methods there is no indication regarding the material flows in the system, neither indication about the consumed and produced resources of each function. In addition, resources are not treated as in simulation by their number where each instance of the resource is presented.

In this paper we lay on a model driven risk analysis method, FIS, which was published for the first time in 2008 (Flaus 2008). Since then it has been repeatedly used to analyze various systems such as Backup communal plan (Girard, Piatyszek, David, & Flaus 2013), Industrial emergency plans (Karagiannis, Piatyszek, & Flaus 2013) and sterilization services (Negrichi, Di Mascolo, & Flaus 2012) According to FIS (Flaus 2013), a system can be modeled using there different views: Structuro-functional, dysfunctional and evolution view, as detailed below.

2.1 *Structuro-functional view*

Functional view is devoted to describe the structure and the function of the analyzed system. The system is decomposed into functional view composed of *functions* and structural view mainly composed of *resources* (human, technical and organizational resources) (see Fig. 1).

Functions are defined as the role of a group of resources expressed in terms of purpose. According to this definition, a function needs a set of resources called *input resources* to be performed. Then the function creates *output resources*. For their, *support resources* are resource needed by the function to be performed but they are not transformed after the function accomplishment.

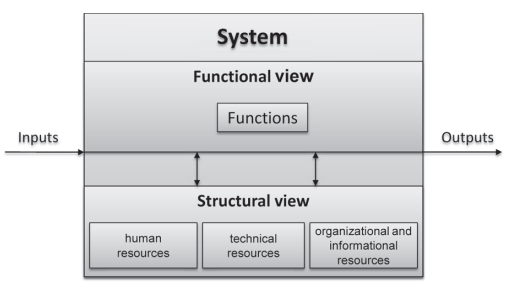


Figure 1. Structuro-functional view of FIS model.

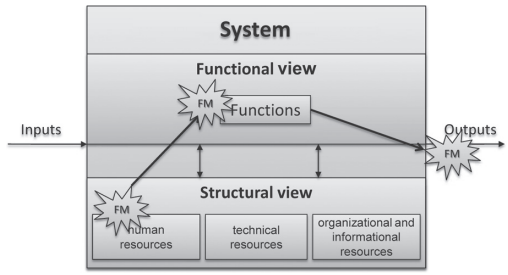


Figure 2. Dysfunctional view of FIS model.

2.2 *Dysfunctional view*

Dysfunctional view represents the failure occurrences in the system and their propagation. First *failure modes* need to be added to the elements defined in the functional view (resources and function see paragraph N 2.1). In a second stage, failure modes propagation relations are added. These propagation relations are causes-effects relations who represent the propagation of failures in a system and are visualized using Fault Trees (see Fig. 2).

2.3 *Evolution view*

The aim of the evolution view is to represent the behavior of the system using the behavior of its functions. FIS gives the possibility to add to each function several behavior modes (see Fig. 3). Each behavior mode is defined by *consumed resources* needed for the function execution (resources selected from the declared input resources of the function (see paragraph 2.1), *produced resources* created of the function execution (resources selected from the declared output resources of the function (see paragraph 2.1), *duration*: the amount of time needed for the function to transform consumed resources to produced resources, *filtering conditions* used to select consumed resources, *input and output actions* that are applied respectively to consumed and produced resources.

During simulation the function can change its behavior according to its state. The state of a function is defined according to the states of its behavior modes. Therefore if a failure mode is activated in the function, this function can change its behavior.

2.4 *Formalization of FIS model*

In order to perform conversion, we need to formalize FIS model. A FIS model M is composed by a set of PR, and a set of systems Sy ($M = \{Sy, PR\}$). Sy is a set of systems ($Sy = \{S_1, S_2, ..., S_n\}$). A system

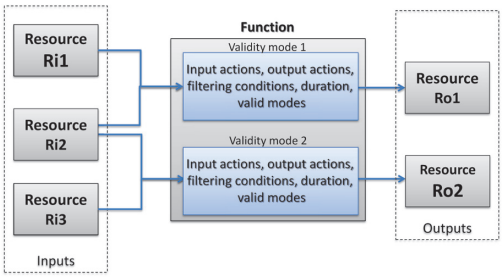


Figure 3. Evolution view of FIS model.

S_i is formally defined as $S_i = \{Fn_i, R_i\}$ (for clarity reasons we will not display the function index (i) in the following) where:

- Fn is a set of functions ($Fn : \{fn_1, fn_2, ..., fn_n\}$)
- R is a set of resources ($R : \{r_1, r_2, ..., r_m\}$).

A function fn_j is formally defined as $fn_j = \{af_j, FM_j, FPR_j, VM_j\}$ (for clarity reasons we will not display the function index (j) in the following) where:

- af is an attribute of the function name
- FM is a set of failure modes associated to the function ($FM : \{fm_1, fm_2, ..., fm_n\}$)
- VM is a set of function behavior modes (($VM : \{vm_1, vm_2, \ldots vm_n\}$). A behavior mode vm_i is definied as $vm_k : \{avm_k, IR_k, OR_k, \theta_k, p_k, IA_k, OA_k, FS_k\}$, where:
  - avm_k is an attribute of behavior mode name
  - IR_k is a set of input resources $\in IR_k$: $\{ir_{k_1}, ir_{k_2}, ..., ir_{k_n}\}$), each input resource ir_{l_m} is defined by $ir_{l_m} : \{irn_{l_m}, irc_{l_m}, RFC_{l_m}\}$, where:
    * irn_{l_m} is the input resource name
    * irc_{l_m} is a number of needed resources
    * RFC_{l_m} is a set of filtering conditions
  - OR_k is a set of output resources, each output resources ($OR_k : \{or_{k_1}, or_{k_2}, ..., or_{k_n}\}$), each output resource or_{l_m} is defined by $or_{l_m} : \{orn_{l_m}, orc_{l_m}\}$, where
    * orn_{l_n} is the output resource name
    * orc_{l_n} is a number of produced resources
  - θ_k is the duration needed to transform input resource to output resources
  - p_k is the priority associated to the behavior mode
  - IA_k is a set of actions applied to input resources ($IA_k : \{ia_{k_1}, ia_{k_2}, ..., ia_{k_n}\}$). Each input action ia_{l_m} defined by $ia_{l_m} : \{iar_{l_m}, iat_{l_m}, IP_{l_m}\}$ where:
    * iar_{l_m} is the input resource name
    * iat_{l_m} is the action type
    * IP_{l_m} is a set of action parameters
  - OA_k is a set of actions applied to output resources ($OA_k : \{oa_{k_1}, oa_{k_2}, ..., oa_{k_n}\}$). Each output action oa_{l_m} defined by $oa_{l_m} : \{oar_{l_m}, oat_{l_m}, OP_{l_m}\}$ where:
    * oar_{l_m} is the output resource name
    * oat_{l_m} is the action type
    * OP_{l_m} is a set of action parameters
  - FS_k is the function state (FS_k: $\{fs_{k_1}, fs_{k_2}, ..., fs_{k_n}\}$) i.e, a set binary constants that represent the state of the function failure modes in a specific date.

A resource r_j is formally defined as $r_j = \{ar_j, RV_j, FM_j, RI_j\}$ (for clarity reasons we will not display the resource index j in the following FIS resource formalization) where:

- ar is an attribute related to the resource name
- RV is a set of resource variables associated to the resource ($RV : \{rv_1, rv_2, ..., rv_m\}$)
- FM is a set of failure modes associated to the resource ($FM : \{fm_1, fm_2, ..., fm_n\}$)
- RI is a set of resource instances ($RI : \{ri_1, ri_2, ri_i\}$), where each resource instance ri_i is defined by a set of constant representing the initial state of the resource variables and failure modes $ri_i = \{IS_1, IS_2, ..., IS_n\}$.

PR is a set of propagation relations ($PR = \{pr_1, pr_2, ..., pr_m\}$). A propagation relation $pr_o = \{Ca_o, Op_o, Ef_o\}$ is composed by a set of causes Ca_o, an operator Op_o and a set of effects Ef_o. Causes and effects are faillure modes associated to FIS functions and resources. Operator is used to describe the relationship between Causes and effects. Propagation Relations (PR) are the formalization of fault trees (see Fig. 10) in the analyzed systems.

3 SIMULATION MODEL

3.1 *Description of the simulation model*

To represent the dynamic behavior of the analyzed system, we need to rely on a simulation model. Several simulation model formalisms exist. Among them we can find PN. PN are a very powerful graphical and mathematical formalism used to representand analyze complex Discrete Event Systems (DES). They were first introduced in 1962 (Petri 1962). They represent a suitable formalism for performance analysis (Ajmone Marsan, Bobbio, & Donatelli 1998). The power of PN relies on their flexibility and their Evolution. In fact many classes of PN were introduced to cope with the increasing complexity of analyzed systems (Reisig, Wolfgang 2013).

According to the requirements of FIS model, we decided to introduce a new class of PN named PTPS PN, which is a class of PN defined using, as its name suggests, Predicate-Transition PN (Genrich & Lautenbach 1981), Prioritized PN (Guan, Yu, & Yang 1998) and Synchronous PN (David & Alla 2010).

3.2 *Formalization of simulation model*

As for FIS model, we need to formalize the PTPS PN in order to perform conversion from risk model into simulation model. Formally, a PTPS PN is is defined by a triplet $< R, A_n, M_0 >$ where:

- R is an ordinay PN, $R = (P, T, F, W)$, where:
  - P is a finite set of places
  - T is a finite set of transitions
  - F is a set of arcs $F(F \subseteq (P \times T) \cup (T \times P))$
  - $W : F \to \mathbb{N}^+$, a set of arc weights
- A_n are the PTPS PN annotations $A_n = < C_{const}, V, E, S, P_r, A_{tc}, A_{ta}, A_c >$ where:
  - C_{const} is a set of constants (belonging to $\mathbb{N}, \{0,1\}, \{a,..,z\}$)
  - V is a formal set of variables, these variables will be substituted by constants during the transitions firing (belonging to $\{a, .., z\}$)
  - E is a set of external events ($E = \{e_1, e_2 \ldots e_n\}$)
  - $S : T \to E \cup \{e\}$ is an application associating to each transition an event, where e is the always occurring event
  - $P_r : T \to N^+$ is an application associating a priority with each transition
  - $A_{tc} : T \to L_c(C_{const}, V)$ is an application associating with each transition a condition using both constants and variables
  - $A_{ta} : T \to L_a(C_{const}, V)$ is an application associating with each transition an action as a result of allocation of the values of formal variables
  - A_c is an application associating with each arc (element of F) a formal set of n-tuples of elements of V. $A_c : F \to V$.

3.3 *Example of PTPS PN*

Figure 4 presents an example of PTPS PN. This simple PTPS PN model consists of three *places* (p_1, p_2, p_3) a *transition* (t_1) and a set of 3 *arcs* $(p_1 - t_1, p_2 - t_1, t_1 - p_3)$. Initially, place p_1 *marking* (M_0) is composed of one *token* that contains two contstants $(t, 31)$, place p_2 marking is composed of two tokens each of them is composed of two constants $(5, true$ and $2, false)$, while place p_3 is empty. All of the three arcs weights are set to one ($W_{p_1 - t_1} = W_{p_2 - t_1} = W_{t_1 - p_3} = 1$). For their, arc functions are present as follows: $A_{c_{(p_1 - t1)}} = \{a, b\}$, $A_{c_{(p_2 - t1)}} = \{c, d\}$, $A_{c_{(t_1 - p3)}} = \{a, b, c, d\}$. Transition t_1 contains only one condition ($A_{tc_{t1}} : d = = false$) and one action ($A_{ta_{t1}} : c = 20$).

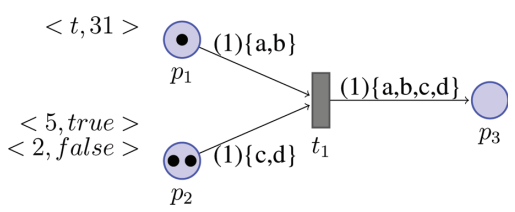


Figure 4. Example of PTPS PN.

Before transition t_1 firing, two tokens need to be reserved, one from place p_1 and one from place p_2 as indicated by the arcs weights ($W_{p_1 - t_1} = W_{p_2 - t_1} = 1$). Then $(p_1 - t_1, p_2 - t_1)$ arcs variables are substituted by reserved tokens constants. This process is called unification. For example, if token $< t, 31 >$ is reserved from the place p_1 and token $2, false$ is reserved from the place $< p_2 >$, unification process will give the following substitution $a = t, b = 31, c = 2, d = false$.

For transition t_1 to be fired, condition $A_{tc_{t1}}$ need to be validated. Therefore among the two present tokens in place p_2, only token $(2, false)$ can be reserved as it is the only token that verifies this condition. After t_1 firing, one token is added to place p_3 as indicated by arc weight ($W_{t_1 - p_3} = 1$). The constants composing this token are calculated from reserved token substituted variables and transitions t_1 action. In this case, t_1 contains one action imposing that c is set to 20. Hence the token added to place p_3 is composed by the following constants: $t, 31, 20, false$.

4 CONVERSION OF FIS MODEL INTO SIMULATION MODEL

In order to convert the FIS model into a simulation model, we implemented a set of conversion algorithms. These algorithms take in input the FIS model and produce a set of two PTPS PNs named function view and resource view. Function view PN is devoted to visualize the state of functions and their evolution over time. For its part, resource view is dedicated to visualize the state of resources and their interactions over time.

4.1 *Functions view conversion*

Algorithm 1 is devoted to obtain the function view from the FIS model. According to this algorithm, every FIS function is converted into a set of two places $(p_{af_i activation}, p_{af_i desactivation})$, two transitions $(t_{af_i activation}, t_{af_i desactivation})$ and four arcs between the created places and transitions. A token is then constitued from the function name (af_i) and the initial state of the function failure modes FM_i. This token is added to the place $p_{af_i activation}$. Finally, for each function failure mode, a set of two transitions are added. The first transition $(t_{fm_i activation})$ includes an action devoted to failure mode activation, while the

Algorithm 1 Function view translation algorithm

for each function fn_i in $Fn, i \in \{1,...,n\}$ **do**
  $P \leftarrow P \cup \{p_{af_i activation}, p_{af_i desactivation}\}$
  $T \leftarrow T \cup \{t_{af_i activation}, t_{af_i desactivation}\}$
  $F_{fn_i} \leftarrow F_{fn_i} \cup \{(p_{af_i desactivation}, t_{af_i activation}),$
    $(t_{af_i activation}, p_{af_i activation}),$
    $(p_{af_i activation}, t_{af_i desactivation}),$
    $(t_{af_i desactivation}, p_{af_i desactivation})\}$
  for each failure mode $fm_j \in FM_i, j \in \{1,...,m\}$ **do**
    $T \leftarrow T \cup \{t_{fm_j activation}, t_{fm_j desactivation}\}$
    $A_{ta}(t_{fm_j activation}) \leftarrow fm_j = true$
    $A_{ta}(t_{fm_j desactivation}) \leftarrow fm_j = false$
  end for
  $W(x,y) = 1 \quad \forall x,y \in F_{fn_i}$
  $A_c(x,y) = V_{fn_i} \quad \forall x,y \in F_{fn_i}$
end for

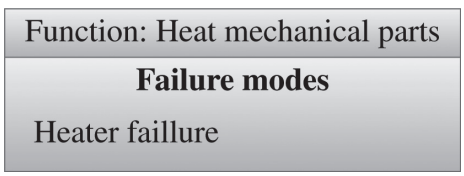


Figure 5. Example of FIS function.

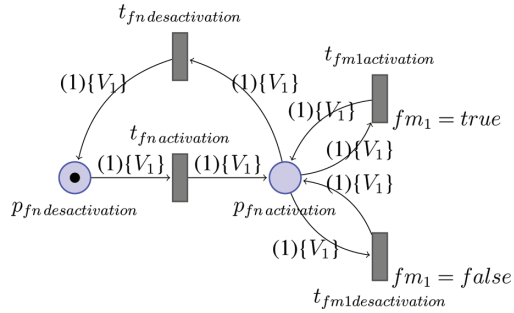


Figure 6. Example of function view conversion.

Algorithm 2 Resource creation and instanciation

for each resource r_i in $R, i \in \{1,...,n\}$ **do**
  $P \leftarrow P \cup \{p_{ari}\}$
  for each resource instance $ri_j \in RI, j \in \{1,...,m\}$ **do**
    for each resource instance state $IS_k \in ri_j, k \in \{1,...,o\}$ **do**
      $to_{ri_j} \leftarrow to_{ri_j} \cup \{IS_k\}$
    end for
    $M_{0_{p_{ari}}} = M_{0_{p_{ari}}} \cup \{to_{ri_j}\}$
  end for
end for

second transition ($t_{fm_i desactivation}$) includes anaction devoted to failure mode desactivation. Finally, an arc functions (composed using another algorithm not presented for space reasons) is associated to all the function view arcs, then all arc weights are initiated to 1. Figure 5 presents an example of FIS function. This function is named *"Heat mechanical parts"*, and is has one faillure mode called *"Heater failure"*. The obtained PTPS PN from the conversion of this function is presented in Figure 6. We can distinguish the places needed for function activation and desactivation ($p_{fndesactivation}, p_{fnactivation}$) the two transitions for function activation and desactivation ($t_{fndesactivation}, t_{fnactivation}$), the two transitions needed for faillure activation and desactivation ($t_{fm_i desactivation}, t_{fm_i activation}$) and the initial marking of place representing the FIS function initial state $p_{fndesactivation}$ is $M_{0pfndesactivation}$ = {< "*Heat mechanical parts", false*>}.

4.2 *Resources view conversion*

To obtain the resource view, we implemented a set of algorithms that are treated in sequence. The first algorithm (see Algorithm 2) is called to convert FIS resources into a set of places and tokens. Then each behavior mode in a FIS function is converted using Algorithm 3. Finally, Algorithm 4 is called to link the obtained resources and behavior modes. For clarity reasons, arc functions, arc weights, transition conditions and transition actions are not presented in the following figures.

Algorithm 2 is the first algorithm to execute. It is devoted to create and instanciate FIS resource. According to this algorithm, each FIS resource is converted into a place named using the resource name attribute (ar_i). Then, each of the resource instance is converted to a token (to_i). This token is composed using the resource instance state variables (Si_j) and then added to the resource place P_{ar_i}.

To illustrate the ressource creation and instanciation, Figure 7 presents an example of FIS resource. According to the example, the presented resource is named *"heater"* and it is parametrized using a binairy variable ("Calibration") and a failure mode ("Heating failure"). This resource has one instance. This instance contains 3 state constantes, one related to the instance identifier (*heater*) and two states constantes representing the initial state of its variable and failure mode (*true*, *false*). The obtained place from this resource conversion is presented in Figure 8. It is a place named using the place of the (p_{heater}). This place containes one token constituted by the resource initial state constants (< "*heater*",*true*, *false* >).

Algorithm 3 Function behavior modes conversion algorithm

for each function behavior mode vm_i in Fn, $i \in \{1,...,n\}$ **do**
  $P \leftarrow P \cup \{p_{avm_i in}, p_{avm_i wat}, p_{avm_i proces}\}$
  $T \leftarrow T \cup \{t_{avm_i in}, t_{avm_i out}, t_{avm_i iowat}, t_{avm_i watio}, t_{watpro}, t_{tprowat}\}$
  $F_{vm_i} \leftarrow F_{vm_i} \cup \{(t_{avm_i in}, p_{avm_i inout}), (p_{avm_i inout}, t_{avm_i out}) (p_{avm_i in}, t_{avm_i iowat}), (t_{avm_i watgio}, p_{avm_i inout}), (t_{avm_i iowat}, p_{avm_i wat}), (p_{avm_i wat}, t_{avm_i watio}), (p_{avm_i wat}, t_{avm_i watpro}), (t_{avm_i prowat}, p_{avm_i wat}), (t_{avm_i watpro}, p_{avm_i proces}), (p_{avm_i proces}, t_{avm_i prowat})\}$
  for each input resources $IR_j \in vm_i$, $j \in \{1,...,m\}$ **do**
    for each resource $r_k \in R, k \in \{1,...,o\}$ **do**
      if $(ar_k == irn_j)$ **then**
        for each failure mode $fm_l \in r_k$, $l \in \{1,...,u\}$ **do**
          $T \leftarrow T \cup \{t_{fm_l}\}$
          $A_{ta}(t_{fm_l}) \leftarrow fm_l = true$
          $A_{ta}(t_{fm_l}) \leftarrow fm_l = true$
          $F_{vm_i} \leftarrow F_{vm_i} \cup \{(t_{fm_l}, p_{avm_i proces}), (p_{avm_i proces}, t_{fm_l})\}$
        end for
        for each propagation relation $rpr_l \in r_k$, $l \in \{1,...,v\}$ **do**
          $T \leftarrow T \cup \{t_{synch_{fm_k}}\}$
          $A_{tc}(t_{synch_{fm_k}}) \leftarrow fm_k == true$
          $F_{vm_i} \leftarrow F_{vm_i} \cup \{(t_{synch_{fm_k}}, p_{avm_i proces}), (p_{avm_i proces}, t_{synch_{fm_k}})\}$
        end for
      end if
    end for
  end for
  $W(x,y) = 1 \quad \forall x,y \in F_{vm_i}$
  $A_c(x,y) = V_{vm_i} \quad \forall x,y \in F_{vm_i}$
end for

After ressource creation and instanciation, the following step is the conversion of FIS function behavior modes. Algorithm 3 is used to convert function behavior mode. According to this algorithm, each behavior mode is converted into a set of places ($(p_{avm_i in}, p_{avm_i wat}, p_{avm_i proces})$), a set of transitions ($t_{avm_i in}$,$t_{avm_i out}$,$t_{avm_i iowat}$,$t_{avm_i watio}$,t_{watpro},$t_{tprowat}$) and a set of arcs between them. In a second stage, each of the input resources failure modes is converted into a transition (t_{tfmi}) which includes an action related to failure activation ($fm_i = true$).

Then each of the propagation relations related to the treated failure is converted to a transition ($t_{synch_{fmi}}$), this transition contains a condition and an action. The condition is used to garantee that the firing of the transition can be performed only if the failure mode is active ($fm_i == true$) while the action presents the propagation relation ($fm_{i_{effect}} = true$).

To illustrate the conversion of FIS function behavior modes, Figure 9 presents an example of FIS beahvior modes. According to this example, we can see that the function *heat mechanical parts* (presented previously in Fig. 5) has 2 behavior modes. The first behavior mode is the *OK mode*.

Algorithm 4 Resources and behavior modes connection algorithm

for each function behavior mode vm_i in Fn, $i \in \{1,...,n\}$ **do**
  for each input resource $IR_j \in vm_i$,$j \in 1,...,m$ **do**
    for each resource $r_k \in R$, $k \in 1,...,o$ **do**
      if $(ar_k == irn_j)$ **then**
        $F \leftarrow F \cup \{(p_{ar_k}, t_{input_{vm_i}})\}$
        $W(p_{ar_k}, t_{input_{vm_i}}) = irc_j$
        $A_{c_{(p_{ar_k}, t_{input_{vm_i}})}} = V_{r_k}$
      end if
    end for
  end for
  for each output resource $OR_j \in vm_i \quad j \in \{1,...,p\}$ **do**
    for each resource $r_k \in Rk \in \{1,...,o\}$ **do**
      if $(ar_k == orn_j)$ **then**
        $F \leftarrow F \cup \{t_{output_{vm_i}}, p_{ar_k}\}$
        $W(t_{output_{vm_i}}, p_{ar_k}) = orc_j$
        $A_{c(t_{output_{vm_i}}, p_{ar_k})} = V_{r_k}$
      end if
    end for
  end for
end for

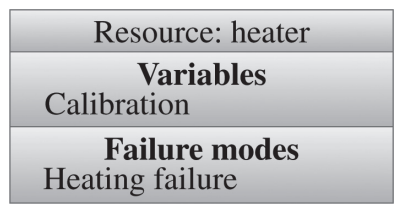


Figure 7. Example of FIS resource.

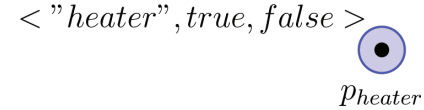


Figure 8. Result of a FIS resource conversion.

To illustrate the conversion of FIS function behavior modes, Figure 9 presents an example of FIS beahvior modes. According to this example, we can see that the function *heat mechanical parts* (presented previously in Fig. 5) has 2 behavior modes. The first behavior mode is the *OK mode*.

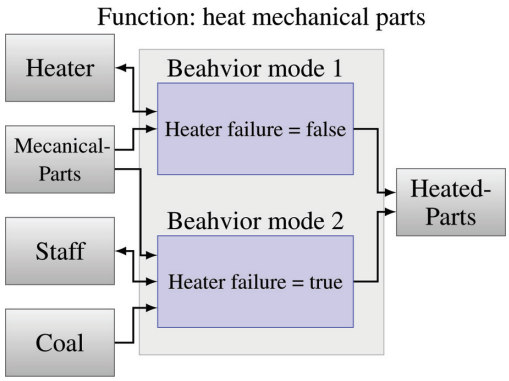


Figure 9. Example of FIS behavior modes.

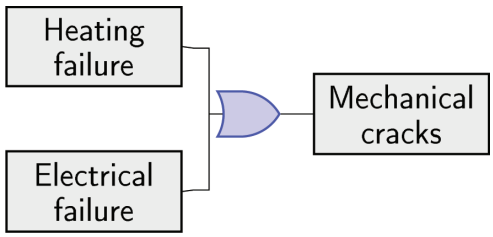


Figure 10. Extract of FIS example fault tree.

It is the mode activated when the failure there is non failure activated on the function (Heater failure = false). In this mode, to perform heating, we need to used *heater* and *mecanical parts* as input and we get as output *heated parts* and the used *heater* (in this case *heater* is a support resource). The second mode is actioned when failure *Heater failure* is activated (Heater failure = true). As we can not use heater due to the failure, to perform heating, we need to used the resources *Staff*, *Coal* and *mecanical parts* as input and in the output we get *heated parts* and *Staff*. Figure 10 presents an extract of the fault tree. According to this fault tree, we can conclude that the failure mode *heating failure* associated to the resource *heater* causes the faillure mode *Mecanicalcracks* on the resource *heatedparts*.

The obtained PTPS PN from the conversion of the *OK mode* is presented in Figure 11. We can see the set of places and transitions related to this *OK mode*. It's important also to highlight that transition $t_{synch_{fm_i}}$ containes a condition $A_{tc}(t_{synch_{fm_i}}) = \{fm_{heatingfailure} == true\}$ and an action $A_{tc}(t_{synch_{fm_i}}) = \{fm_{Mecanicalcracks} = true\}$ which are the conversion of the propagation presented in Figure 10.

After the conversion of the FIS behavior modes, we can see that there in no connexion between the instanciated resources and the converted behavior modes. To complete the conversion process, Algorithm 4 is called to link the created resources and behavior modes.

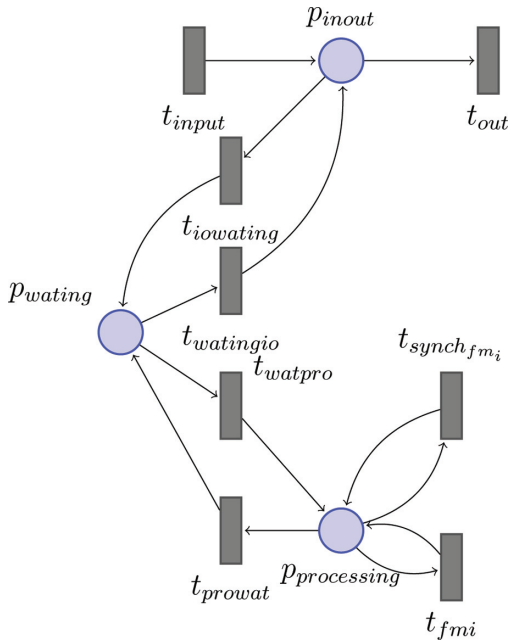


Figure 11. Example of behavior mode conversion.

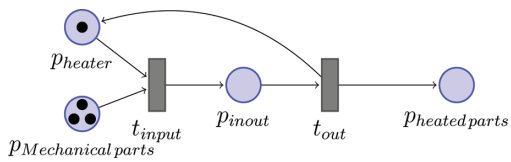


Figure 12. Example of resource and behavior mode connection.

To link FIS behavior modes and instaciated resources, algorithm 12 each function behavior mode. If this behavior mode has an input resource then an arc is created between this resource place and the transition $t_{input_{vmi}}$ of the behavior mode. The created arc weight initiated to the number of required resources and its arc functions is created based on the resource variables and failure modes. If this behavior mode has an output resource then an arc is created between the output transition $t_{output_{vmi}}$ and the resource place. The created arc weight initiated to the number of produced resources and its arc functions is created based on the resource variables and failure modes.

Figure 12 presents the result obtained after applying the Algorithm 4 on the example presented in Figure 9. As *heater* is support resource

(input and output resource in the same time), an arc is created between the place p_{heater} and the mode input transition $t_{input_{vm_i}}$ and an other arc is created between the behavior mode output transition $t_{output_{vm_i}}$ and the heater place p_{heater}. *Mechanicalparts* is an input resource for the mode, so an other arc is created between the place $p_{Mechanicalparts}$ and the transition $t_{input_{vm_i}}$. Similarly an other arc is added between the transiton $t_{output_{vm_i}}$ and the heated parts place $p_{heatedparts}$.

5 SIMULATION RESULTS

Using the two obtained views of the PTPS PN is possible to perform simulation. Simulation alows to observe the dynamic behavior of the modeled system and to generated performance indicators. Performance indicators are quantitave indicators that illustrates the performances of the system in it is different beahvior modes. Among the performance indicators generated by simualtion we can find, the resource rates of use which reflects which of the support resources are over or under used during processing, the mean time spent by resource in each function, the amount of time spent by the function in each beahavior mode and the resources Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR).

6 CONCLUSIONS

In this paper, we presented a method to convert the FIS risk based model into a simulation model based on PTPS PN. We started our work by presenting FIS model through its differents views (structurofunctional, dysfunctional and evolution view). Then to prepare its conversion, we presented a formalization of the FIS model. Therafter, we defined a new class of PN called PTPS used as simulation model. Finally, we exposed as set of conversion algorithms used to convert the FIS model to a set of two PTPS PN named functions and resource views.

Based on FIS risk model that can be obtained using XRisk[1], our work has shown that we can convert this risk model into a simulation model. This simulation model is capable of representing the dynamic behavior of a system in a risk situation including flow of materials, failure occurrence, failure propagation...

This simulation model is designed as a part of a simulation tool called SIMRISK. SIMRISK is a production systems degaraded modes simulation tool used to assess production systems performances in different situations especially when the system is in a riskcircumstances.

Using this tools, it is possible to simulate and visualize the behavior of the system under different circumstances especially in risk situations. It allows the generations of quantitative indicators that reflect the system performances. Using these indicators, managers can improve reliability of their system by appropriate safety barriers targeting the failures that cause the most significant performance degradation.

REFERENCES

Ajmone Marsan, M., A. Bobbio, & S. Donatelli (1998). Petri nets in performance analysis: An introduction. In W. Reisig and G. Rozenberg (Eds.), *Lectures on Petri Nets I: Basic Models*, Volume 1491 of *Lecture Notes in Computer Science*, pp. 211–256. Springer Berlin Heidelberg.

David, R. & H. Alla (2010, January). *Discrete, Continuous, and Hybrid Petri Nets*. Robotics. Springer. 2nd edition. ISBN: 978-3-642-10668-2 Département Automatique Département Automatique.

Flaus, J.-M. (2008). A model-based approach for systematic risk analysis. *J. Risk and Reliability 222*, 79–93. CI CI.

Flaus, J.-M. (2013, Octobre). *Risk Analysis: Sociotechnical and Industrial Systems*. Number ISBN:9781118789995. Wiley.

Genrich, H. & K. Lautenbach (1981). System modelling with high-level petri nets. *Theoretical Computer Science 13*(1), 109–135. Special Issue Semantics of Concurrent Computation.

Girard, C., E. Piatyszek, P. David, & J.-M. Flaus (2013). Emergency Plans Modeling: toward An assessment Tool. In *ESREL 2013 proceedings*, Amsterdam, Pays-Bas, pp. ...

Guan, S.-U., H.-Y. Yu, & J.-S. Yang (1998, Apr). A prioritized petri net model and its application in distributed multimedia systems. *Computers, IEEE Transactions on 47*(4), 477–481.

Karagiannis, G.-M., E. Piatyszek, & J.-M. Flaus (2013, June). Model-Driven and Risk-Based Performance Analysis of Industrial Emergency Plans. *Journal of Contingencies and Crisis Management Volume 21*(Issue 2), pages 96–114.

Lund, M.S., B. Solhaug, & K. Stølen (2011). *Model-Driven Risk Analysis—The CORAS Approach*. Springer.

Negrichi, K., M. Di Mascolo, & J.-M. Flaus (2012, August). Risk analysis in sterilization services: A first step towards a generic model of risk. In *Proceedings GISEH'2012*, Québec, Canada, pp. ? 8 pages GCSP GCSP.

Petri, C.A. (1962). *Kommunikation mit Automaten*. Ph. D. thesis, Institut für instrumentelle Mathematik, Bonn.

Reisig, Wolfgang (2013, 31 July). *Understanding Petri Nets: Modeling Techniques, Analysis Methods, Case Studies*. Springer. 230 pages; ISBN 978-3-642-33277-7.

Villemeur, A. (1992). *Reliability, Availability, Maintainability and Safety Assessment, Assessment, Hardware, Software and Human Factors*. Reliability, Availability, Maintainability & Safety Assessment: Methods and Techniques. Wiley.

[1]Model driven risk analysis software. www.xrisk.net.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Common cause failures modelling by means of Coloured Petri Nets for dependability assessment of a control system of nuclear power plant

N. Brînzei
Centre de Recherche en Automatique de Nancy, CRAN UMR 7039, Université de Lorraine, Vandœuvre-lès-Nancy, France
CNRS, Vandœuvre-lès-Nancy, France

G. Deleuze
Électricité de France (EDF) R&D Management des Risques Industriels 1, France

N. Villaume
École Nationale Supérieure d'Électricité et de Mécanique, Université de Lorraine, Vandœuvre-lès-Nancy, France

J.F. Pétin
Centre de Recherche en Automatique de Nancy, CRAN UMR 7039, Université de Lorraine, Vandœuvre-lès-Nancy, France
CNRS, Vandœuvre-lès-Nancy, France

ABSTRACT: This paper presents an approach to assess the effects of Common Cause Failures (CCF) on dependability of digital systems. Independent failures of system components and partial or lethal shocks are considered in a global CCF model, the Atwood model. The Coloured Petri Nets (CPN) are used to modelize the digital system and the common cause failures. Based on the CPN, the parameters of Atwood model are estimated analytically and by Monte-Carlo simulation. Thereafter, the Atwood model of CCF is modified in order to represent the dominant failures propagation on some system components in the case of partial shocks. The assessment of system dependability, in the presence of CCF failures, becomes possible. This approach is applied to a representative instrumentation and control system of a nuclear power plant. The system is large with a high level of redundancy.

1 INTRODUCTION

Digital Instrumentation and Control systems (I&C) systems have a major role in the control and protection of nuclear power plants. These systems are characterized by a large size, a high level of redundancy and a complex logic of vote. Although digital systems and their components are more reliable than the analog systems they replace, some characteristics raise specific issues on the modelling and assessment of Common Cause Failures (CCF). A CCF can occur in operational or on demand modes and affect groups of identical or similar redundant components having the same function and operating under comparable conditions.

The β-factor model is the most widely used model for taking into account CCF within all types of systems, like nuclear power plants (US-NRC 1987) and, more generally, in the field of power system (Bricman-Rejc et al. 2013). It involves *thefailure of whole set of components* when a common cause event occurs. This model is used when the system is composed of only a few components. However when the system is composed of dozens of identical or similar components, the assumption of failure of whole set of components, when a CCF occurs, is very conservative.

The concepts of partial and lethal shocks are very well adapted to represent the potential effects of stress factors on electronic hardware. In the next section we introduce the Atwood model of CCF that takes into account independent failures of components and CCF failures due to shocks that affect all or only some components. For dependability assessment, the CCF model must be integrated within a system model. Also, the system model must integrate the dynamic behaviour of the digital I&C systems. The Markov chains or Petri nets are such types of models and the β-factor model has been integrated in Markov chains (Lilleheier 2008) and in the classical Petri Nets (Signoret et al. 2013). The main drawback of these

models is the combinatorial explosion of their size when the modelled system is large. To overcome this drawback, we propose to use the Coloured Petri Nets (CPN) for I&C systems modelling. The section three of this paper develops a CPN model for an I&C system and, also, for the CCF Atwood model. In the same section, firstly, we propose two approaches for parameters estimation of Atwood model and, secondly, we modify this model to represent asymmetry in CCF propagation oriented on some types of components. If for I&C modelled system only the hardware architecture is considered, the oriented propagation of CCF on this architecture takes into account the software and human aspects of functional safety analysis. Section four presents the probabilistic assessment of dependability indicators (PFD, MTTF) or of the impact of the oriented CCF. Finally, some conclusions and future outlook are presented.

2 MODELLING OF COMMON CAUSES FAILURES (CCF)

2.1 *The Atwood model*

The model introduced by Atwood (1980) considers that the system components are subject to two types of failures: independent failures and shock failures. Two kinds of shock failures are defined: lethal shocks and partial (or non-lethal) shocks. In a large redundant systems with N components, a shock is assumed to be non-lethal when it affects k components among N with $1 \leq k \leq N$. A shock is lethal when it affects *all* components. In the case of a non-lethal shock, only the failure of some components is considered. Each component has then a *conditional probability p* of failure. Individual failures, non-lethal and lethal shocks are assumed to follow independent processes. The occurrence frequencies of shocks (denoted μ for non-lethal shocks and ω for lethal shocks) are assumed to be constant.

The failure rate of a specific component in a group of N elements, due to an independent failure or to a non-lethal shock is:

$$\lambda_1^N = \lambda_i + \mu \cdot p \cdot (1-p)^{N-1} \tag{1}$$

The failure rate of a group of k components from N with $1 \leq k \leq N$ due to a non-lethal shock is:

$$\lambda_k^{(N)} = \mu \cdot p^k \cdot (1-p)^{N-k} \tag{2}$$

The failure rate of N components due to a non-lethal and lethal shock is:

$$\lambda_N^N = \mu \cdot p^N + \omega \tag{3}$$

For a specific component in a group of N components, the total failure rate is given by:

$$\lambda_{TOT} = \lambda_{IND} + \omega + \mu \cdot \sum_{k=1}^{N} C_{N-1}^{k-1} p^k \cdot (1-p)^{N-k} \tag{4}$$

The Atwood model is considered representative for the phenomena leading to multiple failures in the large digital I&C systems. It allows to represent CCF affecting only a part of the all components of the system. However, it introduces three parameters to estimate p, μ and ω. The results will be sensitive, of course, to the values used, usually given by expert opinion or by using default values. The default values usually used for these parameters are the following:

- $\alpha = \mu / \lambda_{TOT} = 0.405$: the rate of non-lethal shocks.
- $p = 0.2$ *ou* 0.33 *ou* 0.5: conditional probability of component failure in a non-lethal shock.
- $\beta_{letal} = \omega / \lambda_{TOT} = 5 \cdot 10^{-3}$: the rate of lethal shocks.

Later, in this work, we propose to determine the values of these parameters by two approaches: an analytical one, or a second approach based on results of Monte-Carlo simulations.

2.2 *The Coloured Petri Nets (CPN) model*

In order to asses the impact of CCF in the dependability study of digital I&C systems, it is necessary to have a model of this studied system that is able to take into account the system dynamics. A widely used model in the dependability studies of dynamic systems is represented by the Petri nets (Signoret et al. 2013). Since I&C systems are complex and large, we choose to use the coloured Petri nets (CPN) type. CPN (Jensen & Kristensen 2009, Jensen 1997) is a discrete-event modelling language combining the capabilities of Petri nets with the capabilities of a high-level programming language. The main difference between a classical Petri Net and a CPN is that the CPN tokens can have different *colours* representing data types (*e.g.* Boolean, integer or more complex data structure). The formal definition of CPN is as follows.

A Coloured Petri Net is a 9-uplet $CPN = (P, T, A, \Sigma, V, C, G, E, I)$, where:

1. P is a finite set of **places**.
2. T is a finite set of **transitions**, $P \cap T = \varnothing$.
3. $A \subseteq P \times T \cup T \times P$ is a set of directed **arcs**.
4. Σ is a finite set of non-empty **colour sets**.
5. V is a finite set of **typed variables** such that $Type[v] \in \Sigma$ for all variables $v \in V$.
6. $C : P \rightarrow \Sigma$ is a **colour set function** that assigns a colour set to each place.
7. $G : T \rightarrow EXPR_V$ is a **guard function** that assigns a guard condition to each transition t such that

$Type[G(t)]$ = Bool, bool standing for Boolean data type.

8. $E : A \rightarrow EXPR_V$ is an **arc expression function** that assigns an arc expression to each arc a such that $Type[E(a)] = Type[C(p)]$, where p is the place connected to the arc a.
9. $I : P \rightarrow EXPR_\varnothing$ is an **initialisation function** that assigns an initialisation expression to each place p such that $Type[I(p)] = Type[C(p)]$.

Individual CPN models can be hierarchically related to each other in a formal way, *i.e.* with a well-defined semantics. CPN model hierarchy is realized through *substitution transitions*. The idea is to associate a transition to a more complex CPN (a module), which gives a more precise and detailed description of the activity represented by the substitution transition (represented by a double rectangle, *e.g.* in Fig. 2). The places connected to a substitution transition transmit a given marking from a high level (level of substitution transition) to a low level (level of module) and vice versa. CPN concept of hierarchy allows us to propose a *modular modelling* approach for a complex systems, based on generic modules that can be instantiated as often as needed.

Additionally, the probabilistic dependability assessment requires the time evolution of the system. For this, the CPN must take into account the *time* aspect. In a timed CPN (Jensen & Kristensen 2009, Jensen 1997), the time is given by a global clock. In addition to their colour, the tokens contain a time value, also called a *time stamp*. When a transition is enabled, it is fired and changes the time stamps of tokens which are deposited in its output places. In these places, the tokens remain *frozen* and can not be used to enable other transitions until the current model time (given by the global clock) is smaller than their time stamps. As soon as the time stamp of the tokens is greater than or equal to the current time model, these tokens can enable other transitions which are instantly fired. In other words, the time stamp describes the *earliest* model time from which a token can be used.

The following drawbacks can be cited: the low readability (which can be put into perspective by using hierarchical CPN) and the difficulty in verifying a Petri net model. This last drawback can be offset by using a verification of CPN properties. This properties verification is supported by the *state space method*. The basic idea underlying the state space method is to compute all reachable states and state changes of the CPN model and to represent them as a directed graph, where nodes represent states and arcs represent occurring events. From a constructed state space, it is possible to answer a large set of questions concerning the behaviour of the system, such as absence of deadlocks, a possibility to be able to reach a given state. We have used this formal verification of a CPN to study and validate some specific safety properties of an I&C systems (Pinna et al. 2013), but a Monte-Carlo simulation can be also realized without this type of verification.

In this paper, we propose to integrate the Atwood model into a CPN model of an I&C system. The obtained model allows the assessment of the CCF impact on the system dependability. In order to realize this assessment, in the next section, we introduce a case study coming from a nuclear power plant.

3 CASE-STUDY PRESENTATION AND ITS MODELLING

The studied system is a digital protection system. It is a part of the defence in depth of a nuclear power plant.

3.1 *System architecture*

This protection I&C system contains four divisions, which are strictly identical, see Figure 1. These divisions are physically separated. Each division is composed of five "Acquisition & Processing Units" (APU). The APU 0, 1 and 2 represent the subsystem A (SSA). The APU 3 and 4 represent the subsystem B (SSB). The gathering of APU into subsystems takes into account the allocation of control functions of the I&C system. For the same control function, there is one implementation in an APU of SSA and one implementation in an APU of SSB with different inputs and treatment and their outputs must be identical in the normal operating mode.

Different electronic boards *C1* et *C2* are included in each APU. Each APU contains one *C1* board. The APU 0 and 1 contain four *C2* boards, and the APU 3, 4 and 5 contain three *C2* boards. These electronic boards are used for reception, treatment and emission of signals.

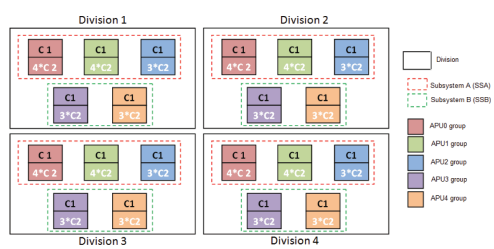


Figure 1. Architecture of the case study I&C system for a nuclear power plant.

A second type of partition is defined: the *groups of APU* (GAPU). A group of APU contains all of the APU i (i [0,4]) of the four divisions.

3.2 *Modelling assumptions*

3.2.1 *Assumptions for the electronic boards modelling*

A constant failure rate is considered for boards.

The *C2* boards of an APU are considered as a series system.

The board failures can be detected by a set of self-tests. When a failure is detected by a self-test (SA), the detection time is considered null. When a failure is not detected by a self-test (NSA), then it is detected offline during a periodical-test. For a given division, these periodical-tests take place at each 18 months. So every quarter of this period, a division is tested during the periodic tests. After the periodic tests, the failed boards are repaired.

According to the supplier of electronic boards, their coverage rate of self-tests (t_c) is 100%, but this value seems to be ambitious. We add to the model the non-detected failures by self-test (NSA failures) in order to take into account the errors due to operation (different parameters or installation of boards from the nominal conditions specified by the provider). Thus the coverage rate is reduced at 85%. The global failure rate of the boards remains identical ($\lambda_{IND} = \lambda_{SA} + \lambda_{NSA}$). The rates of detected failures (λ_{SA}) and non-detected failures(λ_{NSA}) are adjusted by the following equations: $\lambda_{SA} = t_c \cdot \lambda_{IND}$ and $\lambda_{NSA} = (1 - t_c) \cdot \lambda_{IND}$.

3.2.2 *Assumptions for global system modelling*

The hazardous event is represented by the failure of the protection I&C system.

The occurrence of this hazardous event is based on the voting logic of the APU:

- An APU fails when a card *C*1 or *C*2 is failed.
- A group of APU (GAPU) fails when 3 out of 4 APU is failed (3oo4).
- A subsystem (SSA or SSB) fails when a GAPU is failed.
- The I&C system fails when a subsystem is failed (1oo2) *or* when two subsystems are failed (2oo2).

We assume that the mission time of the protection I&C system is ten years. Indeed, this system is retrofitted only during the decennial maintenance operations of the nuclear plant. System unavailability can occur during the ten years. The system changes from unavailable to available state without being as good as new as it is not fully retrofitted on this period of ten years. Some electronic boards may be still failed when the system becomes available.

3.3 *CPN modelling*

We propose to use a modular approach for system modelling. Thus, the CPN model (shown in Fig. 2) is composed by the following modules:

- CCF generating (blue box)
- System representation (red box)
- State system description (green box).

3.3.1 *CCF generating using Atwood model*

Non-lethal CCF are modelled by the CPN sub-net shown in Figure 3. It corresponds to the substitution transition *DCC_non_letale* of the Figure 2. The place *Nb-carte* contains the number of electronic boards *N* in the system. The firing of transition *Save* maintains the number of electronic boards *N* of the system in the place *SNb_carte* and set *N* tokens in the place nb_carteu. The transition *proba* is fired N times. Thefunction *defdcc*() draws a random value using an uniform distribution law of probabilities in the interval [0, 1]. If the

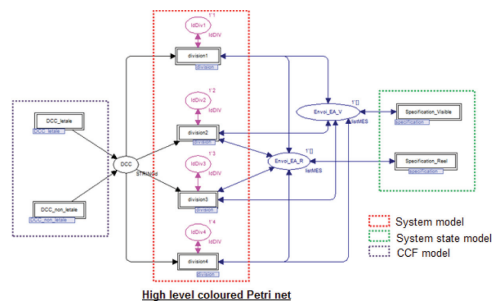


Figure 2. High level coloured Petri net of the I&C system.

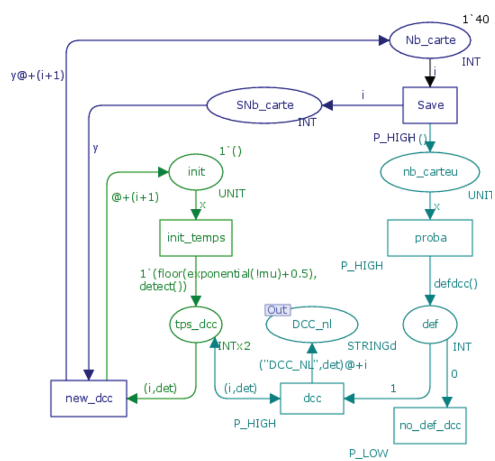


Figure 3. CPN sub-net modelling the *non-lethal CCF*.

drawn value is lower than conditional probability p the considered board will be shock sensitive. The returned value will be 1, otherwise 0.

The firing of *init_temps* transition allows to determine the occurrence time of the non-lethal shock using the function *floor*(*exponential*(*!mu*)+0.5) and, in the same time, to specify if it is detected or not by a self-test. This is done using the function *detect*(). This function draws a random value using an uniform distribution law of probabilities in the interval [0, 1]. If the value is lower than coverage rate of self-tests (t_c), the non-lethal shock is detected. In this case the function return the value *1*, otherwise *0*. The firing of the transition *dcc* assigns the occurrence time of CCF and the variable of failure detection at each token of the system that is shock sensitive. The transition *no_def_dcc* allows to remove the tokens representing boards that are not shock sensitive. The transition *new_dcc* allows to generate the next occurrence time of the non-lethal shock and to redefine the number of boards, which are shock sensitive.

Lethal CCF are modelled by the CPN sub-net shown in Figure 4. It corresponds to the substitution transition *DCC_letale* of the Figure 2. The firing of the transition *gene_dcc_l* allows to determine the occurrence time of the lethal shock using the function *floor*(*exponential*(*!omega*)+0.5). A lethal CCF affects all the components (electronic boards) of the system and is always detected online. Thus, there are issued N temporized tokens with a color ph('DCC-NL',1) (1 for detection). The next occurrence time for a new lethal CCF is calculated since the previous is realized.

The Atwood model introduces three parameters to estimate: p, μ and ω. Two approaches, analytic or by simulation, can be used for doing their estimation.

Analytical approach for estimation of CCF model parameters. From the expressions of α, β_{letal} and λ_{TOT}, we obtain the following equations system:

$$\left(1-\alpha\sum_{k=1}^{N}p^k(1-p)^{N-k}\right)\mu+\alpha\omega=\alpha\lambda_{IND} \tag{5}$$

$$\left(-\beta\sum_{k=1}^{N}p^k(1-p)^{N-k}\right)\mu+(1-\beta)\omega=\beta\lambda_{IND} \tag{6}$$

The value of conditional probability p is considered known (e.g. at classical default values 0.2, 0.33 or 0.5). The independent failure rate for an electronic board is $\lambda_{IND}=2.35\,10^{-6}h^{-1}$. The equations (5) and (6) give the values of occurrence frequencies of non-lethal shocks μ and of lethal shocks ω. The obtained results are presented in Table 1.

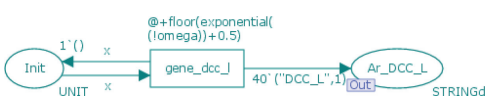


Figure 4. CPN sub-net modelling the *lethal CCF*.

Monte-Carlo simulation approach for estimation of CCF model parameters. We introduce the ratio between the occurrence rate of independent failures λ_{IND} and the total failure rate λ_{TOT} of a component (an electronic board):

$$\gamma=\frac{\lambda_{IND}}{\lambda_{TOT}}=1-\alpha\cdot\sum_{k=1}^{N}C_{N-1}^{k-1}p^k\cdot(1-p)^{N-k}-\beta_{letal} \tag{7}$$

$$\gamma=1-\alpha\cdot p-\beta_{letal} \tag{8}$$

We introduce also E_i that represents the number of independent failure events realized in 10 years of simulations. This number is obtained by simulating only the independent failures in Petri net model and their occurrences are counted. It allows to obtain from the equation 9, the average independent failure rate λ_{IND} for a board in the system. The different rates can be estimated from the following equations:

$$\lambda_{IND}=\frac{E_i}{10ans*N} \tag{9}$$

$$\mu=\frac{\alpha\cdot\lambda_{IND}}{\gamma} \tag{10}$$

$$\omega=\frac{\beta_{letal}\cdot\lambda_{IND}}{\gamma} \tag{11}$$

The expected value of E_i is equal to 8.28 and the value obtained for independent failures rate is: $\lambda_{IND}=2{,}36E^{-6}h^{-1}$. The results obtained by applying this approach are presented in Table 2.

The occurrence frequencies μ and ω for non-lethal and lethal shocks obtained by applying these approaches (analytical and simulation approaches) are almost identical. This result allows, firstly, to validate the proposed CPN modelling approach for the Atwood shock model. Secondly, the Monte-Carlo simulation approach could be used to revisit

Table 1. The values of occurrence frequencies μ and ω for non-lethal and lethal shocks as a function of p using analytical approach.

p	μ in h^{-1}	ω in h^{-1}
0.2	$9.52\,10^{-7}$	$1.18\,10^{-8}$
0.33	$9.52\,10^{-7}$	$1.18\,10^{-8}$
0.5	$9.52\,10^{-7}$	$1.18\,10^{-8}$

Table 2. The values of occurrence frequencies μ and ω for non-lethal and lethal shocks as a function of p using Monte-Carlo simulation approach.

p	γ	λ_{TOT}	μ	ω
0.2	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$
0.33	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$
0.5	0.995	$2.37\ 10^{-6}$	$9.62\ 10^{-7}$	$1.18\ 10^{-8}$

some assumptions supporting the Binomial Failure Rate model underlying the Atwood shock model, especially in the case of digital I&C systems including software.

Introduction of asymmetry in CCF propagation. For a realistic modelling of Common Causes Failures (CCF) and of their impact on the systems dependability, it is interesting to assume that some non-lethal shocks predominantly affect some k components among the all N components of the system, with $1 \leq k \leq N$ (e.g. only some types of electronic boards belonging to the I&C systems). We propose to modify the generation of non-lethal CCF for simulating the asymmetries in their propagation, in other words considering "oriented" CCF.

In a system with N components, a non-lethal shock affects the boards with a conditional probability p. The expected number of affected components is $N * p$. The set of N components can be divided in two sub-sets A (SSA) and B (SSB), containing respectively a et b components, such as $a + b = N$. Let be x (respectively y) the probability that a component of SSA (respectively SSB) is affected by a non-lethal shock. From reasoning on mathematical expectation, we have:

$$ax + by = Np \tag{12}$$

To determine x and y we choose how a CCF will affect the SSA (p_1) and SSB (p_2), such as $p_1 + p_2 = 1$. Thus, we obtain:

$$x = \frac{N \cdot p \cdot p_1}{a} \tag{13}$$

$$y = \frac{N \cdot p \cdot p_2}{b} \tag{14}$$

The solutions of these equations, x and y, are the probabilities of non-lethal shock for the CPN tokens that represent respectively the SSA and SSB components.

3.3.2 *System modelling by CPN*

The hierarchical and modular aspects of Coloured Petri nets are exploited to develop the CPN model of I&C system. Thus, each of its divisions is modelled by means of a substitution transition at the high level of the system, in the Figure 2. A division includes five APU, each of them includes the correct number of electronic boards C1 and C2. The CCF are transmitted to the APU and to the boards by means of CPN places (socket places). The state of an APU is determined by the state of its boards (available or unavailable). Once the state of a board changes, the new state of APU is sent to the specification that determines the state of the whole I&C system.

An electronic board represented in the Figure 5 has three possible tangibles states: operational ("Marche" place), failed and non-detected ("detection" place) and in reparation ("reparation" place). When the board is operational, it can change its state if one of the following four events occurs:

- independent failure detected online by a self-test (modelled by the purple Petri sub-net on the right side of the model)
- independent failure detected offline in periodical-tests (modelled by the purple sub-Petri net on the left side of the model)
- non-lethal CCF detected online and lethal CCF (modelled by the tokens received by "AR_DCC" place from the CCF models of the Figures 3 and 4)
- non-lethal CCF detected offline in periodical-tests (modelled also by the tokens received by "AR_DCC" place from the CCF model of the Fig. 3).

If the failures are detected during the periodic tests, the "rep" transition is fired and the board changes its state to the reparation state. If the failures are detected online, the board changes its state immediately from the operational to the repair state. The repair time is calculated using the function *floor*(*exponential*(1/!MTTR) + 1.0). As soon as the board is repaired, its state changes immediately to the operational state. The next occurrence times of the independent failures detected onlineand offline are also calculated.

This CPN model of electronic boards are generic. For all boards, only the numerical values of parameters (failure and repair rates) are different.

3.3.3 *System state modelling by CPN*

Using the information about the state (available/unavailable) of the APU i ($i \in [0,4]$ of the division j ($j \in [1,4]$)), it is possible to determine the state of the I&C system during the Monte-Carlo simulation using the CPN of Figure 6. The system state is represented by a token whose colour is composed of five booleans, each of them representing the state of one APU. The different configurations on the transitions' guards allow to define the conditions of availability/unavailability of the system.

The entire CPN model obtained for the I&C system has 685 transitions and 504 places. Even if the

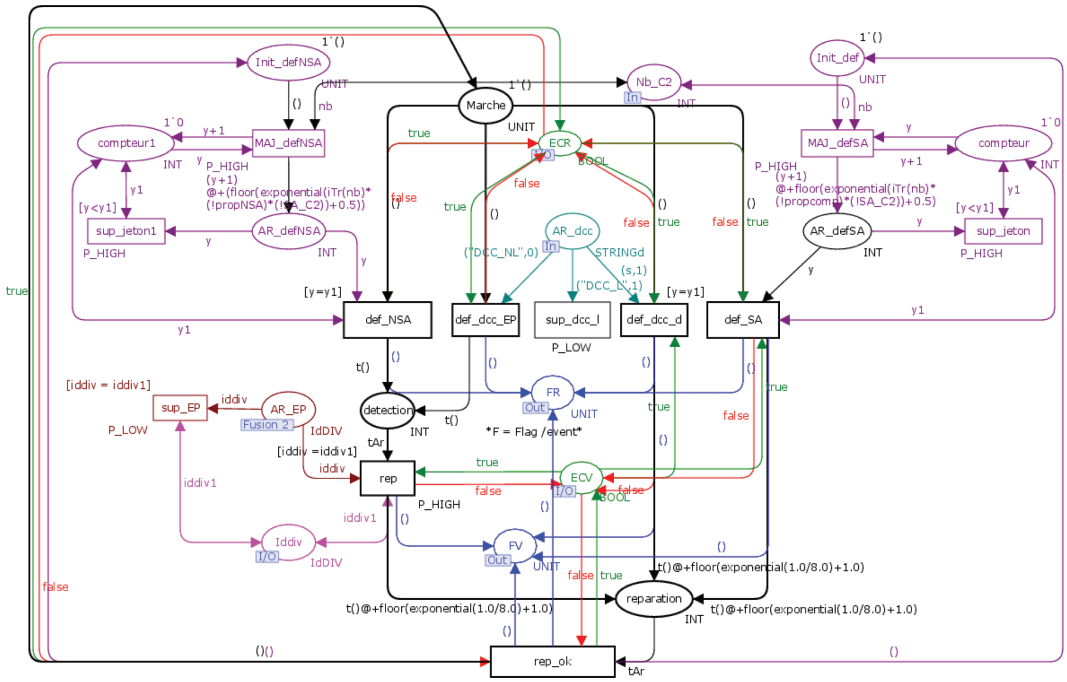


Figure 5. CPN sub-net of an *electronic board*.

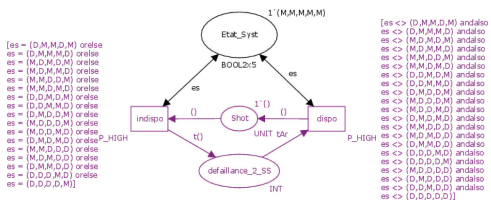


Figure 6. CPN sub-net to determine the state of the whole I&C system (available or unavailable).

model size is large enough, the use of hierarchy and colours concepts have resulted in a modular and readable model obtained through the instantiation of generic templates. We can note, that an equivalent classical Petri net model for the same I&C system should have several thousands places and transitions. The obtained CPN model allows the probabilistic dependability assessment of the system.

4 PROBABILISTIC DEPENDABILITY ASSESSMENT

4.1 *Probability of failure on demand*

Since the I&C system is a protection system (its mission is to protect the nuclear power plant), we are interested to asses only the *Probability of Failure on Demand* (PFD). This is in accordance with the IEC-61508 (2010) standard and its declination IEC-61513 (2011) that address the functional safety of digital systems. We define two kinds of PFD:

- the *real* PFD that represents the I&C system unavailability starting with the moment where the electronic boards are not anymore in their operational state;
- the *visible* PFD that represents the system unavailability only starting with the moment where the boards failure is detected. The time between the occurrence of non-detected failures and their detection by a periodical-test is not considered.

The definition of the two kinds of PFD allows to estimate the difference between the real state of the system and the state observed by plant operators during operation.

The PFD is estimate using Monte-Carlo simulation by the following equation:

$$\mathrm{PFD} = \frac{\text{System unavailability time}}{\text{Mission time}} \tag{15}$$

The results presented in the Table 3 are obtained after 10,000 histories during 10 years. The 95%

Table 3. Real and visible PFD of the protection I&C system for different values of p.

Indicators	p	Average
Real PFD	0.2	$2.5\ 10^{-5}$
Visible PFD	0.2	$<10^{-6}$
Real PFD	0.33	$2.73\ 10^{-4}$
Visible PFD	0.33	$1.0\ 10^{-6}$
Real PFD	0.5	$5.4\ 10^{-4}$
Visible PFD	0.5	$4.0\ 10^{-6}$

Table 4. Combinations of failed boards leading to the system downtime depending on p_1 and p_2.

CCF orientation			
p_1 SSA	0.1	0.2	0.3
p_2 SSB	0.9	0.8	0.7
Only CCF	9404	9723	9787
Indep. SA failures	3	0	1
Indep. NA failures	21	9	9
Indep. SA and NSA	77	46	42
CCF & indep. SA failures	8	6	1
CCF & indep. NSA failures	487	216	160
MTTFF (in h)	49586	28921	22056

confidence interval for all of the results presented in Table 3 is also estimated and its value is $<10^{-6}$.

According to IEC-61513 (2011) "there is not an equivalent scheme to the reliability/risk reduction SIL levels proposed in IEC 61508 in common use in the nuclear sector". Consequently, we do not associate a SIL level for the system under study.

If the conditional probability of failure of one component in a non-lethal shock p increases, there will be more components affected by a shock and the PFD also increases. The difference between the real PFD and the visible PFD is about 10 to 100.

4.2 *Influence of the oriented non-lethal CCF*

To asses the impact of asymmetric propagation of non-lethal CCF, we consider the orientation of CCF on the two sub-systems SSA and SSB, using the approach presented in section 3.3.1.

The conditional probability of failure of one component in a non-lethal shock is $p = 0.2$. The frequency of non-lethal shocks is arbitrary fixed at one shock per year, i.e. $\mu = 1.1410^{-1}h^{-1}$. The lethal shocks are not represented. 10,000 trajectories during 10 years are also realized and the occurrence of system failure ends the trajectory simulation. Table 4 shows the results. The sum of failures' combinations (columns) is equal with the total number of histories (10,000) for a fixed CCF orientation.

We can observe that the more a sub-system is preferred (according to p_1 and p_2), the more the MTTFF increases. The logic vote explains this phenomenon. We observe also that independent failures combinations without CCF rarely leads to system failure, due to the high level of redundancy. Independent failures detected offline lead more easily to system failure than the ones detected online. This aspect can be improved by increasing the frequency of periodic tests or the coverage rate of self-tests.

5 CONCLUSIONS

The coloured Petri nets allow to represent the digital I&C systems and to assess the dependability indicators considering CCF. The shock Atwood model has been transposed in Petri net. It allows to take in account the independent failures, the lethal CCF,but also the non-lethal CCF. An extension of this model was proposed to represent the asymmetric propagation of non-lethal CCF on privileged axes. This allows to relax the assumption of the random repartition of non-lethal shocks on the all components and to represent the effects of diversity. The proposed approach has been applied to a representative case of I&C system of a nuclear power plant.

The extremely low volume of operating experience related to the protection I&C systems makes it difficult to estimate the α factors representing the conditional probability of failures on demand of the k components in a group of N components when a CCF occurs. This CPN model could be used to simulate operating experience for obtaining more data, which make a more accurate estimation of these factors.

Another interesting axis concerns the estimation of the three parameters of the Atwood model. The proposed Monte-Carlo simulation approach for the estimation of these parameters has been validated by an analytical approach. This Monte-Carlo simulation approach could be used to revisit the assumptions supporting the Binomial Failure Rate model underlying the Atwood model.

REFERENCES

Atwood, C.L. (1980). *Estimating common cause failure rates for pumps in nuclear reactors.* Ph. D. thesis, California.

Bricman-Rejc, Z., M. Cepin, & A. Sitdikova (2013). Estimating common-cause failures parameters within power system reliability analysis. In *Annual Conference of the European Safety and Reliability Association, ESREL 2013*, Amsterdam, pp. 2841–2846.

IEC-61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety-related,* Volume 1–7.

IEC-61513 (2011). *Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems.*

Jensen, K. (1997). *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use (Volume 1),* Volume 1. Springer Verlag.

Jensen, K. & L. Kristensen (2009). *Coloured Petri nets: modeling and validation of concurrent systems*. Springer-Verlag New York Inc.

Lilleheier, T. (2008). Analysis of common cause failures in complex safety instrumented systems.

Pinna, B., G. Babykina, N. Brînzei, & J.-F. Pétin (2013). Deterministic and stochastic dependability analysis of industrial systems using Coloured Petri Nets approach. In *Annual Conference of the European Safety and Reliability Association, ESREL 2013*, Amsterdam, pp. 2969–2977.

Signoret, J.-P., Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, & P. Thomas (2013). Make your petri nets understandable: Reliability block diagrams driven petri nets. *Reliability Engineering and System Safety 113*, 61–75.

US-NRC (1987). NUREG/CR-4780. *Procedures for treating common-cause failures in safety and reliability studies,* Volume 1 and 2. Washington, DC: US Nuclear Regulatory Commission.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, *ISBN 978-1-138-02681-0*

Propagation of aleatory and epistemic uncertainties in quantification of systems failure probabilities or safety margins

M. Marquès
CEA, DEN, DER, Saint-Paul-lez-Durance, France

ABSTRACT: Epistemic uncertainties may be taken into account in the probabilistic assessment of complex systems, by a Second Order Probabilistic (SOP) analysis, based on a separate propagation of the aleatory and epistemic uncertainties in two nested-loops. This SOP analysis enables to obtain a confidence interval on the system failure probability or on the safety margin, which takes into account the lack of knowledge. In this approach, a probabilistic description may characterize both random uncertainty and epistemic uncertainty. However, if the probabilistic framework has solid mathematical bases for modeling and processing aleatory uncertainties, its use shows limits in the case of epistemic uncertainty and it seems more appropriate to rely on an adapted framework for representing the imprecisions on the failure probabilities or on the safety margins. Among several alternative modeling frameworks, two approaches: interval analysis and Dempster-Shafer Theory of Evidence (DSTE) have been tested and compared on an example of risk analysis of complex systems. Additionally, thinking has been initiated on the idea to jointly use the DSTE and the probabilistic analysis in order to deal separately with the aleatory and the epistemic uncertainties in the "Best-Estimate Plus Uncertainty" (BEPU) approach. A range of cumulative functions will result from this separate treatment, for the quantile $R_{95,95}$ of the classical BEPU approach. Through this proposed methodology, uncertainties due to a lack of knowledge, and in particular modeling uncertainties, will be coherently integrated into an Extended BEPU approach. However, this proposal may pose some problems related to decision making, which are discussed in the paper.

1 INTRODUCTION

The treatment of uncertainties in the analysis of complex system is essential for determining possible ranges on responses of interest such as safety margins or probabilities of exceeding failure criteria. The input uncertainties may be characterized as either aleatory uncertainties, which represent the intrinsic randomness of a phenomenon, irreducible in nature, or epistemic uncertainties, which are reducible uncertainties resulting from a lack of knowledge (Der Kiuregan 2007, Helton 2011, Swiler et al., 2009). For aleatory uncertainties, sufficient data is generally available enabling the definition of input probability distributions and the use of probabilistic methods. By cons, for epistemic uncertainties, data is generally too sparse to enable precise probabilistic descriptions and consequently the uncertainties are often modeled by variation intervals deduced from expert judgment. In this case, the intervals are assimilated to uniform distributions, which enable a probabilistic treatment of epistemic uncertainties. However, several alternative mathematical structures for the representation of epistemic uncertainty, that we will name extra-probabilistic approaches, such as interval analysis, possibility theory, fuzzy set theory or Dempster-Shafer evidence theory, have been developed in the last decades (Demster 1967, Shafer 1976, Zadeh 1978). When both aleatory and epistemic uncertainties are present in the analysis of a complex system, it is often desirable to maintain segregation between these both types of uncertainties. A common approach to quantifying the effects of mixed aleatory and epistemic uncertainties is to perform what is sometimes called a Second-Order Probability (SOP) analysis (Eldred et al., 2011). The idea of SOP is to treat separately the aleatory variables and the epistemic variables and to perform a two-stage Monte Carlo simulation, typically by sampling the epistemic variables on the outer loop, then by sampling the aleatory variables on the inner loop. If the result of the inner loop is an empirical distribution of the response of interest, the SOP process yields a family of distributions. Then relevant statistics, such as mean or percentiles, may be computed based on this ensemble and the intervals obtained on the statistics can be interpreted as possible ranges for the statistics given the epistemic uncertainties. In the SOP analysis, the aleatory variables are treated generally by probabilistic methods and the epistemic variables

may be considered either by probabilistic methods or by extra-probabilistic methods depending on the assumptions taken for these epistemic variables. The objective of this paper is to show the interest of using extra-probabilistic method for the treatment of the epistemic variables within the framework of the quantification of system failure probabilities or safety margins. In Section 2, two extra-probabilistic approaches, interval analysis and Dempster-Shafer theory of evidence, are presented insisting on two points: the decision taking and their interest in expert elicitation. Section 3 presents an example of application of SOP analysis with extra-probabilistic or probabilistic treatment of epistemic variables. Finally in Section 4, a proposal is made to use SOP analysis with extra-probabilistic treatment of epistemic variables within the framework of the called « Best-Estimate Plus Uncertainty » (BEPU) approach for safety analysis.

2 TREATMENT OF EPISTEMIC VARIABLES WITHIN AN EXTRA-PROBABILITIC FRAMEWORK

The probabilistic framework is usually used for modeling aleatory and epistemic uncertainties. However, although it remains the framework for the representation of random uncertainty, it is not considered best able to properly handle the different concepts associated with epistemic uncertainty (Shafer 1976, Fallet-Fidry 2012). Besides the fact that it does not allow to represent incompleteness (in the probabilistic framework, the space of possibilities is exhaustive and therefore all possible hypotheses are identified and defined), its use for the representation of ignorance implies the choice of a single arbitrary probability distribution and the risk is to not represent faithfully the available knowledge and to distort the results of the analysis. The arbitrary choice of a probability distribution to model ignorance is likely to cause errors in the propagation of uncertainties and to provide inaccurate or inconsistent result with regard to the available knowledge, which may have a very significant impact on the assessment results and therefore in the decisions that may arise. It should then not constrain the expression of knowledge to comply with the probabilistic framework but rather to provide a framework to represent, in a more coherent and flexible way, the different types of knowledge. The need for a consistent modeling of epistemic uncertainties is now widely accepted, especially when analyses generate important decisions as is the case for risk analysis (Der Kiuriegan 2007, Helton 2008 and 2011). Bayesian approach may be suitable to express epistemic uncertainty if prior information, subjectively obtained by expert elicitation, may be updated by objective knowledge coming from measurement for instance. But in the case where no additional information is available, extra-probabilistic approach is used to model epistemic uncertainty. This extra-probabilistic framework consists in modeling the epistemic uncertainty around a not well known value by an interval between two bounds containing the true value. This modeling is based on the general concept of imprecise probabilities, which may be defined as an interval of a probability measure between upper and lower bounds:

$$\underline{P} < P < \overline{P} \tag{1}$$

where the range between the bounds represents the uncertainty around the sought true value. The main extra-probabilistic approaches are:

- Interval analysis.
- P-box modeling.
- Possibility theory.
- Dempster-Shafer theory of evidence.

In the following, the principle of interval analysis and Dempster-Shafer theory are reminded.

2.1 *Interval analysis*

In interval analysis, it is assumed that nothing is known about the uncertain input variables except that they lie within certain intervals. The problem of uncertainty propagation then becomes an interval analysis problem: given inputs that are defined within intervals, what is the corresponding interval on the outputs? Although interval analysis is conceptually simple, in practice it may require a prohibitively large number of function evaluations to determine the maximum and minimum values of the response of interest, especially if the relation between the response and the epistemic variables if very nonlinear, if it exhibits discontinuities or if the epistemic variables have strong interactions. It consists in solving two related bound-constrained problems (Eldred et al., 2011):

– minimize $R(s)$
– subject to $s_L \leq s \leq s_U$
– maximize $R(s)$
– subject to $s_L \leq s \leq s_U$

where $R(s)$ is a response of interest and s the vector of epistemic variables.

This optimization problem can be solved using either direct evaluation function of the response (computer code) or by using a surrogate model (polynomial, neural network, Gaussian processes …) approximating the evaluation function and allowing cheaper simulations. In both cases,

two types of approaches are possible to solve this interval analysis: by sampling or by optimization.

2.2 *Dempster-Shafer Theory of Evidence (DSTE)*

In the DSTE, epistemic variables are represented by one or more intervals (called focal intervals) as shown in Figure 1. A belief mass m_i is associated to each focal interval i, indicating the likelihood that the variable belongs to the corresponding uncertain interval. The sum of the belief masses of all focal intervals must be equal to 1.

From this definition of mass belief, are derived belief and plausibility functions respectively noted, *Bel* and *Pl*. The plausibility (respectively the belief) may be interpreted as the upper bound (respectively the lower bound) of the probability induced by a family of probability distribution. Thus, the interval $[Bel(B),\ Pl(B)]$ may be seen as an interval surrounding a not well known probability $P(B)$:

$$Bel(B) \leq P(B) \leq Pl(B) \tag{2}$$

The difference between $Pl(B)$ and $Bel(B)$ measures the ignorance relative to B.

2.2.1 *Propagation of epistemic uncertainties*

All intervals of all epistemic variables are then propagated in order to calculate the focal intervals of the response of interest and deduce the belief and plausibility functions of the response, which are the upper and lower bounds of its probability function. This interval propagation can be very time consuming as all combinations of intervals must be evaluated. As for interval analysis, it is also possible to implement optimization methods (local or global) to find the limits of each interval of the response.

2.2.2 *Decision making by pignistic transformation*

Decision making from the belief and plausibility functions of the response of interest is a problem difficult to solve in the DSTE approach to make it robust to the process of uncertainty treatment (Dubois, 2011). Several transformations have been proposed to transfer the belief model toward the probabilistic model. We opt for "the pignistic transformation" introduced by Smets (2005).

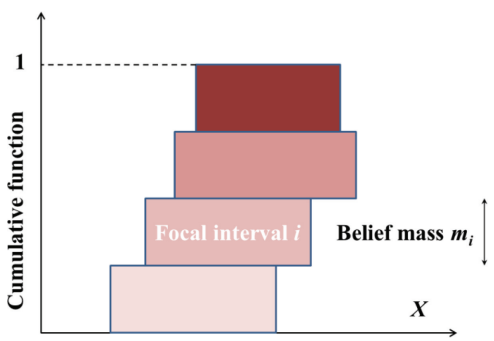


Figure 1. Modeling epistemic variable by DSTE.

2.2.3 *Interest of DSTE for modeling expert opinion*

As stated above, epistemic uncertainties correspond to a lack of knowledge and their modeling can only rely on expert judgment. The DSTE approach consisting in modeling epistemic variables by focal intervals is interesting because it allows to take into account the opinion of one or more experts. The expert must provide at least an interval of variation and in this case, the epistemic variable will be defined by a single focal interval, but he can also provide the median of the variable (two focal intervals in this case) and possibly other quantiles. This approach is also interesting because it allows the aggregation of opinions from several experts (dissenting expert opinions). Different types of aggregation (weighting, envelop…) are possible (Ferson 2003).

3 APPLICATION EXAMPLE TO THE SAFETY ANALYSIS OF AN INDUSTRIAL COMPONENT

Interval analysis and DSTE, for the modeling of epistemic variables, have been compared with classical probabilistic approach on a realistic example concerning the failure risk of an industrial component during an accidental loading.

3.1 *Description of the example*

The purpose of the analysis is to evaluate the failure probability of a component when it is subject to a severe situation. The failure occurs when the loading L applied to the component exceed the strength S of its composing materials. L and S are estimated by a chain of complex thermal-hydraulics and mechanics calculations. In the deterministic assessment, a margin factor (MF), which is equal to the ratio S/L, must exceed a safety factor equal to *1.2*. The deterministic rule to be complied with is thus: $MF > 1.2$. The failure probability is therefore defined as:

$$Pf = P(MF \leq 1{,}2) \tag{3}$$

Segregation of uncertain parameters into two groups (epistemic and aleatory uncertainties) has given:

– 4 aleatory variables: strength of material (modeled by a 3 parameters Weibull distribution, each

parameter being a function of the temperature), depth of an hypothetical flaw (2 parameters Weibull distribution), ratio between depth and length of the hypothetical flaw and effect of irradiation (Gaussian distributions).
– 8 epistemic variables: 6 coefficients of the functions of the temperature for the parameters of the strength distribution (modeled in the probabilistic approach by 6 correlated Gaussian distributions) and 2 parameters of the Weibull distribution of flaw depth (modeled in the probabilistic approach by independent Gaussian distributions).

The failure probability *Pf* is evaluated by Monte Carlo simulation in the inner loop of the SOP analysis and the range of variation of *Pf* is obtained by interval analysis or DSTE (see Figure 2). For the present application, a surrogate model giving accurate estimations of L and S has been used instead of the complex calculation chain.

3.2 *Results of interval analysis*

Two different hypotheses have been taken for the interval of the epistemic variables, based on their previous probabilistic definition (with μ and σ respectively the mean and the standard deviation of the variable):

1. 95% intervals: $[\mu - 1.96\ \sigma, \mu + 1.96\ \sigma]$
2. 99,8% intervals: $[\mu - 3\ \sigma, \mu + 3\ \sigma]$

The bounds of the failure probability have been determined by sampling (1000 simulations) or by optimization in using the global optimization algorithm EGO of DAKOTA software (DAKOTA 2011). Table 1 gives in both case and for the two hypotheses on the intervals, the upper bounds of the failure probability P_f (probabilities are multiplied by 100 in the Table). These values are compared to an analytical solution obtained with the surrogate model. By optimization with EGO algorithm, 10 simulations are sufficient to obtain a value very close to this global maximum in dimension 8. With 1000 simulations, sampling underestimates the upper bound of P_f by about 12% in both cases.

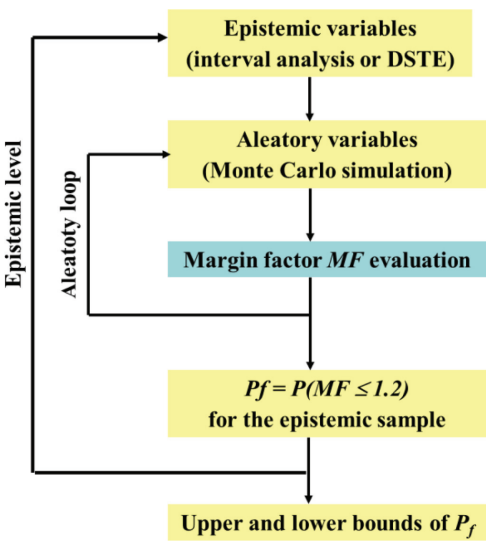


Figure 2. Scheme of the SOP analysis on the example.

3.3 *Results of DSTE*

By way of illustration, different modeling of the epistemic variables have been considered:

A. Each epistemic variable is represented by its median E_{med} and a range $[E_{min}, E_{max}]$.

We have supposed that the true and unknown distributions of the epistemic variables are Gaussian. The results will depend in the capacity of the expert to give quantiles and interval close to the actual values. We have supposed first that the expert gives the true median and the true 95% interval for the epistemic variables (Figure 3). Belief and plausibility functions of the response *Pf* are described here by 256 focal intervals; indeed, the 8 epistemic variables are each described by two intervals, that means 2^8 (= 256) hypercubes to be evaluated in the space of epistemic variables. For each hypercube, the evaluation of the minimum and maximum values of the response P_f provides the corresponding

Table 1. Upper bounds of failure probability P_f (multiplied by 100) obtained by interval analysis.

	Analytical	Sampling	Optimization
95% interval	6.91	6.08	6.89
99.8% interval	9.17	7.88	9.08

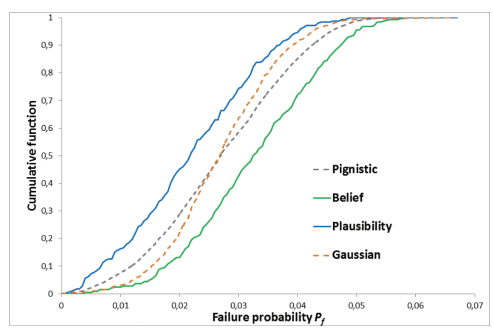


Figure 3. DSTE analysis. Case: true medians and 95% intervals. Belief, plausibility and pignistic function of the response P_f.

focal range. Logically, one finds that the pignistic function and Gaussian reference are equal at the bounds of the 95% interval and at the median of P_f, since these values are correctly evaluated by the expert. By cons, the lack of knowledge outside of these quantiles, results in an overestimation of P_f by the pignistic function beyond the median and an underestimation below.

We have now considered that the expert gives the thrue 95% interval but a median shifted in an unfavorable direction. Accordingly (Figure 4), we see that the belief and plausibility functions as well as the pignistic function deviate significantly from the Gaussian reference in an unfavorable direction, resulting in an overestimation of the failure probability.

B. Each epistemic variable is represented by two quantile ($E_{20\%}$ and $E_{80\%}$) and a range [E_{min}, E_{max}].

In this case, each epistemic variable is described by three intervals with belief masses equal to 20%, 60% and 20%. The response P_f is described here by 3^8 (= 6561) focal intervals. It is seen in Figure 5, that the pignistic function becomes very close to

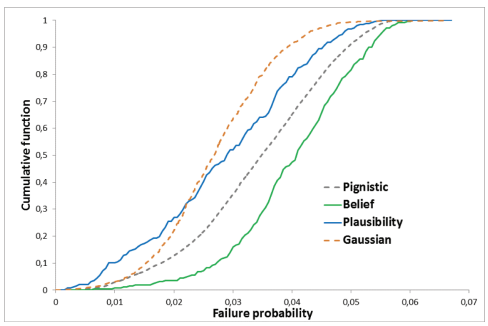


Figure 4. DSTE analysis. Case: true 95% intervals and median unfavorably shifted. Belief, plausibility and pignistic function of the response P_f.

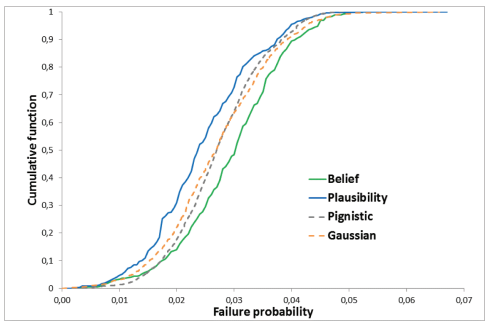


Figure 5. DSTE analysis. Case: true 95% intervals and 20% and 80% quantiles. Belief, plausibility and pignistic function of the response P_f.

the Gaussian reference and the gap between belief functions and plausibility function is tighter. We notice that a description of the epistemic variables by three intervals correctly evaluated enables to obtain results very close to a description by a probability density function.

Table 2 summarizes the results obtained on the upper bound of the failure probability P_f (the upper bound considered is the 95% quantile, except for the interval analysis where it is the upper bound of the interval). The various methods are listed from top to bottom on an increased level of knowledge:

- Case without consideration of epistemic uncertainties: the total lack of knowledge about the epistemic uncertainty variables is expressed here by a single result obtained for the nominal values of the epistemic variables.
- Conservative calculation: epistemic variables are equal to their most unfavorable value.
- Interval analysis: the upper bound obtained by optimization is selected.
- DSTE with different descriptions of epistemic variables: 95% quantile of P_f are evaluated on the pignistic function and on the belief function (pessimistic assumption, between brackets in Table 2).
- SOP analysis: epistemic variable modeled by probability function and 95% quantile of P_f taken on the empirical distribution of the response.

We notice that:

- Interval analysis gives the most penalizing result. The fact that the value obtained is greater than the conservative result indicates that there is a combination of epistemic variable more penalizing that the choice a priori conservative.
- DSTE approach gives results less penalizing even if the 95% quantile is taken on the belief function and not on the pignistic function.

Table 2. Upper bound of failure probability (multiplied by 100) depending on the level of knowledge.

	95% intervals	99.8% intervals
No epistemic uncertainty	2.7	
Conservative calculation	5.5	7.0
Interval analysis	6.9	9.1
DSTE true medians & intervals	4.6 (5)	5.6
DSTE true intervals & favorably shifted medians	4.0	5.0
DSTE true intervals & unfavorably shifted medians	5.2 (5.6)	6.2
DSTE true intervals & 20% and 80% quantiles	4.1 (4.5)	4.3
SOP	4.2	

– DSTE results, which depend on the description of the epistemic variables by the expert, give the upper limit of the results of the SOP analysis.

These results show the interest of DSTE, which enables to take into account the lack of knowledge on certain variables without being as conservative as interval analysis and without requiring a complet probabilistic description of the epistemic variables. In the context of risk analysis of complex systems, we recommend using DSTE for modeling and propagating of epistemic uncertainty in addition to the probabilistic approach which, in turn, treat the random uncertainties.

4 PARTICULAR CONSIDERATION OF EPISTEMIC VARIABLES WITHIN THE FRAMEWORK OF THE BEPU APPROACH

In this section, we will use this extra-probabilistic formalism for taking into account the epistemic uncertainties in the BEPU approach

4.1 *Principle of the BEPU analysis*

The Best Estimate Plus Uncertainties (BEPU) analysis is recommended by IAEA in addition or alternatively to the deterministic approach in the safety analysis of nuclear components and systems (IAEA 2009). The aim of the BEPU analysis is to determine a quantile of an output measure of interest (noted R in the following) with a certain level of confidence (usually the 95% quantile obtained with a 95% confidence, denoted $R_{95,95}$) and to verify that this quantile is below an acceptable limit (acceptance criteria). In order to obtain this quantile, the uncertainty space of input parameters is sampled at random according to their combined probability distribution and a code calculation is performed for each sampled set of parameters. The number of code calculations is determined by the requirement to estimate a tolerance and confidence interval for the quantity of interest. Wilks' formula (Wilks 1941) (or Wald' formula (Wald 1943) when several criteria must be respected simultaneously) is used to determine the number of calculations to obtain the uncertainty bands and the associated quantile with a given confidence level. In classical BEPU analysis, there is no separation between the aleatory variables and the epistemic variables; the epistemic variables, which are often model uncertainties, are generally modeled by uniform probability distributions within intervals provided by expert opinion and propagated in the same way that the aleatory variables by Monte Carlo simulation.

4.2 *Proposal for a separate treatment of epistemic variables in BEPU approach*

We here propose to perform a separate treatment of epistemic and random variables identical to that presented previously in the context of the evaluation of failure probability. This separate processing, through an interval analysis or a DSTE approach will result in, an interval of the quantile $R_{95,95}$ in the case of the interval analysis or two envelops (upper and lower) of its cumulative function in the case of the DSTE. Unlike conventional BEPU analysis where the method consists in comparing the quantile $R_{95,95}$ to an acceptance criteria, we will have here to compare an interval to this acceptance criteria. If the criteria is outside the interval, there will be no difficulty in deciding whether the criteria is met or not; by cons if the acceptance threshold is within the interval, there will be a problem of decision making. One solution to this problem is to try to reduce the uncertainty of the epistemic variables in order to reduce the interval on the response of interest.

4.2.1 *Reduction of epistemic uncertainty*

Reducing the epistemic uncertainty on the response of interest R requires identifying the contributors to this uncertainty. In other words, it is to identify among the input epistemic variables, those whose uncertainty contributes most to the epistemic uncertainty of R. In the case of the two levels analysis proposed in this study, a solution is to perform a global sensitivity analysis of the response uncertainty to the input epistemic uncertainties. Conventionally, an analysis based on the decomposition of the variance of the response is used: that means, calculate the standard regression coefficients in the case of a fairly linear relationship between the inputs epistemic variables and the response or Sobol indices in the general case (Saltelli et al., 2000). Then, the objective will be to reduce the uncertainty of the epistemic variable, which is the largest contributor to the response variance. If the uncertainty of this epistemic variable has been already minimized, the second largest contributor will be concerned by the reduction, etc.

4.2.2 *Decision taking*

Once uncertainty on the response of interest has been reduced and/or shifted at maximum with regard to the available knowledge, two situations are possible: either the uncertainty is small enough to make a decision (i.e. the acceptance criteria is now outside the interval of uncertainty) or the residual uncertainty does not enable easily to make a decision. If the first case does not pose a problem, in the second case the analyst has the

choice between one of two following alternatives (Fallet-Fidry 2012):

1. The analyst is taking no chances and considers that in the present state of available knowledge, the constraint to be satisfied is not met.
2. The analyst decides to interpret the uncertainty in the response of interest according to its risk aversion and then makes a decision to accept or reject.

In the presence of uncertain results, three main behaviors of the analyst for decision making may be distinguished, which depend mainly on the measure on which rely the decision making (Ramasso 2008):

– Pessimistic behavior: the analyst bases its decision on the choice of the belief measure (*Bel*) because it corresponds to the minimum value of belief that he is certain to obtain. This behavior is also called conservatism.
– Optimistic behavior: the analyst relies on the choice of the plausibility measure (*Pl*) because it corresponds to the maximum value that could be been reached if further information reduced the uncertainty.
– Rational behavior: the analyst transforms the distribution of masses in a distribution of probabilities in order to maximize expected utility (i.e. pignistic transformation).

We propose to integrate into an Extended BEPU approach the additional dimension of the inclusion of epistemic variables: that will result, within the framework of DSTE, by obtaining a range of cumulative functions of the 95% quantile $R_{95,95}$ of classic BEPU approach. The decision will therefore be based on:

1. The choice of a confidence level *N%* on the part of uncertainty due to lack of knowledge: we will take, for example, the median (reasonable approach) or the 95% quantile (pessimistic approach); then we will determine the quantile $R_{95,95,N}$, with $N = 50\%$ or 95% following the chosen approach.
2. The comparison between the acceptance criteria and the interval obtained by DSTE for the quantile $R_{95,95,N}$,; so there is the problem of decision previously mentioned. If the acceptance criteria is outside the range, the decision is obvious; if the criteria is within the range, we will try at first, after having performed a global sensitivity analysis, to improve the knowledge (if possible) on the most important epistemic variables and secondly, if the criteria remains in the interval, to make a decision by evaluating the quantile $R_{95,95,N}$ either on the belief function (pessimistic behavior), or on the plausibility function (optimistic behavior) or on the pignistic function (rational behavior). Once the function has been chosen, the decision is simple since it is based on the comparison between the resulting value of $R_{95,95,N}$ and the acceptance criteria. For the Extended BEPU approach taking into account the epistemic variables, it seems reasonable to use as indicator of risk the quantile $R_{95,95,50}$ (thus taking a confidence level of 50% sharing uncertainty due to lack of knowledge) but favoring a pessimistic decision on this quantile, that is to say, in taking its upper bound.

4.3 *Application to the example of industrial component*

In this example, the verification consists in comparing a sufficient low value of the margin factor *MF* (for example, the 5% quantile) to the safety factor.

4.3.1 *Application of the classic BEPU analysis*

We seek the 5% quantile of *MF* obtained with 95% confidence (then for this application the estimated quantile is denoted $MF_{5,95}$). For that, we perform 59 simulations (Wilks's theorem applied at 1st order) in drawing randomly samples of the aleatory variables (epistemic variables are fixed at their nominal values) and in taking the smallest value of *MF*, obtained among the 59 results, as the $MF_{5,95}$. The value obtained is 1.225 and this value is greater than the safety factor (1.2), we can conclude that the rule on the integrity of the component is respected in case of an accidental loading belonging to the 4th category.

4.3.2 *Application of the Extended BEPU analysis with separate treatment of epistemic uncertainty*

As previously proposed, a separate treatment of epistemic and aleatory variables is performed, with a probabilistic treatment of aleatory variables and DSTE for epistemic variables. So this consists in adding an extra loop for the treatment of the epistemic variables (Figure 6).

Epistemic variables are modeled with 95% intervals and medians known. The results obtained on the epistemic uncertainty of the quantile $MF_{5,95}$ are shown in Figure 7. The risk indicator proposed ($MF_{5,95,50}$) is equal to 1.19 on the plausibility function, 1.22 on the pignistic function and 1.26 on the belief function.

We notice that, in this case, the pessimistic choice that we propose will lead to the conclusion of non-compliance with the rule in 4th category, since the indicator proposed ($FM_{5,\ 95.50}$) risk equal

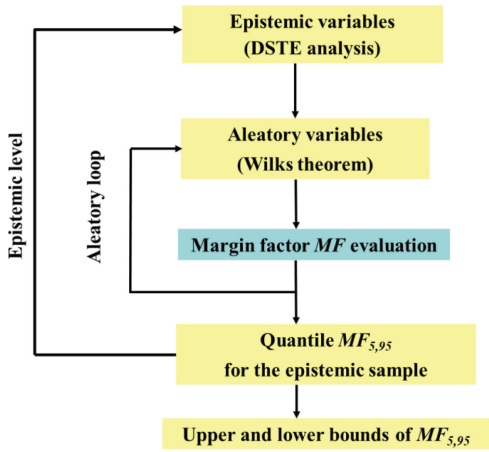


Figure 6. Proposal of a separated treatment of aleatory and epistemic variables in an extended BEPU approach.

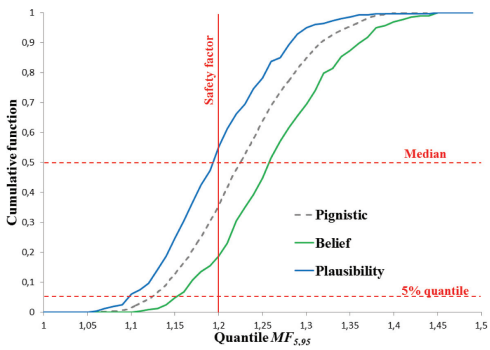


Figure 7. Belief, plausibility and pignistic function of quantile $MF_{5,95}$ obtained by DSTE.

to 1.19 on the lower envelope (envelop to be taken for *MF*).

5 CONCLUSION

In the safety analysis of complex systems, the treatment of uncertainty must distinguish the aleatory uncertainties, which represent the intrinsic randomness of the phenomena, from the epistemic uncertainties resulting from a lack of knowledge. This separation has to be done through a two-level uncertainty propagation: the internal level concerning the aleatory variables and the external level the epistemic variables. For the propagation of epistemic uncertainties, it appears more appropriate to use extra-probabilistic approaches such as interval analysis or Dempter-Shafer Theory of Evidence (DSTE).

The results show the interest of the DSTE, which additionally enables to easily formalize the expert opinion or to aggregate the opinion of several experts. This two-level propagation will provide an interval on the response of interest (failure probability or safety margin), which will be compared to the acceptance criteria. We raised the problems posed by the comparison between a value and an interval within the context of the decision making and attempted to provide some solutions.

Finally, we have proposed an improved Best Estimate Plus Uncertainty (BEPU) approach taking into account the epistemic uncertainties. The main principles of this extended BEPU approach are:

1. Separate treatment of aleatory and epistemic uncertainties by a two-level analysis.
2. Treatment of the aleatory uncertainties within a probabilistic framework (i.e. Monte Carlo simulation) and treatment of the epistemic uncertainty within an extra-probabilistic framework (i.e. DSTE).
3. Interval evaluation of a risk indicator, which is the quantile of the classic BEPU approach (i.e. $R_{95,\ 95}$) but obtained with a 50% confidence level on the part uncertainty due lack of knowledge.
4. Pessimistic decision making on this risk indicator taking the upper or the lower bound of the interval.

The choices of a 50% confidence level in the 3rd step and of a pessimistic decision in the 4th step, are only proposals and will need to be explored more deeply by discussion and application examples.

ACKNOWLEDGEMENTS

This work was performed within the framework of a collaboration supported by CEA/DISN, EDF and AREVA-NP.

REFERENCES

Dakota, 2011. A Multilevel Parallel Object-Oriented Framework for Design Optimization, Parameter Estimation, Uncertainty Quantification, and Sensitivity Analysis. Version 5.2 Reference Manual. SANDIA Report SAND2010–2184.

Dempster, A.P. 1967. Upper and lower probabilities induced by a multivalued mapping. *The annals of mathematical statistics, vol. 38 n°2*, pp. 325–339.

Der Kiuriegan, A. 2007. *Aleatory or epistemic? Does it matter? Special Workshop on Risk Acceptance and Risk Communication*, Stanford University, March 26–27.

Dubois, D. et Guyonnet, D. 2011.Risk-informed decision making in the presence of epistemic uncertainty. *International Journal of General Systems 40*, 145–167.

Eldred, M.S. et al., 2011. Mixed aleatory-epistemic uncertainty quantification with stochastic expansions and optimization-based interval, estimation, *Reliability Engineering and System Safety 96*, 1092–1113.

Fallet-Fidry, G. 2012. *Contribution to uncertainties modeling and processing within multidisciplinary risks analyses of industrial systems. Application to the Heat Sink system of an energy power plant*. PhD thesis of Université de Lorraine.

Ferson, S. et al., 2003. Constructing Probability Boxes and Dempster-Shafer Structures, SANDIA Report 2002–4015.

Helton, J.C. et al., 2008. Representation of Analysis Results Involving Aleatory and Epistemic Uncertainty. SANDIA Report, SAND2008–4379.

Helton, J.C. 2011. Quantification of margins and uncertainties: conceptual and computational basis. *Reliability Engineering and System Safety. 96*, 976–1013.

IAEA, 2009. Deterministic Safety Analysis for Nuclear Power plants, Specific Safety Guide, n° SSG2. IAEA Safety Standards, Vienna.

Ramasso, E. et al., 2008. Transferable Belief Model: Knowledge representation, Information fusion, Decision, GIPSA-Lab report.

Saltelli, et al., 2000. Sensitivity analysis as an ingredient of modelling, *Statistical Science*, 15, 377–395.

Shafer, G.A. 1976. Mathematical Theory of Evidence. Princeton University Press.

Smets, P. 2005. Decision making in the TBM: the necessity of the pignistic transformation. *International Journal of Approximate Reasoning 38*, 133–147.

Swiler, L.P., Paez, T.L., Mayes, R.L. and Elfred, M.S. 2009. Epistemic uncertainty in calculation of margins. 50th AIAA/ASME, *Structures, Structural Dynamics, and Materials Conference, Palm Springs*, USA, 4–7 May 2009.

Wald, A. 1943. An Extension of Wilks' Method for Setting Tolerance Limits. Abraham Wald. Source: Ann. Math. Statist. Volume 14, Number 1, pp 45–55.

Wilks, S. 1941. Determination of sample sizes for setting tolerance limits. *The Annals of Mathematical Statistics, Vol 12,* pp 91–96.

Zadeh, L.A. 1978. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems 1*, pp. 3–28.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safe level of redundancy in Discrete Transportation Systems

D. Caban & T. Walkowiak
Wrocław University of Technology, Poland

ABSTRACT: Discrete transportation systems are designed to operate with minimal resources that guarantee the fulfillment of their transportation tasks. Some redundancy is needed to reduce the risk of not meeting the requirements. This is particularly important, if the system operates in critical regime and cannot reject excessive transportation demand. Safe level of redundancy should ensure operation with acceptable risk, considering both the likelihood of adverse events and their consequences. The level of redundancy should consider normal system operation and occasional faults of the resources, but it should also address catastrophic risks and limiting their impact. We provide a uniform approach to finding the acceptable redundancy level in all these situations. The solution is based on standard stochastic approach, modified by injecting artificially some unlikely events into the system model. This avoids the limitations of Monte Carlo simulation—numerical hardness of analyzing events with a very low probability of occurrence.

1 INTRODUCTION

The logistics of discrete transportation systems DTS are well understood and analyzed in literature. When designing such systems, the main goal is to ensure proper functioning with minimal expenses. Thus, the costly resources (vehicles and employed drivers) are minimized.

In the paper, we address the situations where a level of redundancy of the resources is required. In Chapter 2, we demonstrate that the level of resources based on global throughput analysis can be significantly under-estimated. Simulation results show that there is a level of functional redundancy required to ensure proper quality of service.

In Chapter 3, we consider the reliability aspects of DTS and their impact on the required level of redundancy. The reliability analysis lets us determine the level of redundancy that ensures continuity of service at an economically justified level of assurance. There are a lot of techniques that support this type of analysis (Avizienis et al. 2000, Jarnicki et al. 2008, Walkowiak & Mazurkiewicz 2010, Zio 2007).

In Chapter 4, we analyze the unlikely catastrophic faults and how their consequences can be mitigated by introducing redundant resources. The dependability analysis tends to underemphasize the events that are very improbable. Such situations are addressed by the techniques of risk analysis which consider the probability of risk occurrence and their effects (Flyvbjerg 2006, Kahneman & Tversky 1979, Kaplan & Garrick 1981, Walkowiak & Mazurkiewicz 2009).

2 SIMULATION OF DISCRETE TRANSPORTATION SYSTEMS

2.1 *Monte Carlo simulation*

There are various approaches to the analysis of discrete transportation systems (Gartner et al. 1998). Probably the most versatile is to use simulation. In the simulation approach, the first step is to formulate an adequately detailed model of the system. Then, the model is used to build a program that reflects the model responses to the various events occurring in the system. These responses generate changes to the internal model state and further events that have to be handled.

Monte Carlo simulation is used when the model responses are described stochastically, i.e. some of them are not deterministic, rather they are described by random distributions. In this situation the simulation has to be run repeatedly to obtain several independent realizations of the same process. These are used to build the probabilistic distribution of the results, especially the average measures.

We use a custom designed discrete event simulator, based on the publicly available SSF simulation engine. The engine provides all the required simulation primitives and frameworks, as well as a convenient modeling language DML (Liu 2006) for inputting all the system model parameters. The simulator does not support the models specific to transportation systems, though. These are custom developed. Furthermore, the use of open-source engine and the custom models provide sufficient

flexibility to experiment with the code. This provides a better understanding of its limitations, and allows experimentation with new techniques.

2.2 *DTS model*

The discrete transportation systems (DTS) can significantly differ depending on their type and application. It is very difficult to formulate a general model, applicable to all the various classes of DTS. Still, in all cases, the models distinguish the following resources: the set of terminal nodes, the set of available routes between these nodes, the set of vehicles, the set of vehicle drivers, the fixed or dynamically modified travel schedules, and the set of transportation tasks or assignments, that the system is required to perform.

We consider in this paper a fairly wide class of DTS models, though all the numerical experiments are performed on a test case based on mail delivery system presented by us in (Walkowiak & Mazurkiewicz 2010, Caban & Walkowiak 2012).

It is assumed that the considered class of systems must conform to the following stipulations:

- System is required to perform time critical deliveries, i.e. its quality is characterized by the number of deliveries realized on time.
- System is liable to random faults that affect its operation and should have capabilities to tolerate them.
- System operates in the critical services regime, i.e. it has to accept all the incoming assignments and cannot reject excessive service demand.

The model considers transportation of goods between terminal nodes along specified routes. Assignments determine the entry nodes, at which the goods arrive at specified time, and the exit nodes, where they have to be transported to. Deadline for delivery is also specified. The assignments are generated randomly to model the real demand on services.

The routes represent connections between the nodes. They are characterized by the distance that the vehicles must travel. Taking into account the average travelling speed of vehicles, this fixes the latency connected with moving from one node to another, distorted by the travel delays caused by the traffic congestion.

Vehicles and their drivers constitute the system components directly responsible for realizing the assignments. The DST model assumes a fixed number of vehicles and a fixed number of drivers. At any moment in time a vehicle is either en route realizing assignments, waiting for goods at a node or stopped due to unavailability of a driver or due to regulatory rest period of its driver.

The vehicles are characterized by their capacity (expressed as the number of standard containers) and by the average cruising speed (determining the route latency). It may be realizing multiple assignments at the same time. It is fully loaded with goods if the pending assignments allow it. If there are insufficient assignments for nodes towards which the vehicle is destined, then it may be partially loaded or even travelling empty. It collects goods en route if there are pending assignments in the visited nodes.

A driver must be associated with a vehicle, whenever it is assigned to realize a job. Any unallocated driver can be associated with any vehicle. Only one driver at a time is associated with a vehicle (we do not consider long distance routes with standby drivers). The working time of vehicle operators is regulated by local and EU law. The daily working hours are limited (to 8 hours), there are also compulsory rest breaks while driving. At any time the driver can be either: driving, resting (between work shifts), pausing (i.e. having a compulsory break while driving) or waiting to be assigned a job.

The parameters describing the driver model include the daily working hours limit, maximum uninterrupted driving period, minimum break duration.

Vehicles are travelling in accordance to fixed travel schedules. Each schedule determines a sequence of nodes that must be visited by the vehicle as well as the times of these visits. It describes the daily work of the associated vehicle, independent of the actual needs as determined by the incoming assignments. Vehicles are loaded to their capacity (if there are sufficient assignments) on starting a travel schedule. On reaching each consecutive node, the goods destined to it are unloaded and the goods waiting there are loaded in their place. The time used for unloading and loading is taken into account. If there are other vehicles in the node, then they are queued and the period of loading/unloading is extended commensurately. When a vehicle reaches the end node, it is completely unloaded. It can then be associated with another schedule or it may be pooled, waiting to be associated.

The schedules are not directly associated with vehicles or drivers. Instead, any available vehicle and operator is allocated when needed. If there are no vehicles or drivers available, then the schedule cannot be realized.

2.3 *Level of redundancy ensuring functionality*

The goal of system simulation is to ensure that it is capable to deliver service at the required level of confidence. The proposed DTS model is probabilistic (due to the random nature of assignments input and travel times). For this reason some level

of redundancy in its throughput is required to achieve this confidence.

The measure of the system functionality is derived by monitoring the delays in realizing the assignments. As already mentioned, each assignment has a deadline for goods delivery. The proposed measure of acceptance ratio is defined as the proportion of assignments that are delivered on time to the total number of assignments in the system during a fixed time period. A 24 hour reporting period is assumed for determining this ratio.

The time instances (t_0, t_1, …, t_n) fix the boundaries of the consecutive days, for which the ratio is considered. $N_d(t_i)$ denotes the number of assignments completed in period (t_i, t_{i+1}), while $N_{pd}(t_i)$ denotes the part of them completed on time. The average ratio A_r of on-time deliveries, computed over the multiple runs of the simulator and over all the period (t_i, t_{i+1}) is defined as:

$$A_r = \underset{i}{E}\left[E\left(\frac{N_{pd}(t_i)}{N_d(t_i)+1} \right) \right]. \quad (1)$$

The addition of 1 in the above equation is noteworthy. It does not have any analytical justification. In normal operation, the number of completed assignments is significantly greater than 1 and adding this value does not change the ratio. On the other hand, if the system is down for more than a day, then the constant prevents division by 0.

It is possible to assess the acceptance ratio analytically, assuming average number of assignments and average cruise times. The results of such assessment for the testcase DTS system mentioned in 2.2 is presented in Figure 1. This can be taken as a baseline for system operation without any redundancy to accommodate the random behaviour.

The results of the same system analysis using simulation (with random distributions of assignments and cruise times) are presented in Figure 2.

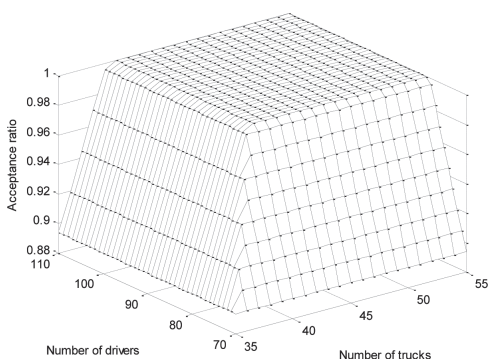


Figure 1. Analytical model of acceptance ratio—the value of 42 vehicles and 84 drivers ensures perfect operation.

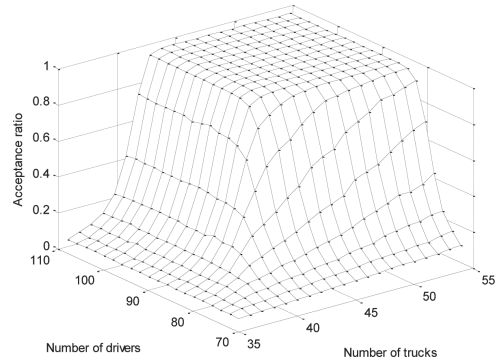


Figure 2. Simulation results for the DTS example—required 45 vehicles and 90 drivers.

It should be noted that the system with 42 vehicles and 84 drivers, analytically determined from Figure 1, ensures average acceptance ratio at the level of approximately 0.2 in Figure 2. Clearly, there is need for some redundancy to ensure that the random fluctuations in system operation do not have excessively adverse impact on its operation. This redundancy is further referred to as the "redundancy ensuring functionality". As further demonstrated even greater redundancy is needed if we aim to achieve a level of fault tolerance, i.e. if we need to preserve the DTS quality in the presence of vehicle or human faults.

3 DTS RELIABILITY ANALYSIS

3.1 *System faults*

The DTS system is prone to be disrupted due to the occurrence of faults in its operation. These faults can affect the system's ability to realize assignments on time.

We consider three types of operational faults. All are temporary. The faults are as follows:

– vehicle breakdowns,
– driver absence at work (e.g. due to illness),
– traffic congestion, causing excessive delays in the vehicles cruise time.

Broken down vehicles are repaired, drivers get well and return to work after a period of absence, traffic gets back to normal in time. In consequence, the system is fully repairable and there is no long term degradation.

The vehicles are assumed to break down occasionally, in accordance to their reliability parameters (failure rates). They stop operation and wait for a maintenance team. On being repaired (after

a random repair time), the vehicles continue the work they were realizing before breakdown.

The model does not distinguish any specific parameters of the maintenance teams, just their number. Each maintenance team repairs only one vehicle at a time. If all the maintenance teams are currently occupied, then the vehicle repair is delayed until one becomes available.

Drivers get ill or otherwise temporarily unavailable. There are multiple causes for absence in the work, all characterized by different frequencies of occurrence. Statistical data published by the Central Statistical Office gives an indication of the likelihood of the various periods of absenteeism. We use a simplified stochastic model of absenteeism (Walkowiak & Mazurkiewicz 2010):

– short sickness (1 to 3 days),
– typical illness (7 to 10 days),
– protracted disability (10 to 300 days).

In the model the three types of disabilities are treated independently. In each case the actual period of absence is randomly chosen from the appropriate range.

3.2 *Level of redundancy ensuring fault tolerance*

The simulation approach, proposed in 2.1 and 2.3, can also be applied to the analysis of the DTS system liable to fault occurrence. The simulation model needs to be extended by the fault occurrence and repair processes.

The results of simulation of the system with likely faults are presented in Figure 3. There is no significant difference in the shape and properties of the obtained acceptance ratio characteristic. It should be noted, though, that the slopes of the surface are shifted towards greater numbers of drivers and vehicles. This indicates that the required level of redundancy ensuring fault tolerance is greater that in case of the functional redundancy.

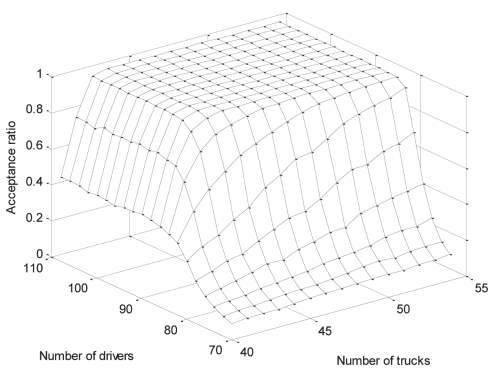


Figure 3. Simulation results for the DTS example with faults hazard—required increased redundancy.

4 ANALYSIS OF UNLIKELY FAULTS

4.1 *Unlikely faults*

Transportation systems are prone to hazards that are very unlikely, i.e. their probability of occurrence is so small that they are not considered in the reliability analysis. This does not mean that they cannot occur, though. If they cause extensive damage to the system, then they still need to be taken into account in contingency risk planning.

The following risks are identified in case of the DTS model:

– Complete stoppage of the DTS system, caused by all the drivers going on strike, sabotage of vehicles, natural disasters disrupting the vehicle fleet or the road infrastructure. As a result the system becomes inoperable for a fixed period of time (a few days).
– Periodic rapid increase in the service demand, e.g. due to unexpected seasonal changes or connected with failures of other, competitive transportation systems operating in the same region. It manifests itself by a much higher rate of assignments arriving in all the nodes. In effect there is a sudden influx of assignments that the system cannot handle.
– Unforeseeable unavailability of a significant proportion of drivers, caused by strikes or an epidemic illness, such as flu or virus infection. As a result, a significant proportion of the drivers may be simultaneously absent from work. This is a generalized version of the periodic stoppage risk, where some parts of the system can still operate.
– Unforeseeable reduction in the number of available vehicles, connected with disrupted supply chains, shortage of fuel or vehicle replacement parts. As a result, some vehicles cannot be kept operational (as if they all failed simultaneously).

4.2 *Assessment of risk of unlikely faults*

Risk assessment plays the key role in any management activity. There are various alternative approaches to risk assessment (Kaplan & Garrick 1981, Zio 2007). Most popular is the qualitative approach, based on expert opinions (Flyvbjerg 2006). The basis of this analysis is to classify the identified risks in accordance to the likelihood of their occurrence and the gravity of their consequences.

The likelihood of any risk occurrence is assessed as either: low, medium, or high. Likewise, the gravity of its consequences is assessed as: insignificant, low impact, or serious. Qualitative risk assessment is based on these two. Obviously, if we regard an

event to be very improbable and its consequences insignificant, then the associated risk is very low. On the other hand, a likely event with serious consequences is associated with very high risk.

The likelihood of the events discussed in 4.1 is low to medium. On the other hand, the consequences cannot be predicted just by expert knowledge. It is proposed to use the simulation technique for this purpose.

4.3 *Modified simulation approach*

As discussed in 2.1, Monte Carlo simulation has to be run repeatedly to obtain several independent realizations of the same process. The results differ, since the model is not deterministic. The number of runs has to be sufficiently high, so the probabilistic distribution of the results captures all the possible situations. The lower the probability of an event, the higher is the required number of runs.

For this reason, the approach is inadequate to analyze the effect of unlikely faults on the DTS system. The number of runs would have to be huge to capture even single occurrences of these events. The simulator had to be modified to enable this analysis.

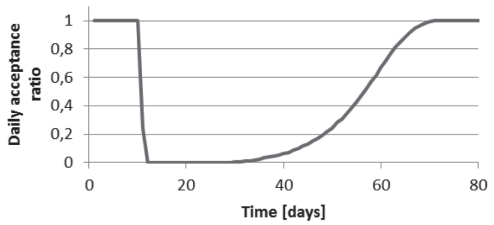


Figure 4. Daily acceptance ratio with complete DTS stoppage from day 10 to 15—consequences observed until day 70.

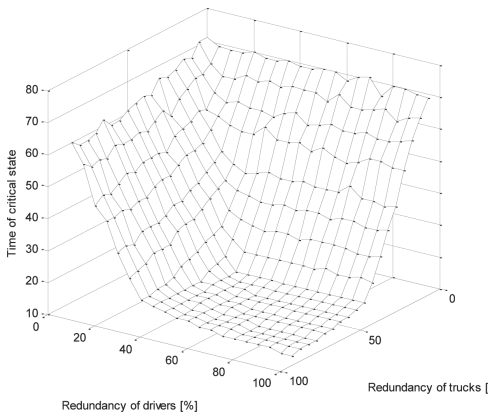


Figure 5. Critical state of operation measured for DTS systems with various level of vehicles/drivers redundancy.

The occurrence of the unlikely faults mentioned in 4.1 can be predetermined manually in the simulator. Then, the simulator can be used to predict their effects on the rate of on-time deliveries. The system is analyzed against its ability to resume normal operation after a disruption of service, i.e. it is used to assess the gravity of consequences (instead of likelihood of occurrence).

The measure of the acceptance ratio, defined by equation (2), is not adequate in this case—it assumes the same distribution in all the time periods (t_i, t_{i+1}), i.e. the stationary property of the stochastic process. Instead, we consider the daily acceptance ratio a_{ri}:

$$a_{ri} = E\left(\frac{N_{pd}(t_i)}{N_d(t_i)+1} \right). \tag{2}$$

In this case, the average is taken only on the same time periods (t_i, t_{i+1}) of the various simulation runs.

Figure 4 presents an example of the simulation results obtained in this approach. The time from the occurrence of the unlikely event (day 10 in the Figure) until its diverse effects are mitigated is called the "time of critical state of operation". In this case, it is about 2 months!

4.4 *Level of redundancy limiting the risk of unlikely faults*

The length of time of the critical state of operation depends on the redundancy in the system resources. Simply speaking, the greater this redundancy, the faster is recovery from an unlikely fault. The results of simulation given in Figure 5 support this intuition.

It should be noted that there is a level of redundancy, above which the impact on limiting the time of critical operation becomes small. This level of redundancy (about 25% in this example) is the obvious choice to limit the risk of unlikely faults.

5 CONCLUSIONS

We have analyzed three different phenomena that lead to the necessity of introducing redundancy in the resources of a discrete transportation system:

– redundancy ensuring proper functionality,
– redundancy ensuring fault tolerance,
– redundancy limiting the risk of unlikely faults.

In each case, the level of required redundancy is different. As expected, the least redundancy is required to ensure functionality and the greatest

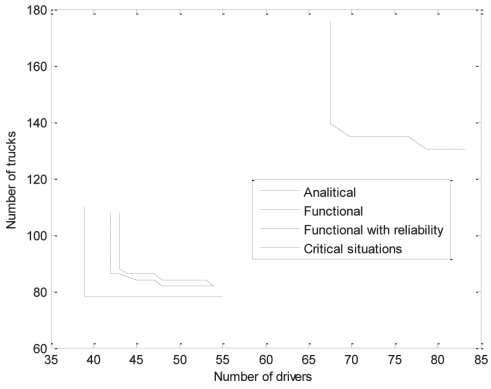


Figure 6. Minimal number of resources (vehicles and drivers) required for the various types of redundancy.

redundancy occurs when limiting the risk of unlikely faults. This is presented in Figure 6.

It should be noted that, unlike the functional and reliability redundancies, the redundancy for limiting the risk of catastrophic faults does not need to be available at all time. It is only used when the system is in the state of disorder after a catastrophic fault. This can be the basis of a number of different risk mitigation strategies. Some interesting approaches to dealing with this are:

– subcontracting some transportation tasks to external systems,
– moving resources between DTS subsystems (this is analyzed in (Caban & Walkowiak 2013),
– centralizing of the redundant resources in a multiple subsystems DTS.

REFERENCES

Avizienis, A., Laprie, J. & Randell, B. 2000. Fundamental concepts of dependability. In *3rd Information Survivability Workshop, Boston*: 7–12.

Caban, D. & Walkowiak, T. 2012. Risk analysis applied to discrete transportation systems. In C. Bérenguer, A. Grall, C.G. Soares (eds). *Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011*: 2731–2738. Leiden:CRC Press/Balkema.

Caban, D. & Walkowiak, T. 2013. Relocation of resources in a hierarchically managed transportation system under critical conditions. *Transport and Telecommunication* 14(4): 282–291.

Flyvbjerg, B. 2006. From Nobel Prize to project management: Getting risks right. *Project Management Journal* 37(3): 5–15.

Gartner, N., Messer, C.J. & Rathi, A.K. 1998. Traffic flow theory and characteristics. In: *T.R. Board (Ed.)*. Texas: University of Texas at Austin.

Jarnicki, J., Walkowiak, T. & Zamojski, W. 2008. Functional availability in discrete transport systems. In *XXXVI Winter School of Reliability*. Radom: Instytut Technologii Eksploatacji.

Kahneman, D. & Tversky, A. 1979. Prospect theory: An analysis of decisions under risk. *Econometrica* 47: 313–327.

Kaplan, S. & Garrick, B.J. 1981. On the quantitative definition of risk. *Risk Analysis* 1(1): 11–27.

Liu J. 2006. Parallel Real-time Immersive Modeling Environment (PRIME), Scalable Simulation Framework (SSF), User's manual. Colorado School of Mines Dept. of Mathematical and Computer Sciences.

Walkowiak, T. & Mazurkiewicz, J. 2009. Analysis of critical situations in discrete transport systems. In: *Proc. of International Conference on Dependability of Computer Systems, Brunow*: 364–371. Los Alamitos: IEEE Comp. Soc. Press.

Walkowiak, T. & Mazurkiewicz, J. 2010. Functional availability analysis of discrete transport system simulated by SSF tool. In *Intern. Journal of Critical Computer-Based Systems* 1(1–3): 255–266.

Zio, E. 2007. An introduction to the basics of reliability and risk analysis. London: World Scientific Publishing Comp.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Using Petri-Net analysis for advanced reliability analysis of polymer electrolyte membrane fuel cells

M. Whiteley, J. Leigh, A. Fly, L.M. Jackson & S.J. Dunnett
Aeronautical and Automotive Engineering Department, Risk and Reliability Research Group, Loughborough University, Loughborough, UK

ABSTRACT: With the ever increasing concerns of anthropogenic climate change in recent years, the scientific community has been tasked with developing low-zero carbon technologies to mitigate climate change. One of the most promising technologies to answer to the concerns is the hydrogen fuel cell, particularly when integrated into an automotive context. Hydrogen fuel cells are an electro-chemical, zero-emission energy conversion and power generation device. They use hydrogen and oxygen gas to produce electricity, with their only by-products of heat and water vapour.

Reliability issues with fuel cells have held back the commercialisation of this promising technology, and as such are required to be studied further. The international fuel cell community has set reliability standards to require an automotive fuel cell to last more than 5000 hours. These standards are difficult meet; therefore in depth reliability analysis can help allude towards the key areas of improvement in fuel cell technology to meet these standards.

Previous failure mode and effect analysis and fault tree analysis work by the authors has shown that the inherently complex system of a PEMFC assembly can harbor dependencies between multiple failure modes. Therefore in this presented work, Petri-Net simulation has been adopted to develop a more accurate degradation model. Operational parameters such as water content, temperature and current density's effects on the occurrence of failure modes can be modelled through this technique. This work will improve previous fuel cell reliability studies by taking into consideration; operating parameters (water content, temperature), ambient weather and fuel cell voltage demand (drive cycles).

1 INTRODUCTION

1.1 *Hydrogen fuel cells*

Climate change worries and sustainability issues have become a poignant talking point in recent years, since it has become impossible to ignore the anthropogenic source of climate change (Solomon, et al. 2007). Man-made pollution contributes towards climate change due to Greenhouse Gas (GHG) emissions, including; Carbon Dioxide (CO_2), Methane (CH_4) and Nitrous Oxide (N_2O) amongst others.

In 2011, the United Kingdom emitted 549.3 million tons of CO_2 equivalent ($MtCO_2e$) (DECC, 2011), with 122.2 $MtCO_2e$ being down to the transport industry. Cars, taxis and busses accounted for 74% of this figure, which is a startling contribution (DfT, 2010).

Not only are GHG emissions affecting the atmosphere in a negative way, energy prices are predicted to increase at ever increasing rates (BERR, 2006), which could potentially lead to disruption in the UK's energy system.

Due to the aforementioned climate and energy issues, the UK's GHG contributions needs to be dramatically reduced.

Hydrogen fuel cells could potentially be the answer (or a part of the answer) to climate change and sustainable energy issues. A hydrogen fuel cell is a zero-emission energy conversion and power generation device. They combine Hydrogen (H_2) and atmospheric Oxygen (O_2) to create Water (H_2O), a little heat, and electricity. If the H_2 can be sourced from renewable means (such using as wind and solar energy electrolysis of water), the whole process of using a fuel cell is zero emissions in use. With all of these factors considered, the hydrogen fuel cell could be used in an automotive context to replace the fossil fuel powered Internal Combustion Engine (ICE).

1.2 *The Polymer Electrolyte Membrane Fuel Cell*

Out of the five main sub-categories of fuel cell, the Polymer Electrolyte Membrane Fuel Cell (PEMFC) has been underlined as the most feasible

to be integrated into an automotive application. This is due to its low operating temperature and rapid start-up time. The main components of a PEMFC are shown in Figure 1.

Currently, there are three main hurdles to the commercialization of PEMFCs; Cost, Infrastructure and Reliability:

Cost—PEMFCs use Platinum (Pt) catalysts, which is inherently expensive. Pt loadings for PEMFCs are coming down year after year with more development.
Infrastructure—For a successful commercial uptake of PEMFCs, there must be an adequate network of filling stations to service PEMFC vehicles.
Reliability—Reliability is the largest stumbling block for PEMFC uptake as the technology stands. Cost and infrastructure can be overcome via investment and policy, whereas reliability requires an in-depth analysis.

PEMFCs in an automotive application need to meet targets set out by the United States (US) Department of Energy (DoE) of; a lifetime of more than 5000 hours with a performance drop of no more than 5% over that period. The Japanese New Energy and Industrial Technology Development Organisation (NEDO) and the European Hydrogen and Fuel Technology Platform (HFP) targets mirror that of the US DoE with a 5000 hour lifetime goal in an automotive application (Borup, et al. 2007).

However, modern day PEMFC systems cannot quite reach these targets due to unforeseen degradation of the membrane, Catalyst Layer (CL), Gas Diffusion Layer (GDL) and Bipolar Plate (BIP) components, leading to a drop in performance of the PEMFC, or even catastrophic failure.

1.3 *PEMFC degradation*

There are three main failure mechanism categories that could affect the operating lifetime of a PEMFC; chemical, thermal and mechanical degradation. These overarching failure categories can contain numerous individual failure modes that a PEMFC can experience.

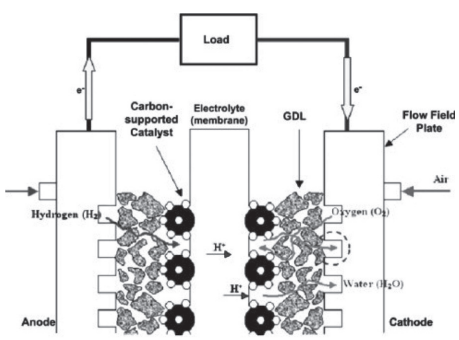


Figure 1. Components of a PEMFC (Kandlikar & Lu, 2009).

To illustrate a chemical degradation mechanism, out of the many chemical degradation events that degrade a PEMFC, Hydrogen Peroxide (H_2O_2) and radical attack (namely Hydroxyl (OH) and Hydroperoxy (OOH)) are of the most prominent.

OH and OOH radicals are formed through the chemical reactions surrounding H_2O_2 production. The membrane of a PEMFC is inherently thin to try to increase performance, however this means that there is always a small amount of gas cross-over between the anode and cathode. The H_2O_2 formation and radical propagation can lead on to a chemical attack of the Polytetrafluoroethylene (PTFE) based membrane and areas of the CL and GDL.

As platinum (Pt) is used as a catalyst in a PEMFC, it can be a catalyst for the formation of H_2O_2 and OOH radicals as described by LaConti, et al. (2003). Another method of H_2O_2 and radical production can be via the presence of foreign metal cations.

Peroxide and radical attack damage the PEMFC via chemical dissolution of the PTFE based membrane material, and even parts of the CL and GDL. Chain scission and end-group unzipping is the process of chemical degradation where the membrane wastes away and loses mass due to peroxide and radical contamination. This can be observed by a presence on fluorine in the exhaust gas stream, where the PTFE based membrane is being pulled apart and is leaving the cell.

2 RELIABILITY ANALYSIS OF PEMFCS

2.1 *Work in the literature*

Reliability analysis of PEMFCs is still in its infancy and needs to be further developed to advance the lifetime of PEMFCs and understanding of degradation mechanisms.

Previous work includes a Failure Mode Identification (FMEA) and fault Tree Analysis (FTA) of a general PEMFC by Rama, et al. (2008). Additionally, a more recent FTA work was presented by Placca. L & Kouta. R (2011), looking at the failure modes that could cause PEMFC degradation, yielding a more detailed fault tree of fuel cell degradation.

Work by Whiteley, et al. (2013a & 2013b), identified areas for improvement in these former works, improving the FMEA and FTA and furthering the reliability and degradation field of PEMFC research. Results from these studies identified the dependent nature of some degradation mechanisms, thus this latest research focusses on the

Petri-Net technique due to its ability to take into account relationships and dependencies between failure modes.

2.2 *Petri-Net analysis*

Petri-Net simulation is based upon a graphical process of representing component relationships, conditions and events. It can be used to model and analyse dynamic behaviors of systems taking into account relationships and dependencies which FTA cannot.

Petri-Nets are comprised of two main symbols; P (places) and T (transitions). Places indicate the state of the system being modelled, and can therefore contain information such as health of a component. Transitions contain the relevant data to facilitate the changeover from one place to another. They can contain data such as probability or timings.

These two nodes are connected by arrows known as 'Arcs' A, which show the direction of flow of 'tokens'. Tokens are used to describe the state of the system, and are used to mark/enable a place as in Figure 2.

Figure 2 shows a basic Petri-Net model that has place one enabled (*P1* containing a token) denoting a system state. The transition (*T1*) will fire based on criteria that could range from time intervals to probability. If the pre-set conditions are met, the transition will take the one token from *P1* and place it into *P2*, representing a new state of the system.

P, *T* and *A* can be defined as per Liu & Chiou (1997):

$$P = \{P_i \mid P_i \text{ is a place, } 1 \le i \le I\},$$

where *i* is a positive integer

$$T = \{T_i \mid T_i \text{ is a transition, } 1 \le i \le I\},$$

$$A \subseteq (P \times T)\ U\ (T \times P).$$

2.3 *Literature on Petri-Net analysis of PEMFCs*

In the literature, there is currently only one example of Petri-Net use for reliability analysis of PEMFCs from Wieland, et al. (2009),

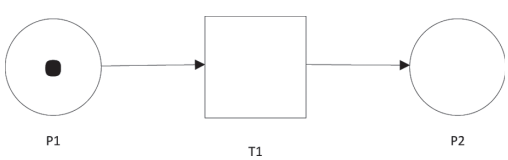


Figure 2. Example Petri-Net.

This work has a basic overall Petri-Net. At the centre of this net, there is an initial place which denotes the operational state of a PEMFC. The model can fire through five main transitions; Degradation, Spontaneous event, Reversible event, Repair and Breakdown. The way in which the transitions fire is based upon degradation rates taken from the literature, or the authors' own assumptions. The degradation rates are selected utilising the normal distribution based upon mean, lower and upper limits, assumed by the authors.

The output of the model is an estimated voltage degradation based upon a simple linear model. Additionally, it was found that (due to their simulation) 'Natural Aging' was the most prominent failure mode in the system.

2.3.1 *Limitations with the modelling*

The limitations found by the authors are acknowledged as a lot of simplification of the model (i.e. with reference to spontaneous events); use of the normal distribution; and time of year effects.

Review has shown that along with these factors, not only would time of year affect fuel cell operation, but load cycle and other operating variables could be considered. A PEMFC will change temperature, gas flow rates and other parameters based upon load demand. Therefore incorporation of a drive cycle such as the New European Drive Cycle (NEDC) would put the fuel cell under differing loads, and thus differing operating parameters.

The authors adopted the normal distribution method to model the degradation rate, which is a potential drawback. Components in a PEMFC don't share features with the normal distribution probability theory. In fact, components aging in a PEMFC system share characteristics with the Weibull distribution and the 'bathtub curve'. Here, the Weibull shape parameter 'β' is indicative of the phase of the component in its lifetime. This shape parameter (alongside the location parameter 'γ') can be changed dependent upon the failure mode in question. That is to say that an early life failure mode such as 'creep' in the initial stages would have a shape parameter of less than one, whereas 'Relative Humidity Cycling' (taking a long time to have an affect) would use a parameter of more than one. Any failure modes experienced throughout the useful life phase would use a shape parameter of one.

The work presented is a good start to develop reliability analysis in this field. However, the model could in addition be further developed to accurately represent all of the previously identified failure modes from FMEA and FTA work presented by Whiteley, et al. (2013a & 2013b).

3 PROPOSED MODEL

As previously discussed in section 2, the reliability analysis of PEMFCs, and more specifically Petri-Net analysis, needs to be evolved. This work attempts to enhance the capabilities of the Petri-Net approach towards PEMFC degradation modelling. The proposed work looks at the inherent complexity of degradation within a PEMFC and therefore can accommodate the interdependencies of failure mode groups, which would change the overall degradation of the cell. Additionally, this work can account for degradation due to operating conditions, such as high temperature or low relative humidity operation of the cell. These changes of input operating conditions will have an effect on the degradation as previously found in (Whiteley, et al. 2013a & 2013b).

The overall 'global' Petri-Net for the PEMFC simulation is presented in Figure 3.

There are two global states 'Operating State' and 'Failed State', The 'Operating State' is initially set to represent 100% health of the PEMFC and fires through the 'Degradation' transition on every time-step of the simulation. Contained within the degradation transition, are individual, separate Petri-Nets. Each failure mode has a relationship Petri-Net to explain its logic, and how it interacts with other failure value to be ascertained for each failure mode, and also its interaction with other individual Petri-Nets to be included in the simulation.

The 'Failure' transition will be fired based upon the criteria of unacceptable system performance. This is set at a lifetime of less than 5000 hours with more than a 5% drop in cell performance over that time as per the US DoE target discussed in section 1.2. If this target threshold is exceeded, the transition will fire into the 'Failed' state and end the simulation run.

3.1 *Degradation modules*

A total of 21 Petri-Net modules have been created, with two being discussed to illustrate the module development. The two failure modes described are 'H_2O_2 Degradation' and 'Radical Attack', which are intrinsically linked.

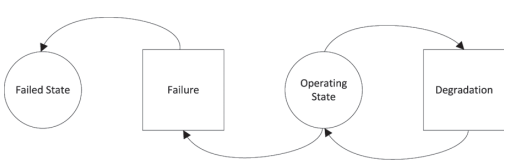


Figure 3. 'Global' Petri-Net of PEMFC.

3.2 *H_2O_2 degradation Petri-Net*

Figure 4 shows the example Petri-Net for 'H_2O_2 Degradation', *P1* is enabled with a token on the first running of the model. It is indicative of a healthy PEMFC, with no H_2O_2 degradation. *T1* can only fire when there is a token in *P2* and *P1* at the same time. *P2* is used to indicate a state of H_2O_2 degradation, agglomerating the lower level transitions. This is for the integrity of the transition logic.

The firing of this transition would enable *P8*, indicating a state of H_2O_2 degradation, and would have an output affecting the performance of the PEMFC and potentially linking into another Petri-Net module. There are a number of contributors to *P2*, stemming from places *P3* 'Pt dissolution/redistribution 'Pt Band'', *P4* 'Low rate of gas crossover', *P5* 'BIP corrosion & release of metal ions' and *P6* 'High rate of gas crossover'. *P3* is enabled by an interaction from a separate Petri-Net module, and indicates the presence of Pt which acts as a catalyst for H_2O_2 formation. Therefore for *T2* to fire, *P3* and *P4* need to be enabled. This would show that there is gas crossover and a free Pt presence to cause a rate of formation of H_2O_2 over and above normal gas crossover formation.

H_2O_2 can form from the crossover of the reactant gasses through the membrane. Thus for a given rate of gas crossover, a corresponding rate of H_2O_2 formation is attributed. This enables the Petri-Net modelling of *T3* and *T5* firing and a corresponding degradation of PEMFC overall performance. Consequently if *P6* is enabled, *T5* will fire, placing a token in *P2*, and if *P4* is enabled, *T3* will fire a token into *P2*.

Pozio, et al. (2003) also showed that the presence of Fe^{2+} and Cu^{2+} (Iron and Copper ions) released from BIP corrosion greatly accelerate the degradation due to H_2O_2 formation when there is gas cross-over. Therefore a separate rate is associated with *T4*.

P7 is an inhibitor and serves to prevent the transition of *T2*, *T3*, *T4* & *T5*. Due to the information in the literature, Borup, et al. (2007), who state that the potential for H_2O_2 formation (E^o H_2O_2) is equal to 0.695 V, and that any potential greater than this would inhibit the formation of H_2O_2 in the PEMFC. Therefore in Figure 4 the inhibitor *P7* is used to reflect this fact.

H. Tang, et al. (2007) show that H_2O_2 degradation reduced the OCV value of a PEMFC over time (Fig. 5). Therefore the degradation rate attributed to H_2O_2 degradation is set at 0.0065 Vh^{-1}. This degradation rate is a contributor towards the overall voltage degradation agglomerated from each individual module's outcome.

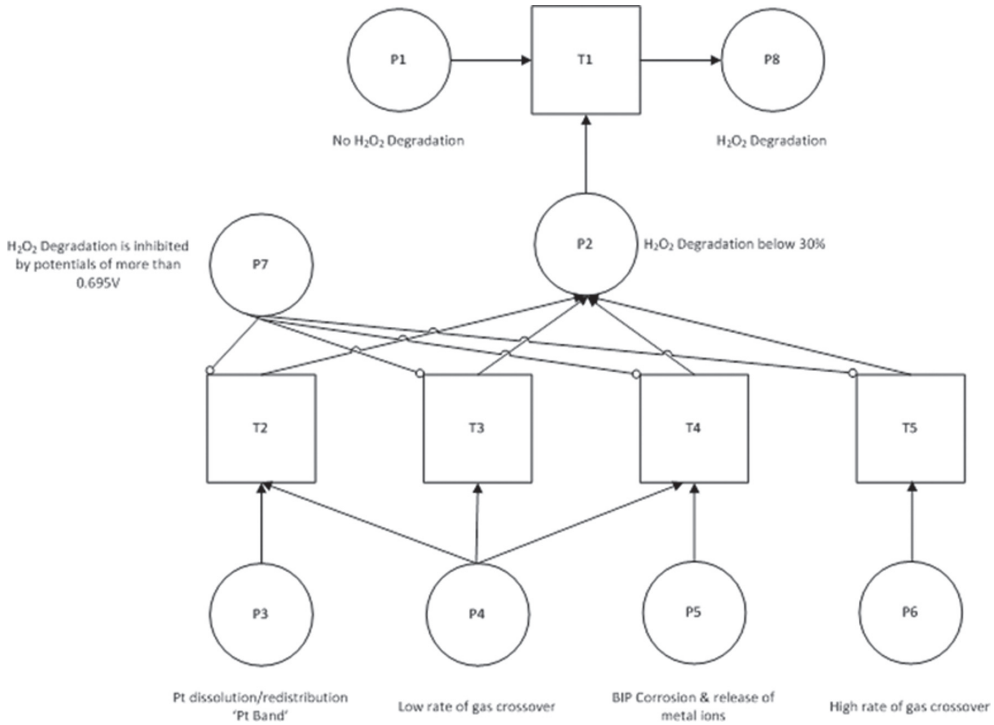


Figure 4. Example of H_2O_2 degradation module Petri-Net.

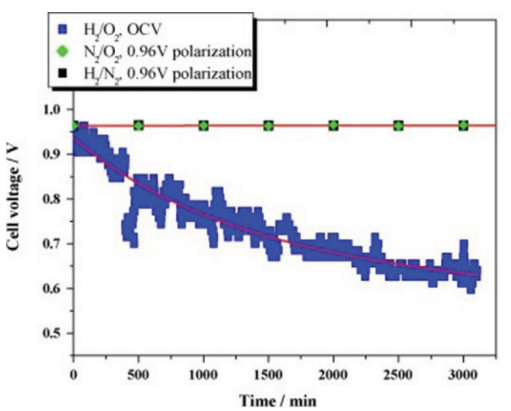


Figure 5. H_2O_2 performance degradation at OCV (Tang, et al, 2007).

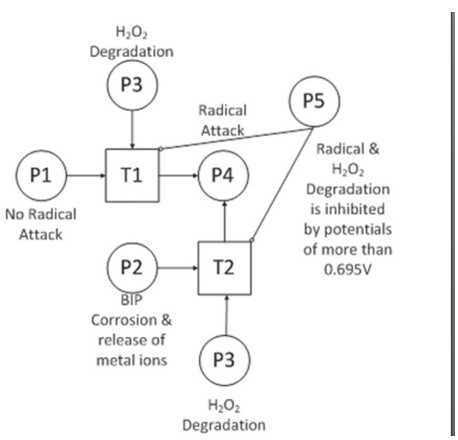


Figure 6. Example of radical attack module Petri-Net.

3.2.1 *Radical attack Petri-Net*

Due to the inherent chemical relationship between H_2O_2 and OH/OOH radical attack, both of these degradation Petri-Nets need to interact to form an accurate degradation model. The Petri net module developed for radical attack is shown in Figure 6.

P1 (in Fig. 6) is indicative of a state of no degradation. *T1* requires *P1* and *P3* to be enabled to fire, and will fire automatically with no delay. *P5* serves as an inhibitor using the same logic as for *P7* in Figure 4. If *P5* is disabled and there are tokens contained within *P3* and *P1*, *P4* would be enabled indicating a state of 'Radical Attack'.

P2 will become enabled via the result of the BIP degradation Petri-Net module. If *P2* is enabled, and *P3* is also, *T2* will fire automatically (as long as *P5* is not enabled), placing a token in *P4*. This will denote the state of 'Radical Attack'.

P3 in Figure 6 is the same place as *P8* in Figure 4 showing the interaction between the 2 modules. Borup, et al. (2007) suggest that radical attack greatly accelerates the membrane degradation rate. As there is no degradation rate available in the literature for radical attack, one can only assume a rate and attribute this to *P4* of Figure 5. An order of magnitude is therefore applied to the H_2O_2 degradation rate of 0.0065 Vh^{-1}, resulting in a degradation rate of 0.065 Vh^{-1} for radical attack.

3.3 *Petri-Net firing mechanism*

The firing of the Petri-Net uses the following equation:

$$M_n = M_0 + A^T \sum \tag{1}$$

where M_n is the final marking, M_0 is the initial marking, A^T is the incidence matrix for the module, and ∑ is the transition firing count vector. The relationship between A^T and ∑ is summarised in Equation 2:

$$A^T \sum = \Delta M = M_n - M_0 \tag{2}$$

For each individual Petri-Net module contained within the 'Degradation' transition of the global Petri-Net, there is a corresponding incidence matrix as in Equation 11 for radical attack degradation.

The logic behind each transition from place to place is noted in each A^T matrix for each module. A—1 indicates the taking of a token from a place, and a 1 indicates the placing of a token into that place.

3.4 *Summary of the model*

The Petri-Net degradation model developed in this work is a comprehensive model of the interactions between the previously identified failure modes in a PEMFC of standard construction. The standard construction is such that there is a PTFE based membrane, Carbon/Pt catalyst, steel BIP and carbon GDL. The individual 'degradation' modules range from relatively simple relationships with 2–3 places and a low number of transitions, to larger modules with 8 places and 8 transitions. It contains 21 separate modules that interact to both; deliver a voltage degradation value, and further interact with other failure modes.

Transition timings for the examples in Figure 4 and Figure 6 are instant, but for others could be timed or based upon enabling criteria.

4 RESULTS

The Petri-Net model was programmed in MATLAB on a desktop PC running a dual core 3.10GHz processor. The simulation model is outlined in Figure 7. The computer script is activated and the initial variables set which include operating temperature, relative humidity, number of Startup/Shutdown Cycles (SSC)s and simulation end time. This data is implicit in placing tokens in the relevant initial places, and inhibitor gates. A dynamic range of inputs can be added to have a varying input (such as temperature) over time.

The incident matrix for the Global Petri net shown in Figure 3 is then generated. This global net is then run for a preset time. The degradation transition fires on every time step initiating the

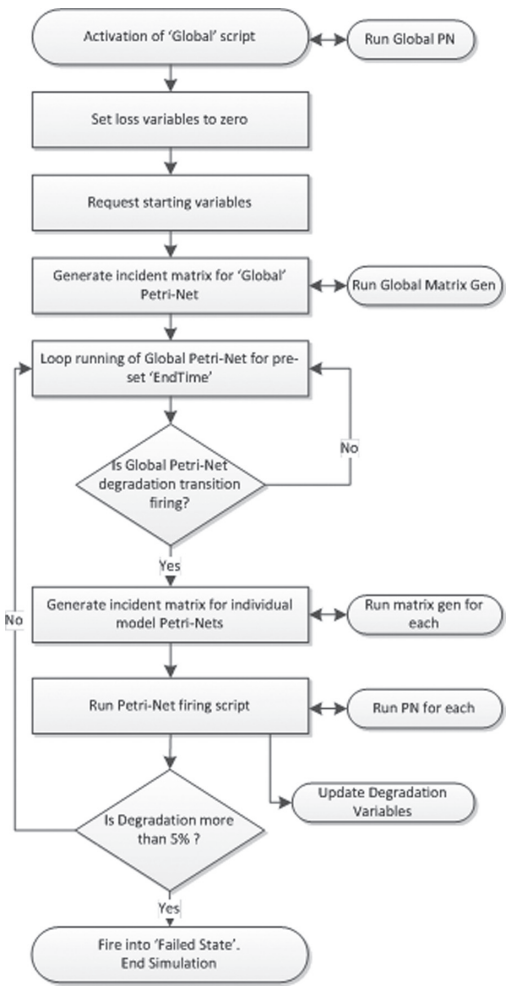


Figure 7. Flow chart of simulation running.

individual Petri Net modules for each failure mode. The incident matrices for each failure mode net are generated and run and the overall voltage degradation value is updated. For all of the individual Petri-Net models, an A^T matrix was constructed with a corresponding transition 'firing' script to use the A^T matrix information.

For each Petri-Net that has an output for which a reduction in performance is noted, a voltage drop count variable is used to store the total amount of degradation in performance due to the failure relationships. Therefore for each output place in a degradation module Petri-Net, a voltage drop figure is added to the overall voltage drop count.

Reversible events will refer back to the initial states of no degradation, and irreversible events will remain in their product states after first firing.

$$A^T = \begin{matrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{matrix} \begin{pmatrix} T_1 & T_2 \\ -1 & 0 \\ 0 & -1 \\ -1 & -1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} \tag{3}$$

A check is made to determine if that degradation has exceeded the threshold of 5% as required by the US DoE. If that threshold has been exceeded then the simulation is terminated and run time logged. If it is not the degradation transition cycle continues.

4.1 *Verification of model*

SSC was chosen as a failure mode to verify initially, as this Petri-Net interaction is relatively simple, and easy to analyse for effective modelling. SSC degradation was considered through a review of the literature in this area. Hong Kim, et al. (2010) conducted extensive experimentation to reveal the relationship between SSC and degradation of fuel cell performance. Their results show that after 1500 instances of SSC, a drop in performance of 0.08 V was observed (Fig. 8). Therefore per cycle it can be considered that SSC causes a drop in performance of 5.333×10^{-5} V.

The degradation rate was programmed to take affect per SSC, through the transition T1 in Figure 9. Therefore, for each time there is an instance of SSC, a degradation rate of 5.333×10^{-5} V is applied to a voltage drop count variable.

The results of the Petri-Net model using a SSC degradation module was tested using a polarisation curve model as in Figure 8. The model shows a good replication of the polarisation curve drop observed by Hong Kim, et al. (2010) in Figure 8.

With the same logic being carried through the entirety of the Petri-Net model. Each failure mode interaction has a voltage degradation value assigned to it, with some acting reversibly dependent upon the state of the system, and some acting as a counter (irreversible).

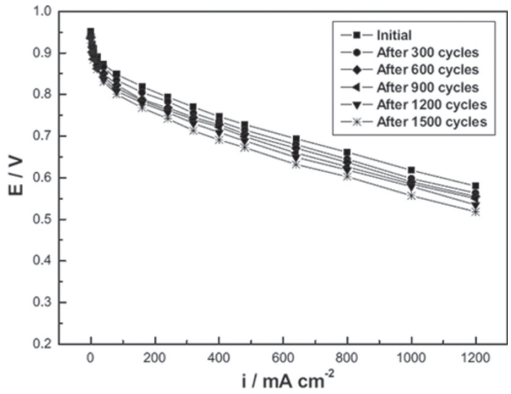


Figure 8. Startup/shutdown cycling tests (Hong Kim, et al. 2010).

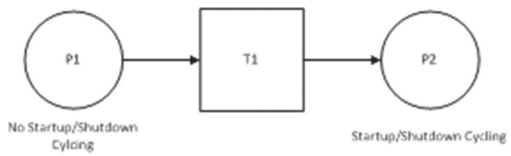


Figure 9. Startup/shutdown cycling Petri-Net.

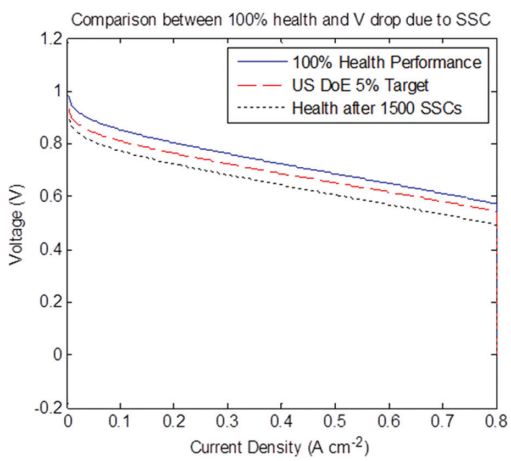


Figure 10. Result of startup/shutdown cycling 1500 cycles.

5 CONCLUSIONS AND FUTURE WORK

The presented work is a step forward in degradation and reliability modelling of PEMFCs.

The previous work by the authors leading to this has ensured that the Petri-Net model proposed, is reliably constructed based upon an in-depth, and up-to-date review of PEMFC failure phenomena. The failure logic is sound based upon current literature. However, if further interactions or modules are discovered that need to be added, the Petri-Net model can easily facilitate this occurrence, with a simple addition to the script files.

A lumped parameter PEMFC model is used to validate voltage degradation predictions against observed degradation from the literature. Additionally it can be used to integrate the degradation model and therefore have a more accurate relationship between degradation and operational performance. As can be seen in Figure 8 & 10, the initial activation range of the polarisation curve does not match up correctly.

Due to the fuel cell model developed, this area can be modified due to SSC and take into account degradation in different regions of the polarization curve through an integration the two models. The result would be capable of plotting polarisation data from key operational inputs of the polarization model, fed into the degradation model.

Currently the degradation model needs operating data in the form of initial inputs from the user. That is to say that operating voltage is set from the outset. Integration into a PEMFC performance model will allow the performance model to output operational data into the degradation Petri-Net model for its inputs. Then after running the Petri-Net model, the outputs would feed back into the performance model. As the process continues, degradation, and its effect on the performance of the cell can be accurately ascertained. Not only does integration with a PEMFC performance model mean more accurate degradation modelling, it also means that PEMFC operational load levels (such as drive cycles) can be preset, and the degradation due to the fluctuation in load (and therefore temperature etc.) can be considered.

ACKNOWLEDGEMENTS

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) and the Doctoral Training Centre in Hydrogen Fuel Cells and Their Applications.

REFERENCES

Borup, R. et al. 2007 Scientific aspects of polymer electrolyte fuel cell durability and degradation, *Chemical reviews, vol. 107, no. 10*, 3904–3951.

Business Enterprise and Regulatory Reform BERR, 2006 Dti energy price scenarios in the oxford models, *BERR, Tech. Rep.*

Department for Energy and Climate Change DECC 2011 2012 UK greenhouse gas emissions, provisional figures and 2011 UK greenhouse gas emissions, final figures by fuel type and end-user, *DECC, Tech. Rep.*

Department for Transport, 2010 Factsheets: UK transport greenhouse gas emissions, *DfT, Tech. Rep.*

Hong Kim, J. et al. 2010 Effects of Cathode Inlet Relative Humidity on PEMFC Durability during Startup-Shutdown Cycling *Journal of The Electrochemical Society, vol. 157*, no.1, 104–112.

Kandlikar, S.G. & Lu, Z., 2009. Thermal management issues in a PEMFC stack—A brief review of current status. App. Therm. Eng., 29, 7, 1276–1280.

LaConti, A. et al. 2003 *Handbook of Fuel Cells: Fundemental, Technology, and Applications., vol. 3*.

Liu, T. & Chiou. S. 1997 The application of Petri nets to failure analysis *Journal of Reliability Engineering and System Safety, vol. 57, no. 2*, pp. 129.

Placca. L & Kouta, R. 2011 Fault tree analysis for pem fuel cell degradation process modelling, *International Journal of Hydrogen Energy, vol. 36, no. 19*, 12 393–12 405.

Pozio, A. et al. 2003 Nafion degradation in pefcs from end plate iron contamination, *Electrochimica Acta, vol. 48, no. 11*, 1543–1549.

Rama, P. et al. 2008 A review of performance degradation and failure modes for hydrogen fuelled polymer electrolyte fuel cells, *Proceedings of the Institution of Mechanical Engineers, Part A: Journal of Power and Energy, vol. 222, no. 5*, 4214–441.

Solomon, S. et al. 2007 Summary for policymakers. in: Climate change 2007: *The physical science basis. contribution of working group i to the fourth assessment report of the intergovernmental panel on climate change*, Cambridge University Press, Tech. Rep.

Whiteley, M. et al. 2013a Enhanced fault tree analysis and modelling considerations of a polymer electrolyte membrane fuel cell, in *Proceedings of the European Safety and Reliability Conference, ESREL*. CRC Press, 29/09/2013. 603.

Whiteley, M. et al. 2013b Fault tree analysis of polymer electrolyte fuel cells to predict degradation phenomenon, in *Proceedings of the 20th Advances in Risk and Reliability Technology Symposium. Loughborough University*, 21/05/2013. 75–89.

Wieland, C. et al. 2009 Reliability computing of polymer electrolyte membrane fuel cell stacks through petri nets, *Journal of Power Sources, vol. 190, no. 1*. 34–39.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Analysis of ship navigation behaviors in the Wuhan Yangtze River Bridge waterway

Xu Chen
School of Logistics Engineering, Wuhan University of Technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

Lingzhi Sang & Zhe Mao
Intelligent Transportation System Research Center, Wuhan University of technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

Qing Wu
School of Logistics Engineering, Wuhan University of Technology, Wuhan, P.R.China
Engineering Research Center of Transportation Safety, Ministry of Education, Wuhan, P.R.China

ABSTRACT: Aiming to find out the navigation method and voyage patterns of ships in the Wuhan Yangtze River Bridge Waterway, and to provide a theoretical basis for vessel traffic flow evolution and safety risk assessment in bridge waterway, ship navigation behaviors need to be analyzed to assist in the authority supervising. The waterway around the Wuhan Yangtze River Bridge is selected, in which the ships' information is received and stored by three AIS based stations to analysis the ship navigation behaviors when passing the bridge. The characteristics of navigation behaviors are statistically analyzed with the collected AIS data, and the distribution function models for ship's behaviors are built as well as a hypothesis testing. In the meanwhile, the basic traffic trajectory of ship could be simulated to pass this bridge clearly.

1 INTRODUCTION

The inland waterway combines the inland area, coastal ports and other major cities together as a transport network (Tak and Ligteringen 2010). With the development of the waterway transport and the increasing number and carrying capacity of ships, the navigation conditions have been changed dramatically (Pan 2010). In the meanwhile, ship accidents occur frequently because of intensive traffic flow and narrow waterways (Dai 2003, Qu 2011). In China, the Yangtze River connects the eastern, the central and the western regions, and plays an irreplaceable role in supporting economic and social development along the river (Tao 2013). However, in the past decades, large areas of shoals with deposition in the Wuhan section of the Yangtze River waterway leads the central channel of the Wuhan Port to become narrower, which affects the navigable holes, worsens the navigation conditions and minifies the area of navigable channel (Ingo 2000). The Wuhan Maritime Safety Administration adjusted the bridge opening mark (lights), pillar lights and other identifiers of the Wuhan Yangtze River Bridge (Figure1) to keep navigation safety. Besides, some other factors have led the bridge to be bottlenecks in the middle reaches of the Yangtze River. The analysis of inland navigable accidents, traffic trend and traffic distribution is based on AIS information, which receives real time navigation information from AIS base stations. And it provides advice for the safety



Figure 1. The Wuhan Yangtze River Bridge.

of ship navigation in the bridge waterway (Yan 2010, Li 2007, Jin 2012, Xiao 2012).

The basic data, received from AIS stations, has been processed effectively to determine the four possible ship steering regions near the Wuhan Yangtze River Bridge. In this paper, the distribution function model for each ship steering region is built with a hypothesis testing based on the analysis of the regions.

2 DATA COLLECTING AND PROCESSING

2.1 *Data collecting*

To receive the real-time information of ships that passing the Wuhan Yangtze River Bridge, three AIS base stations (Figure 2) were installed near the waterway of the bridge.

In this paper, the data was collected during the flood period in July 2012. Due to the influence of uncertain factors in the process of transmission and reception, some information of ships were lost. Consequently, the information of 672 ships was collected, 423 of them was actually available.

2.2 *Data categorization*

From the beginning in May 2012, the water level of Hankou kept rising, the Wuhan Maritime Safety Administration adjusted the navigable holes of the bridge in order to ensure the navigation safety of ships in the waterway near the Wuhan Yangtze River Bridge. After that, the 4th navigable hole replaced the 5th for the upstream ship, while the 6th navigable hole remained the same. At the same time, the 2nd navigable hole was opened for ferries, and also the culverts standards (lights), pillar lights were adjusted accordingly.



Figure 2. AIS base station.

Depending on the different navigable holes for ship navigation, itineraries are divided into three categories: the 2nd navigable hole for upstream ferries, the 4th navigable hole for normally upstream ships and the 6th navigable hole for downstream ships. The ratio of them is shown in Figure 3.

As can be seen, the ratio of the first kind of ship itinerary is 8.75%, the second is 46.81%, and the third is 44.44%. That is, a few ships navigate through the 2nd navigable hole to pass the bridge. Therefore, the 2nd navigable hole is not taken into account.

In Wuhan section, the course angle of the downstream ship is in [0°, 90°], while that of the upstream ship is in [180°, 270°]. Combing with latitudinal and longitudinal location where the ship is, the itinerary has been identified. The 423 ships available are selected to study, and 235 of them are upstream ships, 188 of them are downstream ships. The distribution of ship itineraries is shown in Figure 4.

As is shown, the ship itineraries are almost straightly when passing the 2nd and the 6th, while the ship itineraries of the 4th have been changed obviously. As a result, curvilinear itineraries are

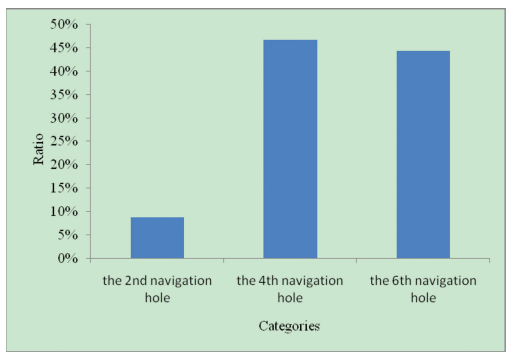


Figure 3. Ratio of three categories.

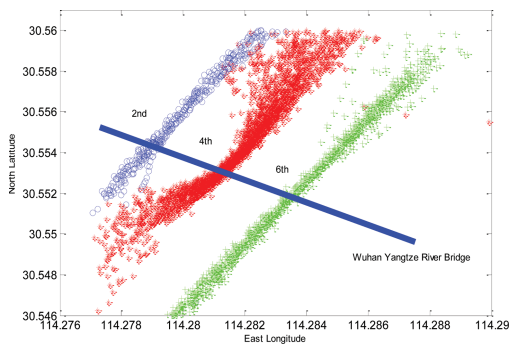


Figure 4. Ship itineraries distribution of the selected data.

formed because of ship navigation behaviors. Therefore, this paper mainly deals with the information of ships that go through the 4th navigable hole to pass the bridge.

2.3 *The first selection of data*

As is shown in Figure 5, the upstream ship that through the 4th navigable hole is generally sailing in tranquil flow at edge of the fairway before region A. After getting closed to the navigable hole, the ship's position will be adjusted gradually because of the navigation behaviors in region A during a period of time. When the ship navigates into region B, the first positional adjustment has been completed, and ship will be back to keep straightly navigating into region C for passing the bridge. Then the position will be adjusted again and approaching to the region D. Finally, the ship returns to navigate normally.

It is possible for the upstream ship to steering within region A, B, C and D. When a ship navigates through the bridge, the curvilinear itinerary will be formed because of the ship's navigation behaviors within A, B, C and D four regions. According to the pattern of ship's navigation, the points within region A, B, C and D will be selected. Taking region A as an example, when a ship navigates straightly before region A, and it will navigate into region A next, the slope of ship trajectory will be changed significantly, and it can be calculated as follow.

$$k = \frac{\Delta_{lat}}{\Delta_{lon}} \tag{1}$$

where Δ_{lat} = latitudinal variation value; and Δ_{lon} = longitudinal variation value.

To judge the ship is navigating normally when the slope changed significantly, a constraint is added as follow.

$$\Delta_1 \times \Delta_2 > 0 \tag{2}$$

The constraint is used to ensure that the direction of changed slope of ship itinerary keeps consistent when ship is navigating, and also delete abnormal points caused by position drift.

$$\begin{cases} \Delta_1 = k_{i+1} - k_i \\ \Delta_2 = k_{i+2} - k_{i+1} \end{cases} \tag{3}$$

Where k_i = the rate of slope in i-th ship's position.

2.4 *The second selection of data*

The emergence of redundant points is inevitable, though we have done our best to reduce that. The positional points within A, B, C, and D four regions are selected roughly by using the first selection method. Consequently, the result is not accurate for our study. Hence, the data should be selected for the second time. As is shown in Figure 5, the slopes of region A, B, C and D have been changed significantly during a period of time when a ship navigates into the waterway. Then the first point of the slope is regarded as available, thus deleting other points which are accordance with the first selection method. Similarly, the points within region B, C and D are selected. Putting the positional points into 8 independent regions to analyze the navigating behaviors of ship.

3 DISTRIBUTION OF SHIP POSITON

3.1 *Distribution function model and hypothesis testing*

After completing data classification, distribution models are built through analyzing frequency histogram of each region, and verified through the t-test. The result is shown as follows.

The longitudinal distribution of region A is shown in Figure 6.

The longitudinal distribution of region A obeys the normal distribution. Through t-test, the

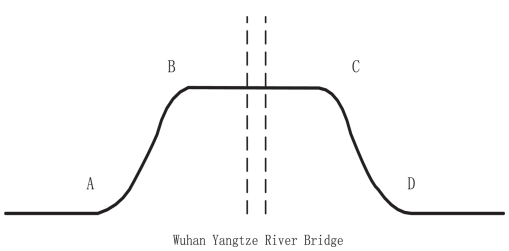


Figure 5. Ship trajectory in special region.

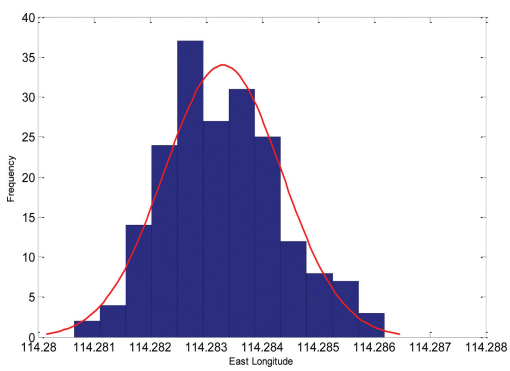


Figure 6. Longitudinal distribution of region A.

value of expectation μ = 114.2833, "the variance σ = 0.0011" the confidence coefficient above 95% is [114.2832; 114.2835]

The latitudinal distribution of region A is shown in Figure 7.

The latitudinal distribution does not obey the normal distribution in region A. On the basis of observation, the linear equation is fitted by using the method of linear least squares.

$$y = 0.0505312 \times 10^5 \times x - 1.5438476 \times 10^5 \quad (4)$$

Where x = the latitudinal average of region A in a range of frequency, and y = the frequency accordingly.

The longitudinal distribution of region B is shown in Figure 8.

The longitudinal distribution of region B obeys the normal distribution. Through t-test, the value of expectation μ = 114.2822, the variance σ = 0.00091, the confidence coefficient above 95% is [114.2821; 114.2823].

The latitudinal distribution of region B is shown in Figure 9.

The latitudinal distribution of region B obeys the normal distribution. Through t-test, the value of expectation μ = 30.5547, the variance σ = 0.0014, the confidence coefficient above 95% is [30.5545, 30.5549].

The longitudinal distribution of region C is shown in Figure 10.

The longitudinal distribution of the ship when it navigates into region C obeys the normal distribution. Through t-test, the value of expectation μ = 114.2811, the variance σ = 0.00096, the confidence coefficient above 95% is [114.2810, 114.2813].

The latitudinal distribution of region C is shown in Figure 11.

The latitudinal distribution of region C obeys the normal distribution. Through t-test, the value of expectation μ = 30.5531, the variance σ = 0.0012, the confidence coefficient above 95% is [30.5529, 30.5533].

The longitudinal distribution of region C is shown in Figure 12.

The longitudinal distribution of the ship when it navigates into region D obeys the normal distribution. Through t-test, the value of expectation μ = 114.2798, the variance σ = 0.0012, the confidence coefficient above 95% is [114.2796, 114.2799].

The latitudinal distribution of region C is shown in Figure 13

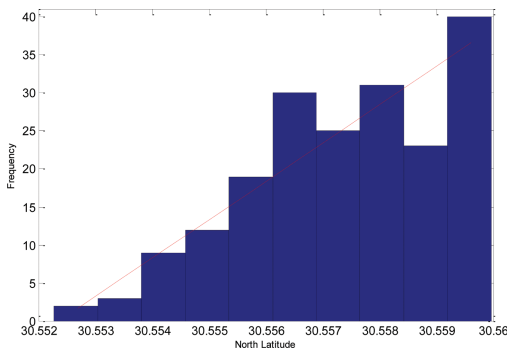


Figure 7. Latitudinal distribution of region A.

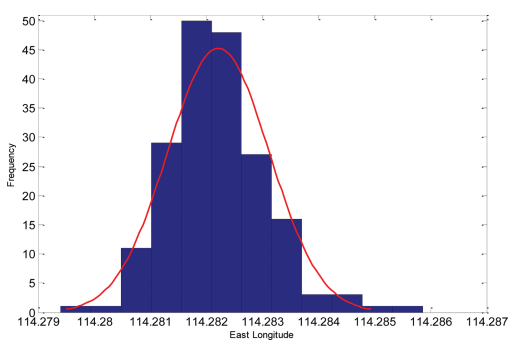


Figure 8. Longitudinal distribution of region B.

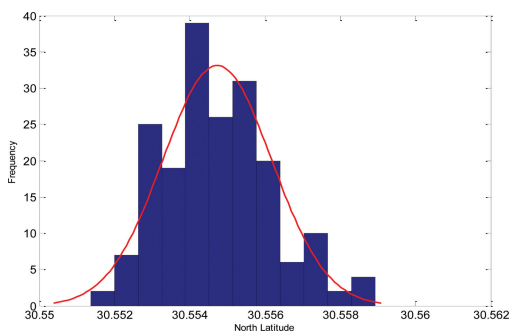


Figure 9. Latitudinal distribution of region B.

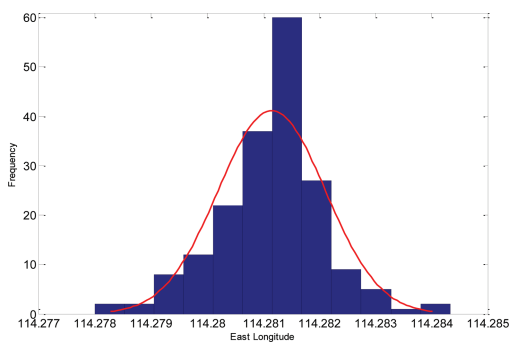


Figure 10. Longitudinal distribution of region C.

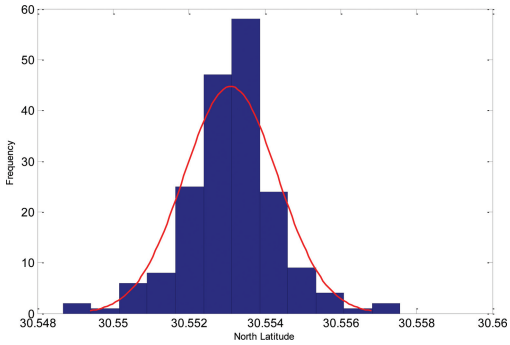


Figure 11. Latitudinal distribution of region C.

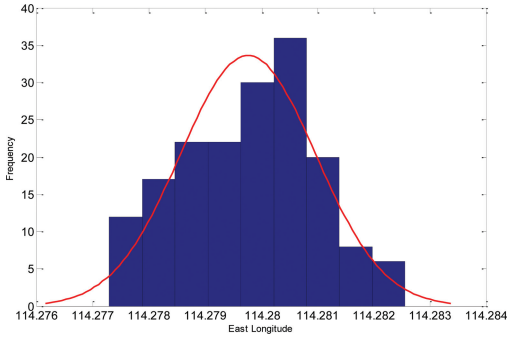


Figure 12. Longitudinal distribution of region D.

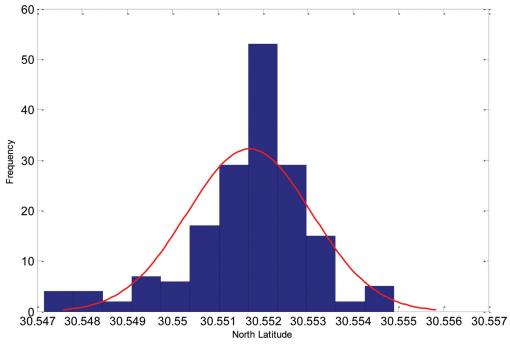


Figure 13. Latitudinal distribution of region D.

The latitudinal distribution of region D obeys the normal distribution. Through t-test, the value of expectation $\mu = 30.5517$, the variance $\sigma = 0.0014$, the confidence coefficient above 95% is [30.5515, 30.5519].

3.2 *A ship-bridge behavioral simulation case*

The simulation data is generated from the longitudinal and latitudinal distribution models, and the result is shown in Figure 14.

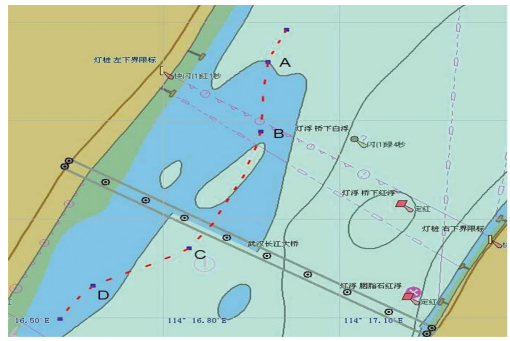


Figure 14. A simulation example.

As is shown, the trajectory is in accordance with the positions of ship steering regions as well as the special location distribution of ship navigation behaviors.

4 CONCLUSION

Upstream and downstream ships go though the Wuhan Yangtze River Bridge from three navigable holes. In order to analyze the navigation method and voyage patterns of ship, AIS information is received from three AIS base stations to analyze the ship navigation behaviors. The paper statistically analyzes the AIS data of ships which go through the Wuhan Yangtze River Bridge, and find out four possible regions for the ship navigation safety. The distribution function models are built and verified by using the t-test. The result shows that only the latitudinal distribution of region A obeys the least squares linear distribution, while the longitudinal and latitudinal distribution of other regions obeys the normal distribution. Finally, simulation is based on the distribution models to verify the models for ship navigation behaviors, which provides a kind of navigational route for the crews to ensure the navigation safety in this waterway.

ACKNOWLEDGEMENTS

This paper is supported by Western Communications Construction, Scientific and Technological Project of Ministry of Transportation of the People's Republic of China (Grant No. 201132820190), Natural Science Foundation of Hubei Province, China (Grant No. 51309187), and FP7 Marie Curie IRSES of European Union (Grant No.314836).

REFERENCES

Dai, T., & Nie, W. (2003). Overview of the vessel bump bridge accident. Communications Science and Technology Heilongjiang, 26(2), 1–3.

Ingo Harre. 2000. AIS Adding New Quality to VTS Systems. *The Journal of Navigation* 53(03):527–539.

Jin, X., Fu, Y., & Zhang, L. (2012). Research on vessel traffic flow at Chengshantou water region based on AIS Data. *Journal of Dalian Maritime University*, 38(1), 33–36.

Li Xudong, Hu Shenping. 2007. Application of AIS information analysis in ship collision cases. *Journal of Shanghai Maritime University* (01): 132–136.

Mou, J.M., Tak, C.V.D., & Ligteringen, H. (2010). Study on collision avoidance in busy waterways by using AIS data. *Ocean Engineering*, *37*(5), 483–490.

Pan, M.Y., Zhang, B., & Hu, J.F. (2010, October). Research on web-based ship navigation system. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Vol. 11, pp. V11–422). IEEE.

Qu, X., Meng, Q. & Suyi, L. (2011). Ship collision risk assessment for the Singapore Strait. *Accident Analysis & Prevention*,*43*(6), 2030–2036.

Tao Y, Zhang S. 2013. Environmental efficiency of electric power industry in the Yangtze River Delta. *Mathematical and Computer Modelling* 58(5): 927–935.

Xiao, F., Ligteringen, H., van Gulijk, C., & Ale, B. (2012). Artificial force fields for multi-agent simulations of maritime traffic: a case study of Chinese waterway. *Procedia Engineering*, 45, 807–814.

Yan, X.P., Ma, F., Chu, X.M., & Chen, C. (2010). Key technology of collecting traffic flow on the yangtze river in real-time. *Navigation of China,* 33(2), 40–45 *(in Chinese)*.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A novel methodology for availability assessment of complex load sharing systems

F. Kristjanpoller & P. Viveros
Department of Industrial Engineering, Universidad Técnica Federico Santa María, Valparaiso, Chile
Department of Industrial Management, School of Engineering, University of Seville, Seville, Spain

A. Crespo
Department of Industrial Management, School of Engineering, University of Seville, Seville, Spain

R. Mena
European Foundation for New Energy-Electricity of France at Central School of Paris-Supelec, Paris, France

R. Stegmaier
Department of Industrial Engineering, Universidad Técnica Federico Santa María, Valparaiso, Chile

ABSTRACT: The methodology for availability assessment of complex systems accounting for load sharing configurations with overcapacity and flexible work levels, allow the possibility that all the equipment have different failure behavior. This methodology is based on event space method, considering the matrix modeling for multistate and dynamic impact evaluation, and the result is expressed as an equivalent availability. At the literature there are models that develop the overcapacity problem, but only for identical equipment and without the multistate work level; others allow the modeling of multistate characteristic but avoid the overcapacity evaluation. This situation is commonly present in continuous process industries with important transportation systems, like mining, steel, paper and wood. The case study based on mining trucks availability modeling to optimize the fleet sizing, show the benefits and summarizes the application, obtaining relevant results to develop a expedite decision making process over reliability and availability indicators. The usage of the simulation model, as a bench tool, validated the proposed methodology.

1 INTRODUCTION

In last years, the process flexibility and productivity is a goal to improve the process efficiency and the overall company results. In this context, the dynamic systems have reached a great level of importance for the productive process modelling.

The dynamic systems are those which change in time. In the case of components and its configuration in a system, dependencies, redundancies and the load they bear, which can be shared, varies in time, that is to say, its dependency relations can change with the environment or change its ability to function in different scenarios. The modelling methods like Reliability Block Diagram (RBD) (Barlow 1996, Birolini 2004) and Failure Tree (FT) (Birolini 2004) have different limits to represent these systems, in the case of RBD it presents restrictions with respect to the dependencies and the large complex systems (Macchi 2009).

For the representation of the dynamic systems, different methodologies will be shown below.

Macchi et al. (Macchi 2014) presents a special analysis for buffer (RBD) showing the possibility to make flexible the structure for a dynamic system. Although some of these restrictions are treated by the method of Dynamic Fault Tree (DFT), particularly the shared load case is not modelled through the FT neither through the DFT[5], although have appeared tools that have enriched them, they are not represented appropriately.

A new named model dynamic reliability block diagram (DRBD), is presented by two publications, S. Distefano, L. Xing (Distafano 2006) and by Xu, L. Xing and R. Robidoux 2009 (Xu 2009) both of

them present two ways of applying and schematize the DRBD, though in both is L. Xing, the last one presents a simpler way than the first work.

S. Distefano, L. Xing (Distefano 2006), introduce some features that may be of special interest, as three patterns of state stand-by and three types of dependency. If one component depends on various other components it can produce an attendance conflict which is solved by a discrimination manner due to a hierarchical level of priorities.

For the analysis of one DRBD there are various alternatives within the literature (Manian 2006, Trivedi 1996, Trivedi 1996, Trivedi 1996):

1. Markov Chains: Where the limit are the few reliability distributions that can be analyzed.
2. Petri nets: Where the redundancies and shared load are tailored.
3. Simulations: Where any distribution can be tailored, Montecarlo technique is one of the most ex-plored.

The other way to present DRBD is one introduced by H.Xu, L. Xing and R.Robidoux 2009 (Xu 2009) previously worked only by the first ones in 2007 (Haiping 2007) where show the DRBD as a system that tailor and catch the dynamic relations between components as dependence states as well as redundancy state, they suggest a simple way and tailor a particular case. For checking, it is transferred to a Petri net model colored by a software support which certifies the correct design of the DRBD.

With respect to works related with resolutions of systems availability of shared load, solved by Mar-kov chains, we can find Shendao et al. (Shengdao 2005), where though there are variable failure rates in time, we find again the explosion state-space. It is calculated the availability of a charge load system with variable failure rates solving different equations, however it is required algebraic operations that depend of the size of the system, since for large systems it becomes a huge problem.

Akthar (Akthar 1994) also contributes respect to this same resolution method, although he considers identical equipment, he adds a new feature, cover the failure in an imperfect manner (that is to say there are failures that are impossible to repair).

Due to the inexistence of description of divided systems, it will be used as basis the system k-out-of-N:G/Load Sharing described in the bibliography and that will have the divided load characteristic.

One of the advances in the model system with DRBD and its validation it is made by Distefano and Puliafito (Distefano 2009) where they analyze three study cases, however, although they make great advances, these must be translated to the OPENSesame system to be validated, where some features cannot be introduced and there appears the lack of a special software.

Similar to the above is what considers Scheuer (Scheuer 1988), who studies the reliability for a k-out-of-n:G system where he holds that in basis to previous studies made by Kapur and Lamberson (Karpur 1997) that when there is a component failure, then there is a higher failure in the surviving ones, however it is for identical components with constant failure rates, similar to made by Shao & Lamberson (Shao 1991) where it is also used identical components but with an imperfect switching and it is used for few components due to it is carried out in Markov chains basis.

Jenab y Dhillon (Jenab 2006) grant a form to analyze not only the reliability and availability of a k-out-of-n system but also for reversible multistate systems, that is to say they can change from state i to i+1 in addition it gives the suggestion that all the compo-nents are identical and independent. Something at a short rate but similar to the former study is made by Hasset, Dietrich and Szidarovsky (Hessett 1995) who investigated the reliability and availability of systems 1 of 2 reparable, both components statistically identical with variable failure rate.

On the other hand, Liu (Liu 1998) introduces a pattern to calculate the reliability of shared load systems k-out-of-n, with non-identical components and general distributions (Weibull, Gaussian, lognormal and Gamma), something similar to intended to do, however due to complex scenario and suggested solution, is not possible the resolution for n> = 5 and with k n-3, however taking these elements, is probable to have some results for higher n.

Amari et al. (Amari 2007) develop a solution through Markov chains where it is indicated that the maximum of the components must be 16, nevertheless they analyze a problem of maximum three components, although tips are given to increase the efficiency of the computational resolution. It applies for exponential distributions and for general distributions, is possible to indicate the suggestion that all failure rates are the same when these vary with t time when elements j fails. Nevertheless this choice can be viable with respect to the problem set up, it considers that the load is delivered in the same way on the surviving elements, something that is not sure to happen due to the capacity of each one and though certain rules of the shared load could relax, we can indicate that when the components are not identical each sequence of failure must be analyzed separately and yet this must be studied for the general case.

2 PROBLEM STATEMENT

Transport systems are characterized usually for its flexibility, huge quantity of equipment and application. In effect the feature of load sharing, allows obtaining the required capacity on the basis of the sum of the available equipment even operating in a lower load than required. The case of overcapacity is characterized by having more capacity installed than required, by which there exists a series of combinations that allow satisfy the required capacity. The above condition requires that the equipment can operate at different work levels. As a conclusion of this problem, we can set up that the impact of each component is variable and depends on its required load as well as its reliability and maintainability behavior, as so also of the characteristics of each one of the equipment that constitutes the system. For the previously situation mentioned above, the availability assessment is a complex system to carry out and follow up it is proposed a methodology for its validation.

3 PROPOSITION FOR METHODOLOGY

Here is present the proposed methodology together with defined variables

i. Variables and Nomenclature
ii. Modeling

Assumption 1:

All equipment in the systems has two possible operating states, (1) operating, (0) unavailable. Under the assumption 1, the first step is to obtain all the possible combinations of operating states,

Table 1. Glossary.

Id	Description
E	set of equipment
nE	$\|E\|$ total number of equipment
i	index of equipment $\in \{1, \ldots, n_E\}$
S	set of operating states of the system
nS	$\|S\|$ total number of possible operating states of the system
j	index of operating states $\in \{1, \ldots, n_S\}$
A	Availability
C_S^R	system required capacity
C^{Max}	maximum capacity
C^A	Available capacity
C^O	Operating capacity
P^A	Availability-based probability
I	Impact
δ	Matrix of possible combinations of operating states
n_{zeros}	Number of zeros $\in \{1, \ldots, n_E\}$

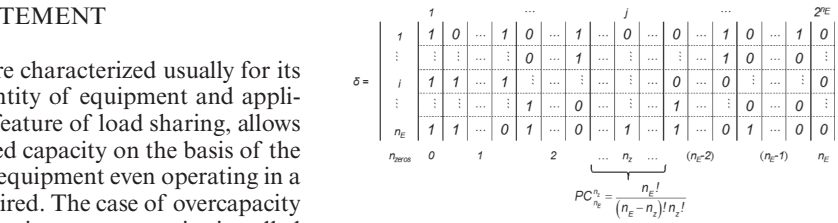


Figure 1. Possible combinations of operating states.

given the total number of equipment in the system. As the operating states are binary, the total number of operating states of the system is 2^{nE}.

Considering one operating state combination $j \in \{1, \ldots, 2^{nE}\}$ of the system, the corresponding binary variables to visualize the individual operating state of each equipment are defined as follows:

$$\delta_{ij} = \begin{cases} 1 & \text{if equipment i is in operating state} \\ 0 & \text{if equipment i is unavailable} \end{cases} \quad \forall i \in \{1, \ldots, n_E\} \tag{1}$$

From the matrix δ, we obtain the available capacity for each operating state combination:

$$C^A{}_j = \sum_{i=1}^{n_E} \delta_{ij} \times C^{\max}{}_i \quad \forall j \in \left\{1, \ldots, 2^{n_E}\right\} \tag{2}$$

Assumption 2:

Given a systemic operating state j, the proportion between the operating capacities of the corresponding equipment $C^O{}_{ij}$ and the maximum equipment capacity $C^{\max}{}_i$ must be the same for all equipment.

To determine the final impact of each equipment, we need to identify the systemic operating states j for which the available capacity of the equipment is less or equal than the required capacity of the system (otherwise the impact is defined *0* since the system is able to satisfy the requirement of capacity).

Then, we define the binary variable ω_j as follows,

$$\omega_j = \begin{cases} 1 & C^A{}_j \geq C^R{}_S \\ 0 & Otherwise \end{cases} \quad \forall j \in \left\{1, \ldots, 2^{n_E}\right\} \tag{3}$$

Then, the operating capacities of the equipment $C^O{}_{ij}$ are:

$$C^O{}_{ij} = \frac{\left(\omega_j \times C_S{}^R + \left(1 - \omega_j\right) \times C^A{}_j\right) \times \delta_{ij} \times C_i^{\max}}{C_i^{\max} + \sum_{k=1 \wedge k \neq i}^{n_E} \delta_{kj} \times C^{\max}{}_k} \quad \begin{array}{l} \forall i \in \{1, \ldots, n_E\}, \\ j \in \left\{1, \ldots, 2^{n_E}\right\} \end{array} \tag{4}$$

When the calculation of the impacts is applicable ($C^R{}_S > C^A{}_j$), the systemic operating state $j = 1$ for which all the equipment are in operating state is considered as the state of reference. The objective is to determine the loss of capacity that the unavailable equipment produces over the system as a function of the operating capacity if that equipment were operating. The formulation of the impact is:

$$I_{ij} = \begin{cases} \dfrac{\left(C^R{}_S - C^A{}_j\right) \times \left(1 - \delta_{ij}\right) \times C^O{}_{i1}}{C^R{}_S \times \sum_{k=1}^{n_E} \left(1 - \delta_{kj}\right) \times C^O{}_{k1}} & C^R{}_S > C^A{}_j \quad \forall i \in \{2,...,n_E\}, \\ & \qquad j \in \{2,...,2^{n_E}\} \\ 0 & Otherwise \end{cases} \tag{5}$$

Assumption 3:

Under systemic operating state $j = 1$ the required capacity is always satisfied.

Then, the availability-based probability of each systemic operating state is defined as follows:

$$P_j{}^A = \prod_{i=1}^{n_E} A^{\delta_{ij}}{}_i \times \left(1 - A_j\right)^{\left(1-\delta_{ij}\right)} \quad j \in \left\{1,...,2^{n_E}\right\} \tag{6}$$

Finally, the weighed impact for each equipment, considering all the possible combinations for the system operating state is:

$$I_i^W = \sum_{j=1}^{2^{n_E}} P_j{}^A \times I_{ij} \quad i \in \{1,...,n_E\} \tag{7}$$

4 CASE STUDY

A company of the great copper mining in Chile requires a transport of an average of 5,200 tons each hour (C_S^R), from the mine to the concentrated plant. This material has between 0.5–1.1% of copper. The transportation system is composed by 20 trucks, of 4 different models, for capacity, manufacturer and antiquity. For each truck, in an independent way, it has obtained its reliability and maintenance data, calculating its main maintenance indexes like: MTBF (Mean Time Between Failure) and MTTR (Mean and Time to repair) respectively.

The expected Availability (A_i) is calculated as shown on equation 8. (Sharma 2008):

$$A_i = \frac{MTBF_i}{MTBF_i + MTTR_i} \tag{8}$$

The Table 2 summarizes the information obtained for each truck and includes the analysis of the individual availability.

As deducted from the information presented, the maximum capacity of the system C^{max} is of 5.590 tons, corresponding to the addition of each individual capacity, which indicates that there is a load sharing system with overcapacity. Additionally, checking the reliability information we can establish that all the equipment has different data and its capacity is in relation with the type classification.

As mentioned above, it can be validated that we are in presence of a load sharing system, overcapacity and flexible work level.

To P_{system}^A (Availability-based probability) determination will use the methodology proposed on point 3.

As first step, the total number of operating states is 1,048,576 states. For example, the state number 96,800 is characterized by 12 available trucks (1, 2, 3, 4, 5, 7, 9, 11, 13, 15, 17, 19), that appears with "1"; and 8 unavailable trucks (6, 8, 10, 12, 14, 16, 18) that appears with "0". In this step, the available capacity is 3,380 tons, that represents an P_j^A equal to 0.6047, as the system has an availability of 60.47% of the time, but this state has only a 3,428E-09 of occurrence probability.

Consolidating the results of each of the 1,048,576 states, the global results obtained indicates an P_{system}^A equal to 0.8955, as the system in each impact over P_{system}^A.

Scenario1: Base case has an equivalent availability of 89.55%.

2.1 *Sensibilization analysis*

- To evaluate and sensibilize the results of the base case, 4 scenarios of improvement will design through the acquirement of new equipment, evaluating
- Scenario 2: Acquisition of 2 new Trucks-Type A (the data given is of the best of the type, which is N°4)
- Scenario 3: Acquisition of 2 new trucks Type B (the data given is of the best of the type which is N°7)
- Scenario 4: Acquisition of 3 new trucks type C (the data given is one of the best of the type, which is N°17)
- Scenario 5: Acquisition of 3 new trucks Type D (the data given is one of the best of the type which is N°20).

The results obtained are shown as follows:

The analysis of the results is very interesting, it is established that the only important is not the number of trucks and the C^{MAX} for the increasing of P_{system}^A, but also the specific values of the A_i of the added equipment, have a relevant impact over the system indicator.

Table 2. Reliability and availability data.

Truck	Type	Capacity (tons)	MTBF	MTTR	Ai
1	A	300	156,4	23,2	0,8708
2	A	300	173,2	26,4	0,8677
3	A	300	168,4	22,5	0,8821
4	A	300	177,3	19,8	0,8995
5	B	350	116,3	27,3	0,8099
6	B	350	125,9	24,1	0,8393
7	B	350	148,7	26,5	0,8487
8	B	350	112,6	30,8	0,7852
9	B	350	151,8	28,5	0,8419
10	B	350	127,3	34,1	0,7887
11	C	220	188,4	14,3	0,9295
12	C	220	178,3	17,5	0,9106
13	C	220	182,9	12,6	0,9355
14	C	220	167,2	11,6	0,9351
15	C	220	159,3	18,4	0,8965
16	C	220	174,2	15,9	0,9164
17	C	220	183,3	9,6	0,9502
18	D	250	203,6	14,6	0,9331
19	D	250	208,5	17,4	0,9230
20	D	250	210,6	13,7	0,9389

Table 3. Scenarios results for the indicator P^{A}_{system}.

Id	Esc 1	Esc 2	Esc 3	Esc 4	Esc 5
C^{R}_{S}	5,200	5,200	5,200	5,200	5,200
C^{MAX}	5,590	6,190	6,290	6,250	6,340
P^{A}_{system}	0.8955	0.9247	0.9220	0.9336	0.9408

To validate the results obtained for the P^{A}_{system}, it was developed a simulation method Montecarlo in order to calculate the availability (Khan 1995). The base for simulations is the states that equipment can take, as described in the Modeling Assumption 1. For this effect, simulations with 100,000; 200,000; and 300,000 iterations are developed with the objective of evaluate the impact of each model over the analytic resolution.

As we can appreciate in the Fig. 2 the deviations obtained respect to the analytic value are extremely low, the maximum deviation is for the Scenario 1 with the model of 100.000 iterations achieving only 0.067% which indicates a high grade of precision of the availability values P^{A}_{system}

To evaluate each one of the models in a more precise way, it is developed the analysis of the absolute deviation, in this case the mean values are:

As we can appreciate in the Fig. 3, increasing the number of iterations the MAD decreases, which implies that the proposed value for P^{A}_{system} as also its methodology of calculus have been validated.

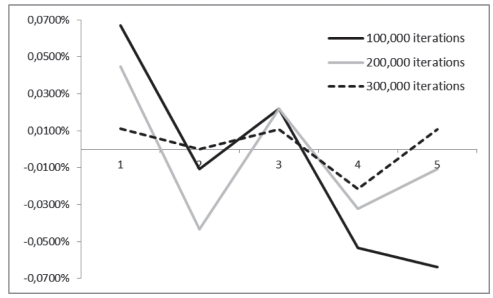


Figure 2. Bench tool deviation from analytical system availability.

Table 4. MAD evaluation for simulation.

Test	Mean Absolute Deviation MAD
100,000 iterations	0.043%
200,000 iterations	0.031%
300,000 iterations	0.011%

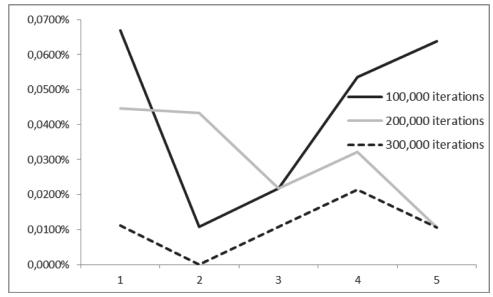


Figure 3. Bench tool absolute deviation from analytical system availability.

5 CONCLUSIONS AND DISCUSSION

It was effectively generated a methodology for the availability assessment of complex systems accounting for load sharing configurations with overcapacity and flexible work levels, presenting its understanding and proving its application in a practical case obtaining positive results in both cases.

In order to implement and compare the results it was developed the analytic application of the methodology with a sensible analysis and with improvement scenarios.

As a result of the earlier, we can establish that the proposed methodology has been validated through the comparison with simulation model such as bench tool since the detected differences between both models exceed a MAD 0.011% for the model with 300.000 iterations.

The case study through the evaluation of the five scenarios (basis case and four of improvements) permits the evaluation of the real impact of rising up the quantity of trucks for the process. The comparison between the scenario 2 and scenario 3 shows that not always the increasing of capacity obtains results in the availability assessment of the system.

In that case there is more impact about the quality of improvement, associated to the availability of the trucks, than the quantity associated to the capacity of the trucks.

Indubitably, we can conclude that the methodology developed is a contribution to model the availability of systems of transport, suggesting an analysis of the evaluation of her, flexible and precise.

As a future step, is thought the possibility to incorporate economic variables to evaluate the scenarios and in this way to determine the profits in the OPEX through the improvement of the availability, versus the costs included in the CAPEX in order to finance these projects.

REFERENCES

Akhtar, Shaki. Reliability of k-out-of-n: G Systems with imperfect Fault-Coverage. IEEE Transactions on reliability, vol. 43, no. 1, 1994.

Amari V., Misra K.B. & Pham H. Tampered Failure Rate Load-Sharing Systems: Status and Perspectives. Chapter 20 in Handbook on Performability Engineering. Springer, 2007.

Barlow R. & Proschan F. Mathematical Theory of Reliability. Philadelphia: Society for Industrial and Applied Mathematics; 1996.

Birolini A. Reliability Engineering: Theory and Practice. Berlin: Springer-Verlag; 2004.

Distefano Salvatore & Antonio Puliafito. Reliability and availability analysis of dependent–dynamic systems with DRBDs. Reliability Engineering and System Safety 94(2009)1381–1393.

Distefano S. & Xing Liudong. A New Approach to Modeling the System Reliability: Dynamic Reliability Block Diagrams. Reliability and Maintainability Symposium. RAMS Annual, Newport Beach, CA, USA. 2006.

Haiping Xu & Liudong Xing. Formal semantics and verification of dynamic reliability block diagrams for system reliability modeling. Proceedings of the 11th IASTED international conference, november, 2007. Cambridge, MA, USA.

Hassett T.F., Dietrich D.L. & Szidarovszky F. Time varying failure rates in the availability and reliability analysis of repairable system. IEEE Duns. Reliability, 1995, Mar, pp 155–160, Vol. 44.

Huamin, Liu. Reliability of a Load-Sharing k-out-of-n:G System: Non-iid Components with Arbitrary Distributions. IEEE Transactions on Reliability. Vol. 47, no. 3, 1998 September

Jenab K. & Dhillon B.S. Assessment of reversible multistate k-out-of-n:G/F/Load-Sharing systems with flow-graph models. Reliability Engineering and System Safety 91 (2006) 765–771.

Kapur K.C. & Lamberson L.R. Reliability in Engineering Design. s.l.: John Wiley & Sons., 1977.

Khan M.R.R. & Kabir A.B.M.Z. Availability simulation of an ammonia plant. Reliability Engineering & System Safety 1995; 48: 217–27.

Macchi Marco, Fredy Kristjanpoller, Adolfo Arata, Marco Garetti, Luca Fumagalli. Introducing buffer inventories in the RBD analysis of production systems. Reliability Engineering & System Safety 2012;104; 84–95.

Manian R., Dugan J.B., Coppit D. & Sullivan K.J. Combining various solution techniques for dynamic fault tree analysis of computer systems. Proc. of the IEEE International High-Assurance Systems Engineering Symposium, 1998.

Scheuer E.M. Reliability of an m-out-of-n system when component failure induces higher failure rates in survivors. IEEE Trans. Reliability, vol 37, pp 73–74, 1988.

Shao J. & Lamberson L.R. Modeling a shared-load k-out of n:g system. IEEE Trans. Reliability, 1991, Jun, pp 205–209, Vol. 40.

Sharma R.K. & Kumar S. Performance modeling in critical engineering systems using RAM analysis. Reliability Engineering and System Safety 2008; 93:891–897.

Shengdao T. & Fengquan W. Reliability analysis for a repairable parallel system with time-varying failure rates. Appl. Math. J. Chinese Univ. Ser. B, 2005, 20(1):85–90.

Trivedi K., Hunter S., Garg S. & Fricks R. Reliability Analysis Techniques Explored Through a Communication Network Example. China. Int. Workshop on CAD, Test & Evaluation for Dependability, 1996.

Trivedi K. & Malhotra M. Reliability and Performability Techniques and Tools: A Survey. MMB, 1993. pp 27–48.

Xu H., Xing L. & Robidoux R. DRBD: Dynamic reliability block diagrams for system reliability modelling. International journal of computers and applications, 2009, international journal of computers and applications, 202.

Structural reliability and safety

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Life distribution and P-S-N curve analysis of TC21 titanium alloy joint with Electron Beam Welding in ultra-high cycle fatigue regime

Z. Zhiteng, D. Shu, Z. Liang & X. Danjun
China Academy of Aerospace Standardization and Product Assurance, Beijing, China

ABSTRACT: In this paper, ultrasonic fatigue life of TC21 titanium alloy joints with Electron Beam Welding (EBW) was tested at 10^6~10^9 cycles and the life distribution and P-S-N curve of the fatigue life were analyzed based on the study of crack initiation sites. The results show that fatigue failures of the welding joints still take place after 10^7 cycles. SEM observation of fracture surface indicates that the crack initiation sites abruptly shift from surface to interior welding defects of the specimen with decreasing the stress amplitude. Kolmogorov criterion indicates that the fatigue life at a certain stress level submits log-normal distribution and the dispersity for internal crack initiation fatigue life is much smaller. Maximum likelihood fitting method is used to analyze P-S-N curve at 10^6~10^9 cycles of the EBW joints considering fatigue life distribution, having important significance for life prediction and reliability design of engineering welding parts with very long life.

1 INTRODUCTION

TC21 is a kind of titanium alloy with high strength and good mechanical properties, mainly applied on aerospace structures as well as bearing components for high strength and durability requirements. Due to high energy density, small welding deformation, flexible processing parameters, vacuum welding environments and other advantages, Electron Beam Welding (EBW) is widely used in aviation, aerospace and industrial manufacturing. In welding structures, fatigue failure modes account for 70% to 80% of structural metal failure accidents. During the longtime service of space structures, some components are subjected to fluctuating and cyclic load, and the service lives are even greater than 10^7 cycles. Recent studies using ultrasonic test systems have shown that many materials including some steels and titanium alloys exhibit a sharp decrease in fatigue strength between fatigue lives of 10^7 and 10^9 cycles, which is in contrast to the classical concept of fatigue limit. It is clear that a large decrease in fatigue strength in the Ultra-High Cycle Fatigue (UHCF) regime could have great impact on spacecrafts design. So traditional fatigue design is incorrect and even unsafe, which can't satisfy the long life and high reliability requirements of welding structures. However, the fatigue tests with weld joints of titanium alloy in the ultra-high cycle fatigue region (10^7~10^9) are rarely reported, so it is necessary to study the ultra-high cycle fatigue properties of weld joints. In this paper, ultrasonic fatigue life of TC21 titanium alloy joints with EBW was tested at 10^6~10^9 cycles and reliability of the fatigue life was analyzed based on the study of crack initiation sites.

2 MATERIALS AND EXPERIMENT

The titanium alloy investigated in this study, has a nominal chemical composition (by wt %) of 6.26Al, 2.13Zr, 2.38Mo, 0.96Cr, 1.84Nb, 1.87Sn and balance Ti. The static tensile properties of TC21 alloy and weld joint are shown in Table 1. The base metal microstructures were obtained by two thermal treatment procedures. The thickness of TC21 plate used for EBW is 10 mm and the weld width is 5~8 mm. The parameters of EBW are as follows, accelerating voltage 150 kV, focusing current 2100 mA, electron beam current 90 mA, welding speed 300 mm/min. Figure 1 shows the microstructures of the weld joint. As is shown in the microstructure, the weld joint consists of Fusion Zone (FZ), Heat Affected Zone (HAZ) and Base Metal (BM). Further details of the heat treatments and

Table 1. The tensile property of TC21 sheet and weld zone.

Material	Tensile strength (MPa)	Yield strength (MPa)
TC21 sheet (BM)	1220	1100
Weld zone of EBW	1280	1120

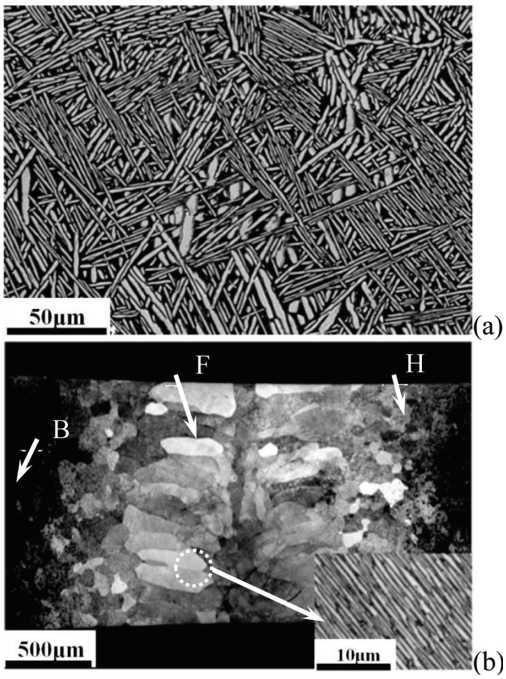


Figure 1. Microstructures of TC21 joint (a) base metal and (b) weld zone.

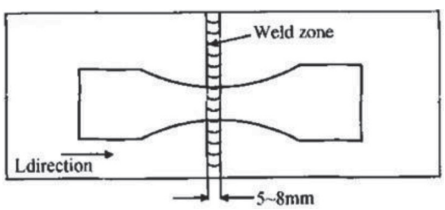


Figure 2. Sampling schematic of TC21 weld plate.

descriptions of microstructure can be found in the references. Fusion zone is the weakest part of the weld joint because of metallurgical defects, and the fatigue crack initiates from this site easily.

The way for fatigue specimens interception as shown in Figure 2 is perpendicular to the weld direction. And the shape and dimension of the specimens for ultra-high cycle fatigue testing is shown in Figure 3. The specimens were fine ground and polished after machining.

Fatigue testing was conducted on Shimadzu USF-2000 testing system with the resonance frequency of 20 kHz, resonance interval of 200 ms, stress ratio of R = −1 and at room temperature in air. During fatigue testing, the specimens were cooled by compressive air. The pause load and compressive air were chosen such that heating of

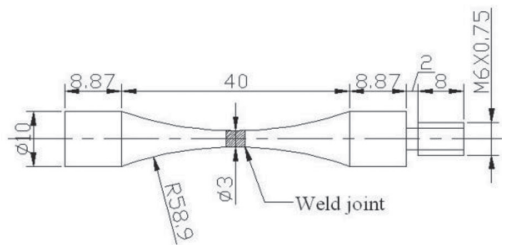


Figure 3. Size and shape of specimen for ultra-high cycle fatigue.

the specimen by internal friction was avoided or much reduced. Details of the ultrasonic fatigue testing procedure and system are described in elsewhere. Scanning Electronic Microscopy (SEM) observation was performed to study the fatigued fracture surface and to determine the fatigue crack initiation sites.

3 RESULTS AND DISCUSSION

3.1 *Characteristics of S-N curve and fatigue crack initiation*

As is shown in Figure 4, the S-N curve decreases continuously and turns less sharply at about 5×10^7 cycles, therefore no horizontal asymptote exits and the fatigue limit is not able to be determined. The fatigue strengths determined using staircase method are 256 ± 10 MPa for the weld joints.

In the fatigue damage stage, cyclic stress attacks both surface and internal defects, and it is considered that the site which is selected for main crack initiation is always competitive and depends on the size of the potential sites and the stress level. SEM investigations show that there is a transition of crack initiation from surface to interior welding defects at the stress 350 MPa, as shown in Figure 4. At high stress level, the fatigue crack occurs on the surface of specimen. However, at lower stress amplitude, internal fatigue cracks were observed. Figure 5 shows examples of surface and internal crack initiation in specimens.

3.2 *Probability distribution of fatigue life in ultra-high cycle fatigue regime*

A large number of experiments show that fatigue life in high cycle regime (10^4~10^6) submits the log-normal distribution, but less research on probability distribution of fatigue life in ultra-high cycle regime. In order to make the fitting of P-S-N curve with TC21 titanium weld joints more logical, generally, we assume that the fatigue life submits the

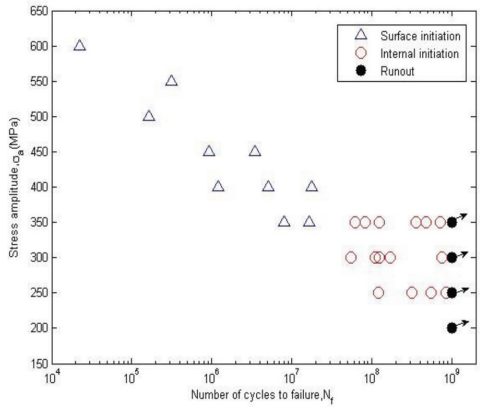


Figure 4. S-N curve for TC21 weld joints.

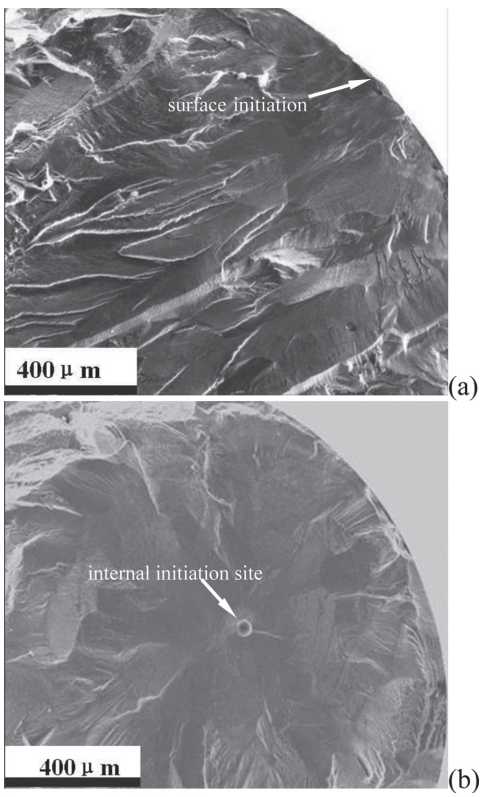


Figure 5. SEM images of fatigue crack initiation sites (a) surface and (b) internal pore.

lognormal distribution, otherwise many work can't be continued. Therefore, lognormal distribution hypothesis testing should be used to test fatigue life distribution under certain stress level in ultra-high cycle regime. Since the purpose of the study is to verify whether the life population submits the lognormal distribution, we start the work from parameter estimation and then the fitting goodness test. And Kolmogorov criterion has the highest sensitivity in a variety of fitting goodness test methods, which is accordingly used to test ultrasonic fatigue life distribution under certain stress level. Due to the apparent difference of fatigue properties under different crack initiation conditions, fatigue life distributions in two kinds of circumstances (surface and interior) are discussed separately, to make the P-S-N curve suitable for fatigue design for engineering components.

3.3 *Fatigue life distribution at stress amplitude 350 MPa*

The fatigue life data obtained at stress amplitude 350 MPa are as follows ($\times 10^7$): 0.802, 1.661, 6.278, 8.324, 12.55, 35.62, 48.43, 72.34, 100 (runout), as for 0.802×10^7 and 1.661×10^7, the fatigue cracks initiate from specimens surface, the rest from interior.

Firstly, we process two kinds of crack initiation site data uniformly. In order to test the probability distribution of fatigue life, we assume that the fatigue life submits the lognormal distribution. To make the runout data ($>10^9$) available (if there is such data), maximum likelihood estimation method with curtailed time data can be used to estimate the mean and standard deviation. If n specimens are tested at a certain stress level, the curtailed time is T, the number of failure specimens is r and their lives are:

$$N_1 \le N_2 \le \ldots N_r \le T \tag{1}$$

Make $t_i = \ln N_i$ (i = 1, 2 … r), $t_T = \ln T$, then the maximum likelihood estimation model is:

$$L = \left[\prod_{i=1}^{r} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{(t_i-\mu)^2}{2\sigma^2}}\right]\left[1-\int_{-\infty}^{t_T} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{(t-\mu)^2}{2\sigma^2}} dx\right]^{n-r} \tag{2}$$

Generally, likelihood function is given by the form of natural logarithm, and the value of μ and σ can be obtained from the solution of

$$\begin{cases} \dfrac{\partial \ln L}{\partial \mu} = 0 \\ \dfrac{\partial \ln T}{\partial \sigma} = 0 \end{cases} \tag{3}$$

Then maximum likelihood estimators obtained by calculation are $\hat{\mu} = 18.7952$ and $\hat{\sigma} = 2.1090$.

Through the Kolmogorov criterion method, we can test the life data whether submits lognormal distribution or not. The Kolmogorov criterion statistic with curtailed time test is:

$$T_0 = \sup_{t \le t_T} \left| F_n(t) - F(t) \right| \tag{4}$$

where $F_n(t)$ is empirical distribution function of the sample, for sample $t_{(1)} \le t_{(2)} \le \ldots \le t_{(r)}$, the empirical distribution function is:

$$F_n(t) = \begin{cases} 0, t < t_{(1)} \\ i/n, t_{(i)} \le t < t_{(i+1)} \\ 1, t \ge t_{(n)} \end{cases} \tag{5}$$

and $F(t)$ is the theory distribution function of population.

If the significance level is α, the critical value of $T_{n,\alpha}$ satisfying the relationship $P[T_0 > T_{n,\alpha}] = \alpha$ can be calculated by the table look-up results according to test curtailed time and the number of samples.

Take the significance level as 0.1, then the calculated critical value $T_{n,\alpha}$ is 0.4444. The calculation process is shown in Table 2.

Then $T_0 = 0.1327 < T_{n,\alpha} = 0.4444$, so we can't refuse the assumption that the fatigue life submits the lognormal distribution. Therefore, the fatigue life ignoring initiation sites submits the lognormal distribution at 350 MPa.

Secondly, since there are two cases of fatigue crack initiation at 350 MPa, and most initiate from interior, so we try to make logarithmic normal distribution hypothesis test for internal initiation data independently including the runout data.

Similarly, the estimators of the mean and standard deviation using maximum likelihood estimation method for curtailed time data is $\hat{\mu} = 19.4409$ and $\hat{\sigma} = 1.3110$. And the critical value $T_{n,\alpha}$ is 0.5714 when significance level takes 0.1. The calculation process is also shown in Table 3.

Table 2. Test statistic calculation process at 350 MPa (the whole data).

No.	t_i	$F(t)$	$F_n(t)$	$\lvert F_n(t) - F(t) \rvert$
1	15.89745	0.0466	0.1111	0.0645
2	16.62491	0.1503	0.2222	0.0719
3	17.95387	0.3066	0.3333	0.0267
4	18.23676	0.3949	0.4444	0.0495
5	18.64382	0.5414	0.5556	0.0142
6	19.69044	0.6023	0.6667	0.0644
7	19.99763	0.6901	0.7778	0.0877
8	20.39892	0.7562	0.8889	0.1327

Table 3. Test statistic calculation process at 350 MPa (internal initiation data).

No.	t_i	$F(t)$	$F_n(t)$	$\lvert F_n(t) - F(t) \rvert$
1	17.95387	0.0668	0.1429	0.0761
2	18.23676	0.2352	0.2857	0.0505
3	18.64382	0.3998	0.4286	0.0288
4	19.69044	0.4901	0.5714	0.0813
5	19.99763	0.6291	0.7143	0.0852
6	20.39892	0.6425	0.7571	0.1146

Because $T_0 = 0.1146 < T_{n,\alpha} = 0.5714$, so we can't refuse the assumption that the internal initiation fatigue life submits the lognormal distribution as well. What needs to be emphasized is that the coefficient of variation ($\hat{\sigma}/\hat{\mu}$) is 0.0674 for internal initiation and 0.1122 for the case of ignorance of initiation sites. That is to say, the data dispersity for two kinds of initiation conditions is larger than single initiation mechanism.

After the distribution analysis of fatigue life in two circumstances, the following conclusions can be obtained: when the fatigue crack initiation sites are in two cases, the fatigue life at a certain stress level necessarily submits lognormal distribution, but the stationarity for internal crack initiation fatigue life is much better. Therefore, when analyzing the P-S-N curve, the crack initiation sites should be distinguished then the fitting curve can be more reasonable.

3.4 *P-S-N curve fitting using maximum likelihood estimation method*

Since the number of fatigue test data is relatively small, only with a group of life data at 350 MPa, conventional method for P-S-N curve fitting can't be used here. In this paper, we use the maximum likelihood estimation fitting method on condition that the following assumption is correct:

1. The fatigue cracks initiate from interior only for tested specimens with very long life;
2. The fatigue life submits logarithmic normal distribution for each stress level;
3. Both the mean and standard deviation of normal population have linear relationship with the corresponding stress level.

Then the mean value and standard deviation of parent population can be written as

$$\mu_i = a_1 + a_2 \lg S_i \tag{6}$$

$$\sigma_i = a_3 + a_4 \lg S_i \tag{7}$$

By the assumption (2), the likelihood function can be written as

$$L(\theta)=\prod_{i=1}^{n}\left[\frac{1}{\sqrt{2\pi}\sigma_i(S_i)}e^{-\frac{\left[X_i-\mu_i(S_i)\right]^2}{2\sigma_i^2(S_i)}}\right] \tag{8}$$

Then the parameters a_1, a_2, a_3 and a_4 can be calculated by the likelihood function.

According to Basquin equation, the P-S-N curve satisfies the relationship:

$$S^{m_P}N_p=C_p \tag{9}$$

where m_p and C_p represent the parameters when the reliability is P, N_p is the lifetime corresponding to the stress amplitude S and reliability P. Then the natural logarithm formation is

$$\ln N_p=\ln C_p-m_p\ln S \tag{10}$$

Assume $X_p=lnN_p$, When $P=0.5$, $\mu=X_{0.5}=lnX_{0.5}$,
then

$$\mu(S)=\ln N_{0.5}=\ln C-m\ln S \tag{11}$$

Since the fatigue life submits the lognormal distribution, then

$$X_p=\mu(S)+u_p\sigma(S) \tag{12}$$

and

$$\sigma(S)=\frac{\ln N_p-\mu(S)}{u_p}=\frac{1}{u_p}\left(\ln\frac{C_p}{C}-m_p\ln S+m\ln S\right) \tag{13}$$

If a group of life test data is got at stress amplitude S_r, then the estimators of the mean value μ_r and standard deviation σ_r for the logarithmic fatigue life are

$$\mu_r=\ln C-m\ln S_r \tag{14}$$

$$\sigma_r=\frac{1}{u_p}\left(\ln\frac{C_p}{C}-m_p\ln S_r+m\ln S_r\right) \tag{15}$$

By formula (9)~(14), the following equation can be obtained:

$$\mu(S)=\mu_r+m\ln\frac{S_r}{S} \tag{16}$$

$$\sigma(S)=\sigma_r+\frac{m}{u_p}\ln\frac{S}{S_r}+\frac{m_p}{u_p}\ln\frac{S_r}{S} \tag{17}$$

When $u_p=-1$, $p=84.1\%$, make $m_{0.841}=m_{-1}$, then

$$\sigma(S)=\sigma_r-\mathrm{m}\ln\frac{S}{S_r}-\mathrm{m}_{-1}\ln\frac{S_r}{S} \tag{18}$$

By formula (15), (17) and (7) the maximum likelihood function parameters m and m_{-1} can be obtained. According to formula (11) the fatigue life under different stress levels in any survival rate can be calculated properly.

According to the shape of stress-life curve with general metal materials the following relationship can be obtained:

$$m>0,\ m_{-1}<50,\ m\geq m_{-1} \tag{19}$$

According to $\sigma(s)>0$, we can get the formula

$$m-m_{-1}<\frac{\sigma_r}{\ln S_{\max}-\ln S_r} \tag{20}$$

We use the Matlab software to calculate the value of m and m_{-1} according to the constraint condition (19). By using Matlab optimization toolbox to find the value of m and m_{-1} through maximum likelihood function. The calculation results are

$m=22.3776$, $m_{-1}=21.3352$

Finally, the P-S-N curve can be got as is shown in Figure 5, and the probability formulas for

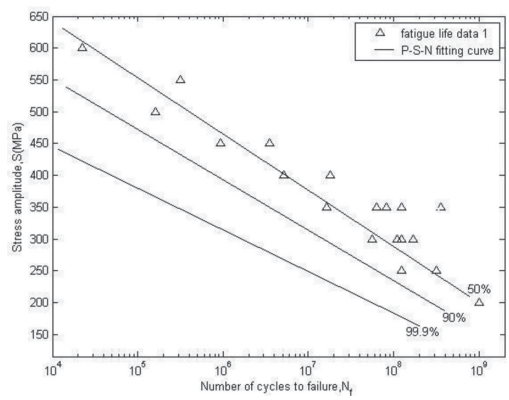


Figure 5. The two parameter P-S-N curve in maximum likelihood method.

stress-life when the reliability is 50%, 90% and 99.9% separately are as follows:

$$P = 50\% \quad lnN = 7.1047 - 0.0722 lnS \tag{21}$$
$$P = 90\% \quad lnN = 6.8821 - 0.07012 lnS \tag{22}$$
$$P = 99.9\% \quad lnN = 5.4867 - 0.06145 lnS \tag{23}$$

4 CONCLUSION

Based on the fatigue life data of TC21 titanium with EBW in ultra-high cycle fatigue regime, the probability distribution of fatigue life at certain stress level is discussed in Kolmogorov criterion method and the P-S-N curve is obtained by maximum likelihood estimation method, the conclusions are as follows:

1. When the fatigue crack initiation sites are in two cases, the fatigue life at a certain stress level necessarily submits lognormal distribution, but the dispersity for internal crack initiation fatigue life is much smaller. Therefore, when analyzing the P-S-N curve for very long life, the crack initiation sites should be distinguished and the fitting curve will be more reasonable.
2. When using the maximum likelihood estimation method to fit long life P-S-N curve of the ultrasonic fatigue life data according to the Basquin equation, we can calculate the value of the relevant parameters according to the relationship equation between probability stress and life for general metals. The P-S-N curve fitting considering fatigue life distribution and cracking initiation sites, which can be used for fatigue design of TC21 titanium EBW engineering components with very long lifetime.

REFERENCES

Bathias C., 2007. Influence of Mean Stress on Ti-6Al-4V Fatigue Crack Growth at Very High Frequency [J]. Engineering Fracture Mechanics, 56(2):255–264.

Chawla N. & B. Jester & D.T. Vonk, 2005. International Journal of Fatigue 27:928–943.

Claude Bathias & Paul C. Paris, 2010. Subsurface crack initiation and propagation mechanisms in gigacycle fatigue [J]. Acta Material, (7):6047.

ECCS recommendations for the fatigue design of steel structure. European convention for constructional steel works. Technical committee fatigue, First Edition, No. 1985, 34.

Hu Yan-hui & Zhang Zheng & HAN Bang-cheng & Zhong Qun-peng, 2007. Recent Development of research on fatigue mechanism in very high cycle range. Proceedings of the 9th International Conference on Engineering Structural Integrity Assessment, Beijing, 1205–1208.

Jing Ling & Jwo Pan. 1997. A maximum likelihood method for estimating P-S-N curves [J]. International Journal of Fatigue, 19(5):415–419.

Manning S.D. & yang J.N, 2008. USAF durability design handbook, Second Edition [M], AFW L-TR-83-3027.

Marines I. & G. Dominguez & G. Baudry & C. Bathias, 2003. J. Fatigue (25):1037.

Stanzl S.E. & Tschegg, 2001. Mayer, Int. J. Fatigue S23:231.

Umezawa O. & K. Nagai, 1997. ISIJ Int. 37, 1170.

Yang & Betal, 2005. Temperature evolution during fatigue damage [J]. Intermetallics, 13:419–428.

Yang Hui-li, 2001. The relationship between microstructure and property of φ350 mm rodlike TC21 titanium [J]. China Titanium Industry, (3):19–22.

Zhang Yi & Zhang Wen-feng, 2000. Quantitative analysis in evaluating fatigue lives of components [J]. Journal of Materials Engineering, (4):45–48.

Zhao xiaohui & Wang Dongpo & Deng Caiyan, 2012. The fatigue behaviors of butt welds ground flush in the super-long life rigime [J]. International Journal of Fatigue, (36):4.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Optimal design of ground-mounted solar systems

R. Boccara
Department of Civil Engineering, University of Pisa, Pisa, Italy

D. Diamantidis
Department of Civil Engineering, OTH Regensburg, Regensburg, Germany

M. Sykora
Klokner Institute, Czech Technical University in Prague, Prague, Czech Republic

ABSTRACT: Solar energy represents a clean, natural and sustainable source of energy. Solar photovoltaic panels can be installed on roofs of structures or in the ground. This contribution focusses on ground-mounted systems, which are presently widely implemented. At present limited guidelines on the design of solar ground-mounted structures are available. Usually standards for the design of normal buildings are applied. However, the design of ground-mounted structures significantly differs from common structural design by: a) a lower design lifetime (20–25 years) is accepted; b) failure is not associated with the loss of human life; c) resistance uncertainties need due attention; d) uplift wind forces dominating structural reliability are associated with a large scatter. That is why the reliability analysis and optimal design of ground-mounted solar systems is investigated herein. The failure costs and especially their ratio to the initial costs are analyzed considering the data provided from the industry. Probabilistic reliability analyses are carried out and optimum design levels are computed for representative cost ratios. The optimal target reliability depends on the ratio between failure and initial costs; reliability index of 3.5 corresponds to a reasonable cost ratio of 10.

1 INTRODUCTION

Current codes focus on traditional structures such as bridges, civil or industrial buildings. The last years have seen an increase of new types of structures, such as geodesic domes, tensile structures or solar panel structures that have some characteristics different from the traditional ones, not explicitly considered in the codes. In particular they can have different design lifetime and different failure consequences not directly included in the European standards such as EN 1990 (2002).

The most common design procedure, the partial factor method, is a semi-probabilistic method based on a design value which is a function of a characteristic value and of a partial factor. The partial factors depend mainly on relevant uncertainties in resistances and load effects, and on the class of failure consequences (reflected by a target reliability level). Designing new types of structures without specific guidelines, using partial factors that do not fit the characteristics of the structure can lead to an uneconomic (non-optimal) design.

Solar energy is a clean natural and sustainable source of energy. Considerable public investments have thus been made worldwide during the last years leading to an enormous increase in the annual world production of solar energy, from 2.2 GW in 2002 to the global production of 100 GW in 2012 as illustrated by Figure 1, REN21 (2013).

This paper focusses on the risk-based optimal design of ground-mounted photovoltaic

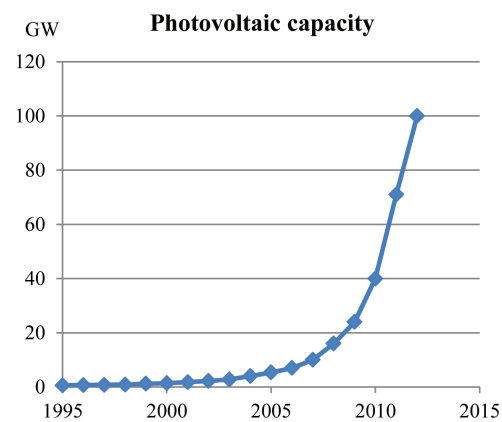


Figure 1. Annual world production of solar energy according to REN21 (2013).

structures. These systems are usually part of a solar production farm and are composed of simple components which can be analyzed based on a probabilistic approach combined with economic optimization. The applied procedure is:

- Flexible to take into account variables that are not considered by the codes,
- Able to consider different variability for the involved stochastic parameters and
- Cost-effective since an optimum design is provided as a function of the failure consequences.

The procedure is illustrated by a case study.

2 PARTIAL FACTOR METHOD

Structural design in current codes is based on the partial factor method. The structural member is reliable if a limit state is not exceeded:

$$r_d > e_d \tag{1}$$

where r_d and e_d = design values for resistance and action effects, respectively.

Design values are calculated trough a representative value (called characteristic value) and a set of partial factors. Through partial factors the designer assigns a certain level of reliability to the structure. The partial factors are fixed values, calibrated using probabilistic methods.

In some circumstances, the aforementioned parameters may vary; for instance uncertainties in soil properties may be reduced based on site investigations; the design working life and the consequence class can be different from those usually considered for the design of traditional structures. In those cases it is possible to apply probabilistic methods in order to recalibrate the partial factors, or directly verify structural reliability.

3 PROBABILISTIC METHOD

3.1 *General framework*

Probabilistic methods, introduced in international standards, are based on the assumption that the reliability of a structure can be measured through the probability of failure. Failure means 'failure to satisfy a limit state criterion' rather than a failure in the sense of a dramatic physical event, Ditlevsen (1997). As a consequence of this, the probability of failure p_f can be expressed in the following way:

$$p_f = \mathrm{P}(R < E) \tag{2}$$

where P = probability; R = random resistance; and E = random load effect. The probability of failure is related to the reliability index β (see also Table 1):

Table 1. Relationship between the failure probability p_f and the reliability index β, EN 1990 (2002).

p_f	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
β	1.28	2.32	3.09	3.72	4.27	4.78	5.20

$$\beta = -\Phi^{-1}(p_f) \tag{3}$$

where Φ^{-1} = inverse cumulative distribution function of the standardized normal distribution.

It should be emphasized that the probability of failure p_f and the reliability index β provide limited information about the actual frequency of failures, they rather serve as a measure of structural reliability in order to perform structural verification, EN 1990 (2002).

A structural component is considered as reliable if during a reference period T_r a limit state is not exceeded, thus the following verification format is considered:

$$\beta \geq \beta_t \tag{4}$$

where β = computed reliability index; and β_t = target reliability level usually recommended by the codes.

Probabilistic methods are not commonly used in design practice despite calculation procedures and software products already enable a direct verification of structural reliability. Detailed guidance is provided by the Joint Committee on Structural Safety Probabilistic Model Code, JCSS (2014).

3.2 *Target reliability level*

The definition of target reliability levels for a considered limit state depends on the physical consequence (and, thus, the socio-economical consequence) of structural malfunction. This leads directly to the rationale of cost-benefit analysis, Ditlevsen (1997). Recommendations concerning the target reliability are provided in several international standards, as a result of experience, calibration and economical optimization, Vrouwenvelder (2002).

In EN 1990 (2002) the recommended values of reliability indexes are given for two reference periods T_r, i.e. 1 year and 50 years, and for different failure consequences (Table 2). It is important here to remember that the reference period is understood as a chosen period of time used as a basis for statistically assessing time-variable basic random variables of loads and the corresponding probability of failure. The reference period is therefore

fundamentally different from the design working life, that is the assumed period of time for which a structure is to be used for its intended purpose without any major repair being necessary, Holicky (2012).

A more detailed recommendation is given in ISO 2394 (1998) where the target reliability indexes are indicated for the whole design working life and related not only to the consequences of failure but also to the relative costs of safety measures (see Table 3).

Similar recommendations are provided in JCSS (2001) and JCSS (2014), where the recommended target reliability indexes are also related to both the consequences and the relative costs of safety measures for the reference period of 1 year (Table 4). The values proposed by the aforementioned documents are based also on calibrations to previous practice.

Table 2. Reliability classification in accordance with EN 1990 (2002).

Reliability classes	Failure Conseq.	Reliability $T_r = 1$ y.	ind. 50 y.	Examples
RC3—high	High	5.2	4.3	Grandstands, public build
RC2—norm	Medium	4.7	3.8	Residences, offices
RC1—low	Low	4.2	3.3	Agricultural buildings

Table 3. Target reliability index (life-time, examples) in accordance with ISO 2394 (1998).

Relative costs of safety measures	Consequences of failure			
	Small	Some	Moderate	Great
High	0	1.5	2.3	3.1
Moderate	1.3	2.3	3.1	3.8
Low	2.3	3.1	3.8	4.3

Table 4. Tentative target reliability indexes β related to a 1-year reference period and ultimate limit states in JCSS (2001) and JCSS (2014).

Relative costs of safety measures	Consequences of failure		
	Minor	Moderate	Large
Large	3.1	3.3	3.7
Normal	3.7	4.2	4.4
Small	4.2	4.4	4.7

4 COST OPTIMIZATION

Codes usually establish a relationship between the target reliability and the reference period; however a clear link between the target reliability and the design working life is missing. Thus, it is not clear which target reliability index should be used for a shorter design working life, Holicky (2012). In general both economic arguments and limits for human safety play a main role in the definition of target reliability for different periods of design working life, Steenbergen & Vrouwenvelder (2010).

ISO 2394 (1998) indicates a possibility to specify the target reliability levels for existing structures by optimization of the total cost related to a reference period. This approach has been recognized to be convenient for structures in which failures lead to economic consequences and human safety is not endangered. Background information for a consequence analysis is provided by Faber et al. (2004), Imam & Chryssanthopoulos (2012), Janssens et al. (2012), JCSS (2001), Kanda & Shah (1997).

The main aim of this contribution is to provide guidance for the specification of the target reliability level for solar structures. A shorter design working life of 25 years is considered according to current practice. The basic assumption is that solar structures have limited consequences compared to usual building structures and that failure is not associated to the loss of human life. Consequently a lower reliability level can be considered. The assumption is supported by the implementation of an optimization procedure, taking into consideration different values of the cost ratios between failure and initial costs.

ISO 2394 (1998) indicates that the target level of reliability should depend on a balance between the consequences of failure and the costs of safety measures. From an economic point of view the objective is to minimize the total working-life cost.

Based on previous studies the expected total costs C_{tot} may be generally considered as the sum of the expected initial costs, costs of inspections, maintenance, and failure consequences. The decision parameter x to be optimized in the assessment may influence resistance, serviceability, durability, maintenance, inspections upgrade strategies etc. In the present study the decision parameter is assumed to concern the initial costs only while the other costs (inspections, maintenance, future repair etc.) are independent of x (and excluded from the optimization). Moreover the benefits related to use of the structure that in general should be considered in the optimization are not affected by value of the decision parameter. These are reasonable assumptions in case of solar panels.

The key aim of the economic optimization is to achieve reduction of risks (by decreasing failure probability) by reasonable initial investments (increasing structural reliability). The optimization procedure proposed by Holicky (2012) is adopted in this case. The total cost is expressed as follows:

$$C_{tot}(x,q,n) = C_f \sum_i P_f(x,i)\ Q(q,i) + C_0 + C_1 x \qquad (5)$$

where q = annual discount rate; n = number of years (reference period); $P_f(x,i) = p(x)(1 - p(x))^{i-1}$ is the failure probability in year i ($i = 1 \ldots n$) obtained from the annual probability of failure $p(x)$; C_f = failure consequences; $Q(q,i)$ = time factor dependent on q and the numbers of years i; C_0 = initial cost independent of the decision parameter x; and C_1 = unit cost of the decision parameter x.

The total cost in equation (5) is standardized κ_{tot} as proposed by Holicky (2012):

$$\kappa_{tot} = p(x)PQ(x,q,n)\ C_f / C_1 + x \qquad (6)$$

where $PQ(x,q,n)$ = time factor evaluated as:

$$PQ(x,q,n) = 1-[(1-p(x))/(1+q)]^n/[1-(1-p(x))/(1+q)] \qquad (7)$$

The optimum solution x_{opt} corresponds to the minimal standardized costs; optimal reliability index is then $\beta_{opt}(x_{opt})$.

5 CASE STUDY: GROUND-MOUNTED SOLAR SYSTEMS

5.1 *Development of solar structures*

The last years have seen a large increase in utilization of solar panels as renewable energy systems (Figure 1). Photovoltaic systems can be divided into two groups:

- Solar structures on roofs;
- Grounded solar structures.

The proposed procedure is applied in the case study of the optimum design of a solar ground-mounted structure (Figure 2). Such a structure can have different types of foundations: spread footing foundation, drilled piles, micro piles or screw piles.

Due to flexibility of installation and to the ability of reuse, screw piles are commonly used as foundations of light structures such as those for solar panels (Figure 3).

5.2 *Cost aspects*

As input to the optimization procedure cost parameters need to be analyzed. Failure consequences and particularly their ratio to the initial costs C_f/C_1 accepted here are based on the data obtained for a photovoltaic farm of 1.4 MW located in Tuscany, Italy.

An optimized parameter is the length of the screw pile subjected to wind uplift forces. The unit cost of the decision parameter is $C_1 = 80$ €/m.

Estimate of the failure consequences C_f is based on the following assumptions:

- Replacement costs are of the order of $1.2C_1$,
- Failure of the system leads to a production loss of 20 days,
- The expected revenue per day per a solar panel is obtained by averaging expected revenues over 2013–2038 (25 years) obtained from a business plan of the farm,
- 100 solar panels in the farm are considered.

The cost ratio becomes $C_f / C_1 \approx 2.3$. To account also for indirect consequences a reasonable cost ratio may range from 5 to 10. The indirect consequences may include production loss and inspections of solar panels connected with a failed panel, loss of credibility as a supplier and subsequent losses of contracts etc. Note that the ratio C_f / C_1 depends on structure-specific conditions and no general guidance for its estimation is available.



Figure 2. Ground-mounted photovoltaic structure.

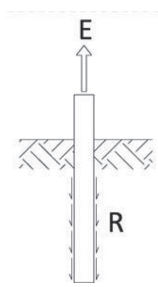


Figure 3. Effect of the wind action on a single pile E and friction resistance of the pile R.

5.3 *Reliability analysis*

Photovoltaic systems are due to their large surface of panels and their light weight mainly affected by the wind uplift action (Figure 3). The resistance of the foundation is the frictional resistance between the pile and the soil, dependent on the soil parameters and the pile geometry.

Initially the partial factor method according to Eurocodes (in particular EN 1997-1 (2004)) is applied to determine design length of the pile. The limit state function reads:

$$R_d = R_k / \gamma_R = [\alpha (C_{u,k} / \gamma_{Cu}) A_l / \xi_3] / \gamma_R \geq \gamma_Q Q_k \quad (8)$$

Characteristic values and partial factors of the basic variables and notation are provided in Table 5. Soil parameters are based on a geotechnical survey (five tests); characteristic value of the wind action effect is obtained from a National Annex to EN 1991-1-4 (2005). The most unfavorable results are obtained using Design Approach 1—Combination 2, EN 1997-1 (2004).

As the structure is very light, the self-weight is negligible and is not considered in the limit state. More details are provided by Boccara (2014).

The design length of the pile is $l_{EC} = 1.60$ m.

In the probabilistic reliability analysis the limit state function accounts for the uncertainties in resistance model θ_R:

$$\theta_R \alpha \cdot C_u \cdot A_l(l) \cdot - Q = 0 \quad (9)$$

Probabilistic models of non-deterministic basic variables are given in Table 6; deterministic basic variables include the diameter and length of the pile, lateral area of friction and adhesion coefficient ($\mu_X / X_k = 1$). The probabilistic models are based on recommendations provided by Huber (2013), JCSS (2014) and Rackwitz (2000). The model uncertainty θ_R is assumed to account for imprecision of the implemented resistance model including the effects covered by the correlation factor (influences of a limited number of piles tested and of profiles of tests).

Reliability of the pile is analyzed considering the pile length l as a study parameter. A sensitivity analysis investigates effects of the coefficients of variation of C_u, θ_R and Q on the reliability index β.

Detailed results are provided by Boccara (2014). Representative results of the analysis are plotted in Figure 4 that shows the reliability index β as a function of the length l for different values of V_{Cu} (0.2, 0.3, 0.4) with fixed $V_{\theta R} = 0.3$ and $V_Q = 0.3$; the vertical dash-point line indicates l_{EC}. Note that for simplicity of computations the mean values of C_u and Q given in Table 6 are kept independent of the relevant coefficients of variation. This approximation has a minor effect on the results of economic optimization.

Table 5. Characteristic values and partial factors of the basic variables applied in the design by the partial factor method.

Basic variable	Sym.	Unit	X_k*	γ_X**
Diameter of pile	ϕ	m	0.159	–
Length of pile	l	m	parameter	–
Lateral area of friction	A_l	m²	$\pi \phi l$	–
Adhesion coefficient	α	–	0.87	–
Unconfined cohesive strength	C_u	kN/m²	50	1.4
Correlation factor	ξ_3***	–	1.31	–
Friction. resist. pile—soil	R	kN	Eq. (8)	1.6
Wind load effect	Q	kN	9.33	1.3

*Characteristic value; **partial factors according to Annex A to EN 1997-1 (2004); ***correlation factor to derive the pile resistance from ground investigation results, not being pile load tests.

Table 6. Probabilistic models of the basic variables.

Basic variable	Sym.	Distrib.	μ_X/X_k*	V_X**
Unconfined cohesive strength	C_u	lognormal	1.4***	0.2–0.5
Uncertainty in resist. model	θ_R	lognormal	1	0.2–0.5
Annual maxima of wind load effect including model uncertainties	Q	Gumbel	0.66****	0.2–0.5

*Mean to characteristic value; **coefficient of variation; ***assuming the characteristic value being a 5% fractile and $V_{Cu} = 0.2$; ***assuming the characteristic value being a 98% fractile of annual maxima and $V_Q = 0.2$.

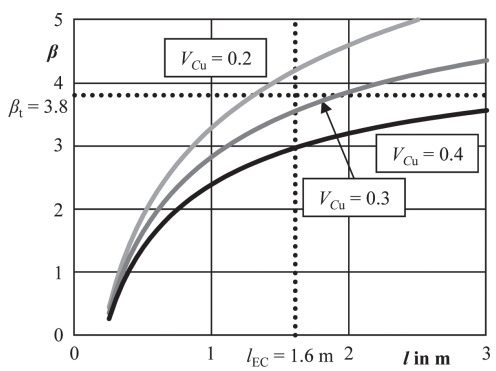


Figure 4. Reliability index β as a function of the length l and V_{Cu} ($V_{\theta R} = 0.3$ and $V_Q = 0.3$).

The following observations follow from Figure 4:

– The reliability level inherent in the design according to Eurocodes for different values of the coefficient of variation of the unconfined cohesive strength ($\beta \sim 3.0$–4.2; for instance $\beta = 3.5$ for $V_{Cu} = 0.3$);
– The pile length needed to reach a specific target reliability level β_t (e.g. $l = 1.9$ m to reach $\beta_t = 3.8$ for $V_{Cu} = 0.3$).

The cost optimization is based on equation (6). The total standardized cost function κ_{tot} is evaluated as a function of the length l of the pile for different values of the cost ratio C_f / C_1 that is a dominating parameter in the optimization.

Figure 5 shows the trend of κ_{tot} with the length l for representative values $C_f / C_1 = 1$, 10, 100 and 1000 (for $V_{Cu} = 0.3$, $V_{\theta R} = 0.2$, $V_Q = 0.3$, $q = 0.03$ and $n = 25$ years). It appears that the target reliability decreases with a decreasing ratio C_f / C_1 as can be expected. For $C_f / C_1 = 10$ the annual target reliability is approximately 3.5. If the cost ratio is around 100, the optimum length approaches that obtained by the partial factor method.

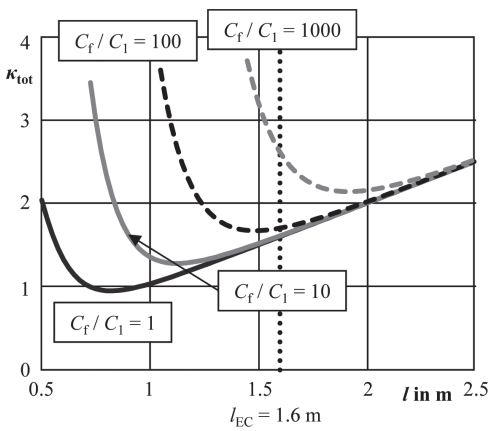


Figure 5. Total standardized cost κ_{tot} as a function of the length l for $C_f / C_1 = 1$, 10, 100 and 1000 (for $V_{Cu} = 0.3$, $V_{\theta R} = 0.2$, $V_Q = 0.3$, $q = 0.03$ and $n = 25$ years).

Table 7. Optimal lengths l_{opt} and corresponding annual β for different C_f / C_1.

Cost Ratio	l_{opt} in m	β
1	0.80	2.85
10	1.10	3.47
100	1.50	4.06
1000	1.90	4.50

Table 7 provides the main results of the economic optimization—optimal lengths l_{opt} and corresponding annual reliability indices β for different cost ratios C_f / C_1.

Note that the discount rate may be greater particularly for private investors; for instance de La Tour et al. (2013) indicated the range $q = 0.05$–0.1.

6 CONCLUSIONS

The present study leads to the following general conclusions concerning the design of ground-mounted solar systems:

– The partial factor method leads to conservative design solutions, desired improvements can be obtained by applications of probabilistic methods;
– The parameters significantly affecting the reliability index include the unconfined cohesive strength of soil, uncertainties in resistance model and effect of wind action;
– Due to considerable variability of soil properties, it is recommended to establish probabilistic models of resistance parameters on the basis of test results;
– The annual target reliability β depends on the ratio between failure and initial costs (for a reasonable ratio 10 $\beta \approx 3.5$ is obtained; this value is lower compared to a value recommended in EN 1990 (2002) for the lowest reliability class).

Further investigations are necessary to in order to propose pre-normative recommendations. In particular uncertainties in the resistance models for geotechnical structures should be improved.

ACKNOWLEDGEMENTS

This study has been supported by the Technology and Science network of Oberpfalz (TWO), Bavaria, Germany, and by the research project TE01020068 of the Technology Agency of the Czech Republic.

REFERENCES

Boccara, R. 2014. *On The Reliability Based Design of Solar Structures*. Master thesis, Universita di Pisa.

de La Tour, A., Glachant, M. & Ménière, Y. 2013. Predicting the costs of photovoltaic solar modules in 2020 using experience curve models. *Energy* 62(0): 341–348.

Ditlevsen, O. 1997. Structural reliability codes for probabilistic design—A debate paper based on elementary reliability and decision analysis concepts. *Structural Safety* 19(3): 253–270.

Faber, M.H., Kübler, O., Fontana, M. & Knobloch, M. 2004. *Failure Consequences and Reliability Acceptance Criteria for Exceptional Building Structures,* July 2004. Zurich: Institute of Structural Engineering, Swiss Federal Institute of Technology.

EN 1990:2002. *Eurocode—Basis of Structural design*. Brussels: CEN.

EN 1991-1-4:2005. *Eurocode 1: Actions on structures—Part 1-4: General actions*—Wind actions. Brussels: CEN.

EN 1997-1:2004. *Eurocode 7: Geotechnical design—Part 1: General rules*. Brussels: CEN.

Holicky, M. 2012. Optimization of the target reliability for temporary structures. *Civil Engineering and Environmental Systems* 30: 87–96.

Huber, M. 2013. *Soil variability and its consequences in geotechnical engineering* (Ph.D. thesis), Institut für Geotechnik der Universitat Stuttgart.

Imam, B.M. & Chryssanthopoulos, M.K. 2012. Causes and Consequences of Metallic Bridge Failures. *Structural Engineering International* 22(1): 93–98.

ISO 2394:1998. *General principles on reliability for structures*. Geneve, Switzerland: ISO.

Janssens, V., O'Dwyer, D.W. & Chryssanthopoulos, M.K. 2012. Assessing the Consequences of Building Failures. *Structural Engineering International* 22(1): 99–104.

JCSS 2001. *Probabilistic Assessment of Existing Structures*. RILEM Publications S.A.R.L., edited by D. Diamantidis.

JCSS 2014. *JCSS Probabilistic Mode Code*. Joint Committee on Structural safety <www.jcss.byg.dtu.dk>.

Kanda, J. & Shah, H. 1997. Engineering role in failure cost evaluation for buildings. *Structural Safety* 19(1): 79–90.

Rackwitz, R. 2000. Reviewing probabilistic soils modelling. *Computers and Geotechnics* 26: 199–223.

REN21 2013. *Renewables 2013 Global Status Report*. Paris: REN21 Secretariat.

Steenbergen, R.D.J.M. & Vrouwenvelder, T. 2010. Safety philosophy for existing structures and partial factors for traffic loads on bridges. *HERON* 55(2): 123–139.

Vrouwenvelder, T. 2002. Reliability Based Code calibration. *The use of the JCSS Probabilistic Model Code. Joint Committee of Structural Safety Workshop on Code Calibration*, 21–22 March 2002, Zurich.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Approximate quantification of the robustness index of concrete beams subjected to deterioration

W. Botte, R. Caspeele & L. Taerwe
Department of Structural Engineering, Ghent University, Ghent, Belgium

ABSTRACT: Deterioration of existing structures due to corrosion of reinforcement has been a growing concern in the last decades since the associated reduction of the steel results in a decrease of the structural reliability. Apart from deterioration, also the assessment of structural robustness has been of particular interest. One way to quantify robustness is through a reliability-based robustness index based on the reliability index of the damaged and undamaged system. Determination of these reliability indices requires the selection of probabilistic and physical models and the estimation of the associated parameters. This introduces uncertainties in the probabilistic models, the reliability indices and hence in the robustness index. These uncertainties are usually not considered. In this contribution, an approximate quantification method is derived in order to assess the influence of uncertainties on the robustness index of deteriorated concrete beams. As an example, a reinforced concrete beam subjected to corrosion is analyzed to demonstrate the influence of uncertainties on the robustness index.

1 INTRODUCTION

In the last decades, deterioration of existing structures has been a growing concern. Deterioration due to corrosion of reinforcement steel has been of particular interest since the associated reduction of the steel section results in a decrease of the structural safety. An other topic which has been the subject of many publications is the assessment of the structural robustness. Different approaches have been proposed in order to quantify this structural robustness through robustness indicators (Sørensen et al. 2012). The robustness indicator based on the reliability index of the undamaged and the damaged system, is the reliability-based robustness index.

Both hot topics are combined in this contribution: the quantification of the structural robustness of reinforced concrete beams subjected to chloride-induced corrosion is discussed. Further, since corrosion is a time-variant process, the associated robustness index will be time-dependent.

In order to assess the structural reliability and robustness with respect to deterioration, it is required to select appropriate models which describe the deterioration process. The parameters associated with these models have to be estimated through statistical inference, which introduces uncertainties in parameter estimates. The reliability index which takes into account these uncertainties is the predictive reliability index (Der Kiureghian 2008). As the structural reliability indices which are incorporated in the reliability-based robustness index can be considered as random variable, this robustness index itself will be a random variable as well. In this contribution, the aforementioned predictive reliability index is used to derive measures of uncertainty in the robustness index with respect to deteriorated structures. To illustrate the proposed concept, the influence of parameter uncertainties on the robustness index of a reinforced concrete beam subjected to chloride-induced corrosion is analyzed.

2 DETERIORATION DUE TO CHLORIDE-INDUCED CORROSION

2.1 *General*

A common deterioration mechanism in reinforced concrete is corrosion of the reinforcement steel. Corrosion affects the steel as well as the concrete by (Rodriguez et al. 1997):

- Reduction of the bar section;
- Reduction of the mechanical properties of the steel;
- Cracking and spalling of the concrete due to the expansion of corrosion products;
- Bond deterioration between the steel and the surrounding concrete.

Because of these phenomena, the safety of deteriorated concrete structures is reduced. According to the Model Code for Service Life Design

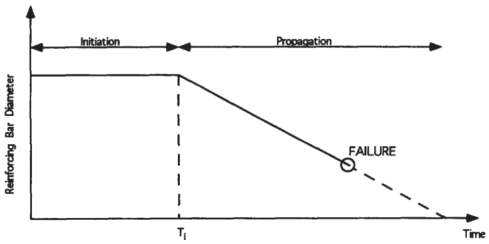


Figure 1. Deterioration process for loss of reinforcing steel (Stewart & Rosowsky 1998).

(fib 2006), the process of corrosion of the reinforcement can be divided roughly into two time periods: the initiation period and the propagation period (Fig. 1). The first phase is defined as the time until the reinforcement becomes depassivated, either by chloride ingress or by carbonatation. During the second phase, the reinforcement itself is affected: the cross-section is reduced. Both phases are governed by different stochastic parameters and can be described by mathematical models, which are presented in the next sections.

2.2 *Initiation period*

Initially, reinforcement steel in concrete is protected by the high alkalinity of the concrete and no corrosion occurs (Val & Melchers 1997). However, in case of chloride-induced corrosion, the diffusion of chlorides through the protective concrete cover results in the depassivation of the concrete. As soon as a critical chloride concentration C_{cr} is reached, the corrosion process starts. Models for the depassivation of concrete can be found in Stewart & Rosowsky (1998) and Vu & Stewart (2000). Generally, the length of the initiation period depends on the concrete cover, the diffusion coefficient, the critical chloride content, the initial chloride concentration in the concrete and the chloride concentration at the surface of the concrete element.

Further in this contribution, the time to corrosion initiation T_i and the associated uncertainties are not considered. For the sake of simplicity, it is assumed that $T_i = 0$. Hence, a possible reduction of the structural safety level during the initiation phase is not considered in this contribution.

2.3 *Propagation period*

Once corrosion is initiated, the corrosion rate is determined by equation (1), as proposed by Vu & Stewart (2000) and Stewart & Suo (2009):

$$i_{corr}(t_p) = i_{corr}(0) \cdot 0.85\, t_p^{-0.29} \quad (1)$$

where $i_{corr}(t_p)$ [μA/cm²] is the corrosion rate at time t_p, t_p [years] is the time since corrosion initiation and $i_{corr}(0)$ [μA/cm²] is the corrosion rate at the start of corrosion propagation. The latter can be calculated from:

$$i_{corr}(0) = \frac{2.70(1 - w/c)^{-1.64}}{a} \quad (2)$$

where w/c [–] is the water cement ratio and a [cm] is the concrete cover. It follows from equation (1) that the corrosion rate decreases in time, which is due to the formation of rust products on the steel surface, obstructing the diffusion of the iron ions away from the steel surface (Vu & Stewart 2000).

Equation (1) is only valid when no spalling occurs, which is assumed in this paper. In case spalling does occur, the corrosion rate can be assumed to be constant (Papadopoulos et al. 2011).

As suggested by Stewart & Rosowsky (1998), the reduction in bar diameter of the reinforcement steel can be derived from the corrosion rate (since 1 μA/cm² = 0.0116 mm/year):

$$Ø(t_p) = Ø_0 - 2 \cdot 0.0116 \int_0^{t_p} i_{corr}(t)dt \quad (3)$$

where $Ø(t_p)$ [mm] is the reinforcement diameter t_p years after corrosion initiation and $Ø_0$ [mm] is the initial diameter.

3 PREDICTIVE RELIABILITY INDEX

The verification of a structure with respect to a certain limit state requires the definition of a limit state function g(.). The theoretical failure probability P_f for that specific limit state is then defined by:

$$P_f = \int_{g(x)<0} f_X(x)dx \quad (4)$$

where $f_{\mathbf{X}}(\mathbf{x})$ is the n-dimensional Probability Density Function (PDF) of the n basic variables X_i (i = 1 … n) and $g(\mathbf{x})$ is the limit state function, defined so that $g(\mathbf{x}) < 0$ corresponds to failure. The n basic variables represent uncertain quantities such as material properties, actions (loads), geometrical properties and model uncertainties.

As stated by Der Kiureghian (2008) the aforementioned formulation is the theoretical formulation of the structural reliability problem, since in practice neither the joint PDF $f_{\mathbf{X}}(\mathbf{x})$ nor the limit state function $g(\mathbf{x})$ are precisely known. Hence, one has to select appropriate probabilistic or physical models and the associated parameters have to be

estimated through statistical inference of experimental data and observations. The model for $f_{\mathbf{X}}(\mathbf{x})$ in which the parameters $\boldsymbol{\Theta}$ are estimated, is designated $\hat{f}_{\boldsymbol{X}}(\boldsymbol{x}\,|\,\Theta)$.

Since the model parameters are uncertain, it follows from (4) that also the failure probability P_f and the reliability index β are uncertain. Hence, the random variables $P = P_f(\boldsymbol{\Theta})$ and $B = \beta(\boldsymbol{\Theta})$ can be introduced. As random variables, P and B have probability density functions, namely $f_P(P_f)$ and $f_B(\beta)$ respectively, and characteristics, such as a mean (μ_P and μ_B) and a variance (σ_P^2 and σ_B^2). The latter expresses the uncertainty of the estimate of the failure probability or reliability index, originating from the parameter uncertainties. Since parameter uncertainties can be reduced by gathering additional information, these variances can also be reduced.

In (Der Kiureghian 2008) the predictive failure probability, denoted as $\tilde{p}$, is defined as the expectation of P over the outcome space of the uncertain parameters $\boldsymbol{\Theta}$:

$$\tilde{p} = \int_{\theta} P_f(\boldsymbol{\theta}) f_{\Theta}(\boldsymbol{\theta}) d\boldsymbol{\theta} \tag{5}$$

where $f_{\boldsymbol{\Theta}}(\boldsymbol{\theta})$ is the posterior joint distribution function for the set of estimated parameters $\boldsymbol{\theta}$. The predictive failure probability is equal to the mean of $f_P(P_f)$.

Consequently, the predictive reliability index is calculated from equation (6):

$$\tilde{\beta} = \Phi^{-1}(1 - \tilde{p}) \tag{6}$$

where $\Phi^{-1}(.)$ is the inverse of the standard normal cumulative distribution function.

Der Kiureghian (2008) provides different methods for calculating the predictive failure probability, predictive reliability index and their measures of uncertainty. One of these methods yields a very simple approximation formula for the predictive reliability index $\tilde{\beta}$:

$$\tilde{\beta} \cong \frac{\mu_B}{\sqrt{1 + \sigma_B^2}} \tag{7}$$

Note that the latter is not equal to the mean of the probability function $f_B(\beta)$.

The only approximation used to obtain equation (7) is the assumption that the reliability index follows a normal distribution, which is in many cases an acceptable assumption (Der Kiureghian 2008).

The calculation of the predictive reliability index according to equation (7) requires the mean and variance of the random variable B. These can be calculated by making use of a first-order approximation of the function $B = \beta(\boldsymbol{\Theta})$. This yields:

$$\mu_B \cong \beta(\mathbf{M}_{\boldsymbol{\Theta}}) \tag{8}$$

$$\sigma_B^2 \cong (\nabla_{\boldsymbol{\Theta}}\beta)^T_{\boldsymbol{\Theta}=\mathbf{M}_{\boldsymbol{\Theta}}} \Sigma_{\boldsymbol{\Theta}\boldsymbol{\Theta}} (\nabla_{\boldsymbol{\Theta}}\beta)_{\boldsymbol{\Theta}=\mathbf{M}_{\boldsymbol{\Theta}}} \tag{9}$$

with $\mathbf{M}_{\boldsymbol{\Theta}}$ the posterior mean vector of $\boldsymbol{\Theta}$, $\boldsymbol{\Sigma}_{\boldsymbol{\Theta}\boldsymbol{\Theta}}$ the posterior covariance matrix of $\boldsymbol{\Theta}$ and $(\boldsymbol{\nabla}_{\boldsymbol{\Theta}}\beta)_{\Theta\,=\,\mathbf{M}\boldsymbol{\Theta}}$ the sensitivity vector of the conditional reliability index with respect to the parameters $\boldsymbol{\Theta}$, evaluated at the posterior mean values. The sensitivity vector in equation (9) is given by:

$$\boldsymbol{\nabla}_{\boldsymbol{\Theta}}\beta = \left(\frac{\partial\beta}{\partial\theta_1}, \frac{\partial\beta}{\partial\theta_2}, \ldots, \frac{\partial\beta}{\partial\theta_n} \right) \tag{10}$$

where:

$$\frac{\partial\beta}{\partial\theta_i} = \boldsymbol{\alpha}^T \left(\frac{\partial\mathbf{u}}{\partial\theta_i} \right)_{\mathbf{u}=\mathbf{y}} \tag{11}$$

and $\boldsymbol{\alpha}$ the sensitivity vector, $\mathbf{u}$ the vector of normalized basic variables, $\mathbf{y}$ the design point in standard normal space and $\beta = \boldsymbol{\alpha}^T\mathbf{y}$.

As an example, consider n independent, normal random variables $\mathbf{X}$ with unknown means and standard deviations. Hence the unknown parameter vector $\boldsymbol{\Theta} = (\mathbf{M}, \boldsymbol{\Sigma}) = (M_1, \Sigma_1, M_2, \Sigma_2 \ldots M_n, \Sigma_n)$. The unknown mean M_i has a mean value $\overline{x_i}$ and standard deviation σ_{Mi}; the unknown standard deviation Σ_i has a mean σ_i and a standard deviation $\sigma_{\Sigma i}$. From equation (11) it follows, in case $\theta_i = M_i$:

$$\frac{\partial\beta}{\partial\theta_i} = \frac{\partial\beta}{\partial M_i} = \alpha_i \frac{\partial}{\partial M_i} \left(\frac{x_i - M_i}{\Sigma_i} \right)_{M_i=\overline{x}_i;\Sigma_i=\sigma_i} = -\frac{\alpha_i}{\sigma_i} \tag{12}$$

And in case $\theta_i = \Sigma_i$:

$$\frac{\partial\beta}{\partial\theta_i} = \frac{\partial\beta}{\partial\Sigma_i} = \alpha_i \frac{\partial}{\partial\Sigma_i} \left(\frac{x_i - M_i}{\Sigma_i} \right)_{M_i=\overline{x}_i;\Sigma_i=\sigma_i} = +\frac{\alpha_i^2\beta}{\sigma_i} \tag{13}$$

With (9), (10), (12) and (13) the variance of the reliability index becomes:

$$\sigma_B^2 \cong \sum_{i=1}^{n} \frac{\alpha_i^2}{\sigma_i^2} \sigma_{M_i}^2 + \sum_{i=1}^{n} \frac{\alpha_i^4\beta^2}{\sigma_i^2} \sigma_{\Sigma_i}^2 \tag{14}$$

The first term represents the contribution of the uncertainty of the mean value of the estimated parameters, while the second term represents the contribution of the uncertainty on the standard deviation.

Equations (8) and (9) show that it is sufficient to perform one single calculation of the reliability index along with the parameter sensitivities in order to determine the mean and variance of the reliability index and the predictive reliability index (equation (6)). This calculation is performed using the mean values of the parameters.

4 QUANTIFICATION OF ROBUSTNESS

4.1 *Structural robustness quantification*

The failure of several structures, such as the Ronan Point Building in 1968, stressed the importance of the robustness of a building. Structural robustness assessment focuses on two states of a building: the undamaged and the damaged state. As stated by Yao (1985) and Frangopol & Curley (1987), 'damaged' may refer to any strength deficiency introduced during the design or construction phase of the structure as well as any deterioration of strength caused by external loading (e.g. sudden column loss) and/or environmental conditions (e.g. corrosion) during the lifetime of the structure.

Different approaches to quantify structural robustness have been proposed by several authors (Sørensen et al. 2012). These approaches can be divided into the following levels, with increasing complexity:

- A deterministic approach based on structural measures (e.g. pushover method on the damaged and undamaged system);
- A probabilistic approach based on the probability of failure of the undamaged and the damaged system;
- A risk-based approach based on a complete risk analysis in which consequences are divided into direct and indirect consequences.

The last approach is the most general one, but, as stated before, also the most complex one. Therefore, in this contribution, a probabilistic approach is used.

4.2 *Reliability-based robustness assessment*

A probabilistic measure of robustness is the redundancy index RI, defined by (Fu & Frangopol 1990):

$$\mathrm{RI} = \frac{P_{f,\mathrm{damaged}} - P_{f,\mathrm{intact}}}{P_{f,\mathrm{intact}}} \tag{15}$$

where $P_{f,\mathrm{damaged}}$ is the probability of failure of the damaged system and $P_{f,\mathrm{intact}}$ is the probability of failure of the undamaged system. This redundancy index takes values between infinity, for structures that are not robust, and zero, for structures that are very robust.

Alternatively, also the redundancy factor β_R defined by (Frangopol & Curley 1987) can be considered:

$$\beta_R = \frac{\beta_i}{\beta_i - \beta_d} \tag{16}$$

where β_i is the reliability index of the intact system and β_d is the reliability index of the damaged system. The redundancy factor takes values between 0 (i.e. $\beta_d = -\infty$), for structures that are not robust, and infinity (i.e. $\beta_d = \beta_i$), for very robust structures.

The redundancy index RI and the redundancy factor β_R are nonlinearly related, since:

$$\beta_R = \frac{\Phi^{-1}(1 - P_{f,\mathrm{intact}})}{\Phi^{-1}(1 - P_{f,\mathrm{intact}}) - \Phi^{-1}(1 - P_{f,\mathrm{damaged}})} \tag{17}$$

Note that the reliability-based robustness index does not require the description of external consequences, unlike risk-based robustness indices, which simplifies the calculations.

4.3 *Approximate quantification of robustness*

As mentioned in paragraph 3, the reliability index is, in practice, never precisely known because of the estimation of parameters. Hence the reliability indices β_i and β_d are not precisely known and the random variables $B_i = \beta_i(\boldsymbol{\Theta})$ and $B_d = \beta_d(\boldsymbol{\Theta})$ are introduced. Based on formulas (8) and (9), the mean (μ_{Bi} and μ_{Bd}) and variance (σ_{Bi}^2 and σ_{Bd}^2) of these random variables can be determined.

Since the reliability index of the undamaged and the damaged system are not precisely known, also the redundancy index, as defined by (16), is not precisely known. Hence, the random variable $B_R = \beta_R(\beta_i(\boldsymbol{\Theta}), \beta_d(\boldsymbol{\Theta}))$ is introduced. As a random variable, B_R has a PDF $f_{BR}(B_R)$ and characteristics such as a mean μ_{BR} and a standard deviation σ_{BR}.

The mean and standard deviation of the redundancy index can be derived by means of Taylor approximations. This yields the following:

$$\mu_{B_R} = \frac{\mu_{B_i}}{\mu_{B_i} - \mu_{B_d}} + \left(\frac{\mu_{B_i}\sigma_{Bd}^2 + \mu_{B_d}\sigma_{B_i}^2}{\left(\mu_{B_i} - \mu_{B_d}\right)^3} \right) \tag{18}$$

$$\sigma_{B_R} = \frac{\mu_{B_d}^2\sigma_{B_i}^2 + \mu_{B_i}^2\sigma_{B_d}^2}{\left(\mu_{B_i} - \mu_{B_d}\right)^4} + (\ldots) \tag{19}$$

The terms between (…) in equations (18) and (19) are higher order approximations. These might

be necessary in case the difference between the reliability index of the undamaged and the damaged system is small. In that case, the second term of the approximation is not negligible.

No assumptions have been made to derive the expressions for the mean and standard deviation (18) and (19). However, one can also find an analytical solution for these characteristics, by assuming a distribution for the reliability indices. For example, one can assume that the uncertain reliability index B follows a lognormal distribution. This enables to find an approximate distribution for the robustness index. In order to do so, the robustness index (16) is rewritten as follows:

$$B_R = \frac{B_i}{\Delta B} \tag{20}$$

where B_i follows a lognormal distribution with mean μ_{Bi} and standard deviation σ_{Bi}; and ΔB also follows a lognormal distribution with mean and standard deviation obtained from Taylor approximations: $\mu_{\Delta B} \approx \mu_{Bi} - \mu_{Bd}$ and $\sigma_{\Delta B} \approx (\sigma_{Bi}^2 + \sigma_{Bd}^2)^{1/2}$. As such, the robustness index B_R also follows a lognormal distribution, with mean and variance calculated from:

$$\mu_{\ln B_R} = \mu_{\ln B_i} - \mu_{\ln \Delta B} \tag{21}$$

$$\sigma^2_{\ln B_R} = \sigma^2_{\ln B_i} - \sigma^2_{\ln \Delta B} \tag{22}$$

and:

$$\mu_{B_R} = \exp\left(\mu_{\ln B_r} + \sigma^2_{\ln B_R}/2\right) \tag{23}$$

$$\sigma^2_{B_R} = \mu^2_{B_R}\left[\exp\left(\sigma^2_{\ln B_R}\right) - 1\right] \tag{24}$$

Hence, assuming that B_i and ΔB follow a lognormal distribution, B_R follows a lognormal distribution with parameters μ_{BR} and σ_{BR}.

Comparable to σ_B^2, σ_{BR}^2 expresses the uncertainty of the estimate of the robustness index, originating from the parameter uncertainties. The uncertainty of the estimate of the robustness index can be reduced by gathering additional information, since parameters uncertainties can be reduced.

5 EXAMPLE

To illustrate the concepts elaborated above, a reinforced concrete beam subjected to chloride-induced corrosion is considered.

5.1 *Characteristics*

The limit state equation with respect to bending, for the most heavily loaded cross-section is expressed as follows:

$$g(x) = A_s \cdot f_y \cdot \left(d - \frac{0.5 A_s f_y}{f_c b}\right) - M_E \tag{25}$$

where A_s [mm²] is the cross-section of the reinforcement, f_y [N/mm²] is the yield strength of the reinforcement, d [mm] is the effective depth of the cross-section, f_c [N/mm²] is the compressive strength of the concrete, b [mm] is the width of the cross-section and M_E [Nmm] is the bending moment acting on the critical cross-section. The characteristics of the beam are summarized in Table 1 (N: normal distribution; LN: lognormal distribution; DET: deterministic). The values for the standard deviations are based on the Probabilistic Model Code (JCSS 2001).

As described in section 2 the cross-section of the reinforcement decreases in time. The reduction of the diameter of the cross-section follows equation (3). Considering this equation and the characteristics in Table 1, the mean reinforcement area as a function of time is shown in Figure 2. Note that the coefficient of variation is constant in time since w/c and a are constant. The cross-section of the reinforcement is reduced from 804 mm² to 670 mm² after 50 years.

Table 1. Characteristics of the reinforced concrete beam.

	Distribution	μ	σ
d [mm]	N	400	10
f_c [MPa]	LN	30	4.25
M_E [kNm]	N	40	18
f_y [MPa]	N	420	30
$Ø_0$ [mm]	N	16	0.16
n* [–]	DET	4	–
b [mm]	DET	200	–
w/c [–]	DET	0.4	–
a [mm]	DET	20	–

* The number of reinforcement bars.

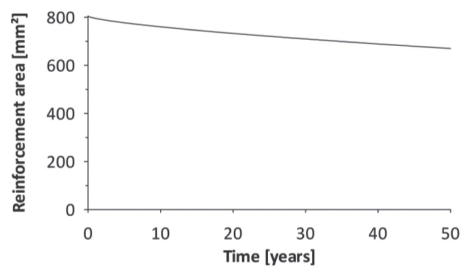


Figure 2. Reinforcement area as a function of time.

5.2 *Predictive reliability index*

Since the cross-section of the reinforcement is a function of time, also the reliability index is a function of time. Moreover, assuming that we have estimated the resistance parameters (i.e. d, f_c, f_y and $Ø_0$) from test data, this reliability index is not precisely known, as explained in section 3. The mean and standard deviation of the estimated parameters are summarized in Table 2. The standard deviation of the mean value $\overline{x}_i$ is calculated from $\sigma_i/\sqrt{(n)}$, where n is the number of samples (here assumed to be equal to 5). The coefficient of variation of the standard deviations Σ_i is assumed to be equal to 0.2 for all basic variables. It should be noted that the cross-section of the reinforcement is the only parameter that changes in time.

Using the characteristics mentioned above, we can calculate the mean and variance of β according to equation (8) and (9), by performing one single calculation of the reliability index and the parameter sensitivities, using the mean values of the parameters. The results of the FORM calculation with mean values of the parameters, as indicated in Table 2, is shown in Figure 3.

Initially, the mean reliability index μ_B is 4.2, which corresponds to a failure probability of 10^{-5}. After 50 years, the mean reliability index has decreased to 3.4, which corresponds to a failure probability of 3×10^{-4}. Hence the failure probability has increased with a factor 10.

Figure 4 shows the sensitivity factors for the basic variables as a function of time. The graph shows that the influence of the basic variables remains more or less constant in time.

Using the sensitivity factors from Figure 4 and the characteristics from Table 2, the standard deviation of the reliability index can be calculated according to equations (9) and (14). To illustrate the results, the dotted lines in Figure 3 show the interval $[\mu_B - \sigma_B; \mu_B + \sigma_B]$. This interval contains approximately 70% probability. As the sensitivity factors remain approximately constant in time, also the width of this confidence interval remains approximately constant. The coefficient of variation σ_B/μ_B varies from 0.110 at t = 0 to 0.108 at t = 50.

Finally, the predictive reliability index can be calculated using equation (7), since the mean and standard deviation of the reliability index are known. The result is shown in Figure 3 as a dashed line. The predictive reliability index decreases from initially 3.84 to 3.15 after 50 years. It is situated in the 70% probability interval.

5.3 *Robustness index*

Now that the mean value and the standard deviation of the reliability index are known, we can calculate an approximate value for the robustness index, as defined in section 4.3. β_i is the reliability index at t = 0 years and β_d is reliability index after a certain time period. The results of this calculation are shown in Figure 5. It shows the evolution in time of the mean value of the robustness index, obtained in different ways. The robustness index takes very high values short after corrosion initiation. This is the result of the small difference between the initial reliability index and the reliability index short after corrosion initiation. Further, the necessity

Table 2. Characteristics of the uncertain parameters.

	Mean M_i		Standard deviation Σ_i	
	$\overline{x}_i$	σ_{Mi}	σ_i	$\sigma_{\Sigma i}$
d	400	4.47	10	2
f_c	30	1.90	4.25	0.85
f_y	420	13.42	30	6
$Ø_0$	16	0.07	0.16	0.032

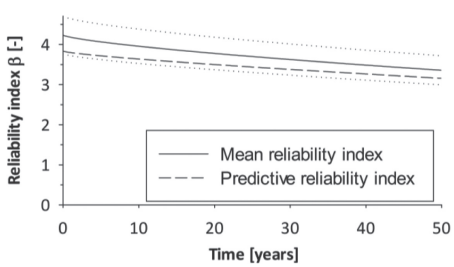


Figure 3. Mean reliability index and predictive reliability index as a function of time.

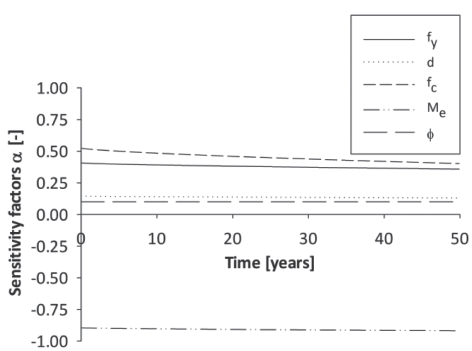


Figure 4. Sensitivity factors as function of time.

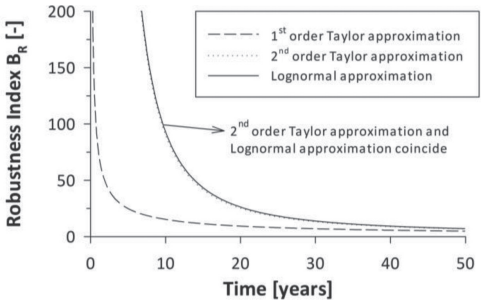


Figure 5. Mean value of the robustness index as function of the time.

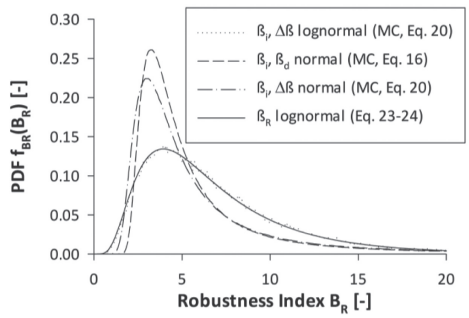


Figure 6. PDF of the robustness index.

of the use of higher-order Taylor approximations becomes clear when calculating the mean value of the robustness index in the first years: there is a big difference between the first order approximation and the second order approximation due to the non-negligible higher-order term. On the other hand, a very good agreement is found between the mean value of the robustness index calculated with a second-order Taylor approximation and the mean value calculated by assuming a lognormal distribution. This indicates that the lognormal approximation as proposed in section 4.3 is acceptable.

In order to compare the influence of the assumptions for the distribution of the reliability index, Monte-Carlo (MC) simulations were performed. Figure 6 shows the results. The curve for 'β_i, $\Delta\beta$ lognormal (MC, Eq. 20)' was obtained by generating 100,000 samples for B_i and ΔB, both following a lognormal distribution. Consequently, the robustness index was calculated according to equation (20). The curve for 'β_i, β_d normal (MC, Eq. 16)' was obtained by generating 10^7 samples for B_i and B_d, both following a normal distribution. The robustness index was calculated according to equation (16). The curve for 'β_i, $\Delta\beta$ normal (MC, Eq. 20)' was obtained by generating 10^7 samples for B_i and ΔB, both following a normal distribution. The robustness index was calculated according to equation (20). More simulations were necessary when using a normal distribution than when using a lognormal distribution, due to a slower convergence. The curve for 'β_R lognormal' represents the theoretical lognormal PDF, with its parameters calculated using equations (23) and (24).

The mode of the different PDF appears, more or less, at the same value for the different MC simulations.

The mean and standard deviations obtained by the MC simulations are summarized in Table 3. Considering the uncertainties, the mean of the robustness index predicted by the different methods is more or less the same. However, the normal approximations yield a higher standard deviation due to the heavy tail of the simulations using normal distributions.

Finally, the influence of parameter uncertainties on the characteristics of the robustness index is investigated. As an example, consider the robustness index at t = 50 years and its characteristics calculated with the lognormal approximation. The results are shown in Figure 7 and Figure 8, where the coefficient of variation or the number of samples for all variables is changed proportionally.

Table 3. Mean and standard deviation of the robustness index, obtained theoretically and by Monte-Carlo simulations.

	μ [–]	σ [–]
2nd order approximation	6.25	2.48
Lognormal approximation	6.44	3.78
MC—β_i, $\Delta\beta$ Lognormal	6.45	3.78
MC—β_i, β_d Normal	6.41	5.89
MC—β_i, $\Delta\beta$ Normal	6.51	6.30

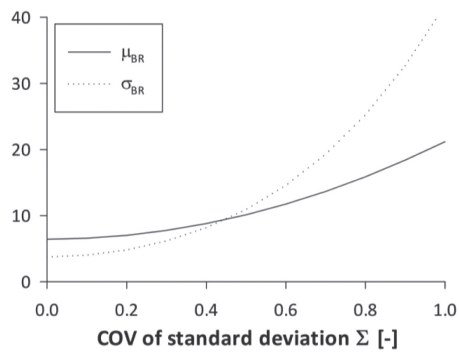


Figure 7. Influence of COV of Σ_i on the characteristics of the robustness index.

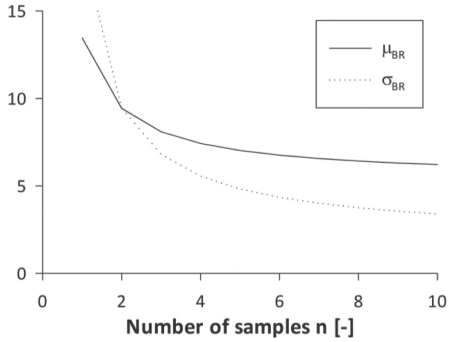


Figure 8. Influence of the number of samples for M_i on the characteristics of the robustness index.

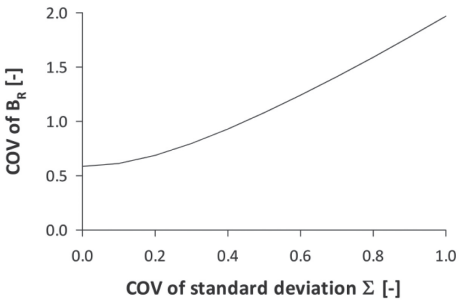


Figure 9. Influence of COV of Σ on the COV of B_R.

Figure 7 shows the influence of the coefficient of variation of the standard deviation of the influencing variables on the mean and standard deviation of the robustness index (the number of samples n remains constant). The graph indicates that both statistics increase significantly as soon as the coefficient of variation is higher than 0.2. The standard deviation increases more than the mean value.

Figure 8 shows the influence of the number of samples n on the characteristics of the robustness index (the coefficient of variation of the standard deviation remains constant). As the number of samples increases, the mean and standard deviation decrease significantly. When the number of samples is higher than five, the value of the characteristics becomes more or less constant.

Figure 9 and 10 summarize these results by showing the coefficient of variation of the robustness index as a function of the coefficient of variation of the standard deviation and the number of samples used to determine the mean value. The influence of the parameter uncertainties is significant: the coefficient of variation of the robustness index increases by a factor of three as the coefficient of variation of the standard deviation increases from

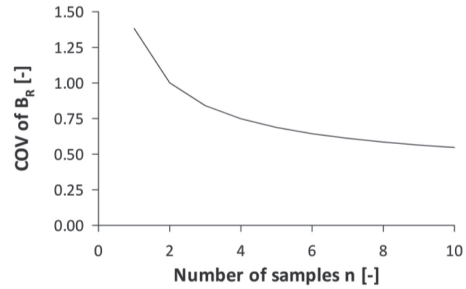


Figure 10. Influence of number of samples on the COV of B_R.

zero to one; and it decreases by a factor of 2.5 when the number of samples in increased from one to ten.

6 CONCLUSIONS

The quantification of the structural robustness under parameter uncertainties was investigated. Therefore, the framework, as developed by Der Kiureghian (2008) for the reliability index under parameter uncertainties, was extended for the reliability-based robustness index. The approximate calculation of the mean and standard deviation of the robustness index, assuming a lognormal distribution for the reliability index, agrees very good with the results from the calculation of these statistics through second-order Taylor approximations. Hence, the lognormal distribution can be considered as a good approximation for the distribution of the robustness index. Finally, the developed framework was applied on a reinforced concrete beam, subjected to chloride-induced corrosion. This showed that parameter uncertainties have a significant influence on the value and uncertainty of the robustness index.

ACKNOWLEDGEMENTS

Wouter Botte is a Research Assistant of the FWO Research Foundation Flanders. The authors wish to thank the FWO for the financial support on the research project “Structural reliability and robustness assessment of existing structures considering membrane action effects and Bayesian updating of test information”.

REFERENCES

Der Kiureghian, A. 2008 Analysis of structural reliability under parameter uncertainties. *Probabilistic Engineering Mechanics,* 23, 351–358.

fib 2006 *Model Code for Service Life Design*, FIB-Féd. Int. du Béton.

Frangopol, D.M. & Curley, J.P. 1987 Effects of damage and redundancy on structural reliability. *Journal of Structural Engineering,* 113, 1533–1549.

Fu, G. & Frangopol, D.M. 1990 Balancing weight, system reliability and redundancy in a multiobjective optimization framework. *Structural Safety,* 7, 165–175.

JCSS 2001 *Probabilistic Model Code.*

Papadopoulos, M.P., Apostolopoulos, C.A., Zervaki, A.D. & Haidemenopoulos, G.N. 2011 Corrosion of exposed rebars, associated mechanical degradation and correlation with accelerated corrosion tests. *Construction and Building Materials,* 25, 3367–3374.

Rodriguez, J., Ortega, L.M. & Casal, J. 1997 Load carrying capacity of concrete structures with corroded reinforcement. *Construction and Building Materials,* 11, 239–248.

Sørensen, J.D., Rizzuto, E., Narasimhan, H. & Faber, M.H. 2012 Robustness: Theoretical Framework. *Structural Engineering International,* 22, 66–72.

Stewart, M.G. & Rosowsky, D.V. 1998 Time-dependent reliability of deteriorating reinforced concrete bridge decks. *Structural Safety,* 20, 91–109.

Stewart, M.G. & Suo, Q. (2009) Extent of spatially variable corrosion damage as an indicator of strength and time-dependent reliability of RC beams. *Engineering Structures,* 31, 198–207.

Val, D.V. & Melchers, R.E. (1997) Reliability of deteriorating RC slab bridges. *Journal of structural engineering,* 123, 1638–1644.

Vu, K.A.T. & Stewart, M.G. (2000) Structural reliability of concrete bridges including improved chloride-induced corrosion models. *Structural safety,* 22, 313–333.

Yao, J.T.P. (1985) *Safety and Reliability of Existing Structures*, Pitman Advanced Publishing Program.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A condition-based deterioration model for the crack propagation in a submerged concrete structure

B. El Hajj & F. Schoefs
Research Institute of Civil Engineering and Mechanics (GeM), Nantes Atlantic University, Nantes, France

B. Castanier & T. Yeung
Research Institute of Communication and Cybernetics of Nantes (IRCCyN), École des Mines de Nantes, Nantes, France

ABSTRACT: In this paper, we want to promote a new approach for modeling the degradation of infrastructures for maintenance purposes. This approach is an intermediate between physical models, that can be complex to apply in a reliability context, and pure probabilistic models, that fail to reflect the physical degradation and therefore suffer from lack of acceptability by the Civil engineering community. We will propose here a new data-driven meta-model. The construction of the state-dependent degradation model will be discussed within an application of the cracking of a submerged concrete structure subject to corrosion. Numerical experiments will be conducted for identifying preliminary properties of our model in terms of statistical inference and reliability concerns.

The consequences of lack or bad maintenance of these infrastructures can be dangerous on human lives and impact the economy, i.e. the Storstrøm Bridge in Denmark built in 1937. In October–November 2011 all train traffic was cancelled immediately after an inspection finding damages. The main plan was to repair everything, but there are doubts on the ability of the bridge to handle the future freight traffic. The cost of a new bridge would be more than 3 billion DKK (400 M€). In August 2012 the Danish government allocated funds for the construction of a new bridge.

The world became aware of the importance of reliability and maintenance, especially after a wave of bridge failing in the USA in these last two decades, i.e. I-35 W Mississippi River Bridge built in 1967 and collapsed in 2007 killing thirteen people.

In Europe, a large number of the infrastructures are built after the Second World War, therefore it is very frequent to find infrastructures built 50 years ago and more. A third of the steel structures in the Atlantic area were built more than 100 years ago.

Hence, many structures require repair and rehabilitation. Some repaired structures exhibit poor repair performance and needs to be assessed and given a reliable safety level.

Furthermore, the growing demand for energy, motivated research to develop new means of production as well as new locations for this production. One of the most targeted sites is clearly coastal areas.

Currently we see more research focusing on the exploitation of offshore wind farms: these farms are located in a very aggressive environment for materials and for inspections to be carried out easily. In addition, the investment cost of these means of production makes the costs of exploitation of this energy not profitable compared to the cost of nuclear energy, for example.

Even thou the repairing and inspection techniques, especially non destructive techniques, are well developed and the mathematical models are highly complex, the ability to use the two of them for one maintenance problem remains extremely hard for both mathematicians and for engineers.

Maintenance decisions are a complex problem since they are a function of many uncertain factors such as material properties, costs, influenced-environment factors (behavior and impacts on the structure), imperfect inspections, manpower and risk expressed with the degradation level. In this study, we deal with the latter one.

A literature review of degradation models of structures and infrastructure in a reliability and maintenance optimization context shows two major trends, on one hand we have rich models based on the explanation of the physical degradation and on the other hand we have probabilistic models based on statistical quantities (Frangopol et al. 2004). In maintenance optimization, the quality of a model is no longer limited to its ability of modeling the pathology and its fit to the data

and available knowledge, but also for its quality to predict the future performance of the structure, its ability to integrate new observations, particularly from Non-Destructive Techniques (NDT) as well as its ease of implementation in a more complex decision optimization criteria.

Since the end of the 1990s degradation models grew to become more and more complex, incorporating physic-chemical and mechanical couplings, leading to an explosion in the number of parameters: i.e. it is common nowadays a 10-parameters propagation deterministic model of chloride ions while Type 90s model included 2. The use of these approaches in a reliability-context raises several problems: how "to randomize" models whose parameters are usually correlated random variables having no prior information on them and how to perform sensitivity studies in the absence of these trends? An alternative for the model's calibration is to associate the integration of expertise in the models and the multiplication of the associated experiments, which grows in number as a function of the parameter number. In addition to this, health-monitoring data usually coming from NDT is not directly linked to these physic-based models and their associated parameters.

One approach seems promising for maintenance optimization in Civil engineering is the construction of meta-models based on stochastic processes such as the gamma process (Van Noortwijk, 2009). It allows modeling the evolution of the degradation using observations via non-destructive techniques while maintaining the most critical aspects of the degradation mechanism in the model for the decision and an ease of integration in a more complex maintenance decision criteria. We may further highlight modeling difficulties when the selected pathologies have non-stationary behavior over time (acceleration or deceleration effects of degradation). Extensions called conditional or state-dependent models (Vatn 2012) and (Zouch et al. 2011) are used to model these non-stationary effects based solely on levels of degradation. However, it may be noted in the construction of their model that they fail to find a robust procedure for the identification of input parameters as well as a lack of application procedure, limitations making them difficult to appropriate and validate in an operating context (Riahi et al. 2010).

The main objective of this article is to promote the approach of meta-models or integrated-degradation models for the decision in the context of optimization of condition-based maintenance of structures and infrastructures. The construction of the state-dependent degradation model will be discussed within an application of the cracking of a submerged concrete structure subject to corrosion. Numerical experiments will be conducted for identifying preliminary properties and advantages of our model in terms of statistical inference and reliability concerns.

We find an advantage in using Meta-Models when addressing two main stakes:

- First, the ageing model description with a physical meaning of the main probabilistic trends and couplings of the inputs (NDT assessment) and outputs (decision parameter). With this approach, we tackle a key issue: the scourge between more and more complex physical models and the increasing complexity of NDT results modeling and assessment (decoupling, fusion …) with heterogeneous developments between these two scientific fields;
- Second, in a condition-based maintenance context, the simple description, flexibility, calibration and statistical calculation make this model easy to implement and beneficial to utilize in a risk management framework. The evaluation of these meta-models is done through state-dependent stochastic processes using information issued from non destructive techniques. The idea is to facilitate the transfer between available information and model.

This paper can be seen as an extension of the preliminary work presented in El Hajj et al. (2014).

This work is a part of the SI3M project (2012–2016 Identification of Meta-Model for Maintenance Strategies) by *Region Pays de la Loire* (*France*).

1 PROBLEM STATEMENT

One of the main risks for a submerged concrete structure is its rupture due to cracking. Several techniques are devoted to measure and monitor the evolution of cracks in concrete. In the case of a reinforced concrete structure, the steel frame has indeed strengthened the material property, but can also be a cause of new cracks because of its own corrosion.

The cracking process of a reinforced concrete structure can be divided into three phases: the diffusion of the aggressive agent (chlorides in this case), the corrosion of the reinforcement steel and the crack propagation from the reinforcement steel towards the surface. The first phase is characterized by the diffusion of chlorides in the concrete. When the chloride concentration on the surface of the reinforcement steel exceeds a threshold concentration, we have steel depassivation followed by the initiation of the corrosion. The second phase is dominated by the expansion of corrosion products in which they slowly fill the pores surrounding the reinforcement steel. Finally, the propagation phase

lies in the accumulation of corrosion which generates tensile stress and results in an excessive crack propagation of concrete cover till rupture. These three phases are shown in the graph in Figure 1. In this study propagation is assumed to result from the corrosion and not from fatigue.

We limit this study to the third phase, crack propagation. Within the context of this phase, the parameters of importance are the corrosion rate and the width of the crack (Li et al. 2006).

The corrosion rate, V_{corr}, represents the volumetric loss of metal per unit of area and unit of time (mm year^{-1}), can be obtained non-destructively from the corrosion current density, i_{corr} (uA/cm^2) through Faraday's law and the density of the metal. i_{corr} is an instantaneous rate of corrosion measured using a nondestructive technique, highly sensitive to external conditions (temperature, humidity …). Thus, it is important to note that for modeling and decision support calibration curves depending on the environmental conditions must be available or that inspections must always be carried out under identical conditions. We assume the second condition is verified, the first one has not been established generally (Breysse et al. 2009). Figure 2 represents the variation of the corrosion rate on all three phases of the cracking.

The crack is considered accessible by its width which is easily measured (Gauge block or image analysis). In Figure 3, Vu et al. (2006) draw the

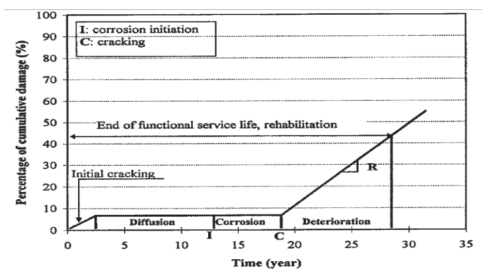


Figure 1. Degradation by corrosion of reinforced concrete (50 mm cover) by (Youping Liu, 1996).

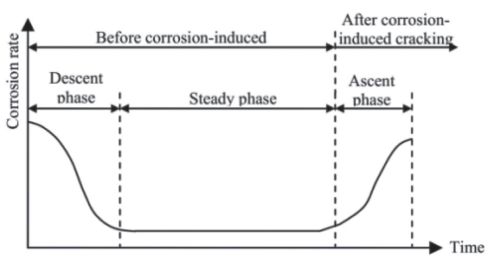


Figure 2. Variation of corrosion rate (Yuan et al. 2009).

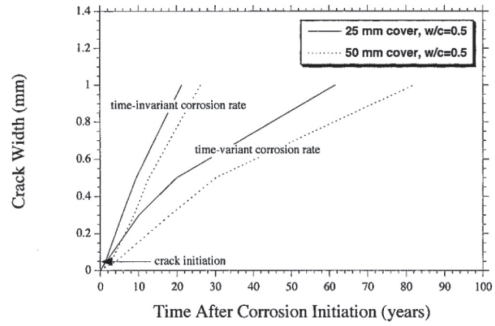


Figure 3. Variation of the width of crack—Phase 3 (Vu et al., 2006).

shape of the variation of the width of a crack versus time for two cases of corrosion rate (invariant or time-varying) and two coatings. The importance of modeling the corrosion rate by a cumulative process is clear. The hypothesis of an invariant corrosion rate is not conservative: in 20 years, it leads to an overestimation of 50% of the crack width.

As far as we know, no work has been published for studying the mutual dependencies of the two processes. One main reason can be attributed to the need of a high number of experiments that is not available for this particular phase; another good reason is that it's virtually impossible to integrate the mutual dependencies in the available physics-based models. However, the idea of modeling the degradation using two processes can be very rewarding in terms of maintenance and inspection optimization. First of all basing the maintenance decision on information coming from two sources of inspections can be more reliable than information coming from one (paragraph 3.2). Secondly, this can be appealing to inspection optimization in a sense that the decision maker can combine the information given by the two inspection modes.

Moreover, the time dependence of the two processes is non-stationary and the patterns can be considered as state-dependent (the evolution laws depend on the level of the current degradation). Finally, these two variables form a bivariate cumulative process where the two sub-processes are mutually dependent.

We propose here to define the bivariate process $(\rho_t, \theta_t)_{\forall t \geq 0}$ as a state dependent stochastic process similar to the one presented in Zouch et al. (2011). The evolution of degradation over a period of time τ is given by positive increments for the degradation processes respectively $(\Delta\rho, \Delta\theta)$ which are continuous random variables. A suitable candidate for these laws of distribution of each increment of the structure's degradation (Van Noortwijk, 2009) is the gamma distribution with two parameters (and

β where: (is the shape parameter and β is the scale parameter. In the described bivariate state-dependent case, we will consider that the shape parameter is a function of the current state.

In summary, the bivariate model is based on the two variables of interest: the size of the crack (maximum size of one structural component) and the rate of corrosion. As a result, the propagation of a crack is controlled by the combination of two state-dependent gamma processes:

– $(\rho_t)_{\forall t \geq 0}$ modeling the width of the crack « a » (mm)
– $(\theta_t)_{\forall t \geq 0}$ modeling the corrosion rate « i_c » (µA/cm^2).

It is essential to describe the relationship between the two sub-processes. To this aim, a choice was made based on a mechanical reason; there is a cause-effect relationship between the corrosion rate and the width of the crack. When the corrosion accelerates (corrosion rate increases), the crack undergoes more stress, which will translate in an acceleration of the cracking.

The correlation will be modeled in terms of mutual acceleration effects directly in each of the shape parameters of the gamma distributions. This model is sequential in the sense that in a first step we seek to characterize the evolution in terms of changes in the corrosion rate (Eq. 1) before doing so for the cracking itself (Eq. 2).

Finally, the advantage of a state dependent approach is that it transforms the process into a stationary one (with respect to time). We can then write, $\forall(\rho,\theta) > 0$:

$$\Delta\theta(\tau:\rho,\theta) \sim gamma(\alpha_\theta(\rho,\theta)\cdot\tau,\beta_\theta) \quad (1)$$

$$\Delta\rho(\tau:\rho,\theta,\Delta\theta) \sim gamma(\alpha_\rho(\rho,\theta,\Delta\theta)\cdot\tau,\beta_\rho) \quad (2)$$

Note.—To simplify the identification process, we consider that the state dependence is exclusive to the shape functions: the scale functions β_θ and β_ρ are considered constant throughout the life cycle. Therefore, we have to define the shape functions α_θ and α_ρ.

The choice for each shape function is based on the evolution of its process in time. In this case, it was found convenient to propose the following shape functions, $\forall(\rho,\theta) > 0$:

$$\alpha_\theta(\rho,\theta) = (a_3\cdot\rho + a_4)\cdot e^{\frac{-(\theta-a_1)^2}{a_2}} \quad (3)$$

$$\alpha_\rho(\rho,\theta,\Delta\theta) = \left(a_6\cdot\left(\theta+\frac{\Delta\theta}{2}\right)+a_7\right)\cdot e^{-a_5\cdot\rho} \quad (4)$$

The definitions of the parameters are presented in the Table 1.

Table 1. Definition of parameters.

Parameter	Definition
β_θ, β_ρ	Proportionality factors common to different structures (materials, …)
a_1	Abscissa of the inflection point of the realizations of corrosion rate
a_2	Reflects the dispersion around the inflection point
a_3, a_6	Acceleration coefficients
a_4	Corrosion rate speed at the origin
a_5	Reflects the kinetics of the process ρ
a_7	Crack growth rate at the origin

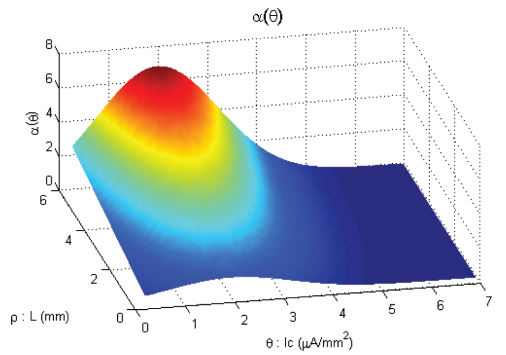


Figure 4. Shape function of the θ process—$\alpha_\theta(\rho,\theta)$.

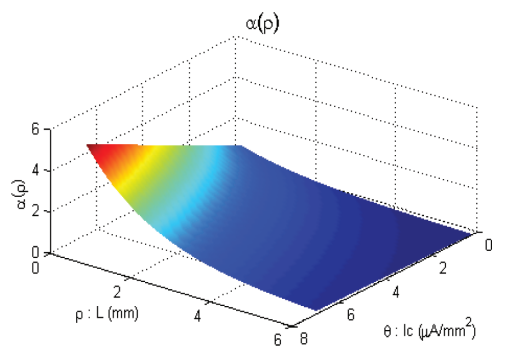


Figure 5. Shape function of the ρ process for constant $\Delta\theta - \alpha_\rho(\rho,\theta,\Delta\theta)$.

Figure 4, 5 illustrate the respective ρ and θ shape functions for given parameters.

The estimation of the parameters is carried using the method of the maximum like-hood on the database. We assume the existence of a database formed by successive perfect measurements of the crack width and the rate of corrosion of n structures denoted $\left\{\left(\rho_t^{(j)},\theta_t^{(j)}\right), t \geq 0,\ j \in [\![1,n]\!]\right\}$.

2 STATISTICAL PERFORMANCE ANALYSIS

In this section, we propose to conduct a set of numerical analyzes to highlight the statistical inference of the model properties.

2.1 *Convergence of the estimation procedure*

We propose an iterative Maximum Likelihood Estimator heuristic for the estimation of the parameters. The objective of this study is to analyze the convergence of our algorithm as a function of the sample size of the database. The Mean Squared Error is used as the performance criteria. We consider that the database is constructed from periodic inspections at a fixed time step τ on independent but identical structures. Two values define the size of the database N: the number of inspected structures n and the number of inspections carried out on each one of these structures T.

To illustrate the performance of our model and its convergence, we propose to evaluate the Mean Squared Error (MSE), Eq. 5, of the estimated parameter vector $\hat{\Theta}$ given the true parameter values Θ^*:

$$MSE = trace\{E\{(\hat{\Theta} - \Theta^*)(\hat{\Theta} - \Theta^*)^T\}\} \quad (5)$$

Table 2 summarizes the MSEs estimations for each one of the 9 parameters, for the total MSE per process, MSE_θ and MSE_ρ, and for the process MSE_t.

These results illustrate the convergence of the approach and more specifically the effects of the number of inspected structures and the number of inspections per structure.

We wanted to investigate the quality of the estimation based on the number of structures to monitor n and on the observation time per structure $T * \tau$.

Before going into the details of the analysis, we can emphasize that the number of data needed to obtain a good estimate may appear important. However, we recall here that we are interested in estimating laws on the entire life cycle of a structure in which the number of parameters, however, remain quite significant.

We can note a variety of behaviors depending on the parameters. We principally retain that the procedure favors the estimation of scale parameters and the parameters of the shape functions directly related to the level of cracking. This is mainly observed for samples of very small size. This can be explained by the fact that the corrosion rate level at $t = 0$ at the in-itiation of the crack is a random variable varying within a given range while the value at the origin of ρ is fixed. It is therefore difficult to calibrate the tails of the distributions when the only observations are concentrated in the early life cycle ($T = 5$) with a small number of structures ($n = 5$). To conclude this section, one can measure the compromise between extending the observation period and increasing the number of structures to monitor (we then take for a sample size $n * T$ with different n and T and we compare the MSE_t). In our experimentation, we can see a very fast compensation when adding new structures. This point is particularly interesting in the sense that it is often easier to find analogous structures than wait for the next inspection.

2.2 *Application to Eurocode 2*

Given the lack of models and data for the cracking propagation phase it is difficult to compare our approach with the literature. We propose here to highlight the benefits, in terms of quality of prediction and propagation of uncertainty for a given

Table 2. Mean Squared Error (MSE).

T	n	n^*T	a_1	a_2	a_3	a_4	β_θ	MSE_θ	a_5	a_6	a_7	β_ρ	MSE_ρ	MSE_t
5	5	25	0,524	246,3	0,485	0,856	0,0030	247,4	0,601	236,149	780,824	0,0029	1011,3	1258,7
	10	50	0,032	5,440	0,193	0,468	0,0016	6,097	0,067	5,190	0,219	0,0015	4,904	11,001
	20	100	0,012	0,054	0,096	0,228	0,0007	0,381	0,028	1,230	0,103	0,0007	1,288	1,668
	50	250	0,014	0,031	0,057	0,075	0,0003	0,161	0,009	0,471	0,188	0,0003	0,652	0,813
10	5	50	0,058	0,123	0,368	0,641	0,0031	1,154	0,040	4,091	0,427	0,0020	4,060	5,214
	10	100	0,081	0,123	0,332	0,327	0,0017	0,803	0,017	1,420	0,568	0,0010	1,917	2,720
	20	200	0,020	0,042	0,091	0,209	0,0007	0,332	0,009	0,548	0,081	0,0005	0,619	0,951
	50	500	0,022	0,036	0,056	0,090	0,0003	0,155	0,003	0,237	0,098	0,0002	0,333	0,489
20	5	100	0,161	0,227	0,672	0,450	0,0040	1,348	0,014	1,615	0,979	0,0018	2,530	3,878
	10	200	0,082	0,153	0,257	0,340	0,0024	0,752	0,006	0,646	0,236	0,0008	0,868	1,620
	20	400	0,048	0,090	0,152	0,237	0,0013	0,450	0,003	0,275	0,086	0,0004	0,359	0,809
	50	1000	0,025	0,051	0,067	0,132	0,0007	0,197	0,001	0,100	0,029	0,0002	0,130	0,326

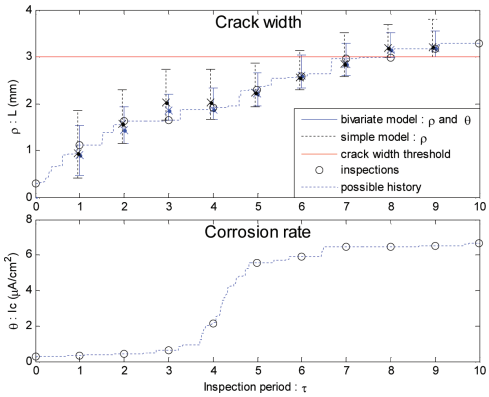


Figure 6. A tracking simulation of a structure and indicators on the quality of prediction of the cracking with and without taking into account the rate of corrosion.

structure, of the introduction of the θ-process in the overall cracking process.

In Figure 6, the dotted lines correspond to one possible history of the cracking structure extracted from the generic database. According to Table 7. N from Eurocode2, for an exposure class XS2 (Corrosion of the reinforcement induced by chlorides from sea water) the performance of the reinforced concrete structure are assumed modified when the width of a crack is greater than or equal to 3 mm.

For each period, τ, an inspection is conducted and the observed values are noted (black circles). For each observation, the expected value of degradation is estimated for the next inspection as well as its confidence interval of 90% when taking into account all the information (ρ and θ), blue lines, or just ρ (green lines). These quantities are obtained using stochastic simulations.

The advantage of our method is clearly illustrated in the decrease of the confidence interval. This illustration provides a better integration of the Eurocode 2 in the reliability decision of structures by adding the corrosion factor; the failure can be then defined as a level of risk related to changes in the performance of the structure for a given interval of time.

3 APPLICATION TO RISK MANAGEMENT

The aim of this section is to illustrate an application of the model in a risk management context. A structure is said to be safe if the probability of failure P_f at any time is lower than a given threshold. Such a safety requirement is given in Eurocode 2 by a failure cracking threshold L as a function of the characteristic of the structure and its environmental conditions.

In case of inspection, the decision criterion becomes the probability of having a failure before the next inspection should be lower than P_f.

The probability of a failure in the next inspection denoted $P_f(\rho_i, \theta_i)$ is a function of the current observation (ρ_i, θ_i) and given by the following equation:

$$P_f(\rho_i, \theta_i) = P(\Delta\rho + \rho_i > L \mid \rho = \rho_i, \theta = \theta_i) \tag{6}$$

For a selected range for ρ ($0 < \rho < L = 3$ mm) and θ, simulations were done for estimating the probability of failure for every possible combination (ρ, θ), Figure 7.

The use of such a curve in risk management could be in a classical way where the P_f threshold defines the acceptance and critical areas (in Figure 8, e.g. the system is said to be safe for any (ρ, θ) in the acceptance area under the iso-curve for a $P_f = 0.05$).

It is also easy to define a safety area with two thresholds and a specific attention or preventive action could be done to reduce the current risk level.

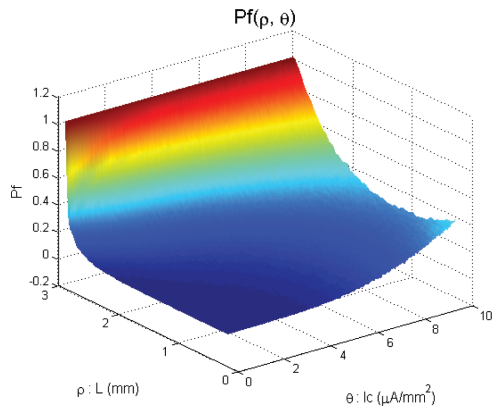


Figure 7. Probability of failure based on degradation level.

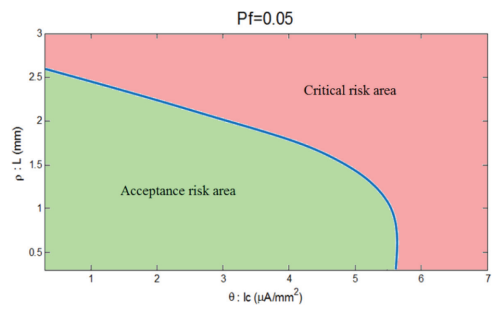


Figure 8. Smoothed iso-curve of the degradation levels for a given probability of failure equals to 0.05.

One major advantage of the proposed approach in risk management is that the decision can be modulated according to additional observation, given that θ can be seen as an acceleration factor of the cracking.

4 CONCLUSION

In this article the Meta-Model approach (El Hajj et al. 2014) is applied and discussed within an application to the cracking of a submerged concrete structure subject to corrosion. The degradation model is based on two correlated processes constructed by NDT data. Expert knowledge is introduced to reflect the main useful degradation properties that the model should tackle for decision-making. This allows both to simplify the construction and the fitness of the model to the data and to overcome some limits in the current practices in Civil Engineering (here the correlation between the crack width and the corrosion rate). We are aware that the construction of the model and, of course, the performance study is not based on field data, but we are confident in the philosophy of the approach and hope that it will help in the future data collection.

This work can also be seen as a preliminary work in the sense that we restrict the cracking phase to the propagation of a crack onto the surface of the structure. From a maintenance optimization perspective, it should be important to have a complete degradation model for the whole lifecycle. The meta-model construction approach will integrate the identification of the different processes in each phase of the cracking and the transition from one phase to the other.

Another perspective could be in modeling the actualization of the degradation model after a new inspection is done. Bayesian updating could be of interest since the bivariate aspect of the degradation process and the state-dependent degradation laws can make the modeling harder.

ACKNOWLEDGMENTS

The authors of this paper would like to thank the *Region Pays de la Loire* (France) for its support to the SI3M project.

REFERENCES

Breysse, D., Yotte, S., Salta, M., Schoefs, F., Ricardo, J. & Chaplain M., 2009. Accounting for variability and uncertainties in NDT condition assessment of corroded RC-structures. *European Journal of Environmental and Civil Engineering*, 13(5): 573–591.

El Hajj, B., Castanier, B., Schoefs, F. & Yeung, T., 2014. Methodology for the construction of a new meta-model for structure maintenance. *8èmes Journées Nationales de Fiabilité des Matériaux et des structures.*

Eurocode 2, Calcul des structures en béton (EN 1992).

Frangopol, D.M., Kallen, M.-J. & Van Noortwijk, J.M., 2004. Probabilistic models for life-cycle performance of deteriorating structures: review and future directions. *Progress in Structural Engineering and Materials*, 6(4): 197–212.

Li, C.-Q., Melchers, R.E. & Zheng, J.-J., 2006. Analytical Model for Corrosion-Induced Crack Width in Reinforced Concrete Structures. *Structural Journal*, 103(4): 479–487.

Riahi, H., Bressolette, P. & Chateauneuf, A., 2010. Random fatigue crack growth in mixed mode by stochastic collocation method. *Engineering Fracture Mechanics*, 77(16): 3292–3309.

Van Noortwijk, J.M., 2009. A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety*, 94(1): 2–21.

Vatn, J., 2012. A state based model for opportunity based maintenance. *In 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 Volume 1*. pp. 1–4.

Vu, K., Stewart, M.G. & Mullard, J., 2006. Corrosion-Induced Cracking : Experimental Data and Predictive Models. *Structural Journal*, 102(5): 719–726.

Youping Liu., 1996. Modeling the Time-to-Corrosion Cracking of the Cover Concrete in Chloride Contaminated Reinforced Concrete Structures, PhD thesis, *Virginia Polytechnic Institute and State University.*

Yuan, Y., Ji, Y. & Jiang, J., 2009. Effect of corrosion layer of steel bar in concrete on time-variant corrosion rate. *Materials and Structures*, 42(10): 1443–1450.

Zouch, M., Yeung, T. & Castanier, B., 2011. A Two-Phase State-Dependent Deterioration Model for Maintenance Optimization.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability assessment of cast-iron heritage structures

J. Marková, M. Holicky, K. Jung & A. Podstawka
Klokner Institute, Czech Technical University in Prague, Czech Republic

V. Bures
Faculty of Art and Architecture, Technical University of Liberec, Czech Republic

ABSTRACT: The reliability methods provided in ISO 13822 are applied for the reliability assessment of heritage structures. For practical application, the actual characteristics of existing materials are needed. The material properties can be updated using material tests of inspected structures. The behaviour of an existing structure and the previous load history should be considered when deciding about its further use and rehabilitation. As it is shown, the probabilistic methods may be effectively applied for reliability verifications and decisions about the intervention of cast-iron columns in an industrial heritage building.

1 INTRODUCTION

A number of factories, textile mills, warehouses and other industrial buildings, built from about 19th century up to beginning of 20th century in the Czech Republic, have been registered as industrial heritage monuments. Such structures are mostly of significant architectural, historic, technological or social value. They often form part of the urban landscape and provide the cityscape with visual historical landmarks, Beran et al. (2007).

When they are put out of service, the heritage buildings often degrade and turn into ruins. Reuse and adaptation of such buildings allows the integration of industrial heritage buildings into a modern urban lifestyle and also helps to protect cultural heritage. The buildings are often rebuilt to hotels, museums, residential buildings, commercial centres etc.

2 ASSESSMENT OF HERITAGE STRUCTURES

The assessment of existing structures including heritage ones differs in many aspects from the procedures taken during the design of new structures and may require the application of sophisticated methods, in many cases beyond the scope of common standards for structural design. The prescriptive documents used for the design or verification of new structures cannot be directly applied to the assessment, as the actual state of the structure and its materials must be considered. Moreover, the current standards have often more severe requirements than the standards that were applied at the time when the structure was originally designed. Although some existing structures appear to have a lower reliability level than is presently required for new structures, they may continue to fulfil their functions for many years.

This situation leads to the question of how to specify a suitable reliability level for existing structures when they are planned to be repaired or upgraded. For the optimal decision on structural rehabilitation, the principles of the theory of structural reliability and probabilistic optimisation may be effectively applied, Markova et al. (2013).

General requirements and procedures for the assessment of existing structures based on the theory of structural reliability are provided in the international standard ISO 13822 (2010) including new Annex I on heritage structures.

For practical applications, information on the properties of various construction materials is given in the set of Czech National Annexes to ISO 13822 (2010) which was developed within the new national standard CSN 73 0038 (2014).

One important requirement should be considered during the assessment of existing structures, though it is not explicitly given in ISO 13822 (2010): how to preserve the appearance and materials of heritage structures. Sustainability considerations are more important for the assessment of existing structures than for the design of new structures. Most important differences in the evaluation of functional criteria on structural reliability of new and existing structures are indicated in Table 1. The heritage value of a historic structure resides in the authenticity and integrity of its character-defining elements. To retain its authenticity and integrity, the structure should be preserved, as far as possible,

Table 1. Different viewpoints concerning functional criteria.

Considerations	Existing structures	New structures
Economic	Usually significant incremental costs for reliability enhancement	Usually lower incremental costs for reliability enhancement
Social	May be significant in the case of restriction or exclusion of exploitation and preservation of cultural heritage	Usually less significant than for existing structures
Sustainability	Preferably, existing building materials would be used (leading to reduction of waste materials)	Mostly new materials are used

with its original materials and structural concept intact. However, in some cases the verification of material properties may represent rather a difficult problem. This is particularly true for existing cast-iron columns having significantly different material properties from current structural steels.

An example of the assessment and successful reconversion of an existing industrial building is shown below.

3 ANALYSED INDUSTRIAL BUILDING

A spinning factory was built in the centre of the city of Liberec in North Bohemia in the year 1868. The factory served its purpose up to 1930. Then the building was out of use until 1990, when it was converted to a gallery with a coffee bar, later to a warehouse. Finally it was closed down, an act which led to its gradual degradation.

Recently, it was decided to include the building in the list of regional monuments and to carry out its rehabilitation. The existing industrial heritage building is intended to be used for residential purposes and as a coffee bar. One of the main concerns during the rehabilitation is to preserve the historical character of the building, including heritage structures with old cast-iron columns.

The building with its ornamental façade, just before its rehabilitation is shown in Figure 1.



Figure 1. Industrial heritage building.



Figure 2. A load bearing structure with cast-iron columns.

4 INSPECTION OF EXISTING STRUCTURES

The building made of fired solid bricks consists of three timber floors supported by cast-iron columns with ornamental heads (Fig. 2) carrying timber beams and timber floors. The wood was in some parts attacked by insects or dry rot.

It should be noted that the cast-iron columns were used in various industrial and public buildings erected in the Czech Republic during the 19th and early 20th centuries.

Visual inspection revealed that the masonry structures and cast-iron columns were without any significant damage of a static character. The geometry of all the cast-iron columns including their thickness were measured in the heights of 1 and 2 m above the floor level. The average values for selected columns are illustrated in Table 2.

The actual thickness of all the columns varied along their height and was surprisingly reduced in all the columns on the second floor. It should be noted that it was very difficult to obtain reliable information about the actual external and internal geometrical imperfections of the cast-iron columns.

Grey cast-iron is characterized by a high compressive strength and significantly reduced tensile

Table 2. Thickness of selected columns in mm.

Floor No.	Height of measurement	Thickness t of column No.		
		1	2	3
1st	1 m	21	22	21.5
	2 m	17.5	18	18.3
2nd	1 m	16	15.8	14.6
	2 m	14.7	15.5	14.4
3rd	1 m	17.4	17.2	16.4
	2 m	17.1	16.8	16.1

strength caused by the relative high carbon content between 2 and 5%. The behaviour of the material is ductile in compression and brittle in tension.

Non-destructive tests of the material hardness of the columns were made by the hardness tester TH 130 and then converted by means of a standardised relationship to the ultimate strength in compression. The results indicated that the ultimate strength of the cast-iron varies in a rather broad range from 665 to 800 MPa.

The material hardness was tested at two levels (1 and 2 m) in different parts of each column, and then converted to ultimate strength. The characteristic value of ultimate strength is estimated on the basis of EN 1990 (2002), Annex D. For example, for the selected column, the mean $m = 702$ MPa and the sample standard deviation $s = 50$ MPa are statistically evaluated for six measurements ($n = 6$) and the coefficient $k_n = 2.18$ (assuming lognormal distribution). The characteristic value of ultimate strength of cast-iron is estimated as

$$f_{u,k} = m - k_n s = 702 - 2.18 \times 50 = 593 \text{ MPa} \qquad (1)$$

The design value of ultimate strength $f_{u,d}$ may be roughly estimated for the column from expression (1), considering here the coefficient $k_n = 6.36$. Therefore, it leads to the estimation of the design value of yield strength $f_{yd} = 385$ MPa.

In case the validity of the ratio $f_u/f_y = 2$ between the ultimate compressive strength f_u and yield strength f_y (0.2% proof stress) could be considered, Rondal & Rasmussen (2004), then the characteristic value of yield strength is $f_{yk} \sim 300$ MPa and the design value may be estimated as 190 MPa. It is known that the tensile strength may be considered about one third of the compressive strength (about 60 MPa).

Due to the demands of preservationists not to damage the heritage structures, the results of the non-destructive tests were not calibrated by destructive tensile tests on the samples. Therefore, only a small sample of the material was extracted for a small punching test and the microscopic

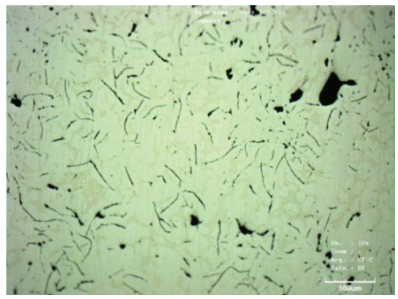


Figure 3. Microscopic analysis of the composition of cast-iron.

analysis of the column material was made (Fig. 3). The prepared material samples were analysed by means of a confocal laser microscope, which confirmed the type of cast iron. Black smudges formed by lamellar graphite are characteristic of gray cast iron. This graphite forms voids or cracks within the iron matrix and leads to considerably reduced tensile strength.

CSN 73 0038 (2014) contains a set of National Annexes to ISO 13822 (2010) and recommends material characteristics of cast-iron which may be applied for the verification of columns when further information is not available. The design value of yield strength under compression, and also compression strength in combination with bending is estimated in CSN ISO 13822 (2010) to 100 MPa (assumed to be a conservative estimate) and modulus of elasticity $E = 100$ GPa.

5 VERIFICATION OF A COLUMN

5.1 *Partial safety method*

Firstly the partial factor method representing the basic method given in EN 1990 (2002) is applied.

For the specification of the load-bearing capacity of the columns on each floor of the heritage building, actions due to self-weight, permanent actions, imposed loads and snow loads are considered. The column on the first floor is furthermore loaded by the masonry vault. Imposed loads for residential areas (category A) and two alternatives of a bearing floor structure are considered (alt. I—reinforced concrete slabs, alt. II—composite timber concrete slabs). Snow is determined according to the Czech snow map given in the nationally implemented EN 1991-1-3 (2003). The characteristic value of snow action in the site location is $s_k = 1.5$ kN/m^2.

Selected results of the analysis of internal forces and using up capacity (in%) are presented in Table 3 for specified material characteristics

Table 3. Reliability assessment of a column for the design strength f_{yd} = 190 MPa.

Alternative	Floor No.	N_{Ed} (kN)	N_{Rd} (kN)	Capacity (%)
I	3rd	350	405	86
	2nd	627	317	198
	1st	985	799	123
II	3rd	199	405	49
	2nd	328	317	104
	1st	530	799	66

Table 4. Reliability assessment of columns for the design strength f_{yd} = 100 MPa.

Alternative No.	Floor No.	N_{Ed} (kN)	N_{Rd} (kN)	Capacity (%)
I	3rd	350	225	155
	2nd	627	176	356
	1st	985	444	222
II	3rd	199	225	89
	2nd	328	176	187
	1st	530	444	119

of the in situ material testing, and in Table 4 for characteristics of the cast iron recommended in CSN 73 0038 (2014).

The results revealed that when the composite, lightweight timber-concrete floor would be designed (alt. II), and for material strengths based on measurements, the columns need not to be further strengthened.

In the cases when heavier floor structures (alt. I) or material characteristics given in ČSN 73 0038 (2014) are considered, most existing columns need to be strengthened, as they do not satisfy the basic reliability condition $R > E$.

Strengthening the columns by concreting their holes may be considered as a common method for which the basis of EN 1994-1-1 (2004) may be applied.

However, the efficacy of such a strengthening in the case of historic materials like cast iron differs from modern steels, and depends considerably on mutual interaction between the cast-iron and the concrete. Therefore, some further guidance is needed than that presently provided in Eurocodes, see e.g. Heider & Geisler (2007).

It should be mentioned that other methods of strengthening might also be applied, e.g. using strips of FRP polymers, see EN 1998–3 (2005).

However, each method of strengthening brings some advantages but also disadvantages which should be taken into account including simplicity of execution, fire resistance and the economic aspects.

5.2 *Probabilistic methods*

Probabilistic methods can be used for the verification of existing structures, or for the assessment of their residual lifetime, when appropriate probabilistic models of the basic variables are known. General guidance for the probabilistic verification of structures including the models of basic variables is given in the JCSS Probabilistic Model Code (2001).

For the probabilistic assessment of existing structures, the limit state function g($\boldsymbol{X}$) should be specified for the vector $\boldsymbol{X}$ of the basic variables. The variables entering the limit state function are random variables. Their characteristics may be described by means of probability theory and mathematical statistics. It is assumed that the structure is reliable for the inequality g($\boldsymbol{X}$) > 0. The reliability indicator, failure probability P_f is given as

$$P_f = \int_{g(X)<0} \varphi_X(x)\,dx \tag{2}$$

where $\varphi_X(\boldsymbol{x})$ is the joint probability density for the realisation of vector $\boldsymbol{x}$. Another reliability indicator is the generalized reliability index $\beta = -\Phi^{-1}(P_f)$ defined on the basis of failure probability P_f where Φ is the standardised normal distribution function.

Reliability analysis is based here on the limit state function g($\boldsymbol{X}$) corresponding to the load effect E and resistance R of the column

$$g(K_E\boldsymbol{E}, K_R\boldsymbol{R}) = K_R\,\boldsymbol{R} - K_E\,\boldsymbol{E} \tag{3}$$

Here $\boldsymbol{X}$ denotes the vector of basic variables (random variables entering the right hand side of this equation), K_R denotes the factor expressing the uncertainty of the resistance model and K_E the factor expressing the uncertainty of action effect model.

Models of basic variables are given in Table 5 (r denotes a column radius). The mean μ_X and the

Table 5. Models of basic variables.

Symbol	Distribution	Mean μ_X	Standard dev. σ_X
f_c	LN	$f_{ck} + 2\,\sigma$	0.10μ
f_y	LN	$1.45 f_{yk}$	0.15μ
r	N	r	$0.05\,\mu$
t	N	t	0.02
K_R	N	1	0.15
K_E	N	1	0.05
G	N	G	0.1G
Q_{Imp}	GUM	$0.6\,Q_{\mathrm{Imp}}$	$0.35 Q_{\mathrm{Imp}}$
Q_{Sn}	GUM	$0.35 Q_{\mathrm{Sn}}$	$0.7 Q_{\mathrm{Sn}}$

standard deviation σ_X of each variable are related to the characteristic value X_k used in the design calculations. For the reliability analysis of the column, the imposed load is considered here as a leading variable action and snow as an accompanying action (combination of 50 year maximum Q_{Imp} and an annual Q_{Sn}).

The results of the probabilistic analysis of a cast-iron columns indicate that when a reinforced concrete slab is applied and material properties of columns updated by testing are considered then the reliability index β is around $\beta \sim 3.5$ which is a little lower than the target value indicated in ISO 13822 (2010) for common types of structures in the consequence class CC2. In case the material properties recommended in the CSN 73 0038 (2014) need to be considered then the resulting reliability is very low ($\beta = 1.5$ only).

In case a lightweight composite timber concrete slab is applied in building rehabilitation then the reliability index $\beta = 4$ is determined for updated material properties, while $\beta = 2.4$ is determined only in case that the default material characteristics recommended for cast-iron columns in CSN 73 0038 (2014) are considered.

It appears that it is unnecessary to strengthen the cast-iron columns in case the updated material properties of the column are considered. However, when material property given in CSN 73 0038 (2014) is used in the analysis and no further information is known then the reliability of the columns is rather low and the columns should be strengthened.

Various uncertainties may exist about the real material properties and geometric imperfections of the cast-iron columns of the industrial heritage building. However, there is a clear evidence that the heritage structure of the spinning factory withstood for more than one hundred years considerably greater imposed loads than presently required for residential purposes.

Therefore, taking into account results of the reliability analyses and the previous good behaviour of a structure it could be recommended to leave the existing columns without any intervention.

6 CONCLUDING REMARKS

General requirements and procedures for the assessment of existing structures based on the theory of structural reliability are provided in the recently revised international standard ISO 13822. Additional guidance on heritage structures is given in the recently developed Annex I to this standard.

The partial factor method and also probabilistic methods are applied for the reliability assessment of a regional industrial heritage building. When the default material properties given in the national codes are applied only, it appears that the historic structures should be commonly strengthened. It is shown that when the actual geometry and material properties based on experimental data are applied, the reliability of the cast-iron columns is acceptable and no intervention is needed.

It is shown that the previous long-term satisfactory performance of the existing cast-iron columns could also be taken into account.

It appears that the characteristics of historic cast—iron materials should be further analysed and a supplementary guidance given in the National Annexes to ISO 13822.

ACKNOWLEDGEMENTS

This study has been conducted as part of research project DF12P01OVV040 which is supported by the Ministry of Culture of the Czech Republic.

REFERENCES

Beran, L. et al., V. 2007. *Industralism of the Liberec region. Technical structures and industrial architecture.* CTU in Prague (in Czech).

CSN 73 0038. 2014. *Design of structures—Supplementary guidance for assessment of existing structures* (in Czech).

EN 1990. 2002. Basis of design.

EN 1991-1-3. 2003. *Eurocode 1 Actions on structures Part 1–3 General actions*—Snow Loads.

EN 1994-1-1. 2004. *Eurocode 4. Design of composite steel and concrete structures. General rules and rules for buildings.*

EN 1998-3. 2005. *Eurocode 8: Design of structures for earthquake resistance—Part 3: Assessment and retrofitting of buildings.*

Heyde S. & Geisler K., 2007. *Strength of concrete filled historic cast-iron columns.*

ISO 13822. 2010. *Basis of design—Assessment of existing structures.*

Markova, J. 2012. *Assessment of working life for bridges,* IALCCE.

Markova, J. & Holicky, M., Podstawka, A. 2013. Assessment and rehabilitation of existing bridges, In: *CESB 2013*, Prague.

Probabilistic *Model Code. 2001*. www.jcss.byg.dtu.dk. JCSS.

Rondal, J. & Rasmussen, K.J.R. 2004. On the strength of cast iron columns, *Journal of Constructional steel research*.

Swailes T. & Fernandes de Retana E.A. 2004. The strength of cast iron columns and the research work of Eaton Hodkinson, *The Structural Engineering*.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability of structures in national codes to Eurocodes

J. Marková & M. Holicky
Klokner Institute, Czech Technical University in Prague, Prague, Czech Republic

ABSTRACT: Alternative procedures for combination of actions together with reliability elements (partial and reduction factors) recommended in the national annexes to Eurocodes in some CEN member states, are investigated using probability-based reliability methods. Presented reliability analyses of structural members indicate that reliability level of some members might be in some cases lower than the required target reliability level and should be further calibrated.

1 INTRODUCTION

Presently the second generation of the Eurocodes for structural design is foreseen to be developed on the basis of document M/515 (2013) and financial support of European Commission. Recently various Working Groups (WGs) of the Committee CEN/TC 250 have been established including WG7 which is responsible for the evolution of the fundamental Eurocode EN 1990 (2002) for the basis of design. Several new topics are foreseen to be developed including provisions for non-linear structural analyses and fatigue. Annexes A1 and A2 for buildings and bridges will be improved and Annexes A3 to A5 for cranes and machinery, silos and tanks and towers and masts will be transferred to EN 1990 (2002) from appropriate parts of EN 1991 and EN 1993. Moreover, Annex B of EN 1990 (2002) on the management of structural reliability for construction works is intended to be further developed considering execution quality management. The revised Annex C will give information about reliability methods and also basis for the calibration of partial factors for actions and material properties. Chambers of civil engineers, construction and design companies and other users working in construction in various CEN Member States require simplification of Eurocodes and reduction of the current number of parameters NDPs (National Determined Parameters).

However, it appears that for further harmonization of Eurocodes the nationally selected NDPs should be verified including reliability elements as partial factors for actions and material properties, and also combination factors. Present activities of various associations in some CEN Member States including the Czech Republic are focused on the reduction of alternative load combinations and verification of partial factors for permanent and variable loads taking also into account original national standards. The technical subcommittees SC2 and SC3 for design of concrete and steel structures of CEN/TC 250 issued a resolution requesting examination and recalibration of the partial factors for permanent loads and for materials.

Such a recalibration of reliability elements should also take into account national decision given in the National Annexes to Eurocodes. Presently the CEN Member States are requested to upload their NDPs to the database of JRC for further statistical and theoretical analyses. It is expected that information on NDPs should also be available for the project teams facilitating analyses of reliability elements, see Resolution CEN BT (2013). About 2/3 of countries are uploading their NDPs to the JRC database.

Presently available information indicates that most European countries have adopted the values of partial factors and other reliability elements recommended in Eurocode EN 1990 (2002) for the basis of structural design. About half of the countries are applying an exp. (6.10) for verification of structures for the Ultimate Limit States (ULS) and other countries exps. (6.10a,b). Both alternatives (6.10) or (6.10a,b) are allowed to be use in some CEN countries including the Czech Republic (limitations in some countries for application of (6.10a,b) are given). Modified exps. ($6.10a_{mod}$,b) are applied in few countries where in the first expression the permanent actions are considered only. Some countries which preferred exps. (6.10a,b) increased the value of reduction factor ξ for permanent actions from the recommended value 0.85 up to 0.93 diminishing the difference in application of both alternative load combinations. Therefore, the reliability of structures designed according to the nationally implemented Eurocodes may differ from country to country (allowed by EC as a matter of their national safety).

It is expected that the feedback of practicing civil engineers and other users obtained during the application of Eurocodes will be used for the preparation of background materials facilitating further development of EN Eurocodes and will lead to their required harmonization. Presently the National annexes include recommendations concerning alternative procedures provided in EN 1990 (2002) for the fundamental combination of actions and selection of partial factors γ_G and γ_Q for permanent and variable actions. It was shown e.g. in Holicky & Markova (2005, 2010) that choice of the reliability elements significantly affects the resulting reliability level of construction works.

Submitted paper analyses nationally selected parameters of various CEN Member States including proposals for modification of material factors for concrete, reinforcement and steel. Structural members exposed to permanent and variable loads designed according to the recommendations of National Annexes to Eurocodes are analysed using probabilistic methods of structural reliability.

2 FUNDAMENTAL LOAD COMBINATIONS

EN 1990 (2002) introduces for the fundamental combination of actions in permanent and transient design situations (ULS of type STR) three alternative procedures, denoted here as A, B and C. Considering for simplicity one permanent action G and two variable actions Q (e.g. imposed loads) and W (wind actions), the exp. (6.10) of the combination rule A is given in EN 1990 for the design value of action effect E_d as

$$E_d = \gamma_G G_k + \gamma_Q Q_k + \gamma_W \psi_W W_k \quad (1)$$

An alternative procedure B is provided in EN 1990 by exps. (6.10a) and (6.10b) given as

$$E_d = \gamma_G G_k + \gamma_Q \psi_Q Q_k + \gamma_W \psi_W W_k \quad (2)$$

$$E_d = \xi \gamma_G G_k + \gamma_Q Q_k + \gamma_W \psi_W W_k \quad (3)$$

The less favourable action effect from (2) and (3) should be considered.

In addition, EN 1990 (2002) allows further modification of alternative B, simplifying equation (2) by considering permanent loads only (alternative C), denoted here as ($6.10a_{mod}$), thus the load effect is then

$$E_d = \gamma_G G_k \quad (4)$$

The less favourable action effect resulting from (3) and (4) is then considered.

If the leading action is wind W, then in equations (1) and (3) instead of reducing the wind action W by factor ψ_W, the imposed load Q should be reduced by appropriate factor ψ_Q. Factors γ_G, γ_Q and γ_W denote the partial factors of actions G, Q and W.

To investigate resulting load effects under various intensities of variable actions, the characteristic values of actions G_k, Q_k and W_k are related using quantity χ given as the ratio of variable actions Q_k+W_k to total load $G_k+Q_k+W_k$, and ratio k of accompanying action W_k to the main action Q_k as

$$\chi = (Q_k+W_k)/(G_k+Q_k+W_k),\ k = W_k/Q_k \quad (5)$$

The parameter χ may be commonly expected within a range from 0 to 0.6 for common buildings, however sometimes approaching to 1, e.g. in case of snow loads on light-weight steel roofs of industrial halls.

For a given design value of the load effect E_d, the characteristic values of individual actions G_k, Q_k, W_k can be expressed using variables χ and k as follows

$$G_k = \frac{E_d}{(\xi)\gamma_G + \dfrac{((\psi_Q)\gamma_Q + k(\psi_W)\gamma_W)\chi}{(1+k)(1-\chi)}}$$

$$\chi = (Q_k+W_k)/(G_k+Q_k+W_k),\ k = W_k/Q_k \quad (6)$$

The factors ξ, γ and ψ indicated in the first relationship of (6) in brackets are applied in the same way (either yes or no) as in equations (1), (3) for appropriate combination rules.

3 PROBABILISTIC ANALYSIS

EN 1990 (2002) allows a design directly based on the probabilistic methods. In accordance with the principles of these methods the basic variables are considered as random variables with appropriate distributions. It is verified that a limit state of a member is exceeded with a probability lower than the target value p_t given as

$$P(g(\boldsymbol{X}) < 0) < p_t \quad (7)$$

Here $g(\boldsymbol{X})$ denotes the limit state function, for which the inequality $g(\boldsymbol{X}) < 0$ indicates that the limit state is exceeded. The condition (7) may be replaced by the inequality $\beta > \beta_t$, where β denotes the reliability index. EN 1990 (2002) recommends the target probability $p_t = 7.24 \times 10^{-5}$ for ULS of common buildings corresponding to the reliability index $\beta_t = 3.8$ for 50 year design working life.

Reliability analysis is based on the limit state function $g(\boldsymbol{X})$ corresponding to load effect given e.g. by equation (1) and resistance R of a generic structural member

$$g(\boldsymbol{X}) = \theta_R R - \theta_E (G + Q + W) \quad (8)$$

Table 1. Probabilistic models of basic variables.

Basic variable	Distr.	Units	Char.	μ_X	σ_X
Permanent	N	MN/m²	G_k	G_k	0.1 μ_X
Imposed (5 y.)	GUM	MN/m²	Q_k	0.25Q_k	1.1 μ_X
Imposed (50 y.)	GUM	MN/m²	Q_k	0.6Q_k	0.35 μ_X
Wind (1 y.)	GUM	MN/m²	W_k	0.25 W_k	1.1 μ_X
Wind (50 y.)	GUM	MN/m²	W_k	0.6 W_k	0.35 μ_X
Concrete resistance	LN	MPa	R_k	R_k+2σ_X	0.15
Steel resistance	LN	MPa	R_k	R_k+2σ_X	0.08
Load uncertainty	LN	–	θ_E	1.0	0.10
Resist. uncertainty	LN	–	θ_R	1.0	0.05

Here $\boldsymbol{X}$ denotes the vector of basic variables (random variables entering the right hand side of this equation), θ_R denotes the factor expressing the uncertainty of the resistance model and θ_E the factor expressing the uncertainty of the action effect model.

An important step in any reliability analysis is the specification of probabilistic models for the basic variables. The limit state function, equation (8), has six basic variables that describe the actions G, Q and W, the resistance R and the model uncertainties θ_R and θ_E.

The probabilistic models of actions are related to their characteristic values used for the determination of the design values of actions (see Table 1). The permanent action is described by normal distribution (N), variable actions by Gumbel distribution (GUM) and material strength by log-normal distribution (LN). These models are primarily intended as "conventional models" in time invariant reliability analysis of structural members using Turkstra's combination rule, see e.g. Holicky (2013).

4 RESULTS OF ANALYSIS

Selected results of reliability analyses of some concrete and steel structural members are shown in Figures 1 to 8.

An effect of alternative load combination rules of a reinforced concrete beam is illustrated in Figure 1 for common structures in consequence class CC2 considering EN 1992-1-1 (2004).

Obviously the combination B given by exps. (6.10a,b) leads to a better balanced reliability than the combination rule A, exp. (6.10). Combination C (6.10a$_{mod}$,b) with parameters NDPs selected in some CEN countries where the values of partial factor for permanent load are γ_G = 1.2 in exp. (6.10a$_{mod}$) and γ_G = 1.0 in exp. (6.10b), for variable loads γ_Q = 1.5, for concrete γ_c = 1.45 and for reinforcement γ_s = 1.2 leads to a rather low reliability

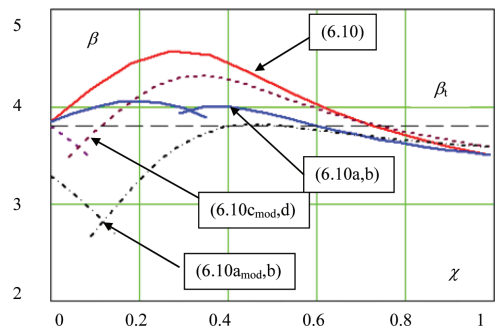


Figure 1. Variation of the reliability index β of the reinforced concrete beam with the load ratio χ (ρ = 0.8%), for the load combinations A to C.

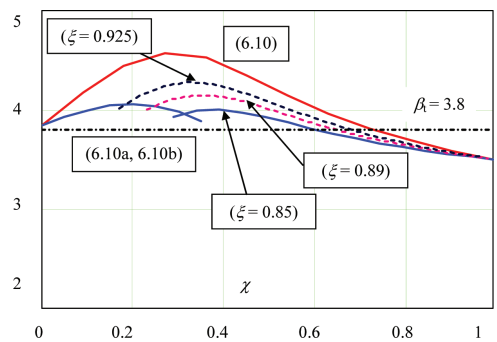


Figure 2. Variation of the reliability index β of the beam with the load ratio χ for the exp. (6.10) and exps. (6.10a,b) considering ξ = 0.85, 0.89 and 0.925.

level of the beam. It should be noted here that the target reliability accepted by these countries for the reliability class RC2 has been modified in comparison to EN 1990 (2002). Figure 1 illustrates also combination (6.10c$_{mod}$,d) where γ_G = 1.3 in exp. (6.10c$_{mod}$) and γ_G = 1,2 in exp. (6.10d) are applied leading to more balanced reliability level.

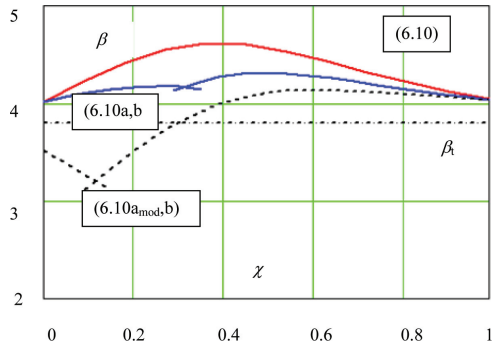


Figure 3. Variation of the reliability index β of the short column with the load ratio χ ($\rho = 1\%$), for the load combinations.

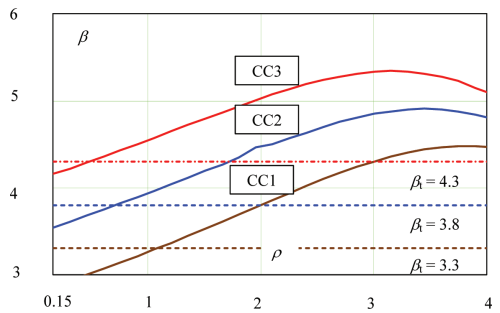


Figure 4. Variation of the reliability index β of the beam with the reinforcement ratio ρ for three consequence classes and load combination (6.10a,b).

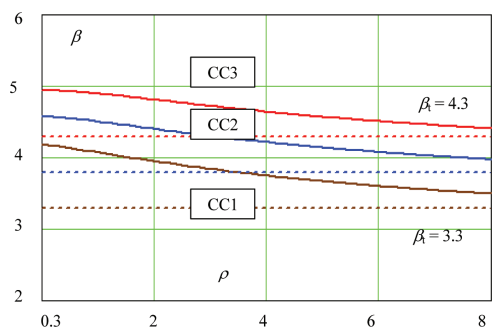


Figure 5. Variation of the reliability index β of the column with the reinforcement ratio ρ for three consequence classes and the load combination (6.10a,b).

Figure 2 shows the significance of national decision concerning the value of reduction factor ξ for permanent actions in alternative B, exp. (6.10b), on the reliability of the concrete beam which is then approaching the alternative A, exp. (6.10).

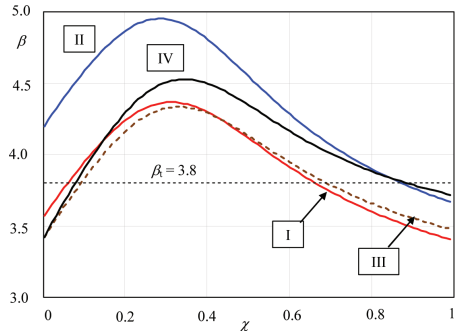


Figure 6. Variation of the reliability index β with the load ratio χ for $k = 0$, the load combination based on exp. (6.10) in EN 1990 and four sets of partial factors.

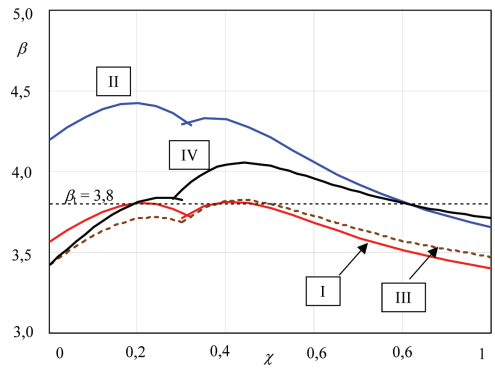


Figure 7. Variation of the reliability index β with the load ratio χ for $k = 0$, the load combination based on exps. (6.10a) and (6.10b) in EN 1990 and four sets of partial factors.

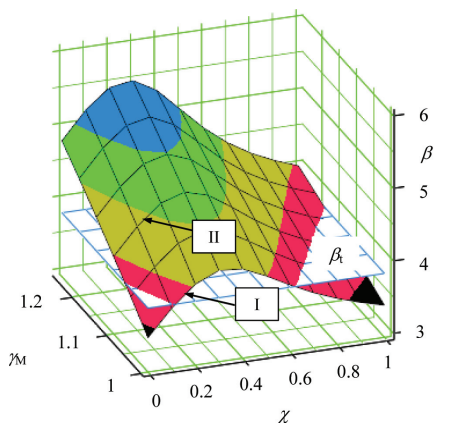


Figure 8. Variation of the reliability index β with the load ratio χ and partial factor γ_M for the load combination based on exp. (6.10) in EN 1990, the study cases I and II are indicated.

The reliability analysis of a short concrete column (axially loaded only, 1% of reinforcement ratio) designed according to Eurocodes, considering the recommended set of partial factors given in EN 1990 (2002), indicates that the reliability index β is greater than the target value β_t (3.8) for the alternative exp. (6.10) and exps. (6.10a,b), see Figure 3. However, for case C (exps. $6.10a_{mod}$,b) the reliability of the column is not meeting requirements.

Figure 4 indicates the favourable effect of increasing reinforcement ratio ρ (for load ratio $\chi = 0.3$) on the reliability level of a reinforced concrete beam for a considered combination B with recommended values of partial factors for variable actions for three reliability classes RC1 to RC3.

Figure 5 indicates the effect of reinforcement ratio on the reliability level of a column for a considered combination B and three reliability classes RC1 to RC3 where with the increasing reinforcement ratio the reliability of column is decreasing.

Next analyses are given for a steel member where presently the material factor $\gamma_M = 1$ is recommended in EN 1993-1-1 (2005) and nationally modified in some Member countries. Following four cases (denoted here by I to IV) characterized by different partial factors for actions and material properties are investigated, see Table 2.

The first two sets of partial factors (I, II) indicated in Table 2 are based on the recommendations of EN 1990 (2002) and EN 1993-1-1 (2003) (or ENV Eurocodes). The third set of γ-factors (III) was recommended in some National application documents of ENV Eurocodes and at present it is also selected as a set of NDPs in some countries. The fourth case (IV) describes a set of γ-factors where importance of material factor is increased and significance of partial factors for actions is reduced.

Figures 6 and 7 illustrate the reliability index β as a function of the load ratio χ assuming the probabilistic models of the basic variables given in Table 1. Further it is considered that the imposed load Q is leading and wind action W is accompanying. The following figures show results for the factor $k = 0$ (one variable action acting only). The reliability level $\beta_t = 3.8$, recommended by EN 1990 (2002) for the fifty year period of design life is indicated by the horizontal dashed line.

Table 2. Sets of partial factors for steel and actions.

No.	γ_M	γ_G	γ_Q
I	1.0	1.35	1.5
II	1.1	1.35	1.5
III	1.1	1.2	1.4
IV	1.2	1.1	1.4

It follows from Figure 6 that the set I of partial factors provides considerably lower reliability level of a steel member than the set II, however still acceptable for the load ratio χ within the common range from 0.1 to 0.6 for combination A. Comparing reliability indexes obtained for the first two cases I and II, it appears that the decrease of γ_M from 1.1 to 1 leads to the considerable decrease in reliability index β (by about 0.6).

Figure 6 (results for the load combination A based on expression (6.10)) and Figure 7 (combination B based on expressions (6.10a,b)) clearly indicate that the partial factor $\gamma_M = 1$ could be applied only in the load combinations based on expression (6.10) and not in the load combinations based on exps. (6.10a,b). It appears that the set of partial factors III may be used in the load combinations A, the set IV in the combinations B provided that the partial factor $\gamma_M > 1$.

It follows from Figure 8 that the set I of partial factors provides considerably lower reliability level of a steel member than the set II, however still acceptable for the common values of load ratio χ.

5 CONCLUSIONS

Submitted analysis of parameters NDPs which were nationally selected by some CEN Member States confirms results of the previous investigations that the reliability of structures, designed according to the alternative combination rules provided in EN 1990 by exps. (6.10) and (6.10a,b) may considerably vary. Exp. (6.10) (combination A) leads to the most reliable but most likely uneconomical structures. Exps. (6.10a,b) (combination B) yield a lower but a more uniform and satisfactory reliability level. It appears that recalibration of partial factors and other safety elements may minimize the deviation of the reliability from its recommended level (given by the reliability index β or probability of failure p_f). Some countries have selected the alternative ($6.10a_{mod}$,b) which leads to a rather low reliability level of structural members.

It is shown that the reliability of the steel members is significantly affected by the material partial factor γ_M. Obviously, any decrease in the factor γ_M leads to a decrease in the reliability level of the member. It appears that for the recommended partial factors γ_G, γ_Q for actions, the partial factor $\gamma_M = 1$ for steel recommended for the strength in EN 1993-1-1 leads to a considerably lower reliability level than previously used value $\gamma_M = 1.1$ in ENV Eurocodes. It appears that $\gamma_M = 1$ should not be used in the combinations based on exps. (6.10a,b) or their modification ($6.10a_{mod}$,b) and could

be used only in the combinations based on exp. (6.10).

ACKNOWLEDGEMENT

This is the partial outcome of the projects LG14012 International co-operation in reliability and risk assessment of structural systems supported by the Ministry of Education and P105/12/0589 Probabilistic optimisation of the target structural reliability supported by the National grant agency.

REFERENCES

CEN BT C105/2013 Eurocodes—Availability of National Annexes.

EN 1990. 2002. Eurocode: Basis of structural design. CEN.

EN 1992-1-1. 2004. Eurocode 2: Design of concrete structures—Part 1–1: General rules and rules for buildings. CEN.

EN 1993-1-1. 2003. Design of steel structures. General rules.

Holicky, M. & Markova, J. 2005. Calibration of Reliability Elements for Steel Members, *In: Eurosteel 2005*. Maastricht: DV Mainz, pp. 1.7–33–38.

Holicky M. & Markova J. 2010. *Reliability elements for assessment of existing bridges*. In: *Esrel 2010*, London: Taylor & Francis, pp. 1487–1492.

Holicky, M. 2013. Introduction to Probability and Statistics for Engineers. Heidelberg: Springer.

JCSS 2001. *JCSS Probabilistic Model Code.* Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>

Response to Mandate M/515. 2013. Towards a second generation of EN Eurocodes. CEN/TC 250.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On climatic actions combinations for probabilistic calibrations

Z. Sadovský
Institute of Construction and Architecture, Slovak Academy of Sciences, Bratislava, Slovakia

ABSTRACT: The contribution addresses combination of time-variant actions, particularly snow and wind loads on a variety of structural design situations. The simplified Turkstra's rule commonly used for probabilistic calibration of standardized design procedures is compared with a an approach employing a direct inclusion of joint action effect. The study is carried out for three representative frames of low-rise industrial buildings designed such that both snow or wind loads could be relevant. For each frame three levels of permanent load realized as light, medium and heavy weight roofs are considered. The frames are designed to the lifetime of 50 years and reliability index $\beta_t = 3.8$ by FORM. The comparison of the values of the resulting design variable—the nominal plastic moment is presented.

1 INTRODUCTION

For the probabilistic assessment of a structure exposed to time-variant loads, the modeling of the maxima of their joint load effect is crucial. Since the load effect varies with the geometry of a structure, the calibration of standardized design approaches derives from simplified combinations of time-variant loads. A basic combination rule was proposed by Turkstra, which assumes that for the combination of two independent time-variant loads, the maximum effect of the combination occurs when one of the loads is at its maximum during the reference period and the other is at an "arbitrary point-in-time value". Another basic combination model is that of Ferry Borghes–Castanheta, see Melchers (2001). Focusing on exceedance probabilities, the rules were checked by pulse processes representations of loads by Wen (1990) and Sýkora & Holický (2011) with outcome appreciating performance of Turkstra's rule for calibration studies.

Adequate probabilistic models of climatic actions and their combinations heavily depend on detailed measurement records of sufficient durations. Such data is available for wind actions, e.g. hourly values of wind speed/pressure. The direct measurements of Snow Water Equivalent values (SWE) (if any) are performed, e.g. in weekly or monthly periods. Daily values have to be recalculated from other meteorological data on various levels of approximation. Consequently, as a starting point for the development of a probabilistic model often only annual or/and monthly snow load maxima with percentage of month with snowfalls (in transitional climates) are available. This allows determination of the annual maxima distribution function used by definition for the assessment of the characteristic value of the action; however combination with wind action then has to be restricted to the basic combination rules.

The present paper utilises database of daily values of snow and wind loads at Bratislava Koliba (BA Koliba) meteorological station. The data allow assessments of both snow and wind load maxima distributions as well as the distribution of maximum action effects on considered frame structures. Three geometries—A, B, C of the frames follow the paper of Schleich et al. (2002) reflecting the cases of dominant snow, wind and combined actions. For each frame three cases of light to heavy weight roofs are considered Sadovský & Páleš (2008) (Sadovský & Sýkora, 2013). The nine design situations provide reasonably broad variety of climatic action effects.

A probabilistic design of the frames for the lifetime of 50 years and the target reliability index $\beta_t = 3.8$ is carried out by FORM. The nominal plastic moments $M_{pl,nom}$ (the design variable) are calculated adopting climatic loads combinations by Turkstra's rule as well as using distribution functions of maxima of their joint action effects developed for each design situation.

The aim of the study is to illustrate differences in design variable values when the simplified combination rule of Turkstra is applied in comparison to a direct inclusion of a joint action effect oriented approach.

The design situations are described in Section 2. The results of probabilistic design are shown in Section 3. Finally short Conclusions Section is given.

2 DESIGN SITUATIONS

2.1 *Basic description*

The dimensions of considered frames are shown in Figure 1 (Schleich et al., 2002). The corresponding limit-state functions Z are given in Eq. (1)

$$Z = M_{pl} - m_{1G}G - m_{1S}S - m_{1W}W, \quad (1)$$

where m_{1G}, m_{1S}, m_{1W} are maximum bending moments found at the leeward corner corresponding to the unit permanent G, wind W and snow load S, Table 1. The products in Eq. (1) represent the load effects of the permanent, snow and wind loads.

The probabilistic model of plastic bending capacity M_{pl} is described by a log-normal distribution. The statistical parameters are expressed in terms of the nominal capacity $M_{pl,nom}$ (Table 2), which is the design variable.

Sadovský and Páleš (2008) extended the number of design situations considering low, medium and high levels of the permanent load. For this purpose, the parameter χ introduced in SAKO (1999) as the ratio of characteristic climatic load effects to the sum of the characteristic climatic and permanent load effects was used

$$\chi = \frac{(m_{1S}S_k + m_{1W}W_k)}{(m_{1G}G_k + m_{1S}S_k + m_{1W}W_k)}. \quad (2)$$

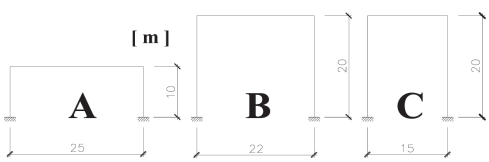


Figure 1. Dimensions of frames.

Table 1. Coefficients of the limit-state functions Eq. (1) (Schleich et al., 2002).

	m_{1G}	m_{1S}	m_{1W}
Frame A	43.37	34.70	7.50
Frame B	27.72	22.18	38.20
Frame C	11.25	9.00	78.03

Table 2. Statistical parameters of the plastic bending capacity (Schleich et al., 2002).

	Mean [kNm]	St. Deviation [kNm]
M_{pl}	1.18 $M_{pl,nom}$	0.08 $M_{pl,nom}$

The values χ = 0.8, 0.5, 0.2 represent light, medium and heavy weight roofs.

Equation (2) allows defining the characteristic value of the permanent load G_k by the characteristic values of snow S_k, wind W_k and χ. The permanent load G is normally distributed with the mean value equal to the characteristic value. The coefficient of variation $V_G = 0.05$ is adopted for the light and medium weight roofs; for the heavy weight roofs $V_G = 0.1$ is considered.

Note that the loads are introduced as uniformly distributed over the unit bay width (1 m). Due to linearity of the limit state function (1), the results obtained can be applied to other bay widths just by multiplication.

2.2 *Probabilistic model of wind and snow action*

The data for the assessment of daily snow and wind loads were collected since the beginning of 1951 up to the half of the year 2006 at Bratislava Koliba (BA Koliba) meteorological station. For snow load with available weekly measurements of SWE the daily values were recalculated from other meteorological data and than fitted to the measurements, Sadovský et al. (2007). SWE are recorded in millimetres; a formal division of the SWE value by 100 is used to obtain the snow load in kN/m^2. The data on wind loads are obtained as transformed daily wind speed maxima of three regular measurements at 7 a.m., 2 p.m. and 7 p.m.

For snow and wind actions the distributions of seasonal and monthly maxima were adjusted from the measurements. Since the minimum size of a sample is 56, which well suites for approximation of the mean value and standard deviation by the sample average and standard deviation, the Gumbel distribution adjusted to these parameters (a, b) was adopted.

Figure 2 shows the approximation of the sample probability of seasonal SWE maxima on the ground. A help line at the 98% probability corresponds to the level of the characteristic value of a climatic action (Eurocode EN 1990: 2002). The cdf of monthly SWE maxima for months with snowfalls are in Figure 3. Including the months without snowfalls, altogether 408 out of 666, a spike probability $1 - p_S$, p_S = (666-408)/666 at zero is added to the cdf from Figure 3 ($F_Y(y)$), which is further correspondingly adjusted and trimmed to $F_{Y,mix}(y)$ Eq. (3), (Fig. 4).

$$F_{Y,mix}(y) = (1 - p_S + p_S F_Y(0))1_{0\le y} + p_S[F_Y(y) - F_Y(0)]_{0\le y} \quad (3)$$

Figures 5, 6 show the sample probability distribution of seasonal and monthly wind pressure maxima measured at the height of 10 m above an

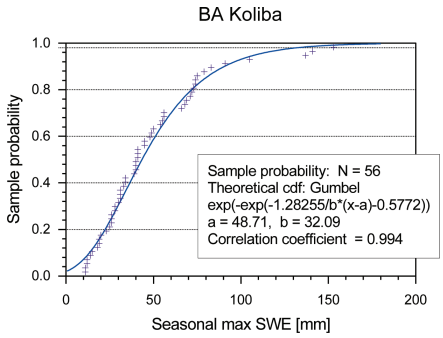


Figure 2. Sample and Gumbel cdf of SWE seasonal maxima.

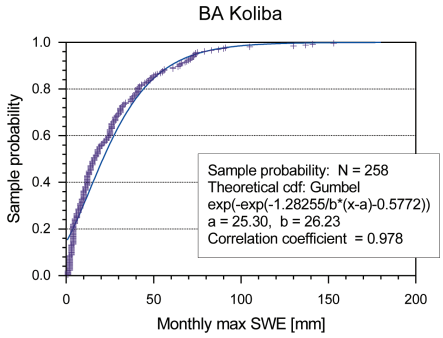


Figure 3. Sample and Gumbel cdf of SWE monthly maxima for months with snowfalls.

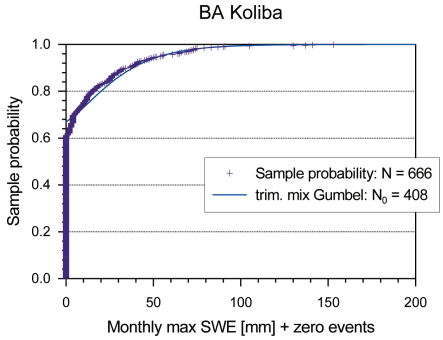


Figure 4. Sample and theoretical cdf of SWE monthly maxima including months without snowfalls.

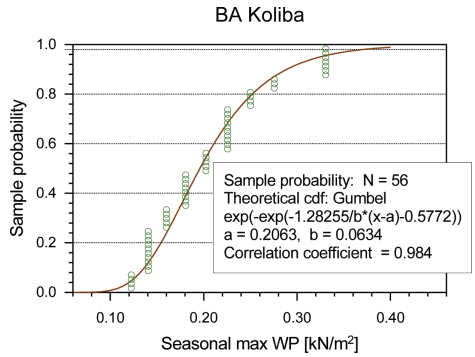


Figure 5. Sample and Gumbel cdf of wind pressure seasonal maxima.

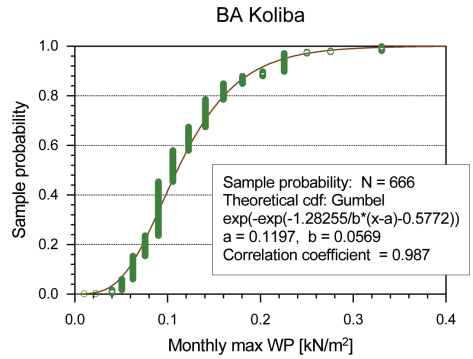


Figure 6. Sample and Gumbel cdf of wind pressure monthly maxima.

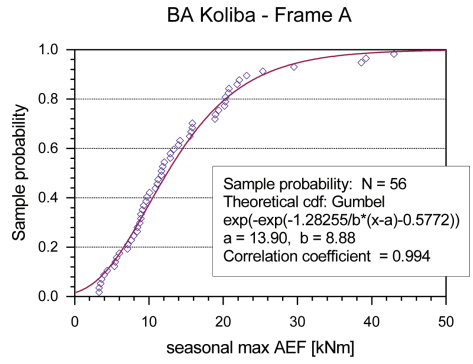


Figure 7. Sample and Gumbel cdf of seasonal maxima of joint climatic actions effect, Frame A.

open terrain. The stepwise values of wind pressure relate to wind speed measurements in whole numbers of meters per second.

Note that the monthly and seasonal maxima provide parameters which do not relate to each other according to Gumbel distribution. For the assessment of a life-time cdf (T = 50 years) the seasonal cdf is employed. The rationale stems from possible dependences in monthly maxima related to occurrences of snow cover durations of more than one month, cf. Coles (2001), Reiss and Thomas (2007).

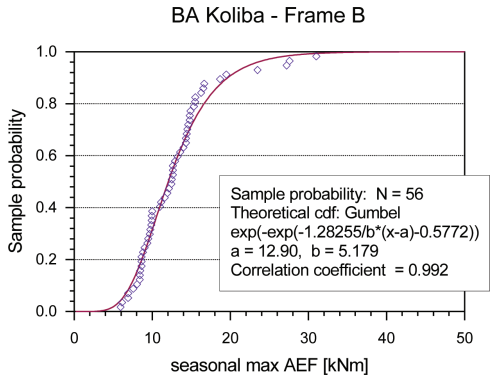


Figure 8. Sample and Gumbel cdf of seasonal maxima of joint climatic actions effect, Frame B.

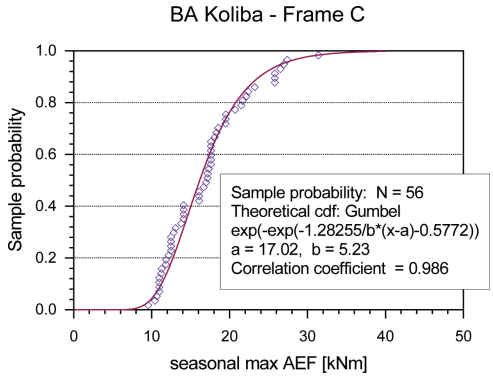


Figure 9. Sample and Gumbel cdf of seasonal maxima of joint climatic actions effect, Frame C.

2.3 *Probabilistic models of joint climatic actions effect*

The sample and approximating Gumbel probability distributions of seasonal maxima of joint climatic actions effect (max AEF) are shown for Frames A, B, C in Figures 7–9. It is obvious that the Frame A is exposed to the occurrence of the highest climatic actions effects.

3 PROBABILISTIC DESIGN OF FRAMES

A probabilistic design of the representative frames is carried out assuming the lifetime of 50 years and the corresponding target reliability index $\beta_t = 3.8$ (EN 1990: 2002). The nominal bending resistance of a cross-section (the design variable) is determined to reach the target reliability in each design situation. An efficient FORM iteration algorithm is applied, Sadovský (2000).

For combinations of snow and wind load by Turkstra's rule the cdf of the lifetime maximum of a dominant load is derived from the cdf of the seasonal maxima. For the accompanying snow action the mixed distribution $F_{Y,mix}(y)$ Eq. (3), (Fig. 4) of the monthly maxima is applied, while for the accompanying wind action the cdf of monthly maxima, Figure 6, is used. The decisive load combination is the one yielding a higher value of the design variable.

The lifetime cdf of maxima of joint action effects is derived from the cdf of seasonal maxima for each frame type, Figures 7–9.

The snow load on the ground should be transformed to the roof by an appropriate shape factor. In conformity to EN 1991-1-3: 2003 the shape factor 0.8 is applied assuming that the thermal and exposure factors are unity.

Nominal plastic moments $M_{pl,nom}$ (the design variable) are compared in Figures 10–12. The notation max AEF relates to the maxima of action effects, while max S_W to Turkstra's rule of time-variant load combinations.

Note that applying for accompanying snow load the monthly maxima cdf without spike (Fig. 3) the

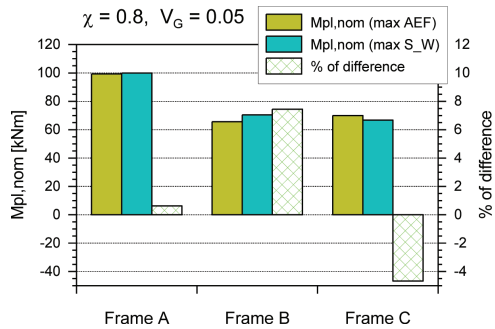


Figure 10. Nominal plastic moments, light weight roofs.

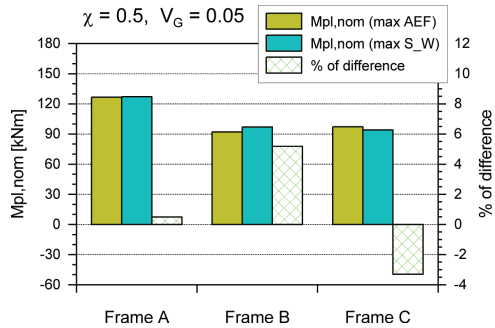


Figure 11. Nominal plastic moments, medium weight roofs.

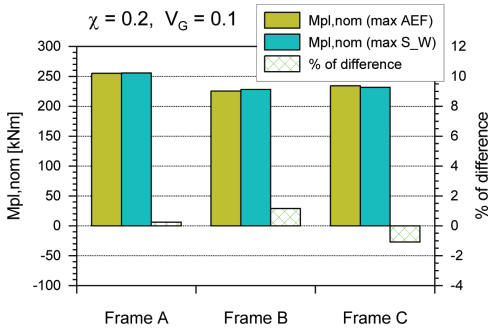


Figure 12. Nominal plastic moments, heavy weight roofs.

differences in the values of design variable shown for Frame C (Figs. 10–12) would be approximately halved.

4 CONCLUSIONS

The in calibration studies of structural design used Turkstra's rule for combination of time-variant loads is checked employing a direct inclusion of joint action effect. Particularly, the combination of climatic actions—snow and wind loads is addressed. The study is carried out for three representative frames of low-rise industrial buildings designed such that both snow or wind loads could be relevant. For each frame three levels of permanent load realized as light, medium and heavy weight roofs are studied.

A probabilistic design of the frames is carried out by FORM considering the lifetime of 50 years and reliability index $\beta_t = 3.8$. Both approaches are compared by the value of the design variable—the nominal plastic moment $M_{pl,nom}$. The results show that Turkstra's rule provides reasonable accurate results. This is in agreement with previous studies employing for time-variant loads pulse processes Wen (1990) and Sýkora & Holický (2011). Nevertheless, an extension of the study to other locations, i.e. to different levels and proportions of the climatic loads is foreseen.

ACKNOWLEDGEMENTS

The work was supported by the Slovak Research and Development Agency under the contract No. APVV-0031-10.

REFERENCES

Coles, S., 2001. An Introduction to Statistical Modeling of Extreme Values. Springer Verlag, London.

Melchers, R.E., 2001. Structural Reliability Analysis and Prediction (2 ed.), John Willey & Son, Chichester.

Reiss, R-D. & Thomas, M. 2007. Statistical Analysis of Extreme values. 3rd Edition. Basel: Birkhäuser Verlag AG.

Sadovský, Z., 2000. Discussion on: An inverse reliability method and its application, Struct. Saf. 22 (1), 97–102.

Sadovský, Z., Faško, P., Mikulová, K., Pecho, J., Vojtek, M., 2009. Special features of the collection and analysis of snow loads. In: Martorell, S., Guedes Soares, C., Barnett, J. (Eds.), Safety, Reliability and Risk Analysis: Theory, Methods and Applications, ESREL 2008 Valencia, Taylor & Francis Group, London, Vol. 2, 1671–1675.

Sadovský, Z., Páleš, D., 2008. Probabilistic Optimization of Partial Safety Factors for the Design of Industrial Buildings. Int. J. Reliab. Qual. Saf. Eng. 15 (5), 411–424.

Sadovský, Z. and Sýkora, M., 2013. Snow load models for probabilistic optimization of steel frames. In Cold Regions Science and Technology, 94: 13–20.

SAKO, 1999. Basis of Design of Structure: Proposal for Modification of Partial Safety Factors in Eurocodes. NKB, Oslo, 81 p.

Schleich, J.B., Sedlacek G. and Kraus, O., 2002. Realistic Safety Approach for Steel Structures. In: Proc. 3rd European Conf. on Steel and Composite Structures, Eurosteel, Coimbra 2002, 1521–1530.

Sýkora, M. and Holický, M., 2011. Comparison of load combination models for probabilistic calibrations. In: Proc. of 11th Int. Conf. on Applications of Statistics and Probability in Civil Engineering, ETH Zurich, ICASP11, Leiden (The Netherlands): Taylor & Francis/Balkema, 977–985.

Wen, Y.K., 1990. Structural load modeling and combination for performance and safety evaluation, Elsevier, Amsterdam.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

In-plane buckling behaviors of shear-deformable columns with variable cross sections

Lijuan Su & Mario M. Attard
School of Civil and Environmental Engineering, The University of New South Wales, Sydney, NSW, Australia

ABSTRACT: A finite strain elastic in-plane buckling analysis is presented for shear deformable Timoshenko–type columns with variable cross-section. The constitutive relationship for stresses and finite strains is defined adopting a consistent hyperelastic constitutive model. Tensor notation is introduced to establish the physical relationships with simplicity in a curvilinear coordinate reference system. The generalized equilibrium equations are derived considering the shear deformations in addition to the bending deformations. The differential buckling equations are derived for tapered cantilever columns under compressive loads. The critical loads are obtained from the differential buckling equations using the Galerkin method. ANSYS software simulation modeling is also carried out to investigate the buckling problem of tapered columns and show close agreement with the results of numerical analysis. The in-plane buckling behaviors of tapered columns agree well with the published results in classic literature which validates the accuracy of the in-plane buckling formulation developed in this paper.

1 INTRODUCTION

The application of variable cross-sectional beams has increased in the engineering industry due to their unique advantage of the combination of efficiency, economy and aesthetics ((Billington 1985)). Tapered columns are common in all kinds of engineering application. Stability analysis of non-uniform columns is a fundamental component in structural design and had been extensively studied in the past few decades ((Coskun & Atay 2009), (Siginer 1992), (Smith 1988), (O'Rourke & Zebrowski 1977), (Serna et al., 2011)).

In the paper, the constitutive relationship for physical Lagrangian stresses and strains is defined based on consistent hyperelastic formulation to investigate the in-plane buckling behavior of variable cross-sectional columns under finite strain. The shear deformations are incorporated in the buckling formulation based on the Timoshenko beam hypothesis. The generalized equilibrium equations are derived from the virtual work equation. Applying the variational method to the equilibrium equations, the differential buckling equations are developed to for tapered cantilever column under compressive loading. In the numerical analysis, the representative elastic-to-shear rigidity ratios of the taper columns equal 3, 25 and 100 respectively, the critical loads are obtained from the differential buckling equations using the Galerkin method. The buckling problem of tapered columns is also investigated using the ANSYS software simulation. Critical buckling loads obtained from ANSYS model agree well with the results of numerical method analysis. The in-plane buckling behaviors of tapered columns are in good agreement with the results in the published classic literature. The obtained curves of behaviors of normalized buckling loads against slenderness are in good agreement with the results of existing literature (Timoshenko & Gere 1961).

2 KINEMATICS

Consider a structural member made from isotropic hyperelastic material with variable cross-section. The material lines follow the pattern of the continuum boundaries as depicted in Figure 1. In the initial configuration the position vector $\mathbf{P}$ of an arbitrary point on a general material line s with respect to the right-handed rectangular Cartesian coordinate system is given by:

$$\mathbf{P} = x\mathbf{i_1} + y(x)\mathbf{i_2} \tag{1}$$

$\mathbf{i}_1$ and $\mathbf{i}_2$ denote the unit base vectors in the x-axis and y-axis directions respectively.

A general curvilinear coordinate system is introduced. The profile coordinate s defines the material line, and a second coordinate t is perpendicular to the tangential length of the reference axis s_o.

The position vector of point $\mathbf{P_o}$ on the reference axis material line s_o is:

$$\mathbf{P_o} = x_o\mathbf{i_1} + y_o(x)\mathbf{i_2} \tag{2}$$

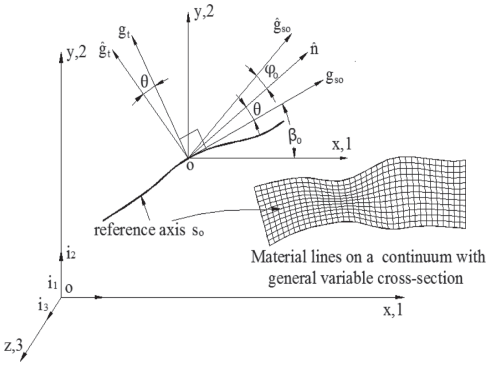


Figure 1. Tangent base vectors at reference axis.

x_o and y_o are the Cartesian coordinates of the reference axis s_o. The position vector **P** on a general material line can be expressed in terms of the curvilinear coordinate t such that:

$$\mathbf{P} = \left(x_o - t\sin\beta_o\right)\mathbf{i_1} + \left(y_o(x) + t\cos\beta_o\right)\mathbf{i_2} \tag{3}$$

Here β_o is the angle between the tangential line of the profile reference axis s_o at point $\mathbf{P_o}$ and the positive direction of the x-axis. The covariant tangent base vectors can be derived using Equation (3), hence:

$$\mathbf{g_s} = \frac{\partial \mathbf{P}}{\partial s} = \left(1 - t\frac{d\beta_o}{ds}\right)\left(\cos\beta_o\mathbf{i_1} + \sin\beta_o\mathbf{i_2}\right) + t_{,s}\left(-\sin\beta_o\mathbf{i_1} + \cos\beta_o\mathbf{i_2}\right) \tag{4}$$

$$\mathbf{g_t} = \frac{\partial \mathbf{P}}{\partial t} = -\sin\beta_o\mathbf{i_1} + \cos\beta_o\mathbf{i_2} \tag{5}$$

The covariant tangent base vector at the reference axis (t=0) is:

$$\mathbf{g_{so}} = \cos\beta_o\mathbf{i_1} + \sin\beta_o\mathbf{i_2} \tag{6}$$

Using Equations (6) and (5), the covariant tangent base vector in equation (4) can be rewritten with respect to the basis $\{\mathbf{g_{so}}, \mathbf{g_t}\}$ as:

$$\mathbf{g_s} = \left(1 - t\frac{d\beta_o}{ds}\right)\mathbf{g_{so}} + t_{,s}\mathbf{g_t} \tag{7}$$

The contravariant base vectors can be derived from equations (4) and (5) as:

$$\mathbf{g^s} = \frac{\mathbf{g_{so}}}{\left(1 - t\frac{d\beta_o}{ds}\right)} \quad \mathbf{g^t} = -\frac{t_{,s}}{\left(1 - t\frac{d\beta_o}{ds}\right)}\mathbf{g_{so}} + \mathbf{g_t} \tag{8}$$

The covariant tangent base vectors in the deformed state are:

$$\hat{\mathbf{g}}_\mathbf{i} = \left(\delta_i^j + u^j\Big|_i\right)\mathbf{g_j} \tag{9}$$

The indices i and j in equation (9) take on values of s or t. δ_i^j is the kronecker delta. $\mathbf{g_j}$ are the covariant tangent base vectors in the initial state and $u^j\Big|_i$ represent the covariant derivatives. The Einstein summation convention is adopted.

The displacement vector **u** is given by:

$$\mathbf{u} = \frac{u_o - t\sin\theta}{1 - t\frac{d\beta_o}{ds}}\mathbf{g}_s + \left(v - t\left(1 - \cos\theta\right) - \frac{t_{,s}\left(u_o - t\sin\theta\right)}{1 - t\frac{d\beta_o}{ds}}\right)\mathbf{g}_t \tag{10}$$

Where θ is the bending rotation taken as a function of the profile coordinate s only. u_o and v are the displacement components of the reference axis in the tangential direction and in the t direction respectively.

In the curvilinear coordinate system, the covariant derivatives of displacement vector are:

$$u^j\Big|_i = u^j{}_{,i} + u^k\Gamma^j_{ki} \tag{11}$$

The Christoffel symbols can be calculated from the base vectors in equations (4) and (5) and are given by:

$$\Gamma^t_{tt} = \Gamma^s_{tt} = 0 \tag{12}$$

$$\Gamma^s_{ss} = -\frac{2t_{,s}\frac{d\beta_o}{ds} + t\frac{d^2\beta_o}{ds^2}}{1 - t\frac{d\beta_o}{ds}} \tag{13}$$

$$\Gamma^s_{st} = \Gamma^s_{ts} = \frac{-\frac{d\beta_o}{ds}}{1 - t\frac{d\beta_o}{ds}} \qquad \Gamma^t_{ts} = \Gamma^t_{st} = \frac{t_{,s}\frac{d\beta_o}{ds}}{1 - t\frac{d\beta_o}{ds}} \tag{14}$$

$$\Gamma^t_{ss} = \frac{t_{,s}\left(2t_{,s}\frac{d\beta_o}{ds} + t\frac{d^2\beta_o}{ds^2}\right)}{1 - t\frac{d\beta_o}{ds}} + \frac{d\beta_o}{ds}\left(1 - t\frac{d\beta_o}{ds}\right) + t_{,ss} \tag{15}$$

Substituting Equations (12)-(15) and (10) into Equations (11), and then substitute Equations (11) into Equations (9), the covariant tangent base vectors in the deformed state can be derived, we have:

$$\hat{\mathbf{g}}_{\mathbf{s}} = \left(1+u^{s}\big|_{s}\right)\mathbf{g}_{s} + u^{t}\big|_{s}\,\mathbf{g}_{t}$$
$$= \left(1+\tilde{u}_{o,s} - t\cos\theta\frac{d}{ds}\left(\beta_{o}+\theta\right) - t_{,s}\sin\theta\right)\mathbf{g}_{\mathbf{so}} \qquad (16)$$
$$+\left(\tilde{v}_{,s} - t\sin\theta\frac{d}{ds}\left(\beta_{o}+\theta\right) + t_{,s}\cos\theta\right)\mathbf{g}_{t}$$

$$\hat{\mathbf{g}}_{t} = u^{s}\big|_{t}\,\mathbf{g}_{s} + \left(1+u^{t}\big|_{t}\right)\mathbf{g}_{t}$$
$$= \frac{-\sin\theta}{1-t\dfrac{d\beta_{0}}{ds}}\mathbf{g}_{s} + \left(\cos\theta + \frac{t_{,s}\sin\theta}{1-t\dfrac{d\beta_{0}}{ds}}\right)\mathbf{g}_{t} \qquad (17)$$

where

$$\tilde{u}_{o,s} = u_{o,s} - v\frac{d\beta_{o}}{ds} \qquad \tilde{v}_{,s} = v_{,s} + u_{o}\frac{d\beta_{o}}{ds} \qquad (18)$$

At the reference axis ($t=0$), we have:

$$\hat{\mathbf{g}}_{s}\cdot\mathbf{g}_{s} = \lambda_{so}\cos\left(\theta+\varphi_{o}\right) = \left(1+\tilde{u}_{o,s}\right) \qquad (19)$$

$$\hat{\mathbf{g}}_{s}\cdot\mathbf{g}_{s} = \lambda_{so}\cos\left(\theta+\varphi_{o}\right) = \left(1+\tilde{u}_{o,s}\right) \qquad (20)$$

where φ_{o} is the shear angle, λ_{so} is the stretch of the reference axis. Rearranging equation (19) gives:

$$\hat{\gamma}_{so} = \lambda_{so}\cos\varphi_{o} = \left(1+\tilde{u}_{o,s}\right)\cos\theta + \left(\tilde{v}_{,s}\right)\sin\theta \qquad (21)$$

$$\hat{\gamma}_{t} = \lambda_{so}\sin\varphi_{o} = -\left(1+\tilde{u}_{o,s}\right)\sin\theta + \left(\tilde{v}_{,s}\right)\cos\theta \qquad (22)$$

where $\hat{\gamma}_{so}$ and $\hat{\gamma}_{t}$ are the normal component and tangential shear component of the stretch of reference axis.

The deformation gradient tensor $\mathbf{F}$ is defined as:

$$\mathbf{F} = \hat{\mathbf{g}}_{\mathbf{i}}\otimes\mathbf{g}^{\mathbf{i}} \qquad (23)$$

The deformation gradient tensor $\mathbf{F}$ can be decomposed into two tensors, such that:

$$\mathbf{F} = \mathbf{R}\mathbf{F}^{*} \qquad (24)$$

where $\mathbf{R}$ is a rotation tensor and $\mathbf{F}^{*}$ is a rotated deformation tensor. Hence:

$$\mathbf{F} = \begin{bmatrix} \dfrac{1+\tilde{u}_{o,s} - t\cos\theta\dfrac{d}{ds}\left(\beta_{o}+\theta\right)}{1-t\dfrac{d\beta_{o}}{ds}} & -\sin\theta \\ \dfrac{\tilde{v}_{,s} - t\sin\theta\dfrac{d}{ds}\left(\beta_{o}+\theta\right)}{1-t\dfrac{d\beta_{o}}{ds}} & \cos\theta \end{bmatrix} \qquad (25)$$

$$\mathbf{R} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \qquad (26)$$

$$\mathbf{F}^{*} = \begin{bmatrix} \dfrac{1}{1-t\dfrac{d\beta_{o}}{ds}}\left(\hat{\gamma}_{so} - t\frac{d}{ds}\left(\beta_{o}+\theta\right)\right) & 0 \\ \dfrac{1}{1-t\dfrac{d\beta_{o}}{ds}}\hat{\gamma}_{t} & 1 \end{bmatrix} \qquad (27)$$

The Green deformation tensor $\mathbf{C}$ can now be expressed in terms of the rotated deformation tensor $\mathbf{F}^{*}$, such that:

$$\mathbf{C} = \mathbf{F}^{\mathbf{T}}\mathbf{F} = \mathbf{F}^{*\mathbf{T}}\mathbf{F}^{*} \qquad (28)$$

The Jacobian J obtained from equation (27) is:

$$J = \det\left(\mathbf{F}\right) = \det\left(\mathbf{F}^{*}\right)$$
$$= \frac{1}{1-t\dfrac{d\beta_{o}}{ds}}\left[\hat{\gamma}_{so} - t\frac{d}{ds}\left(\beta_{o}+\theta\right)\right] \qquad (29)$$

3 HYPERELASTIC CONSTITUTIVE RELATIONS

A physical Lagrangian stress tensor is defined and established by applying vector transformation to the second Piola Kirchhoff stress tensor Π components using equation (27), such that:

$$\mathbf{S} = \prod\mathbf{F}^{*\mathbf{T}} = \begin{bmatrix} S^{nn} & S^{nt} \\ S^{tn} & S^{tt} \end{bmatrix} \qquad (30)$$

where S^{nn} is the normal stress component while S^{nt} is the tangential shear stress component.

The strain energy density function U for a compressible isotropic neo-Hookean material (see Attard & Hunt (2004)) is given by:

$$U = \tfrac{1}{2}G\left(tr\left(\mathbf{C}-\mathbf{I}\right) - 2\ln J\right) + \tfrac{1}{2}\Lambda\left(\ln J\right)^{2} \qquad (31)$$

where tr signifies the trace of a tensor, G is the shear modulus, Λ is the Lamé constant, E is the elastic modulus and μ is the Poisson's ratio. A constitutive relationship for the second Piola Kirchhoff stress tensor $\prod$ and its conjugate Green's stain tensor $\mathbf{C}$ for a hyperelastic material is given by (see Attard & Hunt (2004)):

$$\prod = 2\frac{\partial U}{\partial\mathbf{C}} = G\,\mathbf{I} - p_{h}\mathbf{C}^{-1} \qquad p_{h} = G - \Lambda\ln J \qquad (32)$$

where p_{h} represents a hydrostatic stress. From equations (28) and (32) the constitutive relationship

for the physical Lagrangian stress **S** can be obtained as:

$$\mathbf{S} = \prod \mathbf{F}^{*\mathbf{T}} \cong G\left(\mathbf{F}^{*\mathbf{T}} - \mathbf{F}^{*\text{-}\mathbf{1}}\right) + \Lambda(J-1)\mathbf{F}^{*\text{-}\mathbf{1}} \tag{33}$$

The constitutive relations for the physical Lagrangian stress components in terms of the deformations are obtained as:

$$S^{nn} = \frac{E}{1 - t\dfrac{d\beta_o}{ds}}\left[\left(\hat{\gamma}_{so} - 1\right) - t\frac{d\theta}{ds}\right] \tag{34}$$

$$\mathbf{S}^{nt} = \frac{G}{1 - t\dfrac{d\beta_o}{ds}}\hat{\gamma}_t \tag{35}$$

The reference axis is such selected that the following geometric property is satisfied:

$$\int_A \frac{t}{1 - t\dfrac{d\beta_o}{ds}}\, dA = 0 \tag{36}$$

The cross-sectional area and the second moment of area are defined by:

$$\tilde{A}(s) = \int_A \frac{1}{1 - t\dfrac{d\beta_o}{ds}} dA \quad \tilde{I}(s) = \int_A \frac{t^2}{1 - t\dfrac{d\beta_o}{ds}} dA \tag{37}$$

Integrating the stresses over the cross-sectional area yields the internal actions:

$$N = \int_A S^{nn} dA = E\tilde{A}(s)\left(\hat{\gamma}_{so} - 1\right) \tag{38}$$

$$Q = \int_A S^{n2} dA = G\tilde{A}_s(s)\hat{\gamma}_t \tag{39}$$

$$M = \int_A -tS^{nn} dA = E\tilde{I}(s)\frac{d\theta}{ds} \tag{40}$$

4 VIRTUAL WORK

Writing the virtual work equation δW in terms of the physical Lagrangian stress tensor, we have:

$$\delta W = \int_V tr\left(\mathbf{S}\prod \mathbf{F}^{*}\right) dV + \delta W_E = 0 \tag{41}$$

With V being the volume in the undeformed state, the symbol δ denotes kinematically admissible variations, δW_E is the variation of the external virtual work and the integral represents the internal virtual work.

Incorporating the physical Lagrangian stress tensor and integrating over the cross-sectional area, the virtual work equation is reduced to:

$$\delta W = \int_0^L \left[N\delta\hat{\gamma}_{so} + Q\delta\hat{\gamma}_t + M\delta\kappa\right] ds_o + \delta W_E = 0 \tag{42}$$

where L is the length of the column along the longitudinal reference axis.

From equation (42), the following equilibrium equations can be obtained:

$$\frac{dN}{ds_o} - Q\kappa + p_n = 0 \tag{43}$$

$$\frac{dQ}{ds_o} + N\kappa + p_t = 0 \tag{44}$$

$$\frac{dM}{ds_o} + m_t = N\hat{\gamma}_t - Q\hat{\gamma}_{so} \tag{45}$$

Vectors **p** and **m** are the distributed force and moment load intensities:

$$\mathbf{p} = p_n\,\hat{\mathbf{n}} + p_t\,\hat{\mathbf{g}}_{\mathbf{t}} \qquad \mathbf{m} = m_n\,\hat{\mathbf{n}} + m_t\,\hat{\mathbf{g}}_{\mathbf{t}} \tag{46}$$

5 IN-PLANE BUCKLING OF TAPERED CANTILEVER COLUMNS

5.1 *Kinematics*

We consider a doubly symmetric cantilever column of variable cross sections with an axial concentrated force acted on the top end of the column ($x = L$). The x-axis coincides with the longitudinal reference axis with the origin at the fixed base end of the column ($x = 0$). The geometric characteristics are depicted in Figure 2. For the rectangular

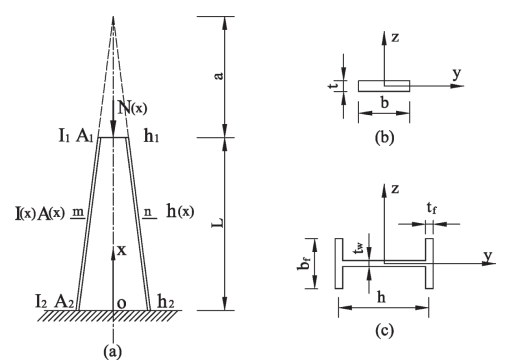


Figure 2. (a) Tapered cantilever column under compression (b) Width-tapered rectangular section (c) web-tapered I-section.

section case, the thickness t is constant while the width tapers from the base of the column to the top end. In the case of the I-section, the column is tapering in web while the other dimensions of the cross-section are uniform along the length of the column.

In the numerical analysis of tapered cantilever columns, the representative elastic-to-shear rigidity ratios $EA/GA_s = 3, 25$ and 100 are adopted. The taper ratio of the column is defined by I_1/I_2. I_1 is the second moment of area at the top free end, while I_2 is the second moment of area at the fixed base end.

The second moment of area of an arbitrary section mn of the tapered cantilever column can be expressed as:

$$I_x = I_2\left(1 + c\frac{x}{L}\right)^n \tag{47}$$

where c is a constant depending on the second moment of area I_1 at the top end of the tapered column. n takes on the value of 2.

The flexural rigidity of an arbitrary section of the tapered column can be written as a power function using the equation (47), such that:

$$EI_x = EI_2\left(1 + c\frac{x}{L}\right)^n \tag{48}$$

5.2 *Cross-section actions*

Consider a rotation angle ς about z-axis as shown in Figure 3. The rotation tensor denoted by the symbol $\mathbf{R}_\varsigma$ and its inverse $\mathbf{R}_\varsigma^{-1}$ are in the forms:

$$\mathbf{R}_\varsigma = \begin{pmatrix} \cos\varsigma & \sin\varsigma \\ -\sin\varsigma & \cos\varsigma \end{pmatrix} \quad \mathbf{R}_\varsigma^{-1} = \begin{pmatrix} \cos\varsigma & -\sin\varsigma \\ \sin\varsigma & \cos\varsigma \end{pmatrix} \tag{49}$$

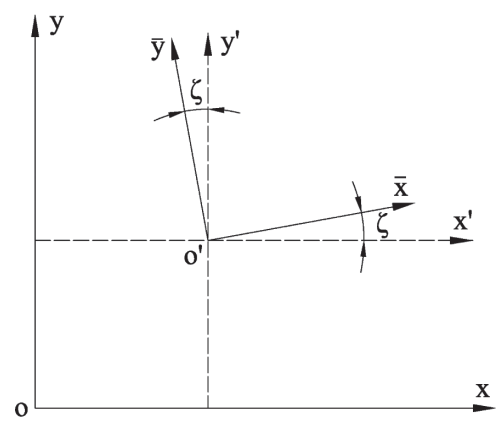


Figure 3. Rotated axes directions at a generic point.

Applying the rotation ς to the x and y axes gives:

$$\bar{\mathbf{y}} = \mathbf{R}_\varsigma \mathbf{y} = \cos\varsigma \mathbf{y} + \sin\varsigma \mathbf{z} \tag{50}$$

$$\bar{\mathbf{z}} = \mathbf{R}_\varsigma \mathbf{z} = -\sin\varsigma \mathbf{y} + \cos\varsigma \mathbf{z} \tag{51}$$

Now applying the bending rotation θ to the cross-section actions as depicted in Figure 4, it gives:

$$\begin{bmatrix} P_x \\ P_y \end{bmatrix} = \mathbf{R}_\theta^{-1} \begin{bmatrix} N \\ Q \end{bmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{bmatrix} N \\ Q \end{bmatrix} \tag{52}$$

Equation (52) can be written as:

$$P_x = \cos\theta N - \sin\theta Q \quad P_y = \sin\theta N + \cos\theta Q \tag{53}$$

where P_x and P_y are the internal force resultants in the x-direction and the y-direction respectively.

5.3 *Buckling equations*

The variation principle is applied to formulate the elasticity problem of tapered cantilever columns under compressive load $N(x)$. Before the buckling takes place, the initial values are:

$$\begin{aligned} &P_x = N_o(x) \quad P_y = 0 \quad N = N_o(x) \\ &Q = 0 \quad M = 0 \quad m_t = 0 \quad \varphi_o = 0 \quad \theta = 0 \end{aligned} \tag{54}$$

where $(.)_o$ denotes the initial values.

The differential buckling equations of equilibrium are derived as:

$$\frac{d}{dx}\left[EI(x)\frac{d\delta\theta}{dx}\right] = -N_o(x)b_o(x)\delta\theta \tag{55}$$

$$\text{where } b_o(x) = \frac{N_o(x)}{GA(x)} - \left(\frac{N_o(x)}{EA(x)} + 1\right) \tag{56}$$

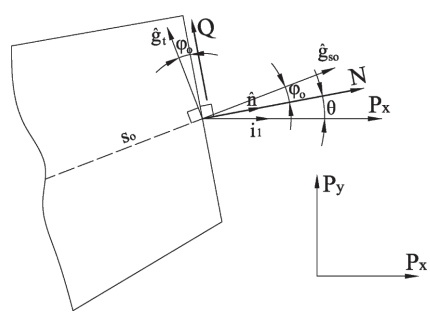


Figure 4. Two-dimensional column cross-section actions.

5.4 *Solution tactics*

The Galerkin method is suitable to solve the differential buckling equations. The assumed approximation deflection function satisfies the boundary conditions as depicted in Figure 5.

The approximation deflection function for the buckled configuration is assumed as:

$$\tilde{\theta} = a_i \sin\left(\frac{(2i-1)\pi x}{2L}\right) \qquad i = 1,2 \tag{57}$$

It can be verified that the assumed deflection function satisfies the required boundary conditions.

According to the Galerkin method, the integral expression should be satisfied, such that:

$$\int_0^L W_i R(x)\,dx = 0 \qquad \text{for } i = 1,2 \tag{58}$$

where $R(x)$ is a residual in domain $(0, L)$ resulting from substituting the approximate deflection function into the governing differential equation (55), that is:

$$R(x) = \frac{d}{dx}\left[EI(x)\frac{d\delta\theta}{dx}\right] + N_o(x)b_o(x)\delta\theta \tag{59}$$

where W_i is the weight function:

$$W_1 = \sin\left(\frac{\pi x}{2L}\right) \qquad W_2 = \sin\left(\frac{3\pi x}{2L}\right) \tag{60}$$

Substituting equations (59) and (60) into equation (58), we have:

$$\int_0^L \sin\left(\frac{(2i-1)\pi x}{2L}\right)\left(\begin{array}{l}\dfrac{d}{dx}\left[EI(x)\dfrac{d\delta\theta}{dx}\right] \\ +N_o(x)b_o(x)\delta\theta\end{array}\right)dx = 0 \tag{61}$$

$i = 1,2$

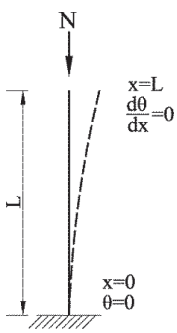


Figure 5. Boundary conditions.

Equations (61) represent the simultaneous algebraic equations that result in a generalized eigenproblem to be solved.

6 NUMERICAL EXAMPLE

Consider a tapered cantilever column of span L (L = *10,000* mm) subjected to a conservative concentrated axial load as illustrated in Figure 2a. Since no distributed loads are acted along the column, $p_n = p_t = m_t = 0$ in equations (43)-(45), the equilibrium equations are written in the forms:

$$\frac{dN}{dx} - Q\kappa = 0 \quad \frac{dQ}{dx} + N\kappa = 0 \quad \frac{dM}{dx} = N\hat{\gamma}_y - Q\hat{\gamma}_x \tag{62}$$

The initial values of loading, shear angle and bending angle:

$$\begin{array}{llll} P_x = N_o & P_y = 0 & N(x) = N_o & \\ Q = 0 & M = 0 & \varphi_o = 0 & \theta = 0 \end{array} \tag{63}$$

The governing differential buckling equations are therefore:

$$\frac{d}{dx}\left[EI(x)\frac{d\delta\theta}{dx}\right] = -N_o b_o(x)\delta\theta \tag{64}$$

The in-plane buckling loads obtained by the numerical results obtained from the differential

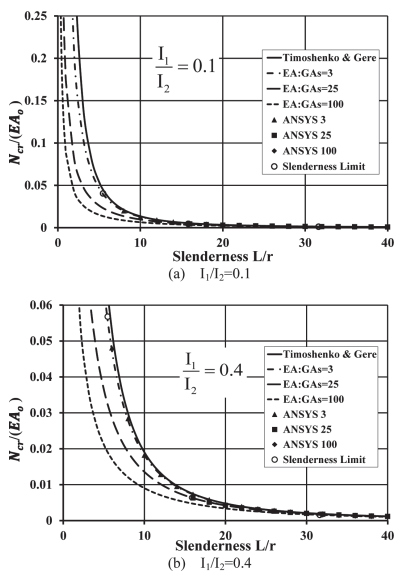


Figure 6. Normalized buckling loads versus slenderness.

buckling equations (61) are also compared with finite element method using the ANSYS software. In the ANSYS simulation, the tapered beam is modelled using the 4-node plane elements (PLANE 182).

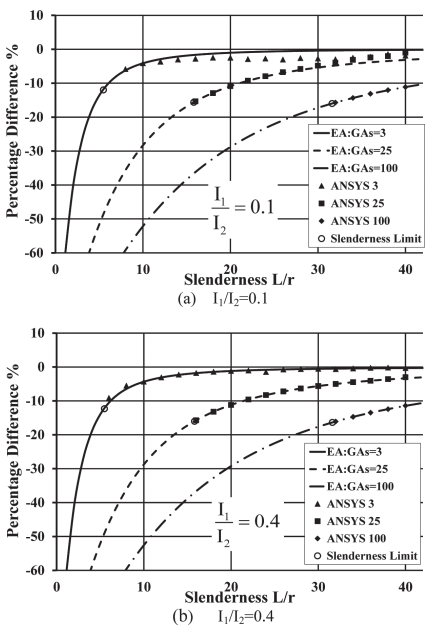
6.1 *Normalized buckling loads*

The governing differential Equation (64) is solved using the Galerkin numerical method for the buckling loads. Finite element method using ANSYS software are included in the curves of the normalized buckling loads versus column slenderness are plotted in Figure 6.

As shown in Figure 6a,b, the comparison of the obtained normalized buckling loads indicates that the behavior of the obtained buckling loads are in good agreement with those by (Timoshenko & Gere 1961).

6.2 *Percentage difference of buckling loads*

Figure 7a,b show the percentage difference between the obtained buckling loads including the effects of shear deformation and those from (Timoshenko & Gere 1961) where the shear deformations were not taken into account in the buckling analysis. Shear deformations are shown to reduce the buckling capacity and are significant for columns of smaller slenderness and columns with larger elastic-to-shear rigidity.



(a) I_1/I_2=0.1

(b) I_1/I_2=0.4

Figure 7. Percentage difference between buckling loads.

7 CONCLUSION

A finite strain elastic stability analysis is presented for the in-plane buckling problem of column with variable cross-section. A consistent hyperelastic constitutive model is adopted to define the constitutive relationship for stresses and finite strain. The shear effects are included in the formulation. The generalised equilibrium equations are derived for columns with variable cross-section using the virtual work principle. The variation method is applied to derive the differential buckling equations for tapered cantilever columns. Numerical solutions are obtained using the Galerkin method. Finite element method by means of ANSYS model is also carried out to investigate the stability of tapered columns under compressive loads. Distribution of the column flexural rigidity is expressed as a power function of the x-coordinate. The representative elastic-to-shear rigidity ratios equal 3, 25 and 100 respectively. Non-dimensional numerical parametric study is performed to exhibit the in-plane buckling behavior of tapered cantilever columns. The behaviors of normalized buckling loads versus slenderness agree well with the results of published classical literature ((Timoshenko & Gere 1961)). By comparison with those of the existing literature of (Timoshenko & Gere 1961), it's indicated that the factor of shear deformations is very significant for short columns and columns weak in shear rigidity.

REFERENCES

Attard, M.M. & Hunt, G.W. 2004. Hyperelastic Constitutive Modeling Under Finite Strain. International Journal of Solids and Structures, 41, 5327–5350.

Billington, D.P. 1985. The tower and the bridge—The new art of structural engineering, Princeton, New Jersey, Princeton University Press.

Coskun, S.B. & Atay, M.T. 2009. Determination of critical buckling load for elastic columns of constant and variable cross-sections using variational iteration method. Computers & Mathematics with Applications, 58, 2260–2266.

O'rourke, M. & Zebrowski, T. 1977. Buckling load for nonuniform columns. Computers & Structures, 7, 717–720.

Serna, M., Ibanez, J. & Lopez, A. 2011. Elastic flexural buckling of non-uniform members: Closed-form expression and equivalent load approach. Journal of Constructional Steel Research.

Siginer, A. 1992. Buckling of columns of variable flexural rigidity. Journal of engineering mechanics, 118, 640–643.

Smith, W.G. 1988. Analytic solutions for tapered column buckling. Computers & Structures, 28, 677–681.

Timoshenko, S.P. & Gere, J.M. 1961. Theory of Elastic Stability, London, McGraw-Hill International.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Lateral buckling of varying arbitrary cross-section beams with shear effects

Lijuan Su & Mario M. Attard
School of Civil and Environmental Engineering, The University of New South Wales, Sydney, NSW, Australia

ABSTRACT: A stability analysis is presented for Timoshenko-type beams with variable cross sections considering the shear effects under nonlinear theory. The constitutive laws for stresses and finite strains are defined adopting the consistent hyperelastic constitutive material modeling using tensor notation to simplify the complex geometric presentation. The second variation of the Total Potential is also derived which enables the application of the finite element modelling where an extra node is introduced in the middle of the element for shear rotation displacement. In presence of tapering, all section properties are not constant, with the aid of the efficient numerical approach and the software development, the locations of the centroidal and shear center axes are precisely determined on every cross section instead of using approximate method. The numerical example of web-tapered doubly symmetric and monosymmetric I- beams under moment gradient is investigated. The obtained flexural-torsion critical load predictions agree well with published solutions.

1 INTRODUCTION

Variable cross-sectional beams are found to be widely used in various kinds of structures in many forms and sizes and in many materials, buckling analyses of thin-walled variable cross-sectional structural members are the fundamental components of structural analysis and design. Shear deformations are important factors in buckling analysis, however, buckling analysis considering shear deformations remains a problem with several unresolved issues ((Ziegler 1982, Attard et al., 2008, Attard & Hunt 2008, Attard 2003, Bažant & Cedolin 1991), (Lee et al., 2009), (Machado 2008), (Reissner 1989)). The different assumptions of the shear force orientation defined in the constitutive laws have given rise to the discrepancy in the two controversial approaches of Engesser and Haringx for the inclusion of shear deformation in the column buckling modelling devisal. The adoption of the conventional constitutive relationship defined between the second Piola Kirchhoff stress tensor and its conjugate Green's strain tensor would lead to incorrect expression of strain energy density for a compressible isotropic neo-Hookean material. To address this, the constitutive relationship for stresses and finite strain is proposed in this paper using a consistent finite strain hyperelastic formulation. The tensor analysis method in the mechanics of continuum is adopted in the formulation to simplify the complex geometrical representation of finite strain analysis of the variable cross-sectional beams including shear deformations.

2 KINEMATICS

Consider a beam of variable cross sections. In the initial configuration the position vector $\mathbf{P}$ of an arbitrary point on a general material line with respect to a right-handed rectangular Cartesian coordinate system is given by:

$$\mathbf{P} = x\mathbf{i_1} + y\mathbf{i_2} + z\mathbf{i_2} \tag{1}$$

$\mathbf{i}_1$ and $\mathbf{i}_2$ signify the unit base vectors aligned with the x and y axes respectively. x, y and z are the coordinates of an arbitrary point on a general material line.

The covariant tangent base vectors on a general material line in the initial state can be obtained using Equation(1), we have:

$$\mathbf{g_1} = \frac{\partial \mathbf{P}}{\partial x} = \mathbf{i_1} + y,_x\mathbf{i_2} + z,_x\mathbf{i_2} \tag{2}$$

$$\mathbf{g_2} = \frac{\partial \mathbf{P}}{\partial y} = \mathbf{i_2} \qquad \mathbf{g_3} = \frac{\partial \mathbf{P}}{\partial z} = \mathbf{i_3} \tag{3}$$

$\mathbf{g}_{1s}$ is the tangent base vector defined at the shear center axis material line, hence:

$$\mathbf{g_{1s}} = \frac{\partial \mathbf{P}}{\partial x} = \mathbf{i_1} + y_{s,x}\mathbf{i_2} + z_{s,x}\mathbf{i_2} \tag{4}$$

In the above equation, y_s, z_s are the coordinates at the shear center axis.

The contravariant base vectors on a general material line are derived as:

$$\mathbf{g^1} = \mathbf{i_1} \qquad \mathbf{g^2} = -y_{,x}\mathbf{i_1} + \mathbf{i_2} \qquad \mathbf{g^3} = -z_{,x}\mathbf{i_1} + \mathbf{i_3} \tag{5}$$

The Euler angles and two shear angles are used to describe the cross-sectional displacement of the beam under twisting, bending and shear deformations. Apply tortuosity ψ, bending rotation θ, twisting rotation ϕ, shear rotations α_o and φ_o to the associated axes, we have:

$$\hat{\mathbf{b}} = -\sin\psi\ \mathbf{i}_2 + \cos\psi\ \mathbf{i}_3 \qquad \hat{\mathbf{h}} = \cos\psi\ \mathbf{i}_2 + \sin\psi\ \mathbf{i}_3 \tag{6}$$

$$\hat{\mathbf{n}} = \cos\theta\ \mathbf{i_1} + \sin\theta\ \hat{\mathbf{h}} \qquad \hat{\mathbf{t}} = -\sin\theta\ \mathbf{i_1} + \cos\theta\hat{\mathbf{h}} \tag{7}$$

$$\hat{\mathbf{g}}_2 = \sin\phi\hat{\mathbf{b}} + \cos\phi\ \hat{\mathbf{t}} \qquad \hat{\mathbf{g}}_3 = \cos\phi\hat{\mathbf{b}} - \sin\phi\ \hat{\mathbf{t}} \tag{8}$$

$$\hat{\mathbf{g}}_{\mathbf{1s}} = L_{sn}\hat{\mathbf{n}} + L_{s2}\hat{\mathbf{g}}_{\mathbf{2}} + L_{s3}\hat{\mathbf{g}}_{\mathbf{3}} \tag{9}$$

Where λ_{1s} is stretch of the shear center axis. $L_{sn,}$ L_{s2} and L_{s3} are the deformed shear center axis components aligned with the axes in the moving triad orthonormal vector system $\hat{\mathbf{n}}$, $\hat{\mathbf{g}}_{\mathbf{2}}$ & $\hat{\mathbf{g}}_{\mathbf{3}}$.

$$\begin{aligned} L_{sn} = {} & \lambda_{1s}\left(\cos\varphi_o - \tilde{y}_{s,x}\sin\varphi_o\right)\cos\alpha_o \\ & - \lambda_{1s}\tilde{z}_{s,x}\sin\alpha_o \end{aligned} \tag{10}$$

$$\begin{aligned} L_{s2} = {} & \lambda_{1s}\cos\phi\left(\sin\varphi_o + \tilde{y}_{s,x}\cos\varphi_o\right) \\ & + \lambda_{1s}\sin\alpha_o\left(\cos\varphi_o - \tilde{y}_{s,x}\sin\varphi_o\right)\sin\phi \\ & + \lambda_{1s}\tilde{z}_{s,x}\cos\alpha_o\sin\phi \end{aligned} \tag{11}$$

$$\begin{aligned} L_{s3} = {} & -\lambda_{1s}\sin\phi\left(\sin\varphi_o + \tilde{y}_{s,x}\cos\varphi_o\right) \\ & + \lambda_{1s}\sin\alpha_o\left(\cos\varphi_o - \tilde{y}_{s,x}\sin\varphi_o\right)\cos\phi \\ & + \lambda_{1s}\tilde{z}_{s,x}\cos\alpha_o\cos\phi \end{aligned} \tag{12}$$

The covariant tangent base vectors in the deformed state are defined by:

$$\hat{\mathbf{g}}_{\mathrm{i}} = \left(\delta_i^j + u^j\big|_i\right)\mathbf{g}_{\mathrm{j}} \tag{13}$$

The indices i and j in Equation (13) take on values of 1, 2 or 3 corresponding to the orthogonal coordinates x, y and z axes. δ_i^j is the kronecker delta. $u^j\big|_i$ is the covariant derivatives of displacement vector $\mathbf{u}$. The Einstein summation convention is adopted.

The covariant tangent base vector in the deformed state in Equation (13) is augmented to include the warping about the unit normal to the plane of the cross section, we have:

$$\begin{aligned} \hat{\mathbf{g}}_{1w} = {} & \left(L_n - (y - y_s)\kappa + (z - z_s)\kappa' - \omega\tau_{,x} - \tau\omega_{,x}\right)\hat{\mathbf{n}} \\ & + \left[L_2 - \tau\left(z - z_s + \omega\kappa\right)\right]\hat{\mathbf{g}}_{\mathbf{2}} \\ & + \left[L_3 + \tau\left(y - y_s + \omega\kappa'\right)\right]\hat{\mathbf{g}}_{\mathbf{3}} \end{aligned} \tag{14}$$

$$\hat{\mathbf{g}}_{\mathbf{2}\omega} = \hat{\mathbf{g}}_{\mathbf{2}} - \tau\,\omega_{,y}\hat{\mathbf{n}} \qquad \hat{\mathbf{g}}_{\mathbf{3}\omega} = \hat{\mathbf{g}}_{\mathbf{3}} - \tau\,\omega_{,z}\hat{\mathbf{n}} \tag{15}$$

In the above Equations (14) and (15), warping ω is a function of cross-sectional geometry. τ, κ, κ' are the deformation torsion, curvature about the y and z axes respectively.

$L_{n,}$ L_2 and L_3 are the components aligned with the axes in the moving triad orthonormal frame $\hat{\mathbf{n}}$, $\hat{\mathbf{g}}_{\mathbf{2}}$ & $\hat{\mathbf{g}}_{\mathbf{3}}$ on a general material line.

The deformation gradient tensor $\mathbf{F}$ is given by:

$$\mathbf{F} = \hat{\mathbf{g}}_{\mathrm{i}} \otimes \mathbf{g}^{\mathrm{i}} \tag{16}$$

The deformation gradient tensor $\mathbf{F}$ can be decomposed into two tensors, a rotation tensor $\mathbf{R}$ and a rotation deformation tensor $\mathbf{F}^*$ such that:

$$\mathbf{F} = \mathbf{R}\mathbf{F}^* \tag{17}$$

Rearranging Equations (16), (17), substituting the covariant tangent base vectors in the deformed state in Equations (14) (15) and the contravariant tangent base vectors in the initial configuration in Equations (5), the rotated deformation tensor $\mathbf{F}^*$ can be derived as:

$$\mathbf{F}^* = \begin{bmatrix} \lambda_n - (y - y_s)\kappa + (z - z_s)\kappa' - \omega\tau' - \tau\omega' & -\omega_{,y}\tau & -\omega_{,z}\tau \\ \left[\lambda_2 - y_{,x} - \tau\left(z - z_s + \omega\kappa\right)\right]\cos\phi - \left[\lambda_3 - z_{,x} + \tau\left(y - y_s + \omega\kappa'\right)\right]\sin\phi & \cos\phi & -\sin\phi \\ \left[\lambda_2 - y_{,x} - \tau\left(z - z_s + \omega\kappa\right)\right]\sin\phi + \left[\lambda_3 - z_{,x} + \tau\left(y - y_s + \omega\kappa'\right)\right]\cos\phi & \sin\phi & \cos\phi \end{bmatrix} \tag{18}$$

3 CONSTITUTIVE RELATIONS

A physical Lagrangian stress tensor is defined using the second Piola Kirchhoff stress tensor $\prod$ components and the rotated deformation tensor $\mathbf{F}^*$ in Equation(18), such that:

$$\mathbf{S} = \prod \mathbf{F}^{*\mathbf{T}} = \begin{bmatrix} S^{nn} & S^{n2} & S^{n3} \\ S^{2n} & S^{22} & S^{23} \\ S^{3n} & S^{32} & S^{33} \end{bmatrix} \tag{19}$$

The constitutive relationship for normal stress component S^{nn} and tangential shear stress components S^{n2}, S^{n3} in terms of the deformations are obtained:

$$S^{nn} = \mathrm{E}\left\{ \begin{pmatrix} (\lambda_n - \omega\tau' - 1) \\ +\frac{1}{2}\begin{pmatrix} \tau\left[\hat{\gamma}_3 (y - y_s) - \hat{\gamma}_2 (z - z_s)\right] \\ +R_o^2 \tau^2 \end{pmatrix} \end{pmatrix} \right\} \tag{20}$$

$$\mathrm{S}^{n2} = G\left(\hat{\gamma}_2 - \tau\left(z - z_s + \omega_{,y}\right)\right) \tag{21}$$

$$\mathrm{S}^{n3} = G\left(\hat{\gamma}_3 + \tau\left(y - y_s - \omega_{,z}\right)\right) \tag{22}$$

Where E is the elastic modulus, G is the shear modulus, $\hat{\gamma}_2$ and $\hat{\gamma}_3$ are the shear deformations.

4 EQUILIBRIUM EQAUTIONS

The virtual work equation is written in terms of the physical Lagrangian stress tensor and the rotated deformation tensor $\mathbf{F}^*$:

$$\delta W = \int_V tr\left(\mathbf{S}\boldsymbol{\delta}\mathbf{F}^*\right) dV + \delta W_E = 0 \tag{23}$$

Where *tr* denotes the trace of a tensor, V is the volume of the beam in the undeformed state, the symbol δ denotes kinematically admissible variations, δW_E is the variation of the external work and the integral signifies the internal work.

Integrating the virtual work over the cross-sectional area, the virtual work Equation (23) can be reduced to:

$$\delta W = \int_0^L \begin{bmatrix} N\delta\left(\hat{\gamma}_1 + y_s\kappa - z_s\kappa'\right) + Q_2\delta\hat{\gamma}_2 + Q_3\delta\hat{\gamma}_3 \\ +M_2\delta\kappa' + M_3\delta\kappa \\ +\left(M_t + M_{wagner}\right)\delta\tau + M_\omega\delta\tau_{,x} \end{bmatrix} dx + \delta W_E \tag{24}$$

The equilibrium equations are developed from the virtual work equation:

$$\frac{dN}{dx} - Q_t\tilde{\kappa} - Q_b\tilde{\kappa}' + p_n = 0 \tag{25}$$

$$\frac{dQ_t}{dx} + N\tilde{\kappa} - Q_b\left(\tau - \frac{d\phi}{dx}\right) + p_t = 0 \tag{26}$$

$$\frac{dQ_b}{dx} + N\tilde{\kappa}' + Q_t\left(\tau - \frac{d\phi}{dx}\right) + p_b = 0 \tag{27}$$

$$\frac{d\tilde{M}_1}{dx} - \tilde{M}_2\tilde{\kappa} - \tilde{M}_3\tilde{\kappa}' + m_n - Q_2 z_{,x} + Q_3 y_{,x} = 0 \tag{28}$$

$$\frac{d\tilde{M}_3}{dx} + \tilde{M}_1\tilde{\kappa}' + \tilde{M}_2\left(\tau - \frac{d\phi}{dx}\right) + m_b = N\lambda_t - Q_t\lambda_n \tag{29}$$

$$\frac{d\tilde{M}_2}{dx} + \tilde{M}_1\tilde{\kappa} - \tilde{M}_3\left(\tau - \frac{d\phi}{dx}\right) + m_t = -N\lambda_b + Q_b\lambda_n \tag{30}$$

Where p_n, p_t, p_b and m_n, m_t, m_b are the distributed forces and moments along the axes in the moving triad orthonormal frame $\hat{\mathbf{n}}, \hat{\mathbf{t}}$ & $\hat{\mathbf{b}}$ respectively.

5 TOTAL POTENTIAL

Take a variation of the equilibrium Equations (25)-(30) and then apply the virtual displacements principle using the Ritz variational technique, incorporating the constitutive relationships, using the section properties parameters, adopting a second order approximation for displacement components and internals actions, and evaluating the conservative surface tractions at the boundaries, for monosymmetric beams, consider the case of no initial force and ignoring the axial displacement terms, the second variation of Total Potential equation can be reduced to:

$$\delta^2 W = \frac{1}{2}\int_0^L \begin{bmatrix} GA\left(\delta\gamma_3\right)^2 + EI_{yy}\left(\delta\omega_{2,x}\right)^2 \\ +GJ_t\left(\delta\omega_{1,x}\right)^2 + EI_\omega\left(\delta\omega_{1,xx}\right)^2 \\ +2Q_2^o\left(\delta\gamma_3 - \delta\omega_2\right)\delta\omega_1 \\ -Q_2^o\dfrac{G^* I_{yy}}{A}\delta\omega_{2,x}\delta\omega_{1,x} \\ -M_3^o\beta_1^* E^*\left(\delta\omega_{1,x}\right)^2 \\ +M_3^o\left(2\delta\omega_{1,x}\delta\omega_2 - \delta\gamma_3\delta\omega_{1,x}\right) \\ +q_y^o e_y\delta\omega_1{}^2 \end{bmatrix} dx + \frac{1}{2}P_y^o a_y\delta\overline{\omega}_1^2 \tag{31}$$

The displacements components and internal actions in the above second variation of Total Potential Equation (31) are second order approximations obtained by truncated the expressions for displacements components and internal actions

in the virtual Equation (24). The solutions thus obtained are comparable to other lateral torsional buckling formulations which are based on second order approximations.

The truncated expressions for the displacements also enable the application of finite element modelling formulation to investigate the lateral buckling behavior of variable cross-sectional beams.

6 FINITE ELEMENT MODEL

In the proposed formulation where the shear deformations are taken into consideration, the displacement derivatives in y and z axes directions are not equal to the bending rotation about y and z axes due to the presence of shear angles. The shear angles are the difference between displacement derivatives and the bending angles about the y and z axes and are expressed as:

$$\gamma_2 = v_{s,x} - \omega_3 \quad \gamma_3 = w_{s,x} + \omega_2 \tag{32}$$

Along a beam element as shown in Figure, each node at the ends of the element consists of the usual six generalised displacement for spatial frame element and the displacement associated with warping. In addition to the aforementioned seven displacements, two rotations about y and z axes are included to account for the shear deformations. An extra node is also introduced in the middle of each element to achieve the compatibility between displacements associated with displacement derivatives and shear rotations.

For the generalized displacements for each element in the finite element model, nine generalised displacements are at each end of the element, while two displacements associated with y and z axes are at the middle note of each element. The generalized displacements are depicted in Figure 1.

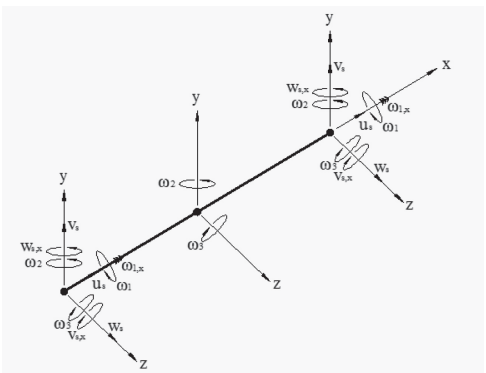


Figure 1. Generalised elemental displacements.

The stiffness and stability element matrices are constructed based on the presented generalized displacements in the finite element model. The stiffness and stability structure matrices are assembled depending on the node numbering at the ends of the element regardless of the node in the middle of the element. The critical buckling loads are then obtained by solving the eigenproblem resulted from the tangent stiffness for the whole structure.

The accuracy of the proposed finite element modeling method in dealing with stability problem of tapered beams is demonstrated by yielding solutions to the numerical examples. In all cases good agreement with published solutions is exhibited.

7 NUMERICAL EXAMPLES

7.1 *Lateral buckling of a simply supported singly symmetric prismatic I-beam under uniform bending*

The accuracy of the lateral buckling analysis formulation and the finite element modelling method is first assessed by considering a 6m simply supported I-beam with constant monosymmetric section under uniform bending moments about its major axis as illustrated in Figure 2.

The geometric dimensions of the monosymmetric cross section are shown in Figure 3. The material properties are elastic modulus E = 65120 MPa and shear modulus G = 25970 MPa. The geometric data of the beam section are computed from its dimensions and are given as:

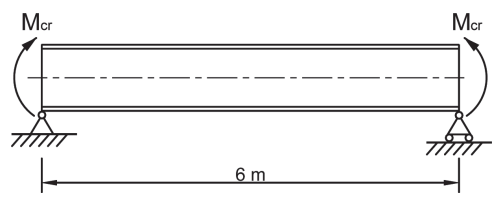


Figure 2. Simply supported prismatic I-beams under uniform bending.

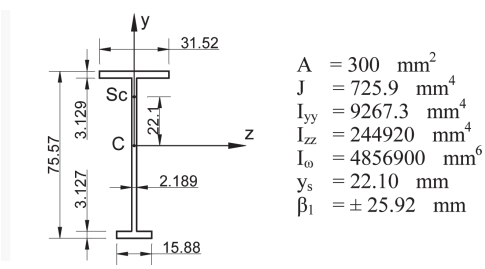


Figure 3. Monosymmetric constant section of simply supported I –beam.

The dimensionless analytical solution was provided by Goodier (1942) to the lateral buckling problem of simply supported singly symmetric I-beam under equal and opposite bending moments. Attard (1986) carried out the finite element method with a beam discretization of six elements based on the lateral buckling formulation developed by the author to investigate the same stability problem. A comparison of the critical bending moments is made and tabulated in Table 1 which shows good agreement.

7.2 *Lateral buckling of simply supported web-tapered I-beams with doubly symmetric and singly symmetric cross-sections under moment gradient*

The accuracy of the developed stability analysis approach and the finite element formulation is further tested by solving the lateral buckling problem of a simply supported web-tapered I-beam under moment gradient as illustrated in Figure 4. The beam tapers from the maximum height h_{max} at the left support to αh_{max} at the other support. The tapering constants are taken as 0.6, 0.8 and 1.0 for the beam lengths of 4m and 6m respectively. For each case, the moment gradient coefficient ψ varies from 0.25 to 1.0.

The lateral buckling behaviors of web-tapered I—beams with doubly symmetric and monosymmetric sections are both investigated. The Young's modulus is E = 210,000 MPa and the shear modulus is G = 80,000 MPa. The dimensions of doubly symmetric and monosymmetric sections for the simply supported web-tapered I-beam are depicted in Figure 5.

The critical buckling moments obtained from the solutions based on the developed formulation and the finite element model are shown in Table 1,2 for doubly symmetric section and in Table 3 for monosymmetric section. In these tables, a comparison is made with the solutions proposed by Zhang & Tong (2008) where the Rayleigh-Ritz method was used by the authors to solve this stability problem, as well as the critical loads results presented by Asgarian et al. (2013) in which the authors employed the finite element method by means of Ansys software and the numerical model by means of power series method.

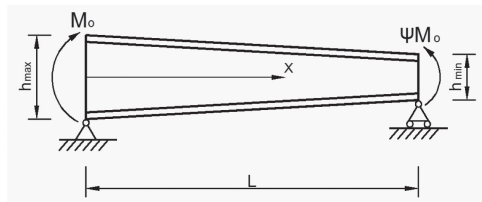


Figure 4. Simply supported web-tapered I-beams under moment gradient.

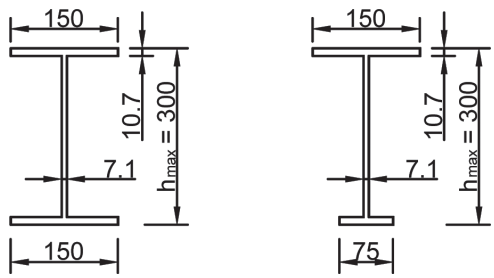


Figure 5. Doubly symmetric and monosymmetric sections of simply supported web-tapered I-beam.

Table 1. Critical moments for simply supported prismatic I-beam with monosymmetric section Nm.

β_1 mm	Goodier [7]	Attard [2]	This study
+25.92	51.87	51.87	51.84
- 25.92	60.45	60.46	60.44

Table 2. Critical bending moments for simply supported web-tapered I-beams with doubly symmetric section kNm.

L		ψ = 0.25				ψ = 0.5			
		Zhang [11]	Asgarian [1]		This study	Zhang [11]	Asgarian [1]		This study
m	α		Ansys	Numerical			Ansys	Numerical	
4	0.6	219.4	207.4	207.4	205.8	182.8	175.6	175.5	174.1
	0.8	227.5	220.8	220.1	219.0	189.6	186.9	186.9	185.9
	1.0	240.1	234.9	233.0	232.2	200.1	198.8	198.3	197.7
6	0.6	124.2	119.0	118.7	117.9	103.5	100.8	100.8	100.1
	0.8	127.6	124.2	123.5	122.8	106.4	105.1	105.0	104.5
	1.0	132.6	129.7	128.8	127.8	110.5	109.8	109.4	109.0

Table 3. Critical bending moments for simply supported web-tapered I-beams with doubly symmetric section kNm.

L		ψ = 0.75				ψ = 1.0			
		Zhang [11]	Asgarian [1]		This study	Zhang [11]	Asgarian [1]		This study
m	α		Ansys	Numerical			Ansys	Numerical	
4	0.6	156.7	151.4	150.8	149.6	132.4	132.3	131.7	130.6
	0.8	162.5	161.1	161.1	160.3	142.2	141.2	140.9	140.2
	1.0	171.5	171.4	171.3	170.9	150.3	150.2	150.2	149.8
6	0.6	88.7	86.9	86.8	86.2	77.6	76.1	75.8	75.3
	0.8	91.1	90.7	90.7	90.2	70.8	79.4	79.3	78.9
	1.0	94.7	94.7	94.6	94.3	82.9	82.9	82.9	82.7

Table 4. Critical bending moments for simply supported web-tapered I-beams with monosymmetric section kNm.

L		ψ = 0.25			ψ = 0.5			ψ = 0.75			ψ = 1.0		
		Asgarian [1]		This study	Asgarian [1]		This study	Asgarian [1]		This study	Asgarian [1]		This study
m	α	Ansys	Numerical		Ansys	Numerical		Ansys	Numerical		Ansys	Numerical	
4	0.6	67.68	59.02	63.79	57.83	53.90	55.87	50.33	49.03	49.13	44.47	44.55	43.50
	0.8	68.71	62.99	64.53	58.17	55.77	56.08	50.30	49.56	49.00	44.23	44.22	43.17
	1.0	70.01	67.74	65.44	58.80	58.01	56.51	55.54	50.41	49.13	44.26	43.91	43.14
6	0.6	49.13	43.50	45.95	41.88	39.34	40.39	36.36	35.57	35.58	32.06	32.11	31.50
	0.8	49.41	46.39	46.12	41.83	40.22	40.32	36.14	35.67	35.32	31.75	31.68	31.14
	1.0	49.80	46.88	46.36	41.90	41.20	40.32	36.04	35.93	35.17	31.57	31.57	30.90

It can be observed that the lateral buckling behaviors agree well with solutions in the existing literatures. It can therefore concluded that the stability problem formulation and finite element modelling method proposed in this paper are capable of making accurate predictions of the elastic flexural- torsional buckling loads of web-tapered doubly symmetric and monosymmetric I-beams incorporating the shear deformations.

8 CONCLUSION

An elastic stability analysis is presented in this paper for Timoshenko-type beams with variable cross sections taking into consideration the effects of shear deformations under the geometrically non-linear theory based on large displacements and rotations. The constitutive relationship for stresses and finite strains based on a consistent finite strain hyperelastic formulation is proposed. The generalized equilibrium equations for varying arbitrary cross-sectional beams are developed from the virtual work equation. The second variation of the Total Potential is also derived which enables the application of the finite element method which is capable of making accurate prediction of the elastic flexural-torsional critical buckling loads of tapered, doubly symmetric and singly symmetric I-section beams including the shear deformations. In the finite element formulation, the element displacement field is assumed using polynomial functions, in discretizing the beam, one extra node is introduced in the middle of the element. The usual generalized displacements are at the ends of each element while the additional displacement associated with shear rotations are both at the ends of each element and at the middle node of each element to achieve compatibility between displacements corresponding to rotations results from bending and shear deformations. In presence of tapering, all section properties are non-constant along the length of the beam, the shear center and centroidal axis representations were abandoned due to difficulties in specifying their positions caused by the cross-sectional tapering in previous studies. In this paper, with the aid of the efficient numerical approach and the software development, the locations of the centroidal and shear center axes on the cross sections are precisely determined

through accurate calculation instead of using approximate method. The accuracy and validation of the developed stability analysis formulation and finite element modelling are tested by solving the numerical examples to which the solutions are available in the published literature. The problems being considered is a 6m simply supported mono-symmetric I-beam under equal and opposite bending moments about its major axis. The accuracy of developed formulations are further investigated by looking at the flexural-torsional buckling problems of a simply supported web-tapered doubly symmetric and singly symmetric I-beams under moment gradient, the moment gradient coefficient varies from 0.25 to 1 for beam lengths of 4m and 6m with tapering constant equal to 0.6, 0.8 and 1.0 respectively. For all the numerical examples being investigated, the obtained lateral critical buckling moments predictions show a great agreement with published solutions.

REFERENCES

Asgarian, B., Soltani, M. & Mohri, F., 2013. Lateral-torsional buckling of tapered thin-walled beams with arbitrary cross-sections. *Thin-Walled Structures,* 62, 96–108.

Attard, M.M., 1986. Lateral buckling analysis of beams by the Fem. *Computers & Structures,* 23, 217–231.

Attard, M.M., 2003. Finite strain—beam theory. *International Journal of Solids and Structures,* 40, 4563–4584.

Attard, M.M. & Hunt, G.W., 2008. Column buckling with shear deformations—A hyperelastic formulation. *International Journal of Solids and Structures,* 45, 4322–4339.

Attard, M.M., Lee, J.S. & Kim, M.Y., 2008. Dynamic stability of shear-flexible beck's columns based on Engesser's and Haringx's buckling theories. *Computers & Structures,* 86, 2042–2055.

Bažant, Z.P. & Cedolin, L., 1991. *Stability of Structures,* New York, Oxford University Press, Inc.

Goodier, J., 1942. Torsional and flexural buckling of bars of thin-walled open section under compressive and bending loads. *J. Appl. Mech., ASME,* 64, A103-A107.

Lee, J.S., Lee, K.C., Kim, M.Y. & Attard, M.M., 2009. Spatial stability of shear-flexible thin-walled beams based on Engesser's and Haringx's theories. *International Journal of Solid and Structures*.

Machado, S.P., 2008. Non-linear buckling and postbuckling behavior of thin-walled beams considering shear deformation. *International Journal of Non-Linear Mechanics,* 43, 345–365.

Reissner, E., 1989. Lateral buckling of beams *Computers & Structures,* 33, 1289–1306.

Zhang, L. & Tong, G.S., 2008. Lateral buckling of web-tapered I-beams: A new theory. *Journal of Constructional Steel Research,* 64, 1379–1393.

Ziegler, H., 1982. Arguments for and against Engesser buckling formulas. *Ingenieur Archiv,* 52, 105–113.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Methodology for the quantitative risk assessment of road bridges exposed to accidental events

M. Sykora & M. Holicky
Klokner Institute, Czech Technical University in Prague, Prague, Czech Republic

P. Maňas
Faculty of Military Technology, University of Defence, Brno, Czech Republic

ABSTRACT: Road bridges in accidental situations represent the most vulnerable components of transportation networks. Accidental situations may be caused by natural or man-made hazards. Decisions concerning protective measures can be based on the probabilistic optimisation of expected costs. In general, total structural costs consist of initial, service costs and consequences of structural failure. The initial cost comprises of construction cost including cost of protective measures; service costs cover maintenance expenditures and safety guards expenses; the failure consequences account for direct costs related to structural failure and follow-up costs due to malfunction of transportation network. Proposed general procedure for the risk assessment is based on Bayesian (causal) networks. It appears that this technique provides valuable background information for the decisions concerning efficient protective measures for bridges endangered by various types of hazards.

1 INTRODUCTION

The European road network has a vital importance for the European economy. Even smaller disruptions due to traffic restrictions or failure of some elements of the network may result in high consequences, Imam & Chryssanthopoulos (2012). Due to the interdependence of the road transport network with rail, air and shipping traffic, a failure of important connections may yield a domino effect, Andersen et al. (2013).

In such a case the network and its major components are classified as a "critical infrastructure (object)" that is defined according to the European *COUNCIL DIRECTIVE 2008/114/EC* (identification and designation of European critical infrastructures and the assessment of the need to improve their protection) as:

an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a state as a result of the failure to maintain those functions.

The *Communication from the Commission on a European Programme for Critical Infrastructure Protection COM(2006) 786* further provides the criteria for designation of critical infrastructures. The unavailability of a particular critical infrastructure should be rated by the extent of affected geographic area, number of population, related economic loss, environmental, political or psychological effects. The protection of critical infrastructures is to be based on an all-hazards approach; recognising the threat from terrorism as a priority.

Bridges (together with tunnels) are perceived as the most vulnerable components of the road network, Bocchini & Frangopol (2011). Due to their bottleneck function terrorist attacks are one of the most dangerous threats for such structures, Andersen et al. (2013).

In this study assessments of individual road bridges exposed to accidental situations are discussed from a general point of view. Stewart (2010) recommended cost-benefit and other risk-based approaches particularly for low probability-high consequence events where public safety is a key criterion for decision making. That is why methodology of the risk optimisation based on Bayesian networks is developed here. It is noted that the terminology accepted in Eurocodes (*EN 1990:2002* for the basis of structural design and *EN 1991-1-7:2006* for accidental actions) and other European documents (*DIRECTIVE 2008/114/EC* and *Communication COM(2006) 786*) is adopted.

2 IDENTIFICATION OF POSSIBLE CRITICAL BRIDGES

According to SeRoN (2012) the following aspects should be taken into account when selecting critical bridges:

- Location in urban environment,
- Conventional construction type,
- Possible traffic bottleneck formation,
- Large bridge over the sea,
- Landmark bridge,
- Very well-known bridge,
- Hard to rebuild bridge,
- Small bridge but important due to traffic volume.

Detailed procedure for the identification of possible critical bridges is provided in SeRoN (2012). Failure consequences can be seen as a good indicator of the importance of a bridge as indicated by Imam & Chryssanthopoulos (2012).

3 PRINCIPLES OF RISK OPTIMISATION

In general, risk analysis aims at consideration of all possible events together with their unfavourable consequences. Such events are often caused by extreme hazards or human errors. Table 1 indicates frequent causes of in-service failures of bridges; overview of recent important failures of construction works was provided by Agarwal et al. (2012).

Table 1. Causes of in-service failures of bridges adapted from Scheer (2010) and Vrouwenvelder et al. (2012).

Cause	Examples
Overload	Impact (vehicle, ship) Flooding, ice floes, floating timber Fire Explosion Seismic activity Wind action
Material degradation	Corrosion fatigue
Problems with foundations	Settlements
Malevolent human actions	Terrorist attack Vandalism
Human error	Design errors including incorrect dimensioning, neglected dynamic effects, unrecognised stability problems Construction errors such as material flaws and incorrect assembly
Unknown (unforeseeable)	Unknown stability problems

Adequate hazard scenarios and relevant occurrence probabilities need to be estimated, often on the basis of expert assessments and judgements. When for mutually independent hazard situations H_i the failure F of the component given a particular situation H_i occurs with the conditional probability $P(F|H_i)$, then the total probability of failure P_f is given by the law of total probability as:

$$P_f = \sum_i P(F|H_i)\, P(H_i) \quad (1)$$

The conditional probabilities $P(F|H_i)$ are determined by analyses of situations H_i. Annual reference period is normally accepted.

The situations H_i may lead to several events E_{ij} (e.g., excessive cracking, failure of a structural member, collapse of the bridge) with adverse consequences C_{ij} that are commonly expressed in monetary units. The total annual risk R corresponding to the hazard situations H_i can be expressed as:

$$R = \sum_{ij} C_{ij}\, P(E_{ij}|H_i)\, P(H_i) \quad (2)$$

If an acceptable risk R_t is specified, the bridge or its structural members can be assessed on its basis, $R < R_t$. When the criterion of acceptable risks is not fulfilled, it is necessary to modify the system by appropriate interventions aiming at the reduction of probability of occurrence of adverse events or at the reduction of their consequences.

Further information on the probabilistic risk analysis can be obtained from *ISO 13824:2009* on the general principles on risk assessment of systems involving structures, the Joint Committee on Structural Safety document JCSS (2008) or the monograph by Stewart & Melchers (1997).

From an economic point of view the objective is to minimize the total working-life cost of the bridge. For simplification assessment of the cost efficiency of a single protective measure is considered hereafter (with straightforward extensions for the decisions concerning several protective measures).

The decision parameter(s) d to be optimised may represent resistance in the case of upgrading, stand-off distance, properties of energy absorbing shields etc. The parameter may be continuous, discrete or attain a single value. In general the costs of the measure consist of:

- Cost C_0 independent of the decision parameter (costs related to surveys, design, administration and management, economic losses due to traffic interruptions in the case of existing structures),
- Marginal cost C_m dependent on the decision parameter (costs of construction materials, safety equipment, monitoring).

The failure consequences C_f can be estimated on the basis of the total annual risk R. Since the main reason for the existence of civil infrastructures is

the public interest, failure consequences need to include all societal losses (see Section 5.2).

For consistency, all the costs need to be expressed on a common basis. Costs of the measure are normally specified in a present value. All the expected failure costs that may occur within a reference period should thus be likewise estimated in the present worth. Assuming almost independent failure events in subsequent years and small probabilities $P(H_i)$, the expected failure cost related to a reference period t_{ref} (in years) can be estimated (Holicky (2013)):

$$E[C_f(t_{ref},d)] \approx R(d)\,[1 - 1/(1+q)^{tref}]/[1 - 1/(1+q)] = R(d)\,Q(q, t_{ref}) \quad (3)$$

where q = annual discount rate; and Q = time factor. The discount rate is commonly around 0.03 (an approved draft of *ISO 2394* from 2014 suggests 0.01–0.03 for most Western economies and 0.05–0.08 for most Asian economies; *ISO 15686-5:2008* on life-cycle costing for buildings assumes typical discount rates 0–0.04).

The expected total costs C_{tot} can now be expressed (omitting the symbol of expectation for convenience of notation) as:

$$\text{Measure: } C_{tot}(t_{ref};d) \approx C_0 + C_m\, d + R(d)Q(q, t_{ref}) \quad (4a)$$

$$\text{No measure: } C_{tot}(t_{ref}) = R(\text{no measure})\, Q(q, t_{ref}) \quad (4b)$$

From Equation (4a) the optimum value of the decision parameter d_{opt} (optimum measure) can be assessed:

$$\text{minimum}_d\, C_{tot}(t_{ref};d) = C_{tot}(t_{ref};d_{opt}) \quad (5)$$

No measure is accepted when the total cost according to Equation (4b) is less than the total cost of the optimum upgrade.

Apparently a more complex cost model would consider costs of inspections, maintenance, upgrades and other life-cycle costs. However, in most cases such extensions hardly improve the optimum measures mitigating risks in accidental situations.

4 RISK OPTIMISATION USING BAYESIAN NETWORKS

4.1 *Advantages of Bayesian networks*

In accordance with Stewart & Melchers (1997) risk of various technical systems in hazard situations can be analysed using the standard techniques such as fault trees, event trees, cause-consequence method, Bayesian (causal) networks and Petri networks.

In case of dependent basic events, fault trees become non-intuitive and difficult to handle, Mahboob & Straub (2011). This may be a serious limitation for civil engineering applications. In principle event trees can deal with such dependencies; however this requires great care during an analysis as observed by Faber & Stewart (2003). Moreover both methods suffer from the difficulty in updating based on new information. Petri Nets provide a powerful platform, but the evaluation often takes basis in Monte Carlo simulations requiring considerable computational demands, Nishijima et al. (2009). These drawbacks can be overcome by the use of Bayesian probabilistic networks with discrete nodes supplemented by decision and utility nodes, Nielsen & Jensen (2007).

With regard to practical applications Bayesian networks facilitate (adopted from Holicky et al. (2013)):

- Breakdown of a complex task (system of structural elements) into smaller sub-tasks (foundations, piers, super-structure) that can be analysed separately by different experts,
- Transparent interpretation of knowledge concerning structural elements based on results of measurements and expert appraisals,
- Consideration of uncertainties in action effects, material and geometrical properties, and also in the applied theoretical models,
- Modelling of complicated dependencies amongst initiation events of actions, their effects, structural properties and effects of protective measures,
- Updating of results when new information is available (Bayesian networks are transparent and can be readily modified).

It is fair to note that Bayesian networks require additional expertise in comparison with tree-based analyses. In addition the logic relations between components of the system (e.g., AND, OR) cannot be directly observed from the graphical representation, Mahboob & Straub (2011).

The analysis of Bayesian network is based on the specification of conditional probabilities of nodes under assumption of information on other nodes (in the direction of casual links). The analysis is based on the concept of conditional probabilities and the theory of probability. Detail information is provided e.g., by Holicky (2009), Nielsen & Jensen (2007) and Stewart & Melchers (1997).

4.2 *Example of the network*

Figure 1 shows an example of the Bayesian network (influence diagram) that provides a general basis for a particular assessment. Note that the network is significantly simplified and has to be modified to reflect specific conditions of an analysed structure and considered accidental

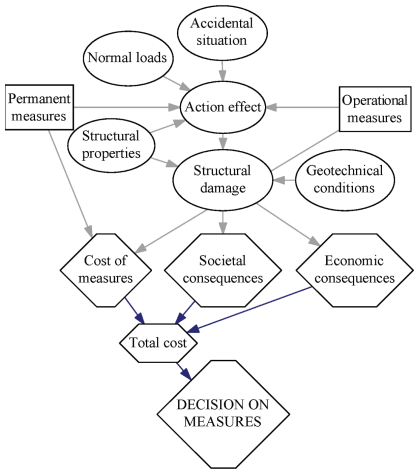


Figure 1. Example of the Bayesian network.

situations. In practical applications each random node may represent a sub-system and additional utility nodes may be needed. The following nodes are included in Figure 1:

- Chance nodes—Accidental situation, Action effect, Structural damage, Geotechnical conditions, and Structural properties,
- Decision nodes—Permanent and Operational measures,
- Utility nodes—Cost of measures, Societal and Economic consequences, and Total cost.

Directional arrows, interconnecting all the nodes, indicate the causal links between parent and children nodes.

Given an accidental situation the action effects, influenced by accepted protective measures, may lead to structural malfunction (covered in the network by the random node Structural damage) due to damage, local failures, partial or total collapse of the bridge. Probability of structural damage and its extent will likely depend on geotechnical conditions and structural properties.

Structural damage may result in societal and economic consequences. The utility node Societal consequences describes the expected number of fatalities and injuries given structural collapse and related compensation costs, which may be based on the so-called societal value of statistical life, Holicky (2009).

5 MODELLING OF SELECTED NODES

5.1 *Action effects*

In accordance with Vrouwenvelder et al. (2012) bridges may be exposed to the following actions (cf. Table 1):

- Normal—self weight, traffic, thermal, wind load,
- Accidental (natural)—earthquake, landslide, wind action, avalanche, rock fall, flood and tsunami,
- Accidental (man-made—malevolent or unconscious)—explosion, fire, impact of vehicle, ship or projectile, mining settlement,
- Human errors—design error, material flaw, construction error, misuse, lack of maintenance.

The model of an accidental action takes into account the annual probability of occurrence of the accidental situation and the conditional probability of the accidental action (e.g., success rate in the case of blast terrorist attack).

To provide more specific information, modelling of a terrorist attack is further discussed. The information needed for the analysis may be gained from experts, scenario analysis and analysis of available data, Stewart & Mueller (2012). Limited statistical information was provided by Stewart (2010). Based on a literature review, the annual probability of terrorist attack on US commercial buildings was estimated as $P(H) \approx 10^{-6}$–10^{-7} per building. Ellingwood (2006) suggested increasing the minimum attack probability $P(H)$ to ~10^{-4}/ building/ year for high density occupancies, key governmental and international institutions, monumental or iconic buildings or other critical facilities with a specific threat. As a first approximation key bridges may be associated with this value. It is interesting to observe that this value is comparable to the annual probability of a vehicular collision ($P(H) \approx 6 \times 10^{-4}$/ building/ year given by Ellingwood (2002)).

However, for terrorism the threat comes from an intelligent adversary who adapts to changing circumstances to maximise likelihood of success, Stewart (2010). Moreover, the probability $P(H)$ depends on a policy of the country (involvement in military operations abroad, approach to minorities). Although some statistical approaches exist for terrorist threat prediction, these rely heavily on judgments of security experts, game theory, etc. so the inherent uncertainties remain still high. For this reason, the report by the US Department of Homeland Security (2009) states that *the assessment of the probabilities that adversaries will choose courses of action should be the outputs of analysis, not required input parameters*. Hence, Stewart (2010) recommended using the cost-benefit analysis to specify the minimum (threshold) threat probability below which a specific protective measure becomes cost-ineffective.

Guidance for the development of probabilistic models of accidental action effects was provided by Vrouwenvelder (2000); for instance the model for blast loading was discussed by Netherton &

Stewart (2010), models for earthquake, impact load and fire by JCSS (2001).

Damage on the bridge exposed to normal and accidental loads is then estimated on the basis of system modelling considering the effects of applied protective measures.

5.2 *Failure consequences*

Overview of possible consequences of bridge failure is provided in SeRoN (2012):

- Direct consequences resulting directly from the structural damage, examples include:
  - Fatalities or injuries due to structural collapse, blast pressure or secondary projectiles (concrete, steel, glass),
  - Economic losses due to cost of rehabilitation or rebuilding, cost of damaged vehicles,
- Follow-up (indirect) consequences describing other impacts on the society, for instance:
  - Fatalities or injuries due to malfunction of the bridge (e.g., in an emergency situation),
  - Losses due to detours, losses of local businesses affected by malfunction of the bridge,
  - Environmental impacts (air pollution, energy use or fuel consumption),
  - Psychological consequences including loss of reputation or undue changes in professional practice,
  - Infrastructure interdependency costs etc.

Guidance for the quantification of these consequences is provided by Imam & Chryssanthopoulos (2012) and Thoft-Christensen (2009).

5.3 *Protective measures*

Permanent or operational protective measures may include (adapted from Berrick (2009)):

- Restriction of physical access (barriers, security officers to control access, eliminated parking near critical structures, landscaping to increase standoff distance),
- Surveillance and detection efforts (inspections, warning that the bridge is being monitored, enhanced lighting, motion sensors, removal of overgrown vegetation),
- Security planning and coordination (security plans to identify critical components and establish their protection, emergency telephones, means for rerouting traffic to enable access of emergency vehicles, restricted access after span failure),
- Structural modifications (protection of lower parts of cables on cable-stayed and suspension bridges, reinforce welds and bolted connections to ensure plastic capacity, use energy absorbing bolts to strengthen connections and reduce deformations, alternate load paths).

It is noted that efficiency has to be assessed for all considered measures. For instance investments into motion sensors may decrease needs for the restriction of physical access. The control of access by guards is often ineffective since they can be intentionally distracted by secondary attacks. For blast attacks the stand-off distance is a key parameter and can be hardly replaced by protective walls. However, quantification of the effects of protective measures may be difficult (e.g., estimating reduction of the probability of attack when safety guards patrol a bridge).

6 DISCUSSION

In accordance with Stewart & Mueller (2012) risk and cost-benefit considerations provide important insights into how security measures should perform, reduce risks and are cost-effective.

A risk-averse attitude in which severe consequences are more weighed is commonly accepted in decision-making, Cha & Ellingwood (2012). Despite this a risk-neutral attitude is suggested in this study to obtain the most efficient option in terms of the expected life cycle cost.

While quantitative decision support tools have many advantages for decision-making, they cannot capture the full and diverse range of societal considerations of risk acceptability, Stewart (2010). More specifically many societal, economic, cultural, environmental, political and other considerations are hardly quantifiable. That is why the probabilistic risk assessment should be viewed only as a tool supporting decision-makers.

Highway and road authorities and network managers may be more interested in the risks of a whole network rather than to the risks of an individual bridge. In this case the methodology proposed here should be extended similarly as proposed by Bocchini & Frangopol (2011).

7 CONCLUDING REMARKS

The present study leads to the following conclusions:

- Bridges and tunnels represent the most vulnerable components of road networks.
- Decisions concerning selection of protective measures can be based on the risk-based optimisation of expected costs; Bayesian networks provide an effective tool for risk estimation under uncertainties.

– Actions to be considered in the assessment may include normal and accidental (natural or man-made) loads and effects of human errors.
– Protective measures may include restriction of physical access, detection efforts, security planning and coordination, and construction modifications aiming to improve structural robustness.

Further research will be focused on illustrative applications on the developed methodology in the assessment of Czech highway bridges and tunnels.

ACKNOWLEDGEMENTS

The study is based on outcomes of the research project VG20122015089 supported by the Ministry of the Interior of the Czech Republic.

REFERENCES

Agarwal, J., Haberland, M., Holicky, M., Sykora, M. & Thelandersson, S. 2012. Robustness of Structures: Lessons from Failures. *Structural Engineering International* 22(1): 105–111.

Andersen, C.A., Jørgensen, K.C. & Lauritzen, E.K. 2013. Cost-effectiveness of protection measures to mitigate terrorist attacks on bridges and tunnels. *Proc. SAFE 2013, Rome, Italy, 17-19 September 2013.* Ashurst Lodge: WIT Press.

Berrick, C.A. 2009. *Highway Infrastructure: Federal Efforts to Strengthen Security Should be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*. DIANE Publishing Company.

Bocchini, P. & Frangopol, D.M. 2011. Generalized bridge network performance analysis with correlation and time-variant reliability. *Structural Safety* 33(2): 155–164.

Bocchini, P. & Frangopol, D.M. 2011. A stochastic computational framework for the joint transportation network fragility analysis and traffic flow distribution under extreme events. *Probabilistic Engineering Mechanics* 26(2): 182–193.

Cha, E.J. & Ellingwood, B.R. 2012. Risk-averse decision-making for civil infrastructure exposed to low-probability, high-consequence events. *Reliability Engineering & System Safety* 104 (August 2012): 27–35.

Ellingwood, B.R. 2002. Load and Resistance Factor Criteria for Progressive Collapse Design. *National Workshop on Prevention of Progressive Collapse, Rosemont (Illinois)*, 10-12 July 2002.

Ellingwood, B.R. 2006. Mitigating risk from abnormal loads and progressive collapse. *Journal of Performance of Constructed Facilities* 20(4): 315–323.

Faber, M.H. & Stewart, M.G. 2003. Risk assessment for civil engineering facilities: critical overview and discussion. *Reliability Engineering & System Safety* 80(2): 173–184.

Holicky, M. 2013. Optimisation of the target reliability for temporary structures. *Civil Engineering and Environmental Systems* 30(2): 87–96.

Holicky, M. 2009. Probabilistic risk optimization of road tunnels. *Structural Safety* 31(3): 260–266.

Holicky, M., Markova, J. & Sykora, M. 2013. Forensic assessment of a bridge downfall using Bayesian networks. *Engineering Failure Analysis* 30(0): 1–9.

Imam, B.M. & Chryssanthopoulos, M.K. 2012. Causes and Consequences of Metallic Bridge Failures. *Structural Engineering International* 22(1): 93–98.

JCSS 2001. *JCSS Probabilistic Model Code.* Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>.

JCSS 2008. Risk Assessment in Engineering—Principles, System Representation & Risk Criteria. Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>.

Mahboob, Q. & Straub, D. 2011. Comparison of fault tree and Bayesian Networks for modeling safety critical components in railway systems. In C. Guedes Soares (ed.), *Proc. ESREL 2011, Troyes (France), 18–22 September 2011.* Rotterdam: CRC Press/ Balkema.

Netherton, M.D. & Stewart, M.G. 2010. Blast load variability and accuracy of blast load prediction models. *International Journal of Protective Structures* 1(4): 543–570.

Nielsen, T.D. & Jensen, F.V. 2007. *Bayesian Networks and Decision Graphs.* Berlin: Springer.

Nishijima, K., Maes, M.A., Goyet, J. & Faber, M.H. 2009. Constrained optimization of component reliabilities in complex systems. *Structural Safety* 31(2): 168–178.

Scheer, J. 2010. Failed Bridges: Case Studies, Causes and Consequences. Wiley.

SeRoN 2012. *Risk Assessment (Deliverable D500)*, The SeRoN Consortium.

Stewart, M.G. & Melchers, R.E. 1997. *Probabilistic Risk Assessment of Engineering Systems.* Berlin: Springer.

Stewart, M.G. & Mueller, J. 2012. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection. In M. Vořechovský, V. Sadílek, S. Seitl, V. Veselý, R.l. Muhanna & R.l. Mullen (eds.), *Proc. Reliability Engineering Computing REC 2012, Brno, 13–15 June 2012.* Brno: Brno University of Technology.

Stewart, M. 2010a. Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. *International Journal of Critical Infrastructure Protection* 3(1): 29–40.

Stewart, M.G. 2010b. Acceptable risk criteria for infrastructure protection. *International Journal of Protective Structures* 1(1): 23–40.

Thoft-Christensen, P. 2009. Life-Cycle Cost-Benefit (LCCB) analysis of bridges from a user and social point of view. *Structure and Infrastructure Engineering* 5(1): 49–57.

US Department of Homeland Security 2009. *National Infrastructure Protection Plan,* Washington, DC:

Vrouwenvelder, T. 2000. Stochastic modelling of extreme action events in structural engineering. *Probabilistic Engineering Mechanics* 15(1): 109–117.

Vrouwenvelder, T., Leira, B.J. & Sykora, M. 2012. Modelling of Hazards. *Structural Engineering International* 22(1): 73–78.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Point estimate of dynamic reliability considering parameter uncertainties

Y.G. Zhao
Department of Architecture, Kanagawa University, Yokohama, Japan

Z.H. Lu
School of Civil Engineering, Central South University, Changsha, China

1 INTRODUCTION

Assessment of dynamic structural reliability is a complex procedure, even with given system parameters. It has been realized that the effect of uncertainties in system parameters including structural properties such as stiffness, damping, and strength and excitation characteristics such as frequency content and duration may be equally important, even dominant, as far as the overall dynamic structural reliability is concerned. An important focus in recent research has been to incorporate parameter uncertainties into reliability analysis.

Approximate methods for evaluating dynamic structural reliability considering uncertainties described in terms of random variables have been developed by many researchers. For a linear oscillator, a first-order reliability method was proposed by Hohenbichler and Rackwitz (1981) in which the distribution of the maximum peak of the response is used, and the method has been used in case of non-stationary excitation by Quek et al. (1990) and Balendra et al. (1991). For the general problem, reliability estimation methods were proposed by Gueri and Rackwitz (1986) and Madsen (1987), in which auxiliary variables were introduced, and the first-order reliability method can be used. A practical treatment of reliability with response as a nonlinear combination of scalar Gaussian processes can be found in the study of Madsen and Moghtaderi-Zadeh (1987). A more general discussion of dynamic structural reliability analysis is provided by Wen and Chen (1987). By incorporating these methods, a nested first-order reliability method is proposed by Madsen and Tvedt (1990) on the basis of a discussion of the calculation of the failure probability with given parameters.

The purpose of this study is to review the recently developed available methods and propose an effective method for evaluating dynamic structural reliability. The general performance function is investigated, and equivalence of several first-order formulations is discussed. A point estimate method for dynamic reliability analysis considering parameter uncertainties is developed, and efficiency of the method is demonstrated using a simple example.

2 DEFINITION OF THE PROBLEM

For time-invariant structural reliability, the problem is generally described by a performance function $G(\mathbf{X})$, in which $\mathbf{X}$ is a vector of random variables of system parameters, and the probability of failure (limit state being reached) can be formulated by

$$P_F = \int_{G(\mathbf{X})\le 0} f_{\mathbf{X}}(\mathbf{x})dX \tag{1}$$

The powerful and efficient first-order method can be used to perform this integration, and the required information includes the explicit form of the performance function, G, and the joint probability density function (PDF) of variables, $\mathbf{X}$.

For dynamic structural reliability, the problem is generally described as a structural system with parameters $\mathbf{X}_1$ under the action of time-varying loadings $\mathbf{S}(t, \mathbf{X}_2)$, where $\mathbf{S}$ is a vector random process of time, and the process is specified by a set of parameters $\mathbf{X}_2$. Let $\mathbf{X}$ denote all parameters in the structure and loadings, where $\mathbf{X}$ is a vector of quantities that are uncertain but time invariant. The performance function must include a vector of random response variables, $\mathbf{R}$, because $\mathbf{R}$ is dependent not only on $\mathbf{X}$ but also on the random process, $\mathbf{S}$. The probability of failure can be similarly formulated by

$$P_F = \int_{G(\mathbf{X},\mathbf{R})\le 0} f_{\mathbf{X},\mathbf{R}}(\mathbf{x},\mathbf{r})d\mathbf{x}d\mathbf{r} \tag{2}$$

For the case of barrier crossing at a constant level, η, of a single-degree-of-freedom oscillator,

Hohenbichler and Rackwitz (1981) formulated the limit-state function as

$$G(\mathbf{X}, S) = h - S(t, \mathbf{X}) \tag{3}$$

where the failure domain is defined by the region $G(\mathbf{X}, S) < 0$. S is a random process of time, which is included as one of the basic variables, together with $\mathbf{X}$. For a stationary Gaussian base acceleration with Tajimi–Kanai frequency spectrum, probability distribution of S can be obtained. The problem can be reduced to a time-invariant one with $n + 1$ uncertain basic parameters, which can be solved by the first-order reliability method. Here n is the number of system parameters, $\mathbf{X}$. The method developed by Hohenbichler and Rackwitz (1981) has been used by Quek et al. (1990) and Balendra et al. (1991) to solve dynamic reliability of a linear oscillator, considering uncertainties of structural and input model parameters in case of non-stationary excitation.

For a general structural system and limit state, similar to the case of barrier crossing at a constant level of a single-degree-of-freedom oscillator, Gueri and Rackwitz (1986) included $\mathbf{R}$ as basic variables, together with $\mathbf{X}$, and reduced the dynamic problem to a time-invariant one with $n + m$ basic variables; therefore, the first-order reliability method can be used, where m is the number of response variables. The required information includes the explicit form of the performance function, G; the probability distributions not only of system parameters, $\mathbf{X}$, but also of response variables, $\mathbf{R}$; and even the joint PDF, $f\mathbf{X}, \mathbf{R}(\mathbf{x}, \mathbf{r})$. The method is very complicated because of the number of response variables and the difficulty of determining the distribution of response variables of interest. For some limit states, it may not be possible to identify $\mathbf{R}$ and determine the performance function in the explicit form.

To simplify the problem, it is assumed that the performance function of the structure can be described by a function $h[\mathbf{X}, \mathbf{R}(t)]$, in which $\mathbf{X}$ denotes system parameters, and $\mathbf{R}(t)$ denotes structural responses, a vector random process. Madsen (1986) formulated the reliability problem as the limit state being reached if the minimum value of $h[\mathbf{X}, \mathbf{R}(t)]$ in the time period under consideration is less than zero; the probability of failure including the uncertainty in $\mathbf{X}$ is

$$P_F = \int_{\mathbf{X}} P\left\{\min h[\mathbf{X}, \mathbf{R}(t)] \le 0\right\} f_{\mathbf{X}}(\mathbf{x}) d\mathbf{x} \tag{4}$$

Introducing an auxiliary variable

$$X_{n+1} = min\ h[\mathbf{X}, \mathbf{R}(t)] \tag{5}$$

and express the performance function

$$\mathrm{G}(\mathbf{X}, \mathrm{X}_{n+1}) = \mathrm{X}_{n+1} \tag{6}$$

where $G < 0$ corresponds to failure, note X_{n+1} depends on $\mathbf{X}$, G is a function of $\mathbf{X}$ implicitly.

To determine the design point on the limit state surface using the first order method, the gradients of the performance function with respect to $\mathbf{u}$ which are the standard normal variables transformed from $\mathbf{X}$ by Rosenblatt transformation are needed.

$$\nabla G_{\mathbf{U}}(\mathbf{u}) = \left[J^{-1}\right]^T \nabla G_{\mathrm{X}}(\mathbf{x}) \tag{7}$$

where $[J]$ is the Jacobian matrix for transformation of variables.

When searching for the design point along the limit state surface, the terms in the Jacobian matrix are needed only at $X_{n+1} = 0$. Thus dynamic reliability problem is much simplified because only one auxiliary variable is introduced. Note however, the determination of the conditional distribution of X_{n+1} with given $\mathbf{X}$ and their derivatives may also not be straightforward, and the function η may not be easy to find especially when damage and collapses of the structures are of concern. Therefore, dynamic reliability problem expressed by Eq. (2) is generally difficult.

On the other hand, if reliability of the structural system for given parameter values of $\mathbf{X} = \mathbf{x}$ can be evaluated from state-of-the-art techniques, e. g., those based on random process and vibration methods, then one can first solve the dynamic problem with given parameters and then integrate over system parameters to find overall reliability formulated by

$$P_F = \int_{\mathbf{X}} P_f(\mathbf{x}) f(\mathbf{x}) d\mathbf{x} \tag{8}$$

where $P_f(\mathbf{x})$ is the conditional probability of failure for given $\mathbf{X} = \mathbf{x}$, which is evaluated from state-of-the-art techniques, and $f(\mathbf{x})$ is the joint PDF of $\mathbf{X}$.

The computation of Eq. (8) is generally excessively difficult because repeated solutions of the structural response under stochastic loadings are required, in particular when a large number of system parameters are considered. Alternatively, one can use Monte Carlo simulations; again, when the safety level is high, a large number of simulation trials are required to obtain results with high confidence. Moreover, the process becomes very expensive for problems of practical interest. To reduce the computational cost, one can also use approximate methods such as the second moment method, in which the overall probability of failure is obtained from the following formulation

$$P_F = P_f(\mu_x) + \frac{1}{2}\sum_i \sum_j \frac{\partial^2 P_f(\mathbf{x})}{\partial_{xi}\partial_{xj}} \rho_{ij}\sigma_{xi}\sigma_{xj} \tag{9}$$

The accuracy depends on variabilities of a vector of random variables **X** and smoothness of the probability of failure, P_f, with respect to **X**. Therefore, approximate methods with good accuracy and numerical efficiency are required.

3 PREVIOUS METHODS FOR DYNAMIC RELIABILITY

3.1 *Performance function for dynamic structural reliability*

Since performance function for solving Eq. (8) is not explicitly konwn, FORM can not be directly used to solve Eq. (8). Wen and Chen (1987) created a performance function directly in the transformed standard normal space:

$$G_U(\mathbf{U}, U_{n+1}) = U_{n+1} - \Phi^{-1}\left\{P_f[T^{-1}(\mathbf{u})]\right\} \tag{10}$$

where U_{n+1} is an auxiliary standard normal variable independent of **U**, $T^{-1}(\mathbf{u})$ are inverse Rosenblatt transformation. Neither the auxiliary variable X_{n+1} nor the Rosenblatt transformation from X_{n+1} to U_{n+1} is needed in equation (10), so the difficulties described above can be avoided.

Introduce an auxiliary variable X_{n+1} which can be taken arbitrary probability distribution but satisfy with

$$F_{X_{n+1}}(0 \mid \mathbf{x}) = P_f(\mathbf{x}) \tag{11}$$

then one can easily obtain

$$\begin{aligned} P_F &= \int_{\mathbf{X}} P_f(\mathbf{x}) f(\mathbf{x}) d\mathbf{x} \\ &= \int_{\mathbf{X}} \left[\int_{X_{n+1} \le 0} f_{X_{n+1}}(x_{n+1} \mid \mathbf{x}) dx_{n+1} \right] f(\mathbf{x}) d\mathbf{x} \\ &= \int_{X_{n+1} \le 0} \left[\int_{\mathbf{X}} f_{X_{n+1}}(x_{n+1} \mid \mathbf{x}) f(\mathbf{x}) d\mathbf{x} \right] dx_{n+1} \end{aligned} \tag{12}$$

Comparing equation (12) with equation (1), one can obtain

$$\mathrm{G}(\mathbf{X}, \mathrm{X}_{n+1}) = \mathrm{X}_{n+1} \tag{13}$$

This is the general performance function, note that it is different from equation (6) because X_{n+1} in equation (6) is defined by equation (5) but here X_{n+1} is defined by equation (11).

In order to obtain the gradients of the new performance function *G*, the Jacobian matrix corresponding to equations (8) and (9) is expressed as:

$$[J_{n+1}] = \left[\frac{\partial \mathbf{u}}{\partial \mathbf{x}}\right] = \begin{bmatrix} J_n & \{0\}_n \\ \left\{\dfrac{\partial u_{n+1}}{\partial x_i}\right\}^T_{i \le n} & \dfrac{\partial u_{n+1}}{\partial x_{n+1}} \end{bmatrix} \tag{14}$$

where

$$\left\{\frac{\partial x_{n+1}}{\partial u_i}\right\}_{i \le n} = -\left[J_n^{-1}\right]^T \left\{\frac{\partial u_{n+1}}{\partial x_i}\right\}_{i \le n} \frac{\partial x_{n+1}}{\partial u_{n+1}} \tag{15}$$

From equation (15) and equation (11) one can finally obtain the gradient of *G* at point on the failure surface with the aid of Rosenblatt transformation,

$$\left\{\frac{\partial x_{n+1}}{\partial u_i}\right\}_{i \le n} = -\left[J_n^{-1}\right]^T \left\{\frac{\partial pf(\mathbf{x})}{\partial x_i}\right\}_{i \le n} \tag{16}$$

$$\frac{\partial x_{n+1}}{\partial u_{n+1}} = \phi(u_{n+1}) \tag{17}$$

where

$$u_{n+1} = \Phi^{-1}\left[p_f(\mathbf{x})\right] \tag{18}$$

where Φ is the normal distribution function, ϕ is the normal distribution density function and $P_f(\mathbf{x})$ the conditional probability of failure for given $\mathbf{X} = \mathbf{x}$.

Based on equations (18), (19) and (20) the integration in equation (10) becomes quite easy to use the first order reliability method. Note it does not include the probability distribution of X_{n+1} and the explicit form of performance function *G* in the equations, and so that X_{n+1} can be a random variable with arbitrary probability distribution as long as it satisfies with equation (13) and the difficulties in identifying **R** and determination of their distribution functions and finding an explicit performance function *G* or *h* can be avoided.

3.2 *Equivalence of the first order formulations and the graphical interpretation of the method*

Since equation (1) and equation (10) are different expressions for the same problem, we have

$$\begin{aligned} P_F &= \int_{G(\mathbf{X},\mathbf{R}) \le 0} f_{\mathbf{X},\mathbf{R}}(\mathbf{x},\mathbf{r}) d\mathbf{x} d\mathbf{r} \\ &= \int_{\mathbf{X}} P_f(\mathbf{x}) f(\mathbf{x}) d\mathbf{x} \end{aligned} \tag{19}$$

From the basic conception of probability theory, one can obtain

$$P_f(\mathbf{x}) = \int_{G(\mathbf{R}|\mathbf{X})\le 0} f_{\mathbf{R}|\mathbf{X}}(\mathbf{r} \mid \mathbf{x}) d\mathbf{r} \tag{20}$$

Let $z = G(\mathbf{r}|\mathbf{x})$, note z is an expression of the actual performance function and it is a function of $\mathbf{X}$, one can obtain

$$F_Z(z=0) = P_f(\mathbf{x}) \tag{21}$$

Note that it is unnecessary to determine the explicit form of performance function and determine the probability distribution of X_{n+1}.

3.3 *Response surface approach*

The performance function expressed by equation (11) or (14), enables an evaluation of the dynamic structural reliability that includes parameter uncertainties can be performed using FORM. Calculation of the gradients of the performance function is an important step of the FORM. However, it is not always easy to obtain these gradients, (especially for the case where non-linearity of the structural performance is considered). Yao and Wen (1996) have introduced response surface approach (RSA) to avoid the sensitivity analysis required in FORM, where the response surface function is expressed as a polynomial of basic random variables in original space. For simplification, the performance function shown in equation (11) is approximated by the following second-order polynomial of standard normal random variables, in which the mixed terms are neglected.

$$G(U) = a_0 + u_{n+1} + \sum_{j=1}^{n} \gamma_j u_j + \sum_{j=1}^{n} \lambda_j u_j^2 \tag{22}$$

where a_0, γ_j, and λ_j are 2_{n+1} regression coefficients with j ranging from 1 to n. If the practical performance function $G(\mathbf{U})$ in equation (11) is fitted by $G(\mathrm{U})$ of equation (22) at the fitting points in the vicinity of the design point, the regression coefficients a_0, γ_j, and λ_j can be determined from the linear equations of a_0, γ_j, and λ_j obtained at each fitting point. For the obtained design point in standard normal space, fitting points along the coordinate axes are selected.

Because the design point is not generally known beforehand, iterative RSA procedure in the point-fitting SORM to approach the performance function (Zhao & Ono 1999) are generally used in the course of obtaining the design point. In the present paper, methods of moments will be used to obtain the probability of failure.

3.4 *Approximate distribution of the performance function*

If the first three or four moments of $G(\mathbf{X})$ expressed by Eq. 11 are obtained, the reliability analysis becomes a problem of approximating the distribution of a specific random variable with its known first three or four moments.

Approximating the distribution of a random variable using its moments of finite order is a well known problem in statistics, and various approximations such as the Pearson, Johnson and Burr systems, the Edgeworth and Cornish-Fisher expansions were developed (Stuart and Ord 1987). Their applications in structural reliability have been examined by Winterstein (1988), Grigoriu (1983), Hong (1996). In the present study, the fourth moment standardization function will be used. For the standardized performance function,

$$Z_s = \frac{Z - \mu_G}{\sigma_G} \tag{23}$$

The fourth moment standardization function is expressed as (Zhao & Lu 2007)

$$Z_s = S(U, \mathbf{M}) = -l_1 + k_1 U + l_1 U^2 + k_2 U^3 \tag{24}$$

where

$$l_1 = \frac{\alpha_{3G}}{6(1+6l_2)} \tag{25}$$

$$l_2 = \frac{1}{36}\left(\sqrt{6\alpha_{4G} - 8\alpha_{3G}^2 - 14} - 2\right) \tag{26}$$

$$k_1 = \frac{1-3l_2}{(1+l_1^2-l_2^2)} \tag{27}$$

$$k_2 = \frac{l_2}{(1+l_1^2+12l_2^2)} \tag{28}$$

Since

$$F(Z_s) = \Phi(U) = \Phi[S^{-1}(Z_s, \mathbf{M})] \tag{29}$$

The reliability index is expressed as

$$\beta_{4M} = D_0 p - \frac{1}{D_0} + l \tag{30}$$

where

$$D_0 = \sqrt[3]{2}\left(\sqrt{q_0^2 + 4p^3} - q_0\right)^{-1/3} \tag{31}$$

$$q_0 = l\left(2l^2 - k_1/k_2 - 3\right) + \beta_{2M}/k_2 \tag{32}$$

$$p = k_1/k_2/3 - l^2; l = l_1/k_2/3 \tag{33}$$

4 POINT ESTIMATE FOR DYNAMIC RELIABILITY

Rewrite Eq. (10) in standard u-space, the probability of failure considering parameter uncertainties is espressed as

$$P_F = \int_{\mathbf{u}} P_f[T^{-1}(\mathbf{u})]\phi(\mathbf{u})d\mathbf{u} \tag{34}$$

where

$T^{-1}(\mathbf{u})$ denotes inverse Rosenblatt transformation.

$\phi(\mathbf{u})$ denotes the PDF of standard normal variables.

Practically, the integral in Eq. (34) cannot be evaluated analytically because of the high dimensionality and the complicated integration. In order to avoid this problem, in the present paper, the point estimate method (Zhao & Ono 2000) is used to determine the moments of the performance function such as Eq. 11 for a series system. For a function of only one random variable $y = y(x)$, the moments of y can be point-estimated as

$$\mu_y = \sum_{k=1}^{m} P_k y\left[T^{-1}(u_k)\right] \tag{35}$$

where μy, iσ the mean value of $y(x)$, T^{-1} is the inverse Rosenblatt transformation. $u_1, u_2, ..., u_m$ are the estimating points and $P_1, P_2, ..., P_m$ are the corresponding weights.

The estimating points *ui* and their corresponding weights P_i can be readily obtained as (Zhao & Ono 2000),

$$u_r = \sqrt{2}x_r, P_r = \frac{w_r}{\sqrt{\pi}} \tag{36}$$

where x_i and w_i are the abscissas and weights for Hermite integration with the weight function $\exp(-x^2)$ that can be found in Abramowitz and Stegum (1972).

Specially, for a five point estimate in standard normal space (Zhao and Ono 2000),

$$u_0 = 0 \; P_0 = 8/15 \tag{37a}$$

$$u_1 + = -u_1 - = 1.3556262 \; P_1 = 0.2220759 \tag{37b}$$

$$u_2 + = -u_2 - = 2.85697 \; P_2 = 1.1257 \times 10^{-2} \tag{37c}$$

whereas for a seven point estimate in standard normal space,

$$u_0 = 0 \; P_0 = 16/35 \tag{38a}$$

$$u_1 + = -u_1 - = 1.1544054 \; P_1 = 0.2401233 \tag{38b}$$

$$u_2 + = -u_2 - = 2.366759 \; P_2 = 3.0757 \times 10^{-2} \tag{38c}$$

$$u_3 + = -u_3 - = 3.75044 \; P_3 = 5.4827 \times 10^{-4} \tag{38d}$$

Since $P_f(\mathbf{x})$ is a function of many variables where $\mathbf{x} = x_1, x_2, ..., x_n$, the joint probability density is generally assumed to be concentrated at points in the m^n hyperquadrants of the space defined by the n random variables, in which m is the number of estimating points used in the point estimates for functions of the respective single random variables. Then the moments of $Z = G(\mathbf{X})$ can be point-estimated as,

$$P_F = \sum \prod_{i=1}^{n} P_{Ci} P_f(T^{-1}(u_{c1}, u_{c1}, ..., u_{cn}) \tag{39}$$

where c is a distinct combination of n terms from a group [1, 2, ..., m], ci is the ith term of c. u_{ci} is the cith estimating point and P_{ci} is the weight corresponding to u_{ci}. n is the number of random variables and m is the number of estimating points, T^{-1} is the inverse Rosenblatt transformation.

Since all the distinct combinations have to be considered, m^n times of function calls for computing $P_f(\mathbf{x})$ are required. The computations involved in Eq. 8, therefore, can be massive when n is large. In order to avoid this problem, using the first order expansion of the function $P_f(\mathbf{x})$, PF can be approximated estimated as

$$P_F = \sum_{i=1}^{n} \mu_{fi} - (n-1)P_f(\mu) \tag{40a}$$

where μ_{fi} is the mean value of

$$P_{fi} = P_f[T^{-1}(\mathbf{U}_i)] \tag{40b}$$

$\boldsymbol{\mu}$ represents the vector in which all the random variables take their mean values, and $\mathbf{U}_i = [u_{\mu 1}, u_{\mu 2}, ..., u_{\mu i-1}, u_i, u_{\mu i+1}, ..., u_{\mu n}]T$, where $u\mu k$, $k = 1, ..., n$ except i, is the kth value of u_μ, which is the vector in u-space corresponding to $\boldsymbol{\mu}$.

Since *Pfi* is a function of only one standard normal random variable *ui*, its mean value can be point-estimated from Eq. 35. For a problem with n variables, if the probability moments of μ_{fi} is estimated using m-point estimate, only mn function calls of $P_f(\mathbf{x})$ are required for estimating the general probability of failure.

Further more, since $P_f(\mathbf{x})$ has strong non-linearity, in this study the conditional reliability index $\beta_f(\mathbf{x})$ will be used instead of $P_f(\mathbf{x})$. The reliability index with consideration of parameter uncertainties is written as

$$\beta = \int_{\mathbf{u}} \beta_f[T^{-1}(\mathbf{u})]\phi(\mathbf{u})d\mathbf{u} \tag{41}$$

5 NUMERICAL EXAMPLES

Consider a example of a linear single degree of freedom system under dynamic excitation. the excitation is modeled as Gaussian white noise, the intensity S, the duration D of the excitation and the natural frequency f, damping ratio ζ are uncertain and modeled as random variables as shown in Table 1. For a simple limit state of a given threshold level of the displacement being exceeded, the failure probability with deterministic system parameters is

$$P_f = 1 - \exp\left\{-fD\exp\left[-\frac{1}{2}\left(\frac{d}{\sigma_r}\right)^2\right]\right\}$$

where

$$\sigma_r = \sqrt{\frac{\pi S}{4(2\pi f)^3\zeta}}$$

With consideration of parameter uncertainties, the problem is expressed as

$$P_F = \int_{s,D,f,\zeta} P_f(s,D,f,\zeta)f(s,D,f,\zeta)dsdDdfd\zeta$$

The problem is solved by Monte-Carlo method, method of moment, and the fast integration described above. For threshold $d = 0.35$, considering only the uncertainties contained in duration D and damping ratio ζ, using Eq. (41), the reliability index obtained as $\beta = 2.372$.

Table 1. Probabilistic properties of uncertain parameters.

Parameter	Distribution	Mean	Uncertainty
s	Type II extreme value	0.25	0.60
D	Lognamal	10 sec	0.3
f	Normal	2 Hz	0.1
ζ	Lognormal	0.02	0.4

Using the MCS with 5,000,000 samples, the probability of failure for this performance function is obtained as 0.00933 with corresponding reliability index of $\beta = 2.352$. One can see that the probability of failure obtained using the proposed method is close to the result of MCS, the reliability analysis can be easily conducted without shortcomings associated with the design points, and do not require iteration or computation of derivatives.

The results of different threshold level are shown in Fig. 2 in which, the results of Monte-Carlo method is obtained by 100,000 sampling and the results of second moment is obtained from Eq. (11).

From Figure 1, it can be seen that the curve obtained by the method of this paper is quite near to the curve obtained by the Monte-Carlo method while that of the moment method is much different, so the method in this paper has a good accuracy. It can be also seen that the degree of the slope of the curve obtained with consideration of parameter uncertainties is much smaller than that with given parameters, that is to say the limit state in the reliability analysis with consideration of parameter uncertainties is not so dominant as in that with given parameters.

From Fig. 1, it can be also seen that for this example when the reliability index is high the limit state probability results with consideration of parameter uncertainties is larger than that with given parameters, on the other hand, when the reliability index is negative (in the case of dangerous structures or structures subjected to large intensity but low occurrence rate load), the results with consideration of parameter uncertainties is smaller than that with given parameters. Therefore the negligence of the parameter uncertainties overestimated the structural reliability for high safety structures and underestimated the structural reliability for low safety structures.

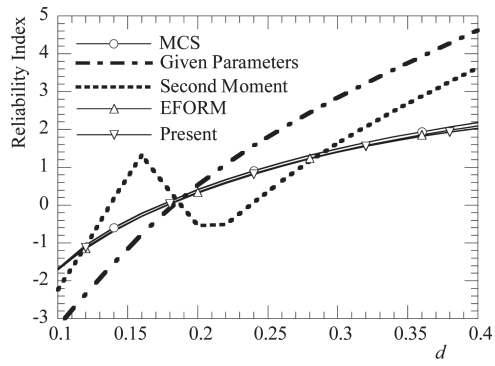


Figure 1. Reliability function.

6 CONCLUSIONS

1. A computationally effective method for dynamic structural reliability is proposed and examined. The method directly calculates the reliability indices (and associated failure probabilities) using point estimate. It does not need the iterative computation of derivatives, and does not require any design points. Thus, the proposed method should be more effective for the reliability evaluation of complex structures than currently available methods.
2. The accuracy of results, obtained with the proposed method has been examined by comparisons with large sample Monte Carlo simulations (MCS).
3. Neglecting effects of parameter uncertainties overestimates structural reliability of high-safety structures and underestimates that of low-safety structures.

ACKNOWLEDGEMENTS

This study is partially supported by the National Natural Science Foundation of China (Grant No. U1134209), PCSIRT-ITR1296, and JSPS KAKENHI Grant No. 24560699. The supports are gratefully acknowledged.

REFERENCES

Balendra, T., S.T. Quek and Y.P. Teo, Time-variant Reliability of Linear Oscillator Considering Uncertainties of Structural and Input Model Parameters, *Probabilistic Engineering Mechanics*, Vol. **6**, No.**1**, 1991.

Gueri, F. and Rackwitz, R., Outcrossing Formulation for Deteriorating Structural Systems, *Structural Congress, ASCE*, New Orleans, Louisiana, Sept., 1986.

Grigoriu, M., 1983. Approximate analysis of complex reliability problems. *Structural Safety*, *Vol*. 1, 277–288.

Hohenbichler, M. and Rackwitz, R., Non-normal Dependent Vectors in Structural Safety, *J. Engrg. Mech., ASCE*, **107(6)**, 1981, pp1227–1238.

Hong, H.P., 1996. Point-estimate moment-based reliability analysis. *Civil Engineering System*, *Vol*. 13, 281–294.

Madsen, H.O., Fast Integration for Time-variant Reliability, *A.S. Veritas Report*, 1986.

Madsen, H.O., and Moghtaderi-Zadeh, M., Reliability of Plates under Combined Loadings, *Proc. of Marine Structural Reliability Symp, Society of Naval Architects and Marine Engineers*, Arlington, Va., 185–191, 1987.

Madsen, H.O., and Lars Tvedt, Methods for Time-dependent Reliability and Sensitivity Analysis *J. Engrg. Mech., ASCE*, **116(10)**, 1990, pp2118–2135.

Quek, S.T., Y.P. Teo and T. Balendra, Non-stationary Structural Response with Evolutionary Spectra Using Seismological Input Model, *Earthquake Engineering and Structural Dynamics*, Vol. **19**, 1990, pp275–288.

Shinozuka, M. Basic Analysis of Structural Safety, *J. of Structural Division ASCE*, **109(3)**, 1983, pp721–740.

Stuart, A. and Ord, J.K., 1987. *Kendall's advanced theory of statistics*. London, Charles Griffin & Company LTD., *Vol*. 1, 210–275.

Wen Y.K. and H-C., Chen, On Fast Integration for Time Variant Structural Reliability, *Probabilistic Engineering Mechanics*, Vol. **2**, No.**3**, 1987.

Wen Y.K. and H-C., Chen, System Reliability under Time Varying Loads, part 1, *J. Engrg. Mech., ASCE*, **115(4)**, pp808–823, 1989.

Wen Y.K. and H-C., Chen, System Reliability under Time Varying Loads, part 2, *J. Engrg. Mech., ASCE*, **115(4)**, pp824–839, 1989.

Winterstein, S.R., 1988. Nonlinear vibration models for extremes and fatigue. *Journal of Eng. Mech*., *ASCE*, 114, 1772–1790.

Yao, H.J. and Y.K. Wen, 1996. Response surface method for time-variant reliability analysis, *J. Struct. Engng. ASCE*, 122(2), 193–201.

Zhao, Y.G. and Ono, T., 2000. New point-estimates for probability moments. *Journal of Engrg, Mech., ASCE,* 126(4), 433–436.

Zhao, Y.G. and Ono, T., 2001. Moment methods for structural reliability. *Structural Safety,* 23(1), 47–75.

Zhao, Y.G., Lu, Z.H., 2007. Fourth moment standardization for structural reliability assessment, *Journal of Structural Engineering, ASCE, Vol*. 133, *No*. 7, 916–924.

Zhao, Y.G., Ono, T. and Idota, H., Response uncertainty and time variant reliability analysis for Hysteretic MDF Structures, *Earthquake Engineering & Structural Dynamics, Vol*. 28, *No*. 10. 1187–1213, 1999.10.

Zhao Y.G. and Ono T., New approximations for SORM: Part 1, Journal of Engineering Mechanics, ASCE, Vol. 125, No. 1, 79–85, 1999.1.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

The reliability analysis of welded tanks for oil storage

Z. Kala
Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT: Large cylindrical steel storage tanks are very thin shell structures of shape and design layout, which ideally meet requirements. Standards EEMUA 159 and API 653 specify the minimum wall thickness of the sheet metal of cylindrical tanks. A storage tank is considered reliable if the wall thickness is higher than the minimum thickness listed in standards. This article aims to determine the failure probability of real crude oil tanks. The material and geometrical characteristics of the steel storage tank are considered as random quantities. The Latin hypercube sampling simulation method will be used for probability evaluation. Methods of standards EEMUA 159 and API 653 will be verified using probabilistic approaches.

1 INTRODUCTION

Oil reserves in the Czech Republic are considered for 90 days. The European Communities adopted legislation obliging member States to maintain oil reserves covering at least 90 days consumption after the oil crisis in the 1970s. The Czech Republic conformed to this law during negotiations on its entry into the European Union. Crude oil is brought into the Czech Republic via the Druzhba pipeline from Russia and the IKL pipeline form Bavarian Vohburg near Ingolstadt, where it is connected with the Transalpine pipeline from the region of the Caspian Sea, Middle East and North Africa.

Crude oil is stored in large cylindrical storage tanks, constructed not far from the village Nelahozeves. If the pipelines were to suddenly dry up, transportation in the Czech Republic could function without problem for another 90 days. Storage tanks are managed by the firm Mero, a.s., which took over management of the pipelines in 1994.

The largest tank has a height of 27 m and can hold 125 000 m^3 of crude oil, see Figure 1. The mentioned storage tank is the largest of its kind in the world. The tanks have floating roofs, which float directly over the crude oil surface to prevent evaporation. The floating roof is the size of a football field and covers crude oil worth 57 million Euros. The actual tank type in the central crude oil tank farm is a Czech invention and is considered the most advanced in the world. Safety is ensured by a double steel cover. A technical curiosity is the double bottom of the tank, where vacuum is created in the gap between the bottom 8 mm plate and top 6 mm riffled plate, which provides tightness of the bottom during operation. Inside the tank is a floating roof chamber, which moves together with the media level in the tank.

In case of damage to the inner shell oil is trapped by the outer shell. Thanks to the double casing tanks can be erected closer to each other leading to savings on space otherwise needed for containment dikes. The most likely place for fire to occur is between the roof and tank, which is fitted with a special rubber seal. Safety is ensured by a highly modern fire system. The tanks are located in a place where sand was once mined. The strategic location of the tanks near the Vltava River enables highly effective cooling of the tanks with water from the river in the event of fire.

Crude oil is a strategically important raw material and therefore it is necessary to pay increased attention to its transportation and storage. The dominant load case of cylindrical tanks is loading of the inner shell by hydrostatic pressure of the oil. The article is aimed at the analysis of failure probability of the inner shell with regard to random geometric and material imperfections. The article



Figure 1. Welded tank for oil storage.

builds on the probabilistic reliability studies, see e.g. (Kala 2007, Kala 2012, Gottvald et al. 2012).

2 REJECTION LIMITS FOR SHELL PLATES

The principal factor, which determines the thickness of the tank shell, is the internal loadings due to the liquid head. The minimum acceptable thickness for welded tank shells may be calculated from the following formula used in BS2654 and in EEMUA 159 for the basic design of tank shells:

$$t_{min} = \frac{D}{20 \cdot S \cdot E}\left(98 \cdot W \cdot \left(H - 0.3\right) + P\right) \tag{1}$$

where:
t_{min} is the minimum acceptable thickness in mm from the above formula (1), but should not be less that 2.5 mm or 50% of the original shell plate thickness, whichever is greater
D is the nominal diameter [m]
H height from the point under consideration to the maximum filling height [m], see Figure 2
W specific gravity of the content
P design vapour pressure in mbar
S maximum allowable stress in MPa
E original joint efficiency for the tank
$E = 0.85$ if original E is unknown
$E = 1.0$ when evaluating the retirement thickness in a corroded plate, when away from welds or joints by at least the greater of 25 mm or twice the plate thickness.

A similar formula is also listed in standard API 653.

It is apparent from Figure 2 that the pressure varies with the liquid head and thus the shell thickness varies from almost zero at the top, to the maximum at the bottom. It is impractical to have a shell with tapering thickness so it is constructed from a number of plate shell courses (the term "course" is used in the standards EEMUA and API) each of uniform thickness. However, each successive shell course is thinner than the one below. The top courses are governed by Codes, which list the minimum recommended thickness. The consequence of using courses with diminishing thickness is that, at the joint between two adjacent courses, the lower, thicker course provides some stiffening to the top, thinner course leading to an increase in stress in the upper part of the lower course and a reduction in stress in the lower part of the upper course. The codes empirically assume that reduction in stress in the upper course reaches a maximum value 0.3 m (one foot) above the joint. The effective acting head is measured at this point on each course. This calculation method is referred to as the "one foot" method (Long 2004).

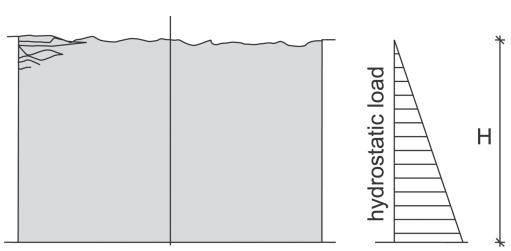


Figure 2. Hydrostatic loading of the tank shell.

3 RELIABILITY CONDITION

Formula (1) is based on the static analysis of the shell of a cylindrical tank with constant wall thickness. Let us consider a thin-walled circular cylindrical tank of height H, internal radius r (distance from the vertical axis of symmetry to the wall surface) and wall thickness t, see Figure 3.

Hydrostatic pressure p [Nm^{-2}] at height h is evaluated as:

$$p = \rho \cdot g \cdot h \tag{2}$$

where ρ is the oil density at temperature 20°, which at present is within the interval of approximately 790–880 kgm^{-3} (worldwide values are 730–1000 kgm^{-3}), g is gravitational acceleration, which is approximately $g = 9.81$ ms^{-2} for our latitude (49°). Perpendicular to the surface of the tank at depth h acts uniform load f:

$$f = \rho \cdot g \cdot h \cdot dh \tag{3}$$

where f has the unit Nm^{-1}. At depth h uniform load f induces normal stress σ perpendicular to the plane passing through axis x.

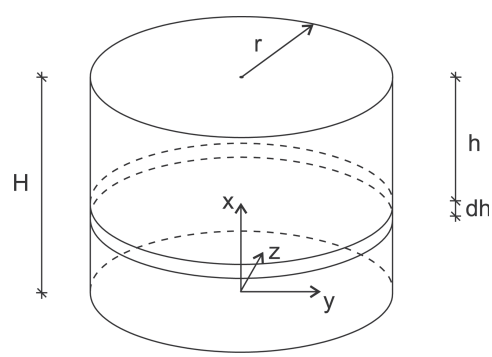


Figure 3. Scheme of circular cylindrical tank.

Normal stress on the surface $dh \cdot t$ is induced by force F, which can be calculated as the reaction of a planar semi-circular arc (half hoop), see Figure 4. The computational model of the planar arc in Figure 4 is based on the assumption that the loaded tank for $x > h$ and $x < h$ does not affect the loading of the tank for $x = h$.

Force dS, which can be decomposed into the horizontal dS_H and vertical dS_V components, acts on arc length $ds = r \cdot d\alpha$. With consideration to symmetry reaction F [N] can be evaluated as:

$$F = \int_0^{\frac{\pi}{2}} dS_V = \int_0^{\frac{\pi}{2}} dS \cdot \sin(a) = \int_0^{\frac{\pi}{2}} f \cdot r \cdot \sin(\alpha) d\alpha$$
$$= \rho \cdot g \cdot h \cdot dh \cdot r \int_0^{\frac{\pi}{2}} \sin(\alpha) d\alpha = \rho \cdot g \cdot h \cdot r \cdot dh \qquad (4)$$

The value of reaction H_y is zero. This can be evaluated, for e.g., using the finite element method. The arc shown in Figure 4 is not stressed by bending moment. Force F evokes normal stress in the direction of the tangent to the centre line of the shell plate of thickness t and height dh, where the centre line has the shape of a circle lying in the plane perpendicular to the axis x. For reliable operation force F must be less than or equal to the plate resistance R:

$$G = R - F \geq 0 \qquad (5)$$

Resistance R can be calculated as:

$$R = f_y \cdot t \cdot dh \qquad (6)$$

where f_y is the yield strength. The reliability condition (5) can be rewritten with consideration to (4) and (6) as:

$$G = f_y \cdot t - \rho \cdot g \cdot h \cdot r \geq 0 \qquad (7)$$

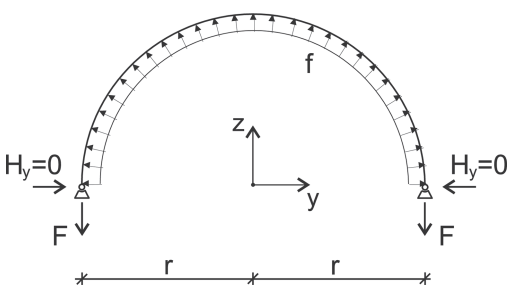


Figure 4. Loading of circular arc at depth h.

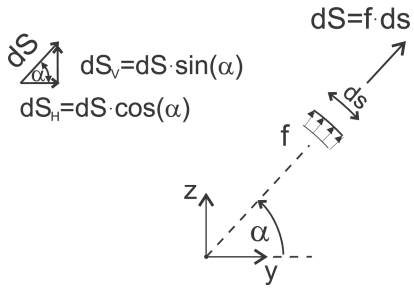


Figure 5. Force decomposition.

Inequality (7) is the basic equation for the assessment of design reliability or service reliability of circular cylindrical tanks of a series of standards, for e.g. EEMUA 159 or API 653, see, for e.g. the comparison of (7) and (1). Standardized approaches ensure reliability primarily by considering conservative (safely low) values of yield strength.

4 FAILURE PROBABILITY

The condition of reliability (7) must be fulfilled for reliable operation of the tank. A possible approach for the assessment of reliability of steel structures is using probabilistic methods based on Monte Carlo simulation methods, see, for e.g. (Kala 2007).

Variables in equation (7) are considered as random during probabilistic reliability assessment. Failure occurs if inequality (7) is not satisfied. Failure probability is evaluated as:

$$P_f = P(G < 0) \qquad (8)$$

Operation of the tank may be considered safe if the probability of failure P_f is sufficiently small.

Let us consider the tank depicted in Figure 1 with a capacity of 125,000 m^3 of crude oil. The tank has the following parameters:

- Tank radius is 42.235 m, fill height is 22.3 m, tank height is 24.0 m.
- Nominal height of shell courses from bottom to top: 2.2 m, 2.4 m, 2.4 m, 2.8 m, 2.8 m, 2.85 m, 2.85 m, 2.85 m, 2.85 m.
- Nominal thickness of shell courses from bottom to top: 39 mm, 35 mm, 30 mm, 26 mm, 22 mm, 17 mm, 12 mm, 11 mm, 10 mm.
- Steel of grade S355 is used apart for the last two top shell courses, which are from steel S235.

The reliability of all shell courses can be evaluated using the reliability index according to Cornell

(Cornell 1969), which is defined as the reciprocal of the variation coefficient of the reliability reserve and is determined under the assumption of normality of the distribution of quantity G according to the relation:

$$\beta = \frac{m_G}{S_G} \tag{9}$$

where m_G is the mean value and S_G is the standard deviation of random variable G. The reliability index according to Cornell is sometimes considered to be more illustrative than P_f, and is introduced due to uncomfortable handling of small values of failure probability.

The tank during operation is exposed to environmental effects, which cause weakening of the thickness of the tank plates. Plate thicknesses are continuously measured by the tank operators. The most common cause of reduction in the thickness of plates is corrosion. The basic criteria for the assessment of service reliability of tanks are provided by standards EEMUA 159 and API 653. The standards list the calculation of the minimum plate thickness, which has to be maintained for reliable operation.

An alternate approach to the assessment of reliability is the analysis of the failure probability. The effect of changes in the thickness of tank plates on the safety and reliability of the tank can be studied using the reliability index β (9).

Let us examine the effect of changes in nominal plate thickness t of the bottom shell course on β. Depth h = 22.3–0.3 = 22 m (depth 0.3 m from bottom) was considered in (7). The spacing 0.3 m is considered because the reliability condition (7) near the edge of the shell course (during change in plate thickness) is imprecise. The spacing value of 0.3 m is considered according to standard EEMUA 159 and API 653. Input random variables for the probabilistic analysis are clearly listed in Table 1.

All input random quantities in Table 1 have Gauss probability density functions. The mean value and standard deviation of yield strength were considered according to results of experimental research (Melcher et al. 2004, Strauss et al. 2006, Kala et al. 2009). It may be noted that experimental research provides important input data for a number of probabilistic reliability studies, see. e.g. (Frydrýšek et al. 2013, Kala 2008, 2010, 2013, Krejsa 2014).

Table 1. Input random quantities.

No.	Quantity	Symbol	Mean value	Std. deviation
1.	Oil density	ρ	880 kgm^{-3}	8.8 kgm^{-3}
2.	Yield strength	f_y	393.5 MPa	25.4 MPa
3.	Thickness	t	t	$0.04 \cdot t$

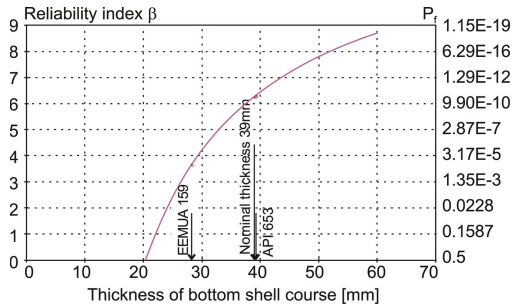


Figure 6. Reliability index β vs t.

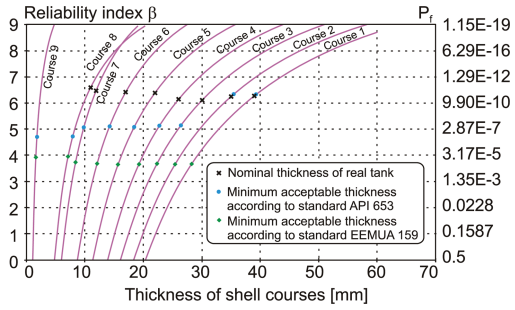


Figure 7. Reliability index β vs thickness t.

Coefficient β (9) was evaluated using the Latin Hypercube Sampling method (McKey et al. 1979) for 100 simulation runs. The dependence of β on t is shown in Figure 6. For clarity the Gauss probability density function and scale P_f, which is evaluated from β, is shown on the right side of the figure.

The procedure was similar for the reliability analysis of other shell courses, see Figure 7. A point 0.3 m from the bottom edge of the corresponding shell course was always considered for each evaluation. The reason for the spacing of 0.3 m is the same as for the calculation of β for the bottom of the shell course. Equation (7) cannot be reliably used to indicate failure in the vicinity of the step change of the plate thickness. Yield strength was considered according to Table 1 for all shell courses apart from the last two shell courses, which are of steel grade S235. Steel grade S235 has a mean value of 284.5 MPa and standard deviation 21.5 MPa.

5 CONCLUSION

It is apparent from Figure 7 that the dependence of β on the thickness of plate courses *t* is non-linear. Reliability index β for nominal thickness of the real tank (cross) is approximately constant with the exception of the top shell course 9, which has a very high reliability $\beta \approx 10.4$. The reliability indices β for the first two shell courses evaluated according to API 653 (blue dots) are $\beta \approx 6.3$, see Figure 7. The minimum acceptable thickness evaluated for the first two bottom shell courses according to standard API 653 (blue dots) is higher than the nominal value of plate thickness of the assessed tank. Strictly speaking, the tank does not comply with the requirements of standard API 653, however, the difference is so small that the tank can be practically considered reliable (blue dot practically overlaps the cross).

Reliability indices β evaluated for standard EEMUA 159 (green squares) are lower than the reliability indices evaluated for standard API 653 in all cases, see Figure 7. At the same time the minimum acceptable thickness evaluated for standard EEMUA 159 (green squares) are lower than the minimum acceptable thickness evaluated for standard API 653. This means that the rejection limits of standard API 653 are safer (more conservative) than the rejection limits of standard EEMUA 159.

Minimum acceptable thickness evaluated according to standard EEMUA 159 are approximately constant, on the contrary standard API 653 prescribes higher reliability for the first two shell courses. If we consider that the greater the depth the more oil could leak during accident, then it is appropriate to have higher reliability for greater depth, thus the approach of standard API 653 can be approved.

It is interesting that the curves of shell course 1 to 7 in Figure 7 are similar in shape (graphically). For example the curve of the second shell course is obtained graphically by shifting the curve of the first shell course to the left and also decreasing the scale of the horizontal size of the rectangular border of the curve. This graphical similarity suggests even more general mathematical dependence. Similarly, the curves of shell courses 8 and 9 from steel S235 are similar in shape.

It should be noted that reliability is affected by many other parameters including soil (Amšiejus et al. 2014, Kelevišius et al. 2014, Martinkus et al. 2014). Tanks are regularly checked and discovered defects are analysed so that obtained data serves as basis for the implementation of the methodology of Risk Based Inspection (Shuai et al. 2012). The results are then used to assess the state of the tank and plan inspections.

The article was elaborated within the framework of projects of GAČR14-17997S and TAČR TA01020307.

REFERENCES

Amšiejus, J. & Dirgėlienėn, N. & Norkus, A. & Skuodis, Š. 2014. Comparison of sandy soil shear strength parameters obtained by various construction direct shear apparatuses. *Archives of Civil and Mechanical Engineering* 14(2): 327–334.

API 653 American Petroleum Institute. 2009. Tank inspection, repair, alteration, and reconstruction. Washington, D.C.: API Publishing Services.

BS 2654:1989 Specification for manufacture of vertical steel welded non-refrigerated storage tanks with butt-welded shells for the petroleum industry.

Cornell, C.A. 1969. *A normative second-moment reliability theory for structural design*, Solid Mechanics Division, University of Waterloo, Waterloo, Ontario, Canada.

EEMUA Users guide to the inspection, maintenance and repair of aboveground vertical cylindrical steel storage tanks. Publication number 159; 2003.

Frydrýšek, K. & Jančo, R. & Gondek, H. 2013. Solutions of beams, frames and 3D structures on elastic foundation using FEM. *International Journal of Mechanics* 7(4): 362–369.

Gottvald, J. & Kala, Z. 2012. Sensitivity analysis of tangential digging forces of the bucket wheel excavator SchRs 1320 for different terraces. *Journal of Civil Engineering and Management* 18(5): 609–620. doi: 10.3846/13923730.2012.719836.

Kala, Z. 2007. Influence of partial safety factors on design reliability of steel structures—Probability and fuzzy probability assessments. *Journal of Civil Engineering and Management* 13(4): 291–296.

Kala, Z. 2007. Stability problems of steel structures in the presence of stochastic and fuzzy uncertainty. *Thin-Walled Structures* 45(10–11): 861–865. doi:10.1016/j.tws.2007.08.007.

Kala, Z. 2008. Sensitivity analysis of carrying capacity of steel plane frames to imperfections. *AIP Conference Proceedings* 1048: pp. 298–301. doi:10.1063/1.2990917.

Kala, Z. & Melcher, J. & Puklický, L. 2009. Material and geometrical characteristics of structural steels based on statistical analysis of metallurgical products. *Journal of Civil Engineering and Management* 15(3): 299–307. doi:10.3846/1392-3730.2009.15.299-307.

Kala, Z. 2010. Sensitivity analysis in advanced building industry. *Procedia—Social and Behavioral Sciences* 2(6): 7682–7683. doi:10.1016/j.sbspro.2010.05.177.

Kala, Z. 2012. Geometrically non-linear finite element reliability analysis of steel plane frames with initial imperfections. *Journal of Civil Engineering and Management* 18(1): 81–90. doi:10.3846/13923730.2012.655306.

Kala, Z. 2013. Elastic lateral-torsional buckling of simply supported hot-rolled steel I-beams with random imperfections. *Procedia Engineering* 57: 504–514. doi:10.1016/j.proeng.2013.04.065.

Kelevišius, K. & Gabrielaitis, L. & Amšiejus, J. & Norkus A. & Sikora, Z. 2014. Study of bearing capacity of vibratory pile applying acceleration record. *Journal of Civil Engineering and Management* 20(1): 142–148. doi:10.3846/13923730.2013.870089.

Krejsa, M. 2014. Probabilistic failure analysis of steel structures exposed to fatigue. *Key Engineering Materials* 577–578: 101–104. doi:10.4028/www.scientific.net/KEM.577–578.101.

Long, B. & Garner, B. 2004. *Guide to storage tanks and equipment*. Wiley, 588 p. ISBN 1860584314.

Martinkus, V. & Norkus, A. & Statkus, T. & Žilionienė, D. 2014. Experimental investigation of stresses in sand during the installation. *The Baltic Journal of Road and Bridge Engineering* 9(1): 10–16. doi:10.3846/bjrbe.2014.02.

McKey, M.D. & Beckman, R.J. & Conover, W.J. 1979. A comparison of the three methods of selecting values of input variables in the analysis of output from a computer code. *Technometrics* 21(2): 239–245.

Melcher, J. & Kala, Z. & Holický, M. & Fajkus, M. & Rozlívka, L. 2004. Design characteristics of structural steels based on statistical analysis of metallurgical products. *Journal of Constructional Steel Research* 60(3–5): 795–808. doi:10.1016/S0143-974X(03)00144-5.

Shuai, J. & Han, K. & Xu, X. 2012. Risk-based inspection for large-scale crude oil tanks. *Journal of Loss Prevention in the Process Industries* 25: 166–175. doi:10.1016/j.jlp.2011.08.004.

Strauss, A. & Kala, Z. & Bergmeister, K. & Hoffmann, S. & Novák, D. 2006. Technologische Eigenschaften von Stählen im europäischen Vergleich. *Stahlbau* 75(1): 55–60. doi:10.1002/stab.200610007.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Determination of design load for a pile-guide system for large floating installations considering Life-Cycle Cost and probabilistic load distribution

Seong-Yeob Lee, Choonghee Jo, Pål Bergan & Daejun Chang
Korea Advanced Institute of Science and Technology (KAIST), Daejoen, Republic of Korea

Bjørnar Pettersen
Norges Teknisk Naturvitenskapelige Universitet (NTNU), Trondheim, Norway

ABSTRACT: Life Cycle Cost Analysis (LCCA) was performed to determine the design load of a pile-guide system that was intended to maintain the position of large-scale floating installations. The positioning system consisted of guide piles supporting the floating installation, a subsea truss structure cross-linking the piles, and a seabed platform fixed to the seabed. For the LCCA, Capital Expenditure (CAPEX), Operating Expenditure (OPEX) and Risk Expenditure (RISKEX) were considered. Environmental loads such as wave, current, and wind loads applied to the positioning system were taken into account. Probability models were used to consider the frequency of external loads in the target area. As a result, the design load of the installation were determined to give the minimum Life Cycle Cost (LCC).

1 INTRODUCTION

This study was performed to determine the design load for offshore large-scale floating installations. To determine the design load of an offshore structure, LCCA and probability models were employed.

Many studies in extreme environmental conditions such as gust wind speed and significant wave height were carried out. Estimation of the extreme wind speeds, using a national wind map with Gumbel & Weibull distribution, for the structural stability of a wind power plant station hub was conducted by B.H. Lee et al. (2010). H.S. Jung (2012) performed stochastic estimation of wind speed when affected by a typhoon for three different sites (Ulsan, Yeonggwng, and Geoge) in which long span bridges were located. Studying the wave itself, S.H. Kwon et al. (1991) used a statistical estimation-methodology of an extreme sea level using Weibull distribution function (Type III). T.I. Lee et al. (1992) developed computational methods based on the Weibull distribution for estimation of extreme sea level. H.J. Ryu & D.Y. Kim (2004) studied the statistical properties of extreme waves in Hong-do, an island in Korea, during typhoons. A study on the projection of future wave climate changes was conducted by J.S. Park et al. (2013). Thus, the extreme environmental conditions that correspond to the return period could be estimated by extreme distribution functions such as Gumbel-distribution (Type I), Frechet-distribution (Type II), and Weibull-distribution (Type III). However, in these studies, a method for making practical use of the extreme environmental conditions estimated for a structure design was not considered.

For the design of an offshore structure, the codes and specifications have been used in prescriptive ways because alternative methods for a newly developed structure have not been considered thus far. The environmental load, occurring once in 100 years, has been generally used for structure design, based on rule-based design. According to International Organization for Standardization (ISO 19902) (2007) and the fixed offshore structure rules of the Korea Register (KR) (2012), a 100 year return period should be taken into account for an offshore structure design. The maximum wave height, wind speed, and current, corresponding to the return period, should be considered. Using a 100 year or more return period for a structure design was quite vague and the design load could be changed depending on the types of structures and installation locations. In other areas such as bridge designs on onshore, many studies on new design methodologies such as using LCCA have been carried out by Sang-Hyo Kim et al. (2013). However, these studies have not included offshore installations.

In this study, a methodology for determining design load was taken into consideration in terms

of an offshore structure newly developed. The Pile Guide System (PGS), an offshore mega-floater, was considered for the case study and Busan New Port in the Republic of Korea was selected as the target site. Gumbel distribution function was employed to estimate the extreme environmental conditions at the target site. ANSYS AWQA, a commercial code for offshore structures, was used to calculate extreme environmental loads, considering wave, wind, and current loads applied to the floater only. Nine return periods (30, 50, 100, 300, 500, 1 000, 3 000, 5 000 and 10 000 years) of extreme environmental loads were considered for the structure design. The PGS structures were designed to withstand each design load case. For the LCCA, CAPEX, which was the initial investment costs which include material cost, fabrication cost, and installation cost, was estimated based on the material costs of the structures. RISKEX, which included the costs of failed components, the rental fee of an offshore crane vessel, and production loss during repair-time, was also taken into account according to the safety philosophy of the PGS.

2 METHODOLOGY: DETERMINATION OF DESIGN LOAD

Unlike the design of a process system, so far rule-based design has been considered to make offshore structures. Most offshore structures have been designed with a load coming once every 100 years (ISO 19902. 2007). However, these offshore structures have occasionally failed due to strong environmental loads which were not taken into account at the early design stage. Sometimes, these accidents have led to considerable production loss. When the strength of the offshore structures was increased to prevent damage in accidents and production loss, CAPEX also increased. Thus, in this study, the most cost-effective design load was found using LCCA and compared with the load occurring once every 100 years. The design procedure for LCCA is shown in Figure 1.

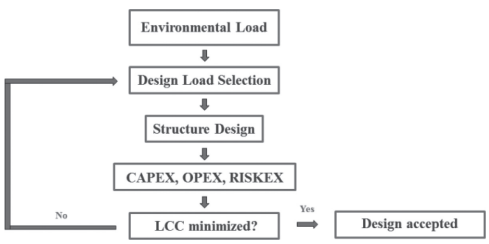


Figure 1. Design procedure for the LCCA.

Step 1: Estimation of external loads applied to mega-scale floaters

- Investigation of environmental conditions for the target site (Busan New Port)
- Estimation of environmental loads with the commercial codes (ANSYS-AQWA)

Step 2: Design Load Selection

- Considering extreme environmental conditions at the target site, using the Gumbel distribution (Type I), an extreme probabilistic model
- Nine return periods taken into consideration for the structure design: 30, 50, 100, 300, 500, 1 000, 3 000, 5 000 and 10 000 years
- Estimation of T-year return values for Significant Wave Height (SWH), wind, and current applied to the floater and selection of a design load for the structure design.

Step 3: Structure design

- Determination of initial dimension for the supporting structures including guide piles and truss structures
- Considering the weight optimization for reducing material costs of the PGS with two commercial codes (ABAQUS, PIANO).

Step 4: Estimation of LCC (including CAPEX and RISKEX)

- Calculation of CAPEX based on material costs of the PGS
- Estimation of RISKEX which included costs of failed components, rental fee of an offshore crane vessel, and production loss during repair-time was also taken into account for LCCA, using the safety philosophy of the PGS.

Step 5: Iteration for minimized LCC

- Repetition of this design procedure and LCC estimation to find minimized LCC and optimized design load.

3 CASE STUDY: PGS IN BUSAN NEW PORT

3.1 *Backgrounds of case study*

Because oceans have continued to provide sites for energy development and utilization, mega-scale floaters have been playing a critical role in energy sectors. Without doubt, their role will continue to increase in the future. Thus, many technologies have been developed to maintain the position of offshore installation. In this case study, PGS, a position keeping solution for mega-scale floaters, was taken into consideration.

3.1.1 *Pile Guide System*

The PGS, shown in Figure 2 is a type of supporting structure for offshore installations such as jacket structures and gravity based structures. Multiple piles are mounted and connected with a seabed base platform, which is fixed to the seabed rock layer with fixing piles. Connection parts between the floater and the guide pile are specially designed to allow the floating giant vessel to have vertical motions only in accordance with the water level. Seabed truss structures are able to prevent the guide piles moving horizontally due to environmental loads applied to the floater.

3.1.2 *Busan New Port (target port)*

Busan New Port in the Republic of Korea is selected as the target site for this case study. Busan Port Authority (BPA) has a plan to make Busan New Port an international logistics center port of Northeast Asia. In accordance with the technical report (J.W. Lee et al. 2009), many offshore installations will be taken into consideration for the shipping infrastructure near the Busan New Port.

3.2 *Step 1: Estimation of external loads applied to mega-scale floaters*

To estimate extreme weather conditions such as wind, Significant Wave Height (SWH) and current, as well as 3 extreme distribution functions (Type I Gumbel distribution function, Type II Frechet distribution function, and Type III Weibull distribution function) are generally employed. Of these extreme distribution functions, Gumbel distribution is used at this step because it can model maximum wind velocity and significant wave height and gives conservative values compared with other distribution functions.

3.2.1 *Maximum wind speed*

Eq. 1 is the cumulative Gumbel distribution function. Scale parameter, a, and location parameter, b, are characteristic values of Gumbel distribution function. They can be calculated by the mean value (23.0955 m/s) and standard deviation (3.3985 m/s) of the maximum instantaneous wind speed, extracted from the numerical weather data for 50 years at the target site. (Lee, B.H. et al. 2010)

$$F(V) = \exp[-\exp^{-Y}],\ Y = a(V-b)$$
$$a = \frac{1}{0.78\sigma}, \qquad b = \mu - 0.45\sigma \tag{1}$$

If it is assumed that the maximum instantaneous wind speed follows the Gumbel distribution, the relation between return period (T) and the cumulative distribution function can be expressed by Eq. 2. Using Eq. 1 and Eq. 2, Eq. 3 is induced to calculate extreme environmental conditions at the target site. (Lee, B.H. et al. 2010)

$$F(V) = 1 - \frac{1}{T} \tag{2}$$

$$V(T) = -\frac{1}{\alpha}\ln\left[\ln\left(\frac{T}{T-1}\right)\right] + b \tag{3}$$

3.2.2 *SWH (Significant Wave Height)*

In terms of the wave, accumulation data are insufficient because a buoy, which is able to measure wave height, has recently been installed near Busan New Port. Change in wind speed can affect the SWH because wind speed and SWH have a strong correlation. Thus, the interaction formula between fully developed SWH and wind speed is expressed as Eq. 4 (J.S. Park et al. 2013).

$$SWH = 0.0246 \times (wind\ velocity)^2 \tag{4}$$

3.2.3 *Current*

Current is divided into two types: wind current and tide current. In terms of current affected by wind, 1% of wind velocity was assumed (K.S. Choi 2013). Thus, the velocity of wind current is not significant at approximately 0.5 m/s. The wind current is at a maximum at sea level and decreases linearly to the seabed. On the target site, Busan New Port, the tide current is more considerable than the wind current. According to records at the buoy near the target site, the maximum velocity of the tide current is 1.869 m/s.

The extreme environmental conditions (wind, current, and SWH) at Busan New Port are shown in Table 1.

3.3 *Step 2: Design load selection*

Extreme environmental loads applied to the PGS are estimated using a commercial code, ANSYS AQWA. In this paper, the detail procedure of

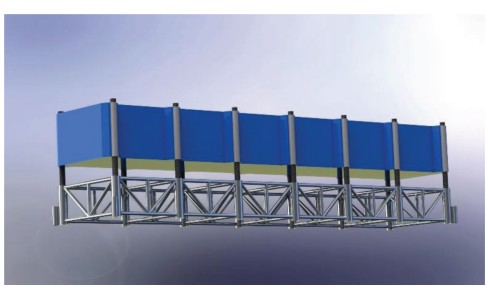


Figure 2. Three-dimensional drawing of pile guide system.

Table 1. Extreme environmental conditions at the target site.

Return period (years)	Wind (m/s)	Current (m/s)	SWH (m)
30	30.5	1.869	2.03
50	31.9	1.869	2.30
100	33.8	1.869	2.70
300	36.7	1.869	3.39
500	38.0	1.869	3.74
1 000	39.9	1.869	4.24
3 000	42.8	1.869	5.09
5 000	44.1	1.869	5.52
10 000	46.0	1.869	6.12

AQWA is ignored. The calculated external loads, occurring once in 30, 50, 100, 300, 500, 1 000, 3 000, 5 000 and 10 000 years, are shown in Table 2. This study are considered the environmental loads applied to the floater, not including seabed truss structures. As a future study, the current load applied to the seabed structures should be taken into account for the structure design.

3.4 *Step 3: Structure design*

At the structure design step, the dimensions of guide piles and seabed truss structures are determined to withstand the selected design load. Commercial codes, ABAQUS and PIANO, are used to conduct optimization, of which the objective function is to reduce the total weight of the PGS structures. Through sensitivity analysis, some design variables are selected. The ABAQUS model for the structure design is shown in Figure 3 and the dimensions of guide piles and truss structures against each design load are shown in Table 3.

3.5 *Step 4: Estimation of LCC (Life Cycle Cost including CAPEX & RISKEX)*

LCCA is performed to determine the design load of the PGS structure. CAPEX and RISKEX are taken into consideration for LCCA. OPEX can be negligible compared with CAPEX and RISKEX because it only included regular maintenance costs in terms of a structural design (D.J. Chang & G.P. Chang 2013). Some assumptions are needed to conduct the LCCA because it is difficult to exactly determine the extent of structure damage.

The CAPEX is the initial investment costs which include material cost, fabrication cost, and installation cost. ASTM A135 steel is employed for piles and truss structures. Price of ASTM A135 is approximately 780 $/ton. Using the dimensions of piles and truss structures, material costs could be calculated. To estimate the CAPEX of the whole structures, it was assumed that the material costs are 38.8% of the CAPEX.

This study assumed that the PGS structure can be used for a LNG bunkering terminal in the near future. The RISKEX consists of replacement costs of 4–6 guide piles, rental fee of offshore crane vessels, and suspension of LNG sales during the repairing time. LNG price is approximately 10 $/MMBTU which is corresponding to

Table 2. Extreme loads applied to the PGS.

Return period (years)	Force/moment				
	X (ton)	Y (ton)	RX (ton·m)	RY (ton·m)	RZ (ton·m)
30	1 590	7 494	163 041	785 613	330 477
50	1 711	7 906	184 578	909 588	375 409
100	2 058	9 135	209 314	1 098 637	434 992
300	2 631	11 479	262 430	1 314 243	554 268
500	2 899	12 454	292 776	1 448 464	611 601
1 000	3 206	15 162	346 916	1 725 239	685 517
3 000	3 955	18 925	426 936	1 974 549	835 338
5 000	4 291	20 864	466 981	2 139 240	905 159
10 000	4 768	23 688	524 545	2 492 259	1 005 146

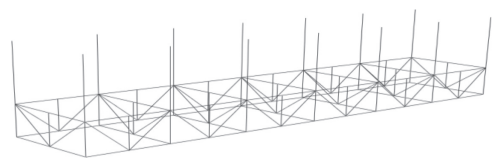


Figure 3. ABAQUS model for the truss structure design.

Table 3. Dimension of guide pile & truss against each design load.

Return period (years)	Diameter		
	Guide pile (m)	Truss X (m)	Truss Y (m)
30	2 535	1 444	1 698
50	2 599	1 480	1 741
100	2 805	1 597	1 879
300	3 132	1 784	2 098
500	3 324	1 893	2 227
1 000	3 598	2 049	2 411
3 000	4 065	2 315	2 724
5 000	4 295	2 446	2 878
10 000	4 626	2 635	3 099

234 $/$m^3$. The following assumptions are considered for the RISKEX:

- Intentionally failed components, guide piles, of which it is easy to conduct maintenance and replacement, are considered. 4–6 guide piles failed only when the loads exceeded the design load due to the yaw motions of the floater.
- Rental fee of an offshore crane vessel for replacement of the guide-piles failed: 100 000 $/day
- Lifespan of the PGS structure: 50 years
- Suspension of LNG sales (Production loss): 10% of the amount of LNG sold per day (LNG sales: 53 700 m^3/day) (S.T. Yun 2012)

3.6 *Step 5: Iteration for minimized LCC*

At the last step, iterations are performed to find the minimized LCC. Nine design loads, which are estimated at the step 2, are taken into consideration to conduct the structure design and to estimate the LCC of the PGS. Finally, the most cost-effective design load for the PGS is determined.

4 RESULTS AND DISCUSSION: DETERMINATION OF DESIGN LOAD

In this study, nine extreme environmental loads are taken into account for the design of the PGS structure and compared with the original design load occurring once in 100 years. The LCC for the nine design loads are shown on Figure 4 as a blue line. When the strength of the PGS structure is increased, the CAPEX also increases. The increasing trend of the CAPEX is very similar to that of extreme design loads. On the other hand, the RISKEX decreased when the design load for the PGS increased. RISKEX initially declined rapidly, but later decreased slowly. Nine return periods considered in this paper are enough to find minimized LCC because the tendency of CAPEX to increase is greater than that of the RISKEX to decrease with the design load occurring once in 300 years, and the difference between 300 years LCC and 500 years

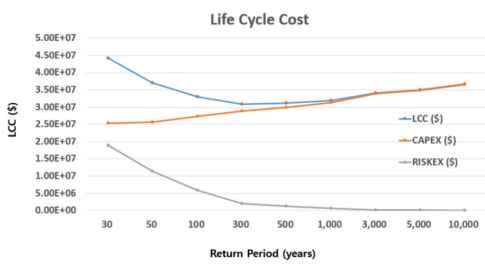


Figure 4. Life Cycle Cost for the nine design loads.

LCC are not significant. Thus, using a smaller interval of return periods might be unnecessary. As a result, preparation for the environmental loads, occurring once in 300 years, is the most economical for the structure design of the PGS at the target site, even though CAPEX of the structure increases.

LCCA for the design load selection of offshore structures has many uncertainty factors because it is conducted at the early design stage in which specific information of the structure is unavailable. Another uncertainty factor is that material cost, rental fee, and production loss during the repair time (which are taken into consideration to estimate the LCC), might be changed in real time. Subdivided levels of the consequence are also required for exactly estimating RISKEX. Some assumptions are needed to calculate structure availability and to estimate CAPEX and RISKEX. Thus, an uncertainty study and sensitivity analysis are required to verify the most sensitive variable in this design load selection procedure.

5 CONCLUSION

A methodology for the determination of design load was taken into account. The PGS was considered and Busan New Port was selected as a target site for the case study. Gumbel distribution was employed to estimate extreme environmental conditions and ANSYS AWQA was used to calculate extreme environmental loads. Nine return periods (30, 50, 100, 300, 500, 1 000, 3 000, 5 000 and 10 000 years) of extreme environmental loads were considered for the PGS structure design. For LCCA, CAPEX was estimated based on material costs and RISKEX, while the costs of failed components, the rental fee of an offshore crane vessel, and production loss were also taken into account.

This study was performed only for the case in which the PGS was installed near Busan New Port. The considerable design load could be changed depending on the types of structures, various types of target sites, and environmental conditions. However, the proposed procedure of design load selection would be meaningful and applicable to design of a newly developed offshore structure.

In this study, only environmental loads such as wave, wind, and current were taken into consideration for estimation of the external loads applied to the PGS. Considering other types of environmental loads and accidental loads such as mooring loads and ship collisions would be required.

ACKNOWLEDGEMENT

This work was supported by the Global Leading Technology Program of the Office of Strategic

R&D Planning (OSP) funded by the Korea Evaluation Institute of Industrial Technology, Ministry of Trade, Industry and Energy, Republic of Korea.

REFERENCES

API Recommended Practice 2A-WSD (RP-2A-WSD); 2th ed., API, Washington, D.C.

Chang, D.J. & Chang. G.P. 2013. Process of Offshore Installation and Safety Design (pp. 134–137). Paju: Dongmyeong.

Choi, K.S. 2013. Offshore Structural Engineering (p. 72). Seoul: Munundang.

ISO 19902. 2007. Petroleum and natural gas industries-Fixed steel offshore structures, first edition. p. 19.

Jung, H.S. 2012. Stochastic estimation of design wind speed by typhoon simulation. Master's Thesis. Division of Civil and Environmental Engineering, Seoul National University, Republic of Korea.

Kim, Sang-Hyo et al. 2013. Determining the Optimal Structural Target Reliability of a Structure with a Minimal Life-Cycle Cost Perspective. Advances in Structural Engineering, Vol. 16. No. 12.

KOREAN RESISTER. 2012. Fixed Offshore Structures Rules.

Kwon, S.H. et al. 1991. A Statistical Method of Estimation of Extreme Sea Level. Journal of Ocean Engineering and Technology, Vol. 5. No. 2: pp. 183~190.

Lee, Bong Hee et al. 2010. An Estimation of Extreme Wind Speeds Using National Wind Map. The Wind Engineering Institute of Korea Vol. 14, No. 1: pp. 29–38.

Lee, J.W. et al. 2009. Investigation of the surrounding environment, technical condition and limitation of the trade ports (except ports between Incheon and Gunsan) for the application of Mobile Harbor.

Lee, T.I. et al. 1992. Applications of the Type III Asymptotic Distribution for Extreme Sea Level Computations. Transactions of the Society of Naval Architects of Korea Vol. 29, No. 2.

Park, Jong Suk et al. 2013. Projection of the Future Wave Climate Changes Over the Western North Pacific. Journal of Korean Society of Coastal and Ocean Engineers 25(5): pp. 267~275.

Ryu, H.G. & Kim, D.Y. 2004. On Statistical Properties of the Extreme Waves in Hong-do Sea Area During Typhoons. Journal of the Korean Society for Marine Environmental Engineering Vol. 7, No. 1: pp. 47–55.

WMO (1998). Guide to Wave Analysis and Forecasting. World Meteorological Organization. WMO-No. 702.

Yun, S.T. 2012. Concept design of topside process for offshore LNG bunkering terminal. Master's thesis. Division of ocean systems engineering, KAIST, Republic of Korea.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Analysis of reliability and retaining levels of safety barriers

K. Jung & J. Marková
Klokner Institute, Czech Technical University in Prague, Czech Republic

ABSTRACT: Retention levels of road safety barriers are specified on the basis of risk assessment taking into account accidental data and further information available in the Czech Republic and also selected recommendations of Road Safety Association PIARC. The method of Bayesian networks is applied in the analysis and compared with event tree method. Newly proposed classes of retention for several categories of road surroundings considering the intensity of heavy traffic and two levels of hazard situation are incorporated to the revision of national prescriptive document that is expected to enhance the road safety.

1 INTRODUCTION

Thousands of human lives are annually lost on European roads. Therefore, the authorities in most countries are concerned about the numbers of people killed and injured, leading to enormous social and economic costs. In the Czech Republic, more than 85 people per one million inhabitants lose their life annually. It means that on the average 897 people was killed per year in the last ten years. It should be noted that the number of fatalities are below the mean in the last 5 years. Protective measures have significant influence on reduction of consequences of car accidents. Various national or European prescriptive documents give basic guidance for their application.

Road safety barriers provide protection of traffic on roads as well as their close surroundings. Various aspects have to be considered for selection of appropriate types of safety barrier including road categories, surface characteristics, road surroundings, allowable velocity of cars, types of danger places in road surroundings and traffic intensity including expected future trends. For selection of appropriate safety measures, the retention level for road barriers has to be determined considering danger sections of roads and protection of road surroundings.

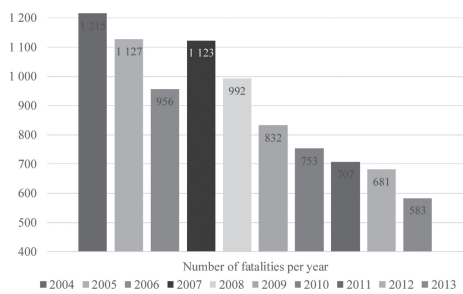


Figure 1. Number of fatalities per year in the Czech Republic.

Presented study is focused on optimization of retention level of safety barriers taking into account accident data recorded in the Czech Republic in the last few years. Results of analyses and further information are expected to be used as background materials for revision of the Czech technical conditions TP 114 (2010).

2 RISK ANALYSIS

The Bayesian network is applied for analysis of retention level of safety barriers facilitating to describe various accidental scenarios, and also for verification of event tree method used in previous studies (Markova & Jung, 2006). Individual risk R_i is given as

$$R_i = p_i \times C_i \tag{1}$$

where p_i is the probability of occurrence of accident i and C_i its expected consequence. The total risk R is specified as a sum of all considered risks given as

$$R = \sum_i p_i \times C_i \tag{2}$$

Five types of vehicles are considered in analyses:

– Heavy Goods Vehicles (HGV),
– Danger Goods Vehicles (DGV),
– buses,

– cars,
– motorcycles.

The traffic composition is based on traffic data provided by the Road and Motorway Directorate of the Czech Republic.

The number of accidents n_{veh} for considered type of vehicles per one year is expressed as

$$n_{veh} = N \times L \times p_{veh} \times p_a \tag{3}$$

where N is the intensity of all vehicles on the road, L is the length of considered road section, p_{veh} is the ratio between the number of relevant type of vehicles to total number of all vehicles in the road, p_a is the annual probability of accident occurrence for the type of vehicle.

For the analysis of retention level of safety barriers, the data of accidents are available, recorded in electronic version in the last few years. Different causes of car impacts are distinguished including impacts to bridge columns, safety barriers, walls, buildings, car collisions etc. Three types of roads are considered: motorways and 1st and 2nd class roads (country national and main roads). Figure 2 and Figure 3 indicate that the main risk with respect to the obstacles near roads is associated with impact to trees, bridge piers and walls.

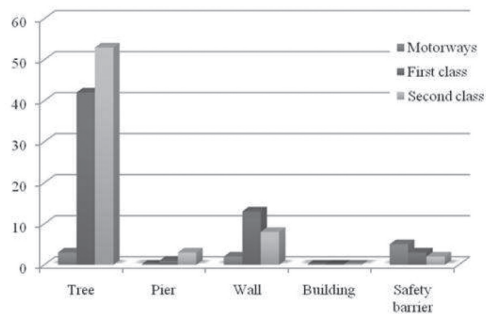


Figure 2. Number of fatalities for motorways and 1st and 2nd class roads in the Czech Republic (year 2007).

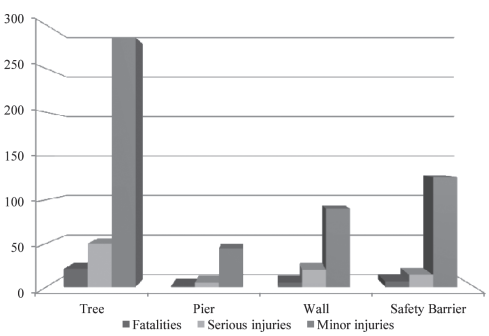


Figure 3. Number of fatalities and injuries for 1st class roads in the Czech Republic (year 2011).

3 CONSEQUENCES

Social, economic and ecological consequences should be considered in accidental situations due to car collisions. Social consequences are the most significant in this consideration as human lives are endangered during accidents.

Consequences of car accidents and probabilities of serious injuries or fatalities are based on comparison of the kinetic energy E_k of considered type of vehicle and the capacity of safety barriers. The kinetic energy of impacting vehicle is given as

$$E_k = \frac{1}{2} m \times (v \times \sin\alpha)^2 \tag{4}$$

where m is the vehicle mass, v its velocity and α a direction angel of impact. The maximum permitted velocities for vehicles in relevant types of roads are considered in the analyses.

It is assumed that the structure reacts rigid plastics, then the maximum displacement follows from

$$\frac{1}{2} m \times \varepsilon \times (v \times \sin\alpha)^2 = F_c \times u_d \tag{5}$$

where F_c is the static force and u_d deformation of the structure at fracture. Failure occurs if u_d exceeds the deformation capacity of the barrier which depends on materials properties. A perfectly elastic collision has a coefficient of restitution of $\varepsilon = 1$. Typical collision has coefficient of restitution ε between 0,55 and 0,8 (Coon & Reid, 2006). It is clear that barriers made of materials with higher deformation capacity could provide better protection and due to less force lower danger for passenger.

The capacities of safety barriers for several levels of retention N1 to H4b are given in Table 1 according to standard EN 1317-1 and national prescriptive document TP 114.

The total risk R may be determined from formula

$$R = 1000 \times C_s \times L + \sum p_{f,n} \times C_n + \sum p_{f,en} \times C_{en} \tag{6}$$

Table 1. Capacity of safety barriers E_k [kNm].

Type	N1	N2	H1	H2	H3	H4a	H4b
E_k	43,3	82,9	126,6	287,5	426,1	527	724,6

where C_s are the costs of getting the safety barriers, L is the length of road section, $p_{f,n}$ is the probability of human fatalities of injuries, C_n are relevant social costs, $p_{f,en}$ is the probability of accident occurrence for different types of vehicles, C_{en} are economical or ecological loses due to accident, expressed in monetary units.

The main risk is connected with lose of human lives. The costs of a human life or an injury applied in presented analysis are based on information of the Transport Research Center (www.cdv.cz). Economical lose for one fatality is considered here as 333 000 EUR, for serious injury as 112 000 EUR and minor injury as 12 500 EUR.

It should be noted that these values seem to be rather low. Each fatality prevented on British roads represents an approximate overall saving of £1,3 m and each serious injury prevented represents a saving of £150,000 (Farmer 2004). These analyses are based on economic as well as social and environmental factors including loss of earnings, costs of hospital treatment and other social costs. The value of preventing the road traffic accident may be estimated on the basis of cost-benefit analysis, see e.g. recently revised ISO/CD 2394 (2014).

Other possibility to describe loses due to accidents may be also described by ICAF (Implied Cost of Averting a Fatality) given as

$$\mathrm{ICAF} = g \times e \times (1\text{-}w) / (4 \times w) \tag{7}$$

where g is the gross domestic product per person per year [€/year], e is the life expectancy at birth [year] and w is the proportion of life spent in economic activity (Diamantidis 2002).

4 RISK ASSESSMENT

The presented study is focused on the determination of retention level of safety barriers taking into account accident data recorded in the Czech Republic in the last few years. The aim is to provide backgrounds for selection of safety barriers.

Accidents involving impact from vehicles can be caused by many factors and include many consequences.

Main parameters affecting accidents are

- Speed, mass and direction of impacting road vehicle
- Rigidity and construction of the structural elements of barriers
- Roads layout and geometry (curves, slope)
- Usage of roads surrounding at time of the incident.

Main parameters affecting accidents which are not covered in this analysis include

- Act of sabotage
- Human failure.

The study is based on minimization of risks. The retention level H1 corresponds to kinetic energy E_k = 126,6 kNm (see Table 1). Lower and higher retention level increases the risk. Selection of lower retention level increases risks as the protection could not be sufficient. Selection of higher retention level increases risks for passengers in cars, while the surrounding is more protected.

5 BAYESIAN NETWORK

A Bayesian network was developed for verification and comparison of achieved result by event tree method. The network was developed in program Genie and contains 5 random nodes, 5 utility nodes, and 2 decision nodes.

5.1 *Decision nodes*

There are two decision nodes in the presented study—the *Intensity of traffic* and the proposed type of the road *Safety barriers*. The decision node "*Intensity of traffic*" has three states.

- Small intensity
- Medium intensity
- High intensity.

The decision node "*Type of safety barriers*" has eight states, first state "No barriers" is unprotected surrounding. Other seven states cover classes of

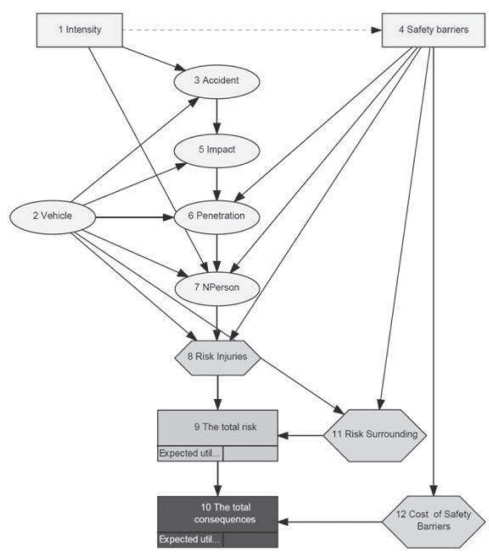


Figure 4. Bayesian Network used for analysis of safety barriers.

the retention capacity of safety barriers. The levels are given in Table 1 according to the standard EN 1317-1. The eighth state is for surrounding without need of protection. No barriers could be accepted only in places not covered by surrounding considered here and where are sufficient and safe leaving zones.

5.2 *Utility/Value node*

A utility node represents an additive contribution to the utility function in an influence diagram. Thus, the utility function is the sum of all utility nodes in the influence diagram. *Cost of Safety Barriers*—this node describes the cost of new safety barriers. The cost is based on the price per 1 kilometre. The utility nodes represent the economic factors and adverse consequences.

A more detailed description of the nodes is provided in the following list, which also indicates difficulties in input data specification.

The utility nodes describe risks due to economic and environmental lose on surroundings considered as:

- Cost of Safety Barriers,
- Risk Surrounding,
- Risk Injuries,
- The Total Risk,
- The Total Consequence.

The Total Risk is a sum of all risks for each type of safety barriers. The Total Consequence is a sum of all Risk, Consequences and Costs of Safety Barriers.

5.3 *Random nodes*

These nodes describe randomness in the proposed analysis. There are five random nodes

- Collisions
- Impact
- Penetration
- Vehicles
- NPersons.

5.3.1 *Node "Accident"*

Node "Accident" describes probability of a collision per one year and one kilometer of road. Following

Tables 2 to 4 show probabilities for three intensities.

5.3.2 *Node "Impact"*

Random node "*Impact*" describes the probability of vehicle collision with safety barriers. The records in the Czech Republic show that about 60% of all accidents on motorways results from impact into safety barriers".

Table 2. Probability of collision per 1 kilometer and 1 year—small intensity.

	HGV	DGV	Car	Bus	Motorbike
NoCollision	0,983	0,999	0,952	0,997	0,993
Collision	0,017	0,001	0,048	0,003	0,007

Table 3. Probability of collision per 1 kilometer and 1 year—medium intensity.

	HGV	DGV	Car	Bus	Motorbike
NoCollision	0,900	0,999	0,723	0,979	0,960
Collision	0,100	0,001	0,277	0,021	0,040

Table 4. Probability of collision per 1 kilometer and 1 year—high intensity.

	HGV	DGV	Car	Bus	Motorbike
NoCollision	0,730	0,998	0,255	0,946	0,891
Collision	0,270	0,002	0,745	0,055	0,110

5.3.3 *Node "Penetration"*

The impacting vehicle either crosses the barrier into opposite carriageway or surrounding, rebounds back into the original carriageway, or remains on, or close to the barrier. Random node "*Penetration*" describes the probability of penetration into surrounding. Williams (2007) shows that about 7% of all accidents involved in impacting a safety barrier crosses through into surrounding.

Further these probabilities are affected by containment level of safety barriers and the type of vehicle.

Probability that the safety barriers for each retention capacity and vehicle type might be overcome should be estimated. Number of endangered passengers is described by probability for each type of vehicle and each type of barriers.

5.3.4 *Node "NPersons"*

Node "*NPerson*" describes the number of endangered persons for each type of vehicle.

This node has six states (No Person, N1, N2, N5, N10 and N25).

5.3.5 *Probability of impact into barriers*

It is estimated for different speed categories and types of vehicles.

The main parameters describing the kinematics of vehicle are the velocity and angle. Data concerning velocity are not available. The direction angle α varies from 0 to 30° or 40°; Raleigh distribution could be used for with a mean equal to 10–15° for tg α.

Table 5. Definition of scenarios and extent for vehicles.

Scenarios	S_{z1}	S_{z2}	S_{z3}	S_{z4}	S_{z5}	S_{z6}
Impact	Yes	Yes	Yes	No	No	No
Penetration	Yes	Yes	No	No	–	–
Secondary condition	Yes	No	Yes	No	Yes	No

5.3.6 *Probability of barriers penetration*

These probabilities are estimated in accordance with the permitted speed and type of vehicle. In case of safety barriers it is supposed that the structure is elastic and the colliding object is rigid. In accordance with EN 1317 it is assumed that the structure is designed to absorb the impact energy by plastic deformations, it must be ensured that its ductility is sufficient to absorb the total kinetic energy of the colliding object. In the limit case of rigid-plastic response of the structure, the above requirement is satisfied where F is the plastic strength of the structure, i.e. the quasi-static limit value of the force F; y_o is the displacement of the point of impact that the structure can undergo.

5.3.7 *Probability of secondary collision*

These probabilities are affected by the intensity of traffic and maximal speed. When the barriers are overcome, the secondary collision means collisions with vehicle going in opposite direction. In case the barriers are not overcome, the secondary collision is rear or side collision with vehicle in some direction. It is supposed that the consequences of secondary condition are lower than the collision with vehicle going in opposite direction.

This is due to the lower number of rear impact leads to serious casualties than frontal casualties and due to less structural possibilities may influence the outcome of a rear impact.

6 RESULTS FOR SELECTED EXAMPLES

6.1 *Drinking water resources*

Total intensity is 33 305 vehicles per day based on statistics of the year 2010.

Maximal allowed speed is 130 km/h for cars and motorbikes, 80 km/h for HGV and DGV and 100 km/h for buses.

The graph in Figure 5 shows results of risk analysis for drinking water resources, when as optimal decision is selected Safety barriers with retention level H4b which corresponds to $E_k = 724{,}6$ kNm.

6.2 *Central barriers*

This example is focused on analysis of the Central barriers on the highways, where the maximal allowed speed is 130 km/h for cars and motorbikes, 80 km/h for HGV and DGV and 100 km/h for buses.

Total intensity is 73 397 vehicles per day based on statistics from the year 2010.

In this case the optimal protection represent barriers with retention level H3 corresponding to $E_k = 426{,}1$ kNm as it is shown in the following Figure 6.

Table 6. Proportion of vehicles.

Type of vehicles	Number	Ratio
HGV	8748	30,78%
DGV	67	0,20%
Buses	373	1,12%
Cars	24023	72,13%
Motorbike	94	0,28%

Table 7. Proportion of vehicles.

Type of vehicles	Number	Ratio
HGV	14410	19,63%
DGV	147	0,20%
Buses	451	0,85%
Cars	6220	79,05%
Motorcycles	45	0,27%

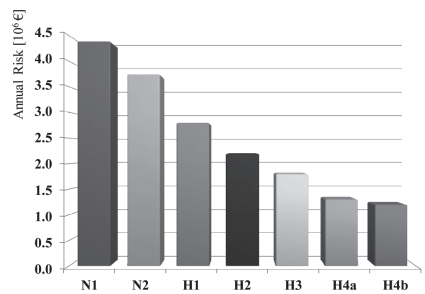


Figure 5. Results of the analysis based on Bayesian network.

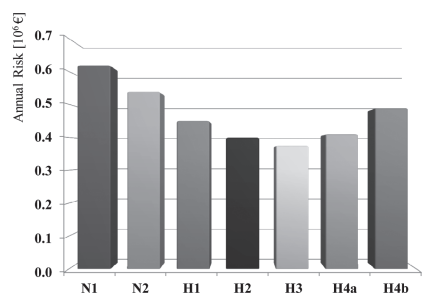


Figure 6. Results of the analysis based on Bayesian network.

7 RECOMMENDED RETENTION LEVEL OF SAFETY BARRIERS

Proposal for retention level of safety barriers was prepared in co-operation with Czech authorities taking into account results of risk assessment, see Tables 8 and 9. Several classes of dangerous surroundings, intensity of heavy vehicles and two hazard levels (common and higher level) are considered.

Proposal for retention levels of safety barriers on roads is shown in Table 8. In case the higher hazard level needs to be considered in specific accidental situation, the level of retention should be increased.

Table 8. Recommended retention levels of safety barriers on roads in common hazard rate.

	Mean value of heavy vehicles per 24 hours		
Class Surrounding	<1000	1000–5000	>5000
1. Drinking water resources	H2	H2	H3
2. Railways	H1	H2	H2
3. Place with high frequency of pedestrians	H1	H2	H2
4. Buildings	H1	H1	H2
5. Central barriers	H1	H1	H2
6. Parallel roads	H1	H1	H2
7. Roads in different level	H1	H1	H2
8. Rivers or water reservoirs	N2	H1	H2
9. Scarps, embankments	N2	H1	H1
10. Other danger places (trees, portals)	N2	H1	H1
11. Noise barriers	N2	N2	N2

Table 9. Recommended retention levels of safety barriers on bridges in common hazard level.

	Mean value of heavy vehicles per 24 hours		
Class Surrounding	<1000	1000–5000	>5000
1. Drinking water resources	H2	H2	H3
2. Railways	H2	H2	H2
3. Places with high frequency of pedestrians	H1	H2	H2
4. Buildings	H1	H2	H2
5. Rivers or water reservoirs	H1	H1	H2
6. Parallel or crossing roads	H1	H1	H2
7. Central barriers	H1	H1	H2
8. Other danger places, portals	H1	H1	H2

Similar Table 9 was proposed for retention levels of safety barriers on bridges taking into account eight classes of surroundings.

8 CONCLUSIONS

Risk assessment based on accidental data for motorways and main roads facilitates to propose new retention levels of safety barriers to the revision of national prescriptive document TP 114.

Several classes of road environment are updated or refined. For decision on the retention levels of safety barriers several significant basic variables are identified including the daily average intensity of heavy vehicles, maximal permitted car velocities and the level of potential risk.

The retention level is analysed by event Bayesian network taking into account the road category, heavy car intensity and various types of road or bridge surroundings. The higher intensity of heavy goods vehicles increases the probability of accident and usually increases the needs for higher retention level of safety barriers. Therefore, for the passenger cars or motorbikes, it leads to significant risk increase.

Analyses of data indicate in some cases discrepancies on reported accidents including location of accidents, impacted safety barriers (central or lateral barriers) and description of consequences.

Many questions and uncertainties remain still open also in the risk analysis of road safety barriers. The behaviour of the barriers made from different materials should be analysed in more detail. Wire-rope barriers represent a special problem. Are the wire-rope barriers dangerous for motorcyclist and could they endanger a convertible car? Is it acceptable to use on our roads the safety barriers which could protect one type of passengers however be danger for other passengers?

It should be noted here that implementation of safety measures is a complex process involving official authorities, designers, road maintenance service, producers of safety barriers, testing institutions etc. It is expected that newly proposed provisions for retention levels will facilitate the selection of appropriate types of safety barriers.

ACKNOWLEDGEMENTS

This research has been conducted in the Klokner Institute of the Czech Technical University in Prague as a part of the project No. TA02030150 "Application of Reliability Methods in Research and Verification of Innovative Road Safety Barriers" supported by the Technological Agency of the Czech Republic and research project P105/12/P281

"Development of Bayesian Networks for Risk Assessment of Structures Exposed to Impacts" supported by the Czech Science Foundation.

REFERENCES

Coon B.A., Reid J.D., 2006. Reconstruction techniques for energy-absorbing guardrail end terminals, In: *Accident Analysis and Prevention*, 38, pp. 1–13.

ČSN EN 1317-1, 1999. *Road restraint systems—Part 1: Terminology and general criteria for test methods*.

Diamantidis, D., 2002. Risk Acceptance Criteria for Long Railway Tunnels: A Need for Periodic Review, In *Proceedings* of *PSAM 6 International Conference San Juan*, Puerto Rico.

Farmer, D., 2005. Road Safety Bill, Regulatory Impact Assessment.

ISO/CD 2394, 2014. *General principles on reliability for structures*.

Markov,a J. & Jung, K., 2006. Report on specification of retention level of road safety barriers on the basis of risk assessment, KI CTU.

Piarc, 2003. *Road Safety Manual*, Quebec,

Švarc, J., 2006. Trend of traffic in period 2001–2005, *Road conference 2006*, Liberec, Czech Republic, pp. 43–48.

Transport Research Centre, 2004. Safety of road traffic, Accident frequency—Specification of loses, (www.cdv.cz).

TP 114, 2010. Road safety barriers. Actions, retention level, design of special safety barriers.

Williams, G.L., 2007. *Whole Life Cost—Benefit Analysis for Median Safety Barriers*, Project report, Transport Research Laboratory.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Safe reliability assessment through probabilistic constraint reasoning

Elsa Carvalho, Jorge Cruz & Pedro Barahona
Centro de Inteligência Artificial, Universidade Nova de Lisboa, Portugal

ABSTRACT: Reliability quantifies the ability of a system to perform its required function under variable conditions. The adequate functioning of a system is often represented by inequality constraints, and its reliability is the probability that such constraints are satisfied, given the uncertainty the variables are subject to. Since this computation is very hard, namely when the systems are modeled with nonlinear constraints, traditional methods adopt a number of approximations, thus computing a value that may be far from the exact one. Moreover, these methods do not provide any guarantees regarding the correctness of the computed results. In this paper, we use the probabilistic continuous constraints framework to efficiently compute safe bounds for the reliability of a system, and illustrate it on a number of representative examples.

1 INTRODUCTION

Reliability analysis studies the ability of a system to perform its required function under variable conditions. In this context, reliability assessment quantifies the chance of system failure at any stage of a system's life. This research area has a wide range of applications, including the aeronautical (Nikolaidis, Ghiocel, & Singhal 2007), chemical (Goel, Grievink, Herder, & Weijnen 2002) and building (Huang, Chan, & Lou 2012) industries.

Reliability is reported in terms of the probability of adequate functioning of a system and its exact quantification requires the calculation of a multi-dimensional integral with a nonlinear integration boundary. Because there is rarely a close-form solution, this calculation is one of the major concerns of classical approaches to solve reliability problems, which adopt approximation methods that rely on several simplifications of the original problem to compute a reliability estimate, often leading to inaccurate results, especially in highly nonlinear problems.

When choosing among several alternative configurations of a system it is important to obtain safe bounds for their reliability, since designs with a high reliability estimate but high uncertainty on such estimation are not credible options. Such safe bounds are not available with classical approaches, but they can be provided by the Probabilistic Continuous Constraint framework that we have been developing to integrate probabilities and constraint programming, and that has already been successfully applied to inverse problems (Carvalho, Cruz, & Barahona 2013).

The paper is organized as follows. Section 2 briefly introduces the concepts of reliability assessment and describes classical techniques, such as FORM (Hohenbichler & Rackwitz 1983), SORM (Fiessler, Neumann, & Rackwitz 1979), and Monte Carlo simulation (Halder & Mahadevan 1999), used to address such problem, discussing their limitations. In sections 3 and 4 we introduce our Probabilistic Continuous Constraint approach, discussing the features that are required toaddress reliability assessment. Section 5 illustrates our framework on a set of representative examples, comparing it with traditional methods, highlighting the importance of the safe bounds we efficiently obtain. The last sectionsummarizes the main conclusions and directions for future work.

2 RELIABILITY ASSESSMENT

A limit-state is a condition beyond which a system no longer fulfills the desired functionality. Reliability assessment calculates and predicts the probability of limit-state violations at any stage of a system's life.

The probability of occurrence of a limit-state violation in a system represents its probability of failure, P_f, whereas $P_s = 1 - P_f$ represents its reliability.

Failure events are represented as limit-state constraints g is a limit-state function and x is a realization of the random vector X (defined in Ω_X) that represents all the relevant uncertainties influencing the probability of failure and has joint Probability Density Function (PDF) f_X. Thus,

the failure event is $F = \{x \in \Omega_{\boldsymbol{X}} : g(x) < 0\}$ and the probability of failure is the probability of the failure event:

$$P_f = P(x \in F) = \int_{g(x)<0} f_{\boldsymbol{X}}(x)dx \tag{1}$$

More generally, we are interested in problems that can be defined by one or more limit-state functions. In series systems, global failure occurs when at least one limit-state functions is violated, whereas in parallel systems, it occurs when all limit-state functions are violated. So, the failure events for series and parallel systems with k limit-state functions, are, respectively:

$$F = \bigcup_{i=1}^{k} \{x \in \Omega_{\boldsymbol{X}} : g_i(x) < 0\} \qquad \text{and} \tag{2}$$

$$F = \bigcap_{i=1}^{k} \{x \in \Omega_{\boldsymbol{X}} : g_i(x) < 0\} \tag{3}$$

2.1 *Classical techniques*

Reliability assessment involves the calculation of a multi dimensional integral in a possibly highly nonlinear integration boundary (Equation (1)). Analytical computation of such integral is usually impossible, so various simulation-based and numerical methods have been proposed to deal with this problem.

In (Hasofer & Lind 1974), Hasofer and Lind introduced the reliability index technique for calculating approximations of the desired integral with reduced computation costs. The reliability index has been extensively used in the first and second order reliability methods (FORM (Hohenbichler & Rackwitz 1983) and SORM (Fiessler, Neumann, & Rackwitz 1979)).

The main idea is to move the reliability problem from the space of random vector $\boldsymbol{X}$ to the space of standard normal statistically independent random variables $\boldsymbol{U} = \langle U_1, \ldots, U_n \rangle$ using a suitable transformation $\boldsymbol{U} = T(X)$, such as Rosemblatt (Rosenblatt 1952) or Nataf (Nataf 1962) transformations (see (Hohenbichler & Rackwitz 1981, Melchers 1999) for an overview). In the $\boldsymbol{U}$ space, Equation (1) can be expressed as:

$$P_f = \int_{g(\boldsymbol{u})<0} f_{\boldsymbol{U}}(\boldsymbol{u})d\boldsymbol{u} = \prod_{i=1}^{n} \int_{g(u)<0} \phi_{U_i}(u_i)du_i$$

where ϕ_{U_i} is the standard normal PDF of U_i.

In FORM an approximation to the probability of failure is obtained by making the failure surface, $g(\boldsymbol{U}) = 0$, linear at the design point, $\boldsymbol{u}^*$, often called the Most Probable Point of failure (MPP). This is the point on the failure surface closest to the origin and with the highest probability (local maximum) in the failure domain of the standard normal space. The distance from the origin to the design point is the reliability index $\beta = \|\boldsymbol{u}^*\|$.

Since the standard normal space is rotational symmetric, probability of failure can be directly obtained using the reliability index, $P_f = \Phi(-\beta)$, where Φ is the standard normal cumulative probability function.

As the limit state function is in general nonlinear it is not possible to know the design point in advance and this has to be found iteratively. The design point is thus, the solution to the constrained optimization problem:

$$\beta = \min_{u \in \{g(u)=0\}} \|u\|$$

This problem, being the most expensive part of FORM algorithm, may be solved in a number of different ways (see (Eldred, Bichon, & Adams 2006) for an overview). An appropriate iteration scheme converges after some iterations, providing the design point $\boldsymbol{u}^*$ as well as the reliability index β, which may be related directly to the probability of failure. However, with non convex optimization problems, it is not guaranteed that the solution point will be the global minimum-distance point.

FORM usually works well when the failure surface has only one minimal distance point and the function is nearly linear in the MPP neighborhood. However, for increasingly nonlinear failure surface the probability of failure estimated by FORM becomes increasingly inaccurate (and possibly unreasonable) (Melchers 1999). To address such non linearity SORM incorporates some curvature in the limit state approximation through a parabolic approximation to the failure surface (Breitung 1984).

In both methods, it is assumed a single limit-state function with a single design point where only the region around such point contributes to the probability of failure. In limit-state functions with multiple design points (and in problems with multiple limit-state functions), application of FORM or SORM around a single design point results in erroneous estimates for the probability of failure. So, the problem of identifying the multiple design points was addressed by several authors (e.g. (Kiureghian & Dakessian 1998, Barranco-Cicilia, de Lima, & Sudati-Sagrilo 2009)).

In series systems, generally there exists one design point for each limit-state function (which contributes to the identification of the feasible region). In contrast, in parallel systems there usually exists one design point for each pairwise inter-

section of limit-state functions (again contributing to the identification of the unfeasible region).

Once all design points are identified, FORM or SORM approximations are constructed at these points and the failure probability is computed by series system reliability analysis (for multiple design points in a single limit-state function or series systems) or by parallel system reliability analysis (for parallel systems) (see (Sørensen 2004, Notes 6 and 7) for details).

Other techniques include sampling, based on Monte Carlo simulation (MCS) (Halder & Mahadevan 1999) and work well for small reliability requirements. Nevertheless, as the desired reliability increases, the number of samples must also increase to find at least one infeasible solution.

Since Monte Carlo method is basically a sampling process, the results are subjected to sampling error that decreases with the sample size. However, using procedures known as variance reduction techniques the error may be reduced without significantly increasing the sample size. One of such procedures with a high convergence rate is the Monte Carlo with Importance Sampling (MCIS) (Melchers 1999). In MCIS, the regions of interest for the simulation process are those around the points in the failure domain having the largest values, i.e., the design points.

Given the simplifications adopted and their approximate nature, none of the above methods provides guarantees on the reliability values computed, specially for nonlinear problems. In contrast, the Probabilistic Continuous Constraint framework does not suffer from this limitation, guaranteeing safe bounds for the probability of failure.

3 CONTINUOUS CONSTRAINT PROGRAMMING

Continuous constraint programming has been widely used to model safe reasoning in applications where uncertainty arises. A Continuous Constraint Satisfaction Problem (CCSP) (Lhomme 1993, Benhamou, McAllester, & van Hentenryck 1994, Sam-Haroud & Faltings 1996) is a triple $\langle X, D, C \rangle$ where X is a tuple of n real variables $\langle x_1, \ldots, x_n \rangle$, D is a Cartesian productof intervals $I_1 \times \ldots \times I_n$ (a box), where each I_i is the domain of variable x_i and C is a set of numerical constraints (equations or inequalities) on subsets of the variables in X. A solution of the CCSP is a value assignment toall variables satisfying all the constraints in C. The feasible space $\mathcal{F}$ is the set of all CCSP solutions within D.

Constraint reasoning relies on branch-and-prune algorithms to obtain sets of boxes that cover exact solutions for the constraints (the feasible space). These algorithms begin with an initial crude cover of the feasible space (the initial search space, D) which is recursively refined by interleaving pruning and branching steps until a stopping criterion is satisfied. The branching step splits a box from the covering into sub-boxes (usually two). The pruning step either eliminates a box from the covering or reduces it into a smaller (or equal) box maintaining all the exact solutions. Pruning is achieved through a constraint propagation algorithm ($\mathcal{CPA}$) which combines constraint propagation and consistency techniques (Benhamou, Goualard, Granvilliers, & Puget 1999) based on interval analysis methods (Moore 1966).

Interval analysis is an extension of real analysis that allows computations with intervals of reals instead of reals. Common operations and unary functions are extended for interval operands. For instance, [1,2] + [3,6] results in the interval [4,8], which encloses all the results from a point-wise evaluation of the real arithmetic operator on all the values of the operands. In practice these extensions simply consider the bounds of the operands to compute the bounds of the result, since the involved operations are monotonic.

Interval extensions [f], allow computing enclosures of the range of real functions f, over boxes. The natural interval extension of a function is obtained by evaluating its expression for interval arguments using interval arithmetic.

The branch-and-prune algorithm usually maintains two coverings of the feasible space $\mathcal{F}$ of a CCSP $\langle X, D, C \rangle$: one outer and one inner box cover, as follows.

Outer Box Cover A set of almost disjoint boxes[1] $\mathcal{F}_{\square} = \{B_1, \ldots, B_n\}$, where $\forall_{1 \le i \le n} (B_i \subseteq D \wedge vol(B_i) > 0)$, is an outer box cover of $\mathcal{F}$ iff $\mathcal{F} \subseteq \bigcup_{i=1}^{n} B_i$.

A complementary concept is that of inner box cover, where an inner box of a CCSP is a box totally contained in the feasible space.

Inner Box A box $B \subseteq D$ with $vol(B) > 0$ is an inner box of $\mathcal{F}$ iff $B \subseteq \mathcal{F}$.

Inner Box Cover A set of almost disjoint boxes $\mathcal{F}_{\blacksquare} = \{B_1, \ldots, B_n\}$ is an inner box cover of $\mathcal{F}$ iff $\bigcup_{i=1}^{n} B_i \subseteq \mathcal{F}$.

We are particularly interested in maintaining an inner box cover that is a subset of the outer box cover.

[1]Two boxes B_1 and B_2 are almost disjoint iff $vol(B_1 \cap B_2) = 0$. The volume of a box $B \subseteq \mathbb{R}^n$ is the product of the width of its intervals, i.e., $vol(B) = wid(I_1) \times \ldots \times wid(I_n)$.

Joint Box Cover A joint box cover $\mathcal{F}_{\boxplus}$ of $\mathcal{F}$ is a pair $\langle \mathcal{F}_{\square}, \mathcal{F}_{\blacksquare} \rangle$, with $\mathcal{F}_{\blacksquare} \subseteq \mathcal{F}_{\square}$.

Often it is important to know whether a joint box cover represents the feasible space more accurately than another. For this purpose we define a partial order ($\preceq$) as follows.

Tighter Joint Box Cover Given a CCSP $\langle X, D, C \rangle$ and two joint box covers of $\mathcal{F}$, $\mathcal{F}_{\boxplus 1} = \langle \mathcal{F}_{\square 1}, \mathcal{F}_{\blacksquare 1} \rangle$ and $\mathcal{F}_{\boxplus 2} = \langle \mathcal{F}_{\square 2}, \mathcal{F}_{\blacksquare 2} \rangle$, $\mathcal{F}_{\boxplus 2}$ is a tighter joint box cover of $\mathcal{F}$ than $\mathcal{F}_{\boxplus 1}$, (written $\mathcal{F}_{\boxplus 2} \preceq \mathcal{F}_{\boxplus 1}$) iff:

$$\bigcup \mathcal{F}_{\square 1} \supseteq \bigcup \mathcal{F}_{\square 2} \text{ and } \bigcup \mathcal{F}_{\blacksquare 1} \subseteq \bigcup \mathcal{F}_{\blacksquare 2}$$

The branch-and-prune algorithm *B & P* (Algorithm 1, similar to (Granvilliers & Benhamou 2006)) receives a joint box cover and computes a tighter one. For that purpose, and while the stoping criterion is not satified, the algorithm removes a box from the outer box cover that, simultaneously, verifies the *eligible* predicate and is selected by the *order* function (line 2), and splits it (line 3). Subsequently it modifies the inner and outer box covers of the joint cover. If the retrieved box is already in the inner box cover (line 4) then it is replaced by the boxes resulting from the *split*, which are also added to the outer box cover. Otherwise (line 5) the boxes resulting from the *split*, are pruned by the constraint propagation algorithm and added to the outer box cover (line 6). Those that are inner boxes are also added to the inner box cover (line 7).

Typically, in Algorithm 1, the *split* function splits the box by the midpoint of its largest interval; the *inner* predicate relies on natural interval extensions

```
   Input: ⟨F□, F■⟩: joint box cover; C: set of
          constraints; ε: real; stop, order:
          function;
   Output: ⟨F□, F■⟩out: joint box cover;
1  while (¬stop(⟨F□, F■⟩)) do
2      B ← remove(F□, eligible, order);
3      if B = ∅ then break;
4      S ← split(B);
5      if B ∈ F■ then
6          F■ ← F■ \ {B};
7          L■ ← S;    L□ ← S;
8      else
9          L□ ← {CPA(Bi, C) : Bi ∈ S};
10         L■ ← {Bi ∈ L□ : inner(Bi, C)};
11     end
12     ⟨F□, F■⟩ ← ⟨F□ ∪ L□, F■ ∪ L■⟩;
13 end
14 return ⟨F□, F■⟩;
```

Algorithm 1. *B & P* ($\langle \mathcal{F}_{\square}, \mathcal{F}_{\blacksquare} \rangle$, C, ε, *stop*, *order*).

induced by each constraint[2], replacing the variables by the intervals of the box, and checking whether all values in the resulting interval are solutions for that constraint; and the $eligible_{\varepsilon}$ predicate requires the width of the largest interval of the box to be larger than a given ε. The *stop* predicate imposes the stopping criterion and the *order* function specifies which box is selected for processing. Both *stop*, *order* and ε are parameterizable.

4 PROBABILISTIC CONSTRAINT PROGRAMMING

In classical CCSPs, uncertainty is modeled by intervals that represent the domains of the variables. Constraint reasoning reduces uncertainty providing a safe method for computing a set of boxes enclosing the feasible space. Nevertheless this paradigm cannot distinguish between different scenarios and all combination of values within such enclosure are considered equally plausible. In (Carvalho 2012) and (Carvalho, Cruz, & Barahona 2013) the authors proposed the Probabilistic Continuous Constraint paradigm (hereafter referred as PC), that extends the continuous constraint framework with probabilistic reasoning, allowing to further characterize uncertainty with probability distributions over the domains of the variables.

4.1 *Probabilistic continuous constraints*

Probability provides a classical model for dealing with uncertainty (Halpern 2003). The basic elements of probability theory are a) random variables and b) events, which are appropriate[3] subsets of the sample space Ω. A probabilistic model is an encoding of probabilistic information that allows the probability of events to be computed, according to the axioms of probability. In the continuous case, the usual method for specifying a probabilistic model assumes a full joint PDF over the considered random variables.

In order to complement the interval bounded representation of uncertainty with a probabilistic characterization of the values distributions, we define a probabilistic continuous constraint space. Firstly, a probability space is associated with a CCSP.

PC Probability Space Given a CCSP $\langle X, D, C \rangle$, the associated probability space is $\langle \Omega, \mathcal{B}^n, P \rangle$ where $\Omega \supseteq D$, $\mathcal{B}^n$ is the n-dimensional Borel σ-algebra on Ω and P is a probability measure.

Secondly, the variables of the CCSP are mapped onto random variables.

[2] In this paper we consider only inequality constraints.
[3] In the sense that it is possible to assign them a measure.

PC Random Vector Given a PC probability space on $\langle\langle x_1, \ldots, x_n\rangle, D, C\rangle$, an identity random vector $\mathbf{X} = \langle X_1, \ldots, X_n\rangle$ is considered, such that $X_i : \mathbb{R}^n \to \mathbb{R}$ is defined as $X_i(\Omega) = \Omega_i$.

Thirdly, the probability measure P is defined.

PC Probability Measure Given a PC probability space, PC random vector $\mathbf{X}$ with joint PDF $f(\cdot)$ and an event $\mathcal{H} \in \mathcal{B}^n$, the probability measure P is defined as:

$$P(\mathcal{H}) = \int \cdots \int_{\mathcal{H}} f(x_1, \ldots, x_n) dx_n \ldots dx_1$$

Finally, a probabilistic continuous constraint problem space may be defined.

PC Problem Space A PC problem space is a pair $\langle\langle X, D, C\rangle, f\rangle$ where $\langle X, D, C\rangle$ is a CCSP and f is the joint PDF of the PC random vector $\mathbf{X}$.

In this context, a PC event, hereafter referred as $\mathcal{H}$, is the feasible space of a CCSP $\langle X, D, C\rangle$.

4.2 *Multidimensional integration over a region*

In general the multidimensional integral to obtain the probability of a PC event cannot be easily computed, since it may have no closed-form solution or the event may establish a complex nonlinear integration boundary. The PC framework relies on continuous constraint programming to get a tight joint box cover $\langle \mathcal{H}_{\square}, \mathcal{H}_{\blacksquare} \rangle$ of the region of integration $\mathcal{H}$ and on Taylor models integration techniques to compute safe enclosures for the integrals over the obtained boxes.

Taylor Models A Taylor model of $g : \mathbb{R}^n \to \mathbb{R}$ inside an n-dimensional box B is a pair $\langle p, R\rangle$, where p is a polynomial and R is an interval satisfying, $\forall \boldsymbol{x} \in B$, $g(x) \in p(x) + R$. The order of the Taylor model is the degree of p.

A Taylor model of a function can be obtained from its multivariate Taylor expansion, using the interval evaluation of the highest order derivatives to compute rigorous bounds for the remainder.

Lemma 4.1 (From (Berz & Makino 1999)) *Given a Taylor model $\langle p, R\rangle$ of a function $g : \mathbb{R}^n \to \mathbb{R}$ inside an n-dimensional box B*:

$$[I]_{TM}(B, g) = \int_B p(x) dx + R\, vol(B) \ni \int_B g(x) dx$$

$[I]_{TM}$ can be used to obtain a sharp enclosure for the integral of a function over some region defined as a box (for more details about verified quadrature with Taylor models see (Goldsztejn, Cruz, & Carvalho 2014)).

Input: $\langle\langle X, D, C\rangle, f\rangle$: PC problem space; ε, δ: double
Output: I: interval;
1 $stop_\delta(\mathcal{H}_{\boxplus}) \equiv wid([P_{\mathcal{H}}](\mathcal{H}_{\boxplus}, f)) \leq \delta$;
2 $\mathcal{H}_{\boxplus} \leftarrow B\&P(\langle\{D\}, \varnothing\rangle, C, \varepsilon, stop_\delta, order_P)$;
3 **return** $[P_{\mathcal{H}}](\mathcal{H}_{\boxplus}, f)$;

Algorithm 2. *probEnclose*($\langle\langle X, D, C\rangle, f\rangle, \varepsilon, \delta$).

4.3 *Probability of a PC event*

The probability of a PC event can be enclosed by summing up the integral contributions of all the boxes from its joint cover, as follows.

Enclosure for the Probability of $\mathcal{H}$ Given a joint box cover $\mathcal{H}_{\boxplus} = \langle \mathcal{H}_{\square}, \mathcal{H}_{\blacksquare} \rangle$ of a PC event $\mathcal{H}$, an enclosure for the probability of $\mathcal{H}$ is given by[4]:

$$[P_{\mathcal{H}}](\mathcal{H}_{\boxplus}, f) = \sum_{B_i \in \mathcal{H}_{\blacksquare}} [I]_{TM}(B_i, f) + \sum_{B_i \in \mathcal{H}_{\square} \setminus \mathcal{H}_{\blacksquare}} [0] \uplus [I]_{TM}(B_i, f)$$

Notice that for non inner boxes, where the feasible region is some unknown subset of the box, the integral ranges from zero to the integral of the function over the box. In this case it is no longer worth computing a sharp (and more costly) enclosure and a lower order Taylor model can be used.

Since Taylor Models are used to compute safe enclosures for the integral over each box, the result is guaranteed to include the correct probability value.

Algorithm 2 computes bounds for the probability of a PC event. It uses the *B & P* algorithm where the $stop_\delta$ predicate imposes a specified accuracy δ for the probability enclosure computed over its joint box cover argument (line 1) and the $order_P$ function specifies that the box with highest uncertainty in its probability enclosure is chosen first.

For a PC problem space, with an associated PC event $\mathcal{H}$, *B & P* computes increasingly tighter covers of $\mathcal{H}$ until the intended accuracy δ for its probability is reached (line 2). The final joint box cover is used to compute an enclosure for the probability of $\mathcal{H}$[5] (line 3). The parametrization of *B & P* implies choosing boxes with higher uncertainty in their probability, in order to reduce such uncertainty. In practice, the accumulation of round-

[4]The union hull interval operator $\uplus$ returns the smallest interval containing both interval arguments.

[5]In fact, in the implementation of the algorithm, the probability enclosure is maintained and updated during the process, to check the stop criterion, and then returned in the end.

ing errors may prevent the algorithm to deliver the required accuracy. When this accuracy is too sharp, *B & P* may stop because there are no more eligible boxes (all the boxes are already small wrt ε) without achieving the required accuracy.

4.4 *Reliability assessment*

Reliability analysis can be used to analyze existing systems, thus being a significant support for those in charge of decision-making. In the following we describe how the PC framework can be used to obtain safe results on such problems.

For the formulation of a reliability assessment problem as a PC problem space, we distinguish between series and parallel systems.

Parallel and Series Systems as a PC problem space Consider a parallel system with an associated random vector $\boldsymbol{X} = \langle X_1, \ldots, X_n \rangle$ with joint PDF f_x defined in $\Omega_{\boldsymbol{X}} \subseteq \mathbb{R}^n$ and a set of k limit-state functions that define the failure event F as in (3). This system is modeled as a PC problem space, $\langle \langle X, D, C \rangle, f \rangle$, such that:

$$D \subseteq \Omega_{\boldsymbol{X}} \qquad X = \langle x_1, \ldots, x_n \rangle$$
$$C = \{g_i(x) \leq 0 : 1 \leq i \leq k\} \qquad f = f_{\boldsymbol{X}}(x)$$

Its probability of failure is $P_f = P(\mathcal{F}(\langle X, D, C \rangle))$ and its reliability is $P_s = 1 - P_f$.

The formulation of a series system as a PC problem space is adapted from the previous, where $C = \{g_i(x) \geq 0 : 1 \leq i \leq k\}$ and $\mathcal{F}(\langle X, D, C \rangle)$ defines the success event. So the computed probability $P_s = P(\mathcal{F}(\langle X, D, C \rangle))$ is the reliability of the system.

From these formulations, Algorithm 2 can be used to compute the probability of event $\mathcal{H} = \mathcal{F}(\langle X, D, C \rangle)$ and obtain enclosures for the reliability (or probability of failure) of series or parallel systems.

Notice that reliability problems do not impose bounds on the random variables, which is not possible to model in the PC framework, where $D \subseteq \Omega_{\mathbf{X}}$ must be a bounded box. Thus, to guarantee the safety of the computed probability enclosures when $D \subset \Omega_{\mathbf{X}}$, a small correction term must be added to such enclosure. This is done by computing $[P](\mathcal{D})$, an enclosure for the probability of event $\mathcal{D} = \mathcal{F}(\langle X, D, \{\} \rangle)$ and $[P](\boldsymbol{\Omega}_{\mathbf{X}} \backslash \mathcal{D}) = 1 - [P](\mathcal{D})$, an enclosure for the neglected probability. Then the term $[0] \uplus [P](\Omega_{\mathbf{X}} \backslash \mathcal{D})$ is added to the enclosure computed by Algorithm 2.

5 EXPERIMENTAL RESULTS

To illustrate the limitations of the classical techniques (FORM, SORM and Monte Carlo) described in Section 2.1, several examples of reliability assessment problems found in the literature are modeled as PC problem spaces. The algorithms were implemented over RealPaver 1.0 (Granvilliers & Benhamou 2006), and the experiments were carried out on an Intel Core i7 CPU at 2.4 GHz.

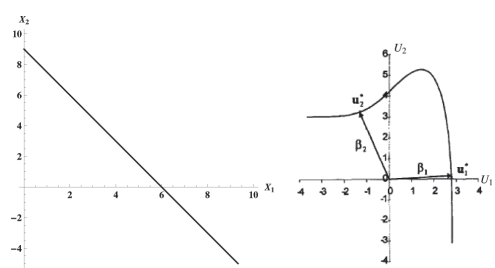
The results obtained with the classical approaches are compared with those computed with algorithm 2 with $\delta = 10^{-6}$, $\varepsilon = 10^{-15}$ and a Taylor order of 6 for inner boxes (and 1 otherwise), hereafter referred as PCTM. All the results obtained with the PCTM algorithm are presented after adding the correction term.

In the experiments, function *NProbability* (from *Mathematica* v9.0.0.0 Wolfram Research 2012)) with the default parametrization, is also used to compute the required probabilities as a complementary source of comparison. Although, in the proposed examples, all *Mathematica* estimates are within the enclosure computed by the PCTM algorithm, this is not the case in general (see (Carvalho, Cruz, & Barahona 2013) for some examples). Moreover different parameterizations provide different values. Although the differences might be small, *Mathematica* does not provide bounds for the errors.

The first example illustrates the non linearity induced in the limit-state function resulting from the transformation of a non Gaussian distribution into a standard normal distribution.

Example 5.1. Consider the reliability problem, originally introduced in Hohenbichler & Rackwitz 1981, with $\boldsymbol{X} = \langle X_1, X_2 \rangle$, joint PDF $f_{\mathbf{X}}(x_1, x_2) = (x_1 + x_2 + x_1 x_2) e^{-(x_1 + x_2 + x_1 x_2)}$ defined in $\Omega = [0, \infty] \times [0, \infty]$ and limit-state function $g(x_1, x_2) = 18 - 3x_1 - 2x_2$.

Although the limit-state function is linear in the original space, it becomes highly nonlinear and has two design points in the standard normal space, due to the strong non normality of the random variables. Figure 1 shows the limit-state function



(a) Linear limit-state. (b) $\boldsymbol{U} = T_1(\boldsymbol{X})$.

Figure 1. Linear limit-state in the original space and nonlinear in the standard normal space.

(a) in the original space and (b) in the standard normal space.

The problem is formulated as a PC problem space:

$$X = \langle x_1, x_2 \rangle \qquad D = [0,30] \times [0,30]$$
$$C = \{g(x_1, x_2) \le 0\} \qquad f = f_{\boldsymbol{X}}(x_1, x_2)$$

The bounds for D guarantee a negligible probability for the neglected Ω region, $[P](\Omega \backslash \mathcal{D}) \le 4.5 \times 10^{-11}$.

The results obtained with the classical approaches (from) and with the PCTM algorithm are shown in Table 1. It presents the approximations obtained by FORM and SORM methods when only one of the design points is considered and when both are considered for both transformations $T_1(\mathbf{X})$ and $T_2(\mathbf{X})$, described in (Hohenbichler & Rackwitz 1981). For Monte Carlo (MC) and PCTM algorithms this does not apply.

It is clear from Table 1 that the results obtained with FORM and SORM have a great variability, depending on the chosen configuration, and, except for one, are outside the safe enclosure computed by PCTM algorithm (in 0.12 seconds CPU time). Using *Mathematica* the obtained result (in 0.12 seconds CPU time) was 0.294486×10^{-2}.

The next example illustrates a nonlinear limit-state function where the original space is normal (although not standard normal).

Example 5.2. Consider the reliability problem from (Choi, Grandhi, & Canfield 2010), with $\boldsymbol{X} = \langle X_1, X_2 \rangle$, where $X_1 \sim \mathcal{N}(10,5)$ and $X_2 \sim \mathcal{N}(10,5)$ are independent random variables defined in $\Omega = \mathbb{R}^2$, and limit-state function $g(x_1, x_2) = x_1^4 + 2x_2^4 - 20$. The problem is formulated as a PC problem space:

$$X = \langle x_1, x_2 \rangle \qquad D = [-40,60] \times [-40,60]$$
$$C = \{g(x_1, x_2) \le 0\}$$
$$f = \frac{1}{50\pi} e^{-\frac{1}{2}\left[\left(\frac{x_1-10}{5}\right)^2 + \left(\frac{x_2-10}{5}\right)^2\right]}$$

The bounds for D guarantee a negligible probability for the neglected Ω region, $[P](\Omega \backslash \mathcal{D}) \le 2.8 \times 10^{-13}$.

The results obtained with the classical approaches (from (Choi, Grandhi, & Canfield 2010, pag. 132–136)) where two SORM versions are considered (see (Choi, Grandhi, & Canfield 2010, Chapter 4) for details) and with the PCTM algorithm are shown in Table 2.

The result obtained with FORM grossly overestimates the probability of failure. Those obtained with both versions of SORM are closer to the correct value, however are still far from the exact value. Simulation with Monte Carlo produces the result closer to the correct value with an 5.23% error. Using *Mathematica* the obtained result (in 1.17 seconds CPU time) was 0.185252×10^{-2}, which is within the enclosure computed by the PCTM algorithm (in 0.84 seconds CPU time).

The problems in the following example are found in (Sørensen 2004) to illustrate series and parallel systems.

Example 5.3. Consider the reliability assessment problems from (Sørensen 2004, Note 6) (series system) and (Sørensen 2004, Note 7) (parallel system), with $\boldsymbol{X} = \langle X_1, X_2 \rangle$, where X_1 and X_2 are independent standard normal random variables defined in $\Omega = \mathbb{R}^2$, and the limit state functions of Table 3.

Table 1. Probability of failure $\times 10^2$.

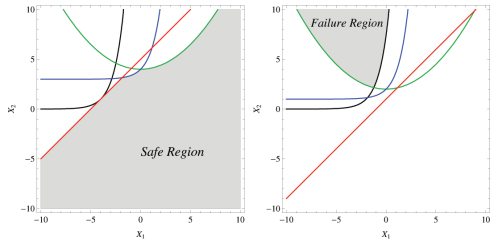
	u_1^* alone		u_2^* alone		u_1^* and u_2^*			
	FORM	SORM	FORM	SORM	FORM	SORM	MC	PCTM
$T_1(X)$	0.269	0.279	0.023	0.016	0.292	0.296		
$T_2(X)$	0.404	0.294	0.014	0.015	0.417	0.308	0.294	[0.294429, 0.294530]

Table 2. Probability of failure $\times 10^2$.

FORM	0.9005
SORM Breitung	0.2221
SORM Tvedt	0.2087
MC	0.1950
PCTM	[0.185162, 0.185263]

Table 3. Limit state functions.

	Series system	Parallel system
$g_1(x_1, x_2)$	$e^{x1} - x_2 + 3$	$e^{x1} - x_2 + 1$
$g_2(x_1, x_2)$	$x_1 - x_2 + 5$	$x_1 - x_2 + 1$
$g_3(x_1, x_2)$	$e^{x1+4} - x_2$	$e^{x1+2} - x_2$
$g_4(x_1, x_2)$	$0.1x_1^2 - x_2 + 4$	$0.1x_1^2 - x_2 + 2$



(a) Series system. (b) Parallel system.

Figure 2. Series and parallel systems.

Table 4. Probability of failure $\times 10^2$.

	Series system	Parallel system
SB	[0.02241, 0.05190]	[0.0762, 2.1692]
DB	[0.03516, 0.04091]	[0.1264, 0.2256]
PCTM	[0.031265, 0.031366]	[0.170314, 0.170415]

Figure 2 shows the limit-state functions and the safe/failure regions of these problems. The problems are formulated as PC problem spaces:

$$D = [-10,10] \times [-10,10] \qquad X = \langle x_1, x_2 \rangle$$

$$f = \frac{1}{2\pi} e^{-\frac{1}{2}(x_1^2 + x_2^2)}$$

$$C = \{g_i(x,y) \geq 0 : 1 \leq i \leq 4\} \quad \text{series system}$$

$$C = \{g_i(x,y) \leq 0 : 1 \leq i \leq 4\} \quad \text{parallel system}$$

In both problems 10 standard deviations around the mean value are assumed for the bounds of D, with $[P](\Omega \backslash \mathcal{D}) \leq 2.8 \times 10^{-13}$.

The results obtained with the classical approach for series and parallel systems analysis, where simple (SB) and Ditlevsen (DB) bounds are considered (see (Sørensen 2004, Notes 6 and 7) for details) and with the PCTM algorithm[6] are shown in Table 4.

We conclude that the simple bounds are too wide to be informative. The more accurate Ditlevsen bounds, for the series system, do not include the exact value in the safe enclosure computed by the PCTM algorithm (in 0.38 seconds CPU time). For the parallel system, they do include the safe enclosure computed by the PCTM algorithm (in 0.73 seconds CPU time) but are much wider. The results obtained with *Mathematica* were, for the series system, 0.0312962×10^{-2} (in 0.92 seconds CPU time) and, for the parallel system, 0.170394×10^{-2} (in 0.47 seconds CPU time).

[6]For the series system, the probability of failure was obtained from the reliability computed by the PCTM algorithm.

6 CONCLUSIONS AND FUTURE WORK

In this paper we propose to use the Probabilistic Continuous Constraints framework to deal with reliability assessment problems. Given its grounding on continuous constraint solving, this framework computes safe bounds for the reliability of series and parallel systems, contrary to classical approaches. The various kinds of approximations used by these approaches may turn the computed reliability value of little practical use, since they do not provide any bounds to the errors incurred. This is particularly significant in systems modeled by means of nonlinear constraints.

Moreover, the proposed framework, while guaranteeing the robustness of the computed values, does it very efficiently, being highly competitive when compared with *Mathematica*, that computes non-guaranteed results.

In the future the authors aim to extend the framework to address systems that are formulated as a combination of series and parallel components. Another interesting add-on would be the ability to model problems with a mixture of integer and continuous random variables, since these are an important class of problems appearing in science and engineering.

REFERENCES

Barranco-Cicilia, F., E.C.-P. de Lima, & L. Sudati-Sagrilo (2009). Structural Reliability Analysis of Limit State Functions With Multiple Design Points Using Evolutionary Strategies. *Ing. invest. y tecnol. 10*, 87–97.

Benhamou, F., F. Goualard, L. Granvilliers, & J. Puget (1999). Revising hull and box consistency. In *Procs. Int. Conf. on Logic Programming*, pp. 230–244. MIT Press.

Benhamou, F., D. McAllester, & P. van Hentenryck (1994). CLP (intervals) revisited. In *ISLP*, pp. 124–138. MIT Press.

Berz, M. & K. Makino (1999). New methods for high-dimensional verified quadrature. *Reliable Computing 5*, 13–22.

Breitung, K. (1984). Asymptotic Approximation for Multinormal Integrals. *J. Eng. Mech. 110*(3), 357–366.

Carvalho, E. (2012). *Probabilistic Constraint Reasoning*. Ph. D. thesis, Universidade Nova de Lisboa, Faculdade de Ciênciase Tecnologia.

Carvalho, E., J. Cruz, & P. Barahona (2013). Probabilistic constraints for nonlinear inverse problems. *Constraints 18*(3), 344–376.

Choi, S., R. Grandhi, & R. Canfield (2010). *Reliability-Based Structural Design*. Springer.

Eldred, M., B. Bichon, & B. Adams (2006). Overview of Reliability Analysis and Design Capabilities in DAKOTA. In *Workshop on Reliable Engineering Computing*, pp. 1–26.

Fiessler, B., H.-J. Neumann, & R. Rackwitz (1979). Quadratic limit states in structural reliability. *J. Engrg. Mech. Div. 105*, 661–676.

Goel, H., J. Grievink, P. Herder, & M. Weijnen (2002). Integrating reliability optimization into chemical process synthesis. Reliability Eng. and System Safety 78(3), 247–258.

Goldsztejn, A., J. Cruz, & E. Carvalho (2014). Convergence analysis and adaptive strategy for the certified quadrature over a set defined by inequalities. *J. of Comp. and Applied Math. 260*(0), 543–560.

Granvilliers, L. & F. Benhamou (2006). Realpaver: an interval solver using constraint satisfaction techniques. *ACM Trans. Math. Softw.* 32(1), 138–156.

Halder, A. & S. Mahadevan (1999). Probability, Reliability and Statistical Methods in Engineering Design. Wiley.

Halpern, J.Y. (2003). *Reasoning about Uncertainty*. MIT Press. Hasofer, A.M. & N.C. Lind (1974). Exact and invariant second-moment code format. *J. Engrg. Mech. Div.*

Hohenbichler, M. & R. Rackwitz (1981). Non-normal dependent vectors in structural safety. *J. Engrg. Mech. Div. 107*, 1227–1238.

Hohenbichler, M. & R. Rackwitz (1983). First-order concepts in system reliability. *Struct. Safety* (1), 177–188.

Huang, M., C. Chan, & W. Lou (2012). Optimal performance-based design of wind sensitive tall buildings considering uncertainties. *Comput. Struct. 98–99*, 7–16.

Kiureghian, A. & T. Dakessian (1998). Multiple design points in 1st and 2nd-order reliability. *Str. Safety 20*(1), 37–49.

Lhomme, O. (1993). Consistency techniques for numeric CSPs. In *Proc. of the 13th IJCAI*, pp. 232–238.

Melchers, R. (1999). *Structural Reliability Analysis and Prediction*. Civil Engineering Series. John Wiley & Sons.

Moore, R. (1966). *Interval Analysis*. Prentice-Hall, Englewood Cliffs.

Nataf, A. (1962). Remarks on a multivariate transformation. *Comptes Rendus de l'Academie des Sciences 225*(1), 42–43.

Nikolaidis, E., D. Ghiocel, & S. Singhal (2007). *Engineering Design Reliability Applications: For the Aerospace, Automotive and Ship Industries*. CRC Press.

Rosenblatt, M. (1952). Remarks on a multivariate transformation. *Ann. Math. Stat. 3*(23), 470–472.

Sam-Haroud, D. & B. Faltings (1996). Consistency techniques for continuous constraints. *Constraints 1*(1/2): 85–118.

Sørensen, J. (2004). Notes in Structural Reliability Theory.

Wolfram Research, I. (2012). *Mathematica Edition: Version 9.0*. Champaign, Illinois: Wolfram Research, Inc.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Structural reliability for containment of VVER 440/213 type

J. Králik
Faculty of Civil Engineering, Slovak University in Bratislava, Slovakia

P. Picca, F. Pierro, M. Giovannini & N. Zaccari
Enel Ingegneria & Ricerca S.p.a., Italy

P. Baumeister
Slovenské elektrárne a.s., Slovakia

ABSTRACT: The paper presents an application of the probabilistic analysis of structural resistance of the containment of a VVER 440/213. The evaluation is based on an extension of the smeared crack model developed on the basis of Kupfer's bidimensional failure criterion and implemented into ANSYS. The non-linear analysis is considered for the median values of the input data and the probabilistic analysis models the uncertainties of loads, material resistance and other modeling issues. Results show that the effects of thermal load are relevant mainly for the bubble condenser and at the interface between the floor of hermetic zone and the rooms beneath. A comparison of the performance of linear and non-linear analyses is also reported.

1 INTRODUCTION

The definition of the fragility curve for containment of a Nuclear Power Plant (NPP) generally represents a crucial step for the level 2 probabilistic safety assessment (PSA L2), where the probability of containment failure can be evaluated as the convolution of the fragility curve with the load curve (SSG-4). The assessment of the structural strength of the containment of a nuclear power plant has acquired even a greater importance in the framework of post-Fukushima stress tests where the assessment of the safety margin and off-design conditions.

The overpressure in the containment can arise after a loss-of-coolant accident initiating event or a progression of an accident to severe accident conditions (after primary depressurization). In such cases, the primary steam is released in the hermetic zone and expands from the reactor hall to the bubble condenser.

In the past, the calculation of the structural reliability for containment of the type of VVER 440/213 was carried out determining the probability density function for the ultimate pressure before leakage and rupture. These calculations were based both on linear and non-linear analysis, depending whether the update of the properties were considered in the modeling.

The present work analyses the impact of combination of pressure load with thermal load that can arise in extreme situations related to severe accident progression. For the purpose, a detailed finite-element analysis of the concrete structure is carried out with ANSYS software combined with the program CRACK (Králik 2009, 2013). In the following, the basis for the probabilistic evaluation of structural reliability are reviewed, considering the uncertainties connected with loads and material properties. In the result section, a comparison with linear evaluation is also reported.

2 STRUCTURAL MODEL OF THE CONTAINMENT

The NPP buildings with the reactor VVER 440/213 consists the turbine hall, middle building, reactor building and bubble condenser (Fig. 1).

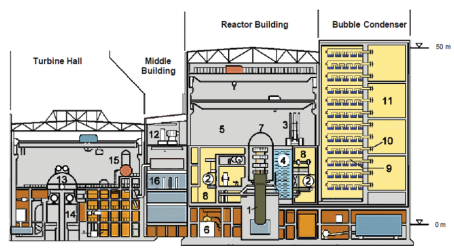


Figure 1. Section plane of the condenser containment.

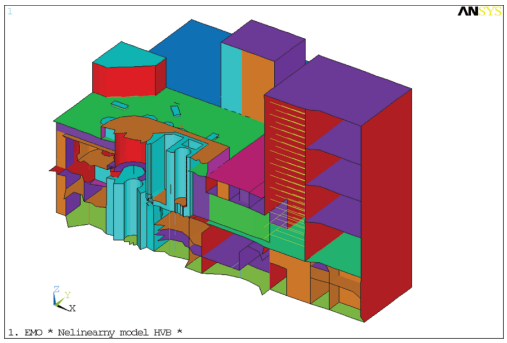


Figure 2. Calculation model of NPP VVER 440/213.

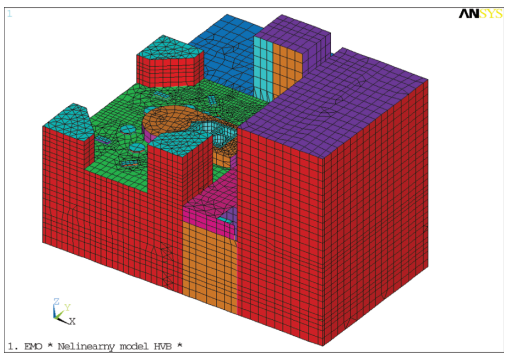


Figure 3. FEM model of NPP with reactor VVER440/213.

The building of the power block was idealized with a FEM model consisting of 28.068 elements with 104.287 DOF (Figs. 2 and 3).

3 DEFINITION OF LOADS AND BOUNDARY CONDITIONS

The definition of loads connected with the accident evolution is derived from an extreme scenario with a loss of primary coolant combined with the total loss of containment cooling (all means for hermetic zone heat removal are considered as not available, including external spraying of borated water). In such scenario, the environmental condition evolution in the long term is characterized by a combined pressurization and heating of the containment. An example of pressure evolution is reported in Figure 4; as for the temperature, while in a first approximation it can be considered as saturated in equilibrium with the temperature, in severe accident conditions the energetic contribution to heating from hydrogen recombination and explosion shall also be accounted.

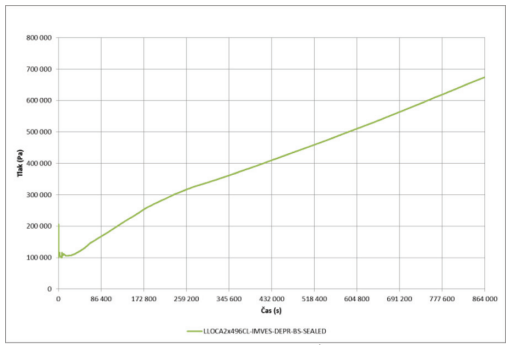


Figure 4. Pressure evolution (in kPa^{abs}) in the hermetic zone of a VVER 440/213 in an extreme scenario of total loss of containment heat removal.

The temperature boundary conditions are defined in accordance with the updated revision of reference temperature from the Slovak hydrometeorological institute (SHMU) and relevant standard STN EN 1991-1-5 NA. A return period of 10000 year is a reasonable choice for this type of evaluation. The lowest annual temperature where chosen as they correspond to the case where the thermal stress is maximized (i.e., largest heat flux at the external walls). An estimation for the ground temperature is consider in accordance with STN EN 1991-1-5 NA for defining the boundary conditions at the bottom of the hermetic zone, considering a simplified but conservative modeling for the rooms underneath.

A standard thermal model with convection and conduction is consider in ANSYS to model the temperature propagation in the containment structure due to internal and external thermal boundary conditions.

4 NON-LINEAR MODEL OF REINFORCED CONCRETE STRUCTURE

The theory of large strain and rate-independent plasticity is modeled using layered shell element SHELL181 from ANSYS library (Kohnke, 2008).

The vector of the displacement of the *l*th shell layer $\{u^l\} = \{u_x^l, u_y^l, u_z^l\}^T$ is approximated by the quadratic polynomial (Králik, 2009) in the form

$$\left\{u^l\right\} = \begin{Bmatrix} u_x^l \\ u_y^l \\ u_z^l \end{Bmatrix} = \sum_{i=1}^{4} N_i \cdot \begin{Bmatrix} u_{xi} \\ u_{yi} \\ u_{zi} \end{Bmatrix} + \sum_{i=1}^{4} N_i \cdot \frac{\zeta \cdot t_i}{2} \cdot \begin{bmatrix} a_{1,i} & b_{1,i} \\ a_{2,i} & b_{2,i} \\ a_{3,i} & b_{3,i} \end{bmatrix} \cdot \begin{Bmatrix} \theta_{xi} \\ \theta_{yi} \end{Bmatrix} \quad (1)$$

where N_i is the shape function for i-node of the 4-node shell element, u_{xi}, u_{yi}, u_{zi} are the motion of i-node, ζ is the thickness coordinate, t_i is the thickness at i-node, $\{a\}$ is the unit vector in x direction, $\{b\}$ is the unit vector in plane of element and normal to $\{a\}$, θ_{xi} or θ_{yi} are the rotations of i-node about vector $\{a\}$ or $\{b\}$.

In the elastic case, the stress-strain relations for the lth-layer are defined in the form

$$\{\sigma^l\} = [D_e^l]\{\varepsilon^l\} \tag{2}$$

where strain and stress vectors are as follows

$$\{\varepsilon^l\}^T = \{\varepsilon_x, \varepsilon_y, \gamma_{xy}, \gamma_{yz}, \gamma_{zx}\}, \{\sigma^l\}^T = \{\sigma_x, \sigma_y, \tau_{xy}, \tau_{yz}, \tau_{zx}\}$$

and the matrix of the material stiffness

$$[D_e^l] = \begin{bmatrix} B^l E_x^l & B^l \mu_{xy}^l E_x^l & 0 & 0 & 0 \\ B^l \mu_{xy}^l E_x^l & B^l E_y^l & 0 & 0 & 0 \\ 0 & 0 & G_{xy}^l & 0 & 0 \\ 0 & 0 & 0 & \dfrac{G_{yz}^l}{k_s} & 0 \\ 0 & 0 & 0 & 0 & \dfrac{G_{zx}^l}{k_s} \end{bmatrix} \tag{3}$$

where $B^l = (E_y^l)/(E_y^l - (\mu_{xy}^l)^2 E_x^l)$, E_x^l (versus E_y^l) is Young modulus of the lth-layer in the direction x (versus y), $G_{xy}^l, G_{yz}^l, G_{zx}^l$ are shear moduli of the lth-layer in planes XY, YZ and ZX; k_s is the coefficient of the effective shear area ($k_s = 1 + 0.2\,A/25t^2 \geq 1.2$), A is the element area, t is the element thickness. In the following sub-sections, various sources of non-linearity considered in the modeling of containment capacity are briefly reviewed.

4.1 *Geometric non-linearity*

If the rotations are large but the mechanical strains are small, then a large rotation approximation can be used in ANSYS (Kohnke, 2008).

The strain in the n-step of the solution can be computed from the relations

$$\{\varepsilon_n\} = [B_o][T_n]\{u_n\} \tag{4}$$

where $\{u_n\}$ is the deformation displacement, $[B_0]$ is the original strain-displacement relationship, $[T_n]$ is the orthogonal transformation relating the original element coordinates to the convected (or rotated) element coordinates. The convected element coordinate frame differs from the original element coordinate frame by the amount of rigid body rotation. Hence $[T_n]$ is computed by separating the rigid body rotation from the total deformation $\{u_n\}$ using the polar decomposition theorem.

4.2 *Material non-linearity*

The presented constitutive model is a further extension of the smeared crack model (Bažant et al., 2007; Červenka, 1985; Hinton and Owen, 1984; Hughes, 1984), as developed in (Králik, 2009). Following the experimental results (Červenka, 1985; Jerga and Križma, 2006) a new concrete cracking layered finite shell element was developed and incorporated into ANSYS (Králik, 2009). The processes of the concrete cracking and crushing are developed during the increasing of the load, whereas the concrete compressive stress f_c, the concrete tensile stress f_t and the shear modulus G are reduced after the crushing or cracking of the concrete (Kolmar, 1986).

The stress-strain relation, plotted in Figure 5, is defined following STN EN 1992-1-1 as

➲ Loading—compression region $\varepsilon_{cu} < \varepsilon^{eq} < 0$

$$\sigma_c^{ef} = f_c^{ef} \cdot \frac{k \cdot \eta - \eta^2}{1. + (k-2) \cdot \eta}, \quad \eta = \frac{\varepsilon^{eq}}{\varepsilon_c} \tag{5}$$

($\varepsilon_c \doteq -0.0022$, $\varepsilon_{cu} \doteq -0.0035$)

➲ Softening—compression region $\varepsilon_{cm} < \varepsilon^{eq} < \varepsilon_{cu}$

$$\sigma_c^{ef} = f_c^{ef} \cdot \left(1 - \frac{\varepsilon^{eq} - \varepsilon_c}{\varepsilon_{cm} - \varepsilon_{cu}} \right) \tag{6}$$

➲ The tension region $\varepsilon_t < \varepsilon^{eq} < \varepsilon_m$

$$\sigma_c^{ef} = f_t \cdot \exp(-2 \cdot (\varepsilon^{eq} - \varepsilon_t)/\varepsilon_{tm}) \tag{7}$$

($\varepsilon_t \doteq 0.0001$, $\varepsilon_{tm} \doteq 0.002$)

In the plane of principal stresses (σ_{c1}, σ_{c2}), the relation between the one-and bi-dimensional stresses state due to the plasticity function by Kupfer can be defined as follows (see also Fig. 6):

➲ Compression-compression

$$f_c^{ef} = \frac{1 + 3.65.a}{(1+a)^2} \cdot f_c, \quad a = \frac{\sigma_{c1}}{\sigma_{c2}} \tag{8}$$

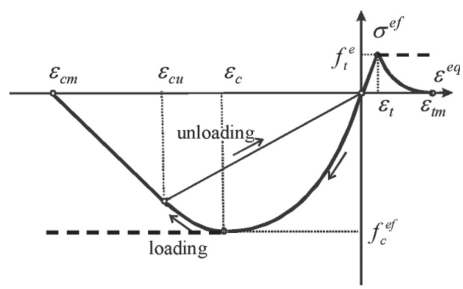


Figure 5. The concrete stress-strain diagram.

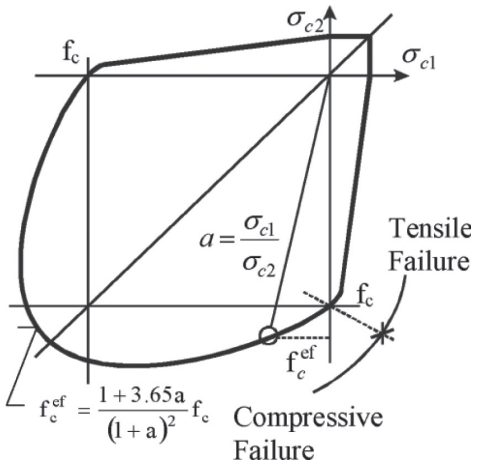


Figure 6. Kupfer's plasticity function.

➲ Tension-compression

$$f_c^{ef} = f_c \cdot r_{ec}, \quad r_{ec} = \left(1 + 5.3278\frac{\sigma_{c1}}{f_c}\right), \quad r_{ec} \geq 0.9 \quad (9)$$

➲ Tension-tension

$$f_t^{ef} = f_t \cdot r_{et}, \quad r_{et} = \frac{A + (A-1)\cdot B}{A \cdot B}, \quad B = K \cdot x + A,$$
$$x = \sigma_{c2}/f_c, \quad r_{et} = 1. \Leftrightarrow x = 0, \quad r_{et} = 0.2 \Leftrightarrow x = 1 \quad (10)$$

The shear concrete modulus G is defined for cracking concrete as in (Kolmar, 1986) in the form:

$$G = r_g \cdot G_o, \; r_g = \frac{1}{c_2}\ln\left(\frac{\varepsilon_u}{c_1}\right), \; c_1 = 7 + 333(p - 0.005),$$
$$c_2 = 10 - 167(p - 0.005) \quad (11)$$

where G_o is the initial shear modulus of concrete, ε_u is the strain in the normal direction to crack, c_1 and c_2 are the constants dependent on the ratio of reinforcing, p is the ratio of reinforcing transformed to the plane of the crack ($0 < p < 0.02$).

The crack in each layer of shell element is oriented perpendicular to the orientation of principal stresses. The membrane stress and strain vector depends on the direction of the principal stress and strain in each layer

$$\{\varepsilon_{cr}\} = [T_\varepsilon]\{\varepsilon\}, \quad \{\sigma_{cr}\} = [T_\sigma]\{\sigma\} \quad (12)$$

where $[T_\varepsilon]$, $[T_\sigma]$ are transformation matrices for the principal strain and stress in the direction θ in the layer.

The strain-stress relationship in the Cartesian coordinates can be defined as a function of the direction of the crack as:

$$[\sigma_{cr}] = [D_{cr}]\{\varepsilon_{cr}\} \text{ and } [\sigma] = [T_\sigma]^{\mathrm{T}}[D_{cr}][T_\varepsilon]\{\varepsilon\} \quad (13)$$

The stiffness matrix of the reinforced concrete for the lth-layer can be written in the following form

$$[D_{cr}^l] = [T_{c.\sigma}^l]^{\mathrm{T}}\left[D_{cr}^l\right]\left[T_{c.\varepsilon}^l\right] + \sum_{s=1}^{N_{rein}}\left[T_s^l\right]^{\mathrm{T}}\left[D_s^l\right]\left[T_s^l\right] \quad (14)$$

where $[T_{c.\sigma}]$, $[T_{c.\varepsilon}]$, $[T_s]$ are the transformation matrices for the concrete and the reinforcement separately, N_{rein} is the number of the reinforcements in the lth-layer.

After cracking the elasticity modulus and Poisson's ratio are reduced to zero in the direction perpendicular to the cracked plane, and a reduced shear modulus is employed. Considering the principal directions in the plane of the structure, the stress-strain relationship for the concrete lth-layer cracked is

$$\begin{Bmatrix}\sigma_1\\ \sigma_2\\ \tau_{12}\\ \tau_{13}\\ \tau_{23}\end{Bmatrix}_l = \begin{bmatrix}0&0&0&0&0\\ 0&E&0&0&0\\ 0&0&G_{12}^{cr}&0&0\\ 0&0&0&G_{13}^{cr}&0\\ 0&0&0&0&G_{23}^{cr}\end{bmatrix}_l \begin{Bmatrix}\varepsilon_1\\ \varepsilon_2\\ \gamma_{12}\\ \gamma_{13}\\ \gamma_{23}\end{Bmatrix}_l \quad (15)$$

where the shear modulus are reduced by the coefficient of the effective shear area k_s and parameter r_{g1} by Kolmar (11) as follows:

$$G_{12}^{cr} = G_o \cdot r_{g1}, \quad G_{13}^{cr} = G_o \cdot r_{g1}, \quad G_{23}^{cr} = G_o / k_s$$

When the tensile stress in the 2nd direction reaches the value f_t', the latter cracked plane perpendicular to the first one is assumed to occur and the stress-strain relationship becomes:

$$\begin{Bmatrix}\sigma_1\\ \sigma_2\\ \tau_{12}\\ \tau_{13}\\ \tau_{23}\end{Bmatrix}_l = \begin{bmatrix}0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&G_{12}^{cr}/2&0&0\\ 0&0&0&G_{13}^{cr}&0\\ 0&0&0&0&G_{23}^{cr}\end{bmatrix}_l \begin{Bmatrix}\varepsilon_1\\ \varepsilon_2\\ \gamma_{12}\\ \gamma_{13}\\ \gamma_{23}\end{Bmatrix}_l \quad (16)$$

where the shear moduli are reduced by the parameter r_{g1} and r_{g2} by Kolmar in Eq. (11) as follows:

$$G_{12}^{cr} = G_o \cdot r_{g1}, \quad G_{13}^{cr} = G_o \cdot r_{g1}, \quad G_{23}^{cr} = G_o r_{g2}.$$

The cracked concrete is anisotropic and these relations must be transformed to the reference axes *XY*. The simplified averaging process is more convenient for finite element formulation than the singular discrete model. A smeared representation for the cracked concrete implies that cracks are not discrete but distributed across the region of the finite element. The smeared crack model used in this work is based on the assumption that the field of multiple micro-cracks is created (Červenka, 1985). The validity of this assumption is determined by the size of the finite element, hence its characteristic dimension $L_c = \sqrt{A}$, where A is the element area (versus integrated point area of the element).

5 NON-LINEAR DETERMINISTIC ANALYSIS

The critical sections of the structure are determined on the basis of the deterministic non-linear analysis. The resistance of these critical sections is considered taking into account the design values of material characteristics and loads. The combination load and design criteria is considered for the Beyond Design Basic Accident (BDBA) state in accordance with the international standard (IAEA, 2010).

The leakage condition is connected to the expansion of cracking, which is here linked to the assumption of constant failure energies G_f =*const* in the form

$$G_f = \int_0^{\infty} \sigma_n(w)\, dw = A_G \cdot L_c, \quad w_c = \varepsilon_w .\, L_c \tag{17}$$

where w_c is the width of the failure, σ_n is the stress in the concrete in the normal direction, A_G is the area under the stress-strain diagram of concrete in tension. Concrete modulus for descend line of stress strain diagram in tension (crushing) can be described according to (Červenka, 1985) as a function of the failure energies in the form

$$E_{c,s} = \frac{E_c}{1-\lambda_c}, \quad \lambda_c = \frac{2G_f E_c}{L_c \cdot \sigma_{\max}^2} \tag{18}$$

where E_c is the initial concrete modulus elasticity, σ_{max} is the maximal stress in the concrete tension. From relation in (18), it can be proven that the characteristic dimension of element must satisfy the following condition:

$$L_c \le \frac{2G_f E_c}{\sigma_{\max}^2} \tag{19}$$

The characteristic dimension of the element is determined by the size of the failure energy of the element. The CEB-FIP Model Code (1991) define the failure energies G_f [N/mm] depending on the concrete grades and the aggregate size d_a as follows

$$G_f = \left(0.0469 d_a^2 - 0.5 d_a + 26\right)\left(f_c\,/10\right)^{0,7} \tag{20}$$

The limit of damage at a point is controlled by the values of the so-called crushing or total failure function F_u. The modified Kupfer's condition for the *l*th-layer of section is following

$$F_u^l = \sqrt{\beta(3J_{\varepsilon 2}) + \alpha I_{\varepsilon 1}} - \varepsilon_u = 0, \tag{21}$$

where $I_{\varepsilon 1}$, $J_{\varepsilon 2}$ are the strain invariants, and ε_u is the ultimate total strain extrapolated from uniaxial test results ($\varepsilon_u = 0.002$ in the tension domain, or $\varepsilon_u = 0.0035$ in the compression domain), α, β are the material parameters determined from the Kupfer's experiment results (i.e., $\beta = 1.355$, $\alpha = 0.355\varepsilon_u$).

The failure function of the whole section will be obtained by the integration of the failure function through to the whole section in the form

$$F_u = \frac{1}{t} \cdot \int_0^t F_u^l\left(I_{\varepsilon 1}; I_{\varepsilon 2}; \varepsilon_u\right) dz = \frac{1}{t} \sum_{l=1}^{N_{lay}} F_u^l\left(I_{\varepsilon 1}; I_{\varepsilon 2}; \varepsilon_u\right) t_l \tag{22}$$

where t_l is the thickness of the *l*th-shell layer, t is the total shell thickness and N_{lay} is the number of layers. The failure state of the reinforced concrete structure is determined by the maximum strain ε_s of the reinforcement steel in the tension area ($\max(\varepsilon_s) \le \varepsilon_{sm} = 0.01$) and by the maximum concrete crack width w_c ($\max(w_c) \le w_{cm} = 0.3\,\text{mm}$).

In the present analysis, two critical areas are identified, namely the walls and the top plate of the bubbler tower building. The tension forces and the bending moments are concentrated along of the middle section of the wall. The difference between the interior end the exterior temperature has the significant influences to the peak strain in the structures. Based on the non-linear analysis of the containment resistance for median values of the material properties and failure function in Eq. (22) the mean value of the critical overpressure is above 350 kPa^g and the maximal strain

is lower than 0.002 in the middle plane of the reinforced concrete panel. The cracking process ($\varepsilon_1 \geq \varepsilon_t \doteq 0.0001$) at any layers of the section of the reinforced concrete is not experienced for overpressure below 250 kPa^g, hence as described in next section the only failure mode of interest in the load range under analysis is the leakage (catastrophic rupture is excluded).

6 PROBABILISTIC ASSESSMENT

After the identification of the critical sections using deterministic FEM calculation, the probability of the containment failure for the critical structure areas are considered for the various level of the overpressure. Most problems concerning the reliability of building structures are defined today as a comparison of two stochastic values, loading effects E and the resistance R, depending on the variable material and geometric characteristics of the structural element (Haldar and Mahadevan, 2000; Králik, 2009, 2013; Bažant et al., 2007; Kala, 2011; Novák et al., 2003). The variability of those parameters is characterized by the corresponding functions of the probability density $f_R(r)$ and $f_E(e)$.

The probabilistic definition of the reliability condition is of the form:

$$RF = g(R,E) = R - E \geq 0 \tag{23}$$

where $g(R,E)$ is the reliability function.

The probability of failure can be defined by the simple expression

$$P_f = P\left[R < E\right] = P\left[(R-E) < 0\right] \tag{24}$$

The reliability function RF can be expressed generally as a function of the stochastic parameters X_1, X_2 to X_n, used in the calculation of R and E.

$$RF = g(X_1, X_2, ..., X_n) \tag{25}$$

The failure function $g(\{X\})$ represents the condition of the reliability, which can be either an explicit or implicit function of the stochastic parameters. $g(\{X\})$ can be single (defined on one cross-section) or complex (defined on several cross-sections, e.g., on a complex finite element model).

In the case of simulation methods the failure probability is calculated from the evaluation of the statistical parameters and theoretical model of the probability distribution of the reliability function $Z = g(X)$. The failure probability is defined as the best estimate on the basis of numerical simulations in the form

$$p_f = \frac{1}{N}\sum_{i=1}^{N} I\left[g(X_i) \leq 0\right] \tag{26}$$

where N in the number of simulations, $g(\cdot)$ is the failure function, $I[\cdot]$ is the characteristic function with value 1, if the condition in the square bracket is fulfilled, and 0 otherwise.

The semi-probabilistic method is applied for the evaluation of the containment fragility and the propagation of uncertainty is carried out as detailed in next section.

7 UNCERTAINITIES OF THE INPUT DATA

Among the various simulation methods for uncertainty propagation, the RSM (Response Surface Method) approximation is considered in this paper. The RSM method generates the explicit performance function for the implicit or complicated limit state function. The RSM method is based on the assumption that it is possible to define the dependency between the variable input and the output data through the approximation functions in the following form:

$$Y = c_o + \sum_{i=1}^{N} c_i X_i + \sum_{i=1}^{N} c_{ii} X_i^2 + \sum_{i=1}^{N-1}\sum_{j>i}^{N} c_{ij} X_i X_j \tag{27}$$

where c_o is the index of the constant member; c_i are the indices of the linear member and c_{ij} the indices of the quadratic member determined using the regression analysis after calculating the response (here based on 5 structural analysis corresponding to different pressure loads). Approximate polynomial coefficients are given from the condition of the error minimum, usually by the "Central Composite Design Sampling" (CCD) method or the "Box-Behnken Matrix Sampling" (BBM) method (Kohnke, 2008).

The uncertainties on the input data are set in accordance with the standard requirements (see Table 1).

Table 1. Probabilistic model of the input data.

	Quantities		Histograms		
Input data	Charact. value	Variable value	Type	Mean (μ)	Deviation σ [%]
Dead load	G_k	g_{var}	*N*	1	10
Live load	Q_k	q_{var}	*Beta*	0.643	22.6
Pressure	P_k	p_{var}	*N*	1	8
Temper.	T_k	t_{var}	*Beta*	0.933	14.1
Model	E_k	e_{var}	*N*	1	5
Resist.	R_k	r_{var}	*N*	1	5

The action effect E are calculated considering the uncertainties of the input data:

$$E = G_k g_{\text{var}} + Q_k q_{\text{var}} + P_k p_{\text{var}} + T_k t_{\text{var}} \tag{28}$$

where the resistance R can be written as follows:

$$R = R_k r_{\text{var}} \tag{29}$$

8 EVALUATION OF THE FRAGILITY CURVE

The PSA approach to the evaluation of probabilistic pressure capacity involves limit state analyses. The limit states represent the ensemble of possible failure modes of the confinement functions. In principle, containment failure may be interpreted as incipient leakage (which may be a small controlled leak) or a large catastrophic break. The median capacity of a given failure mode is typically dependent on several factors, including material properties, modelling assumption and failure criteria. Considerable uncertainty and variability may be introduced in these factors and should be properly accounted for in the probabilistic overpressure fragility evaluation. To incorporate the uncertainty and variability in the formulation, the pressure capacity for each failure mode is represented as a random variable with a lognormal distribution.

The first step of a probabilistic evaluation is the identification of potential failure modes. Once the potential failure modes are identified, failure criteria are estimated from the median capacities. For each failure mode, the median capacities are to be evaluated by conducting independent limit state analyses using the specific failure criteria with the application of temperature, pressure and dead load.

In the present work, the probability of the containment failure is determined for the critical sections on the basis of the non-linear deterministic analysis of the containment for the various level of the overpressure Δp = 250, 300, 350, 400, 450 kPa^g. No catastrophic containment rupture at this pressure are evidenced, hence only potential failure mode considered here is the leakage. The function of the failure was considered as in Eqs. (21) and (22) and 10^6 Monte Carlo simulations are carried out in program FReET (Novák et al., 2003). The probability of containment failure is calculated from the probability of the reliability function RF in the form:

$$P_f = P(RF < 0) \tag{30}$$

where the reliability condition RF is defined depending on a concrete failure condition in Eq. (26)

$$RF = 1 - F_u\,(\mathrm{I}_{\varepsilon 1};\, J_{\varepsilon 2};\, \varepsilon_u)/\varepsilon_u, \tag{31}$$

where the failure function $F_u(.)$ was considered in the form of Eq. (23). As an example, Figure 7 shows the probability density function for a section at the bottom level of the bubble condenser with overpressure corresponding to 5% probability of failure.

A comparison of the linear and non-linear results is provided in Table 2, where the increase in the resistance connected with non-linear evaluation for different quantile is shown. The advantage of non-linear methodology is particularly evident at low probability, with resistance increase above 25% (i.e., non-linear estimation of containment capacity for the given quantile is more than ¼ higher than the linear estimation).

A comparison of strains from the linear and non-linear solution is reported in Figures 8 and 9. As expected, in comparison with the linear model, strains increase in the non-linear solution, whereas it can be shown that corresponding non-linear stresses decrease.

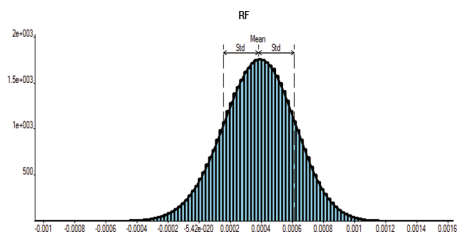


Figure 7. Density of the failure function RF at bottom level of the bubbler tower plate with overpressure corresponding to 5% probability of failure.

Table 2. Comparison of non-linear versus linear results (% increase in resistance).

Quantiles	Variation non-linear vs linear
5th	+25%
10th	+38%
20th	+12%
50th	+6%

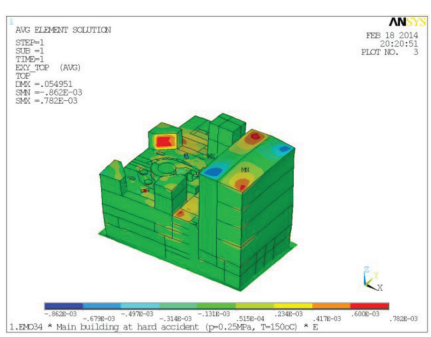


Figure 8. Strain deformation from the linear analysis.

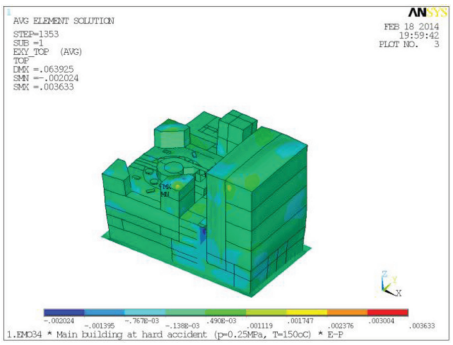


Figure 9. Strain deformation from the non-linear analysis.

9 CONCLUSIONS

The probability analysis of the loss of the concrete containment integrity is evaluated in a range of overpressure from 250 kPa^{g} to 500 kPa^{g} using the non-linear solution of the static equilibrium problem, considering both geometric and material non-linearity of the reinforced concrete. The non-linear analyses are performed in the CRACK program, which was developed by one of the Authors and implemented into the ANSYS system (Králik, 2009, 2013). The uncertainties of the loads level (temperature, dead and live loads), the material model of the composite structure (concrete cracking and crushing, reinforcement) and other influences following from the inaccuracy of the calculated model and the numerical methods are taken into account in the Monte Carlo simulations (Králik, 2009). The reliability function RF is defined in dependency on the failure function F_u ($I_{\varepsilon 1}$; $J_{\varepsilon 2}$; ε_u) for requirements of the PSA analysis in the form of Eq. (23). The analysis confirms that even for the combined case of temperaturee and pressure loads the probability of the loss of the concrete containment integrity is significantly below 1% for a load of 250 kPa^{g} (350 kPa^{abs}).

ACKNOWLEDGEMENT

The project was performed in the framework of the contract no. 4600009153 with Slovenské elektrárne a.s. The theory of the non-linear probabilistic analysis was developed in the framework of the VEGA grant project (VEGA 1/1039/12).

REFERENCES

ACI 349-90, 1990. "Code Requirements for Nuclear Safety Related Concrete Structures", American Concrete Institute, Detroit.

Bažant, Z.P. Pang, S.D. Vořechovský, M. and Novák. D. 2007. Energetic-statistical size effect simulated by SFEM with stratified sampling and crack band model. International Journal for Numerical Methods in Engineering (Wiley), 71(11):1297–1320, Rep. Dept. of Civil Eng., Northwestern University, Evanston, Illinois.

BNSI, 2006. Requirements for the study of PSA, BNSI.4.2.

CEB-FIP Model Code 1990, Design Code, Thomas Telford, ISBN 0727716964.

Červenka, V., 1985. Constitutive Model for Cracked Reinforced Concrete, ACI Journal 82, 877.

ENV 1992-1-1. Eurocode 2: Design of Concrete Structures, Part 1, Brussels: CEN 1992.

ENV 1992-1-2. Eurocode 2: Design of Concrete Structures—Part 1–2 Fire Résistance of Concrete Structures, CEN 1997.

Haldar, A. and Mahadevan, S., 2000. Probability, Reliability and Statistical Methods in Engineering Design, John Wiley & Sons, New York.

Hinton, E. and Owen, D.R.J., 1984. Finite Element Software for Plates and Shells, DCE University College Swansea U.K., Pineridge Press Swansea.

Hughes, T.J.R., 1984. Numerical Implementation of Constitutive Models: Rate-Independent Deviatoric Plasticity, Theoretical Foundation for Large-Scale Computations for Non-linear Material Behavior, eds. S. Nemat-Nasser, R.J. Asaro, G.A. Hegemier, Martinus Nijhoff Publishers, Dordrecht.

IAEA-SSG-4, 2010. Development and Application of Level 2—Probabilistic Safety Assessment for Nuclear Power Plants.

JCSS 2011. JCSS Probabilistic Model Code. Zurich: Joint Committee on Structural Safety. <www.jcss.byg.dtu.dk>.

Jerga, J. and Križma, M., 2006. Assessment of Concrete Damage, Building Research Journal 54, p. 211.

Kala, Z., 2011. Sensitivity analysis of steel plane frames with initial imperfections, Engineering Structures, 33, 8, pp. 2342–2349.

Kohnke, P., 2008. ANSYS, Theory, SAS IP Inc. Canonsburg.

Kolmar, W., 1986. Beschreibung der Kraftuebertragung ueber Risse in nichtlinearen Finite-Element-Berechnungen von Stahlbeton-tragwerken, PhD Thesis, T.H. Darmstadt, Darmstadt.

Králik, J., 2009. Safety and Reliability of Nuclear Power Buildings in Slovakia. Earthquake-Impact-Explosion. Monograph. Published by STU Bratislava, 307pp. ISBN 978-80-227-3112-6.

Králik, J., 2013. Non-linear Probabilistic Analysis of the Reinforced Concrete Structure Failure of a Nuclear Power Plant Considering Degradation Effects. In: Applied Mechanics and Materials Vols. 249–250 (2013) pp 1087–1098, © Trans Tech Publications, Switzerland, doi:10.4028/www.scientific.net/AMM.249-250.1087.

Novák, D. Vořechovský, M. Rusina, R., 2003. Small-sample Probabilistic Assessment—software FReET, ICASP 9, 9th Inter. Conf. on Applications of Statistics and Probability in Civil Engineering, San Francisco, USA, July 6–9, pp. 91–96.

STN ENV 1991-1-5 NA, 1997. Actions on structures—Part 1–5: General actions—Thermal actions.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability updating based on monitoring of structural response parameters

B.J. Leira
Department of Marine Technology, Trondheim, Norway

ABSTRACT: Short- and long-term aspects related to measurement of structural response parameters are addressed. Two specific examples of such measurements are considered for the purpose of illustration as well as to focus the discussion. These examples are taken from the petroleum industry (monitoring of riser response) and from the shipping industry (monitoring of ice-induced strains in a ship hull). Similarities and differences between the two cases are elaborated with respect to which are the most relevant mechanical limit states. Furthermore, main concerns related to the inherent reliability levels both with respect to extreme response and accumulated damage are highlighted.

1 INTRODUCTION

What is the benefit of monitoring structural response parameters? This question is generally addressed within the framework of so-called structural health monitoring which has received increasing attention and accordingly also attracted significant research efforts during the last decades.

The main objective of the present paper is to address the short- and long-term benefits of measurements/monitoring of structural response. Two specific examples are considered in order to focus the discussion: The first example deals with monitoring of the angular components at the lower flex joint of a marine drilling riser, while the second example is concerned with measurement of strains that are induced by ice loading on a ship hull.

There are usually multiple objectives associated with measurement of structural response processes and parameters. One such objective is frequently to monitor "the conditions" (or performance indicators) on-line such that counteractive measures can be activated when a critical threshold is reached. A second objective can be to perform extrapolation of key parameter values into the future in order to estimate when a critical condition will be reached. A third objective is related to the long-term learning process, i.e. to gain improved understanding of structural behavior as well as updating of the calculation models that are applied. Hence, an overarching objective is to provide a tool that may serve to supply basic information for the purpose of decision support in a wide sense. This applies both to the short-term and long-term time horizons.

In relation to updating of the applied calculation models, possible observed deviations between the measured and computed response implies that the calculation model needs to be revised. Such a revision can in some cases consist of more than a pure updating of particular parameters in the sense that the whole analysis framework needs to be upgraded.

An important issue in relation to how the measurements are processed is also which type of limit state that is critical. For the case that the fatigue limit state is anticipated to be the dominant one, the accumulated effects caused by a sequence of short-term stationary conditions is estimated. Prediction of the time until the critical threshold is reached will be the "performance measure". On the other hand, if the extreme response within a short-term condition (with a duration of a few hours) could possibly exceed the critical level, response prediction within a much shorter time horizon will be required.

These issues are highlighted in the following. The presented results which are obtained from measurements and calculated response are mainly based on the following sources: Stange (2013), Stange and Leira (2013), Suyuthi (2013) and Suyuthi et. al. (2012a, 2012b, 2013).

2 MONITORING OF RISER ANGLES FOR ASSESESSMENT OF WELLHEAD FATIGUE

2.1 *General*

The first example is related to the issue of wellhead fatigue during offshore drilling. This potential

failure mode has been increasingly focused upon during the last decade. There are multiple reasons for this increasing concern, such as: (i) The specific values which were assumed for the design parameters during initial design may no longer apply. (ii) The size and weight of the Blow-Out Preventers (BOPs) that are being applied have steadily been increasing. (iii) Larger surface vessels which operate in more and more hash weather are put into operations. (iv) For each well, there are more BOP days than assumed during initial design. Accordingly, it does not come as a surprise that well-head fatigue and the associated potential failure modes are coming strongly into focus.

Extreme response on the other hand is (at least in principle) taken care of: For angles exceeding a certain level, automatic emergency disconnect of the riser from the BOP is assumed to occur. Such a disconnect can be initiated e.g. by a drift-off or a drive-off of the surface vessel which frequently is associated with failure of the positioning system (e.g., errors related to the GPS-measurements). This implies that extreme loading which will endanger the integrity of the well-head can be disregarded (if the automatic disconnect system is activated).

Monitoring of the riser angles will also provide guidance in relation to when a manual disconnect action will need to be initiated in the case that the automatic emergency disconnect should fail. The time scale associated with such an operation is quite short, i.e. of the order of minutes.

Assuming that extreme loading is properly taken care of, the fatigue limit state comes into focus for all the mechanical components of the system. The riser itself can be inspected at regular intervals after retrieval when the drilling operation is completed. This implies that the condition of the permanently installed seabed components are of most concern as these cannot easily be inspected. In particular, estimation of the accumulated fatigue damage at the well-head is of key importance.

2.2 *The measurement system*

A schematic layout of the marine drilling riser is shown in Figure 1. The riser is attached to an Aker H-3 rig at a water depth of 325 m in the North Sea. The interface between the local and global analysis models are at the transition between the top of the wellhead and the lower face of the BOP.

The components of the instrumentation system are shown in Figure 2. The two orthogonal components of the riser angles at the Lower Flex Joint (LFJ) are measured by means of Inertial Measurement Units (IMU). Based on the measured angles, the loads which are acting on the wellhead can be estimated by introducing a local stress analysis model (i.e., by application of a Finite Element representation).

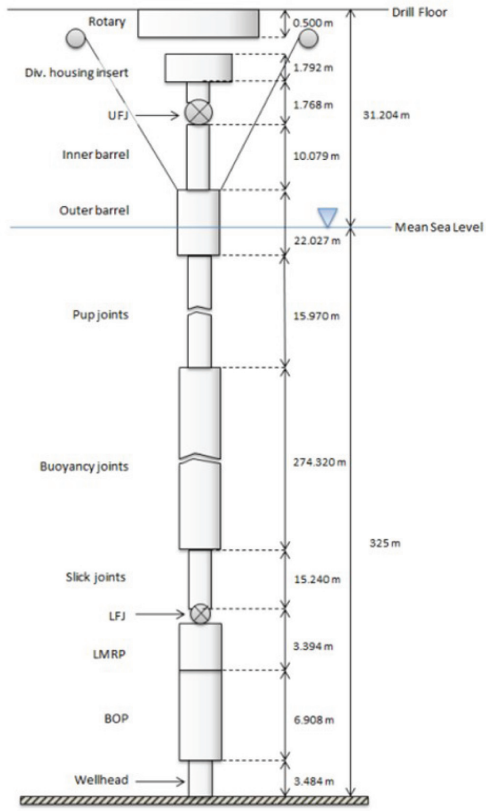


Figure 1. Basis for numerical riser model, Stange (2012).

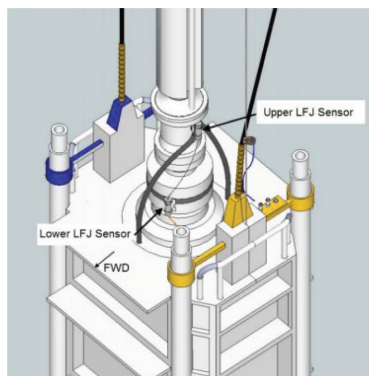


Figure 2. Overview over IMU location at the Lower Marine Riser Package (LMRP), from Stange (2012).

This is shown schematically in Figure 3 where the tension, bending moment and shear force are indicated (for the case of a 2D load-effect representation). These force components are

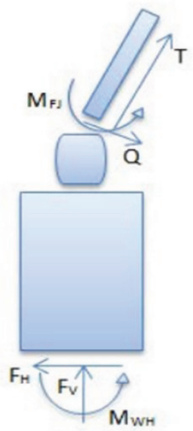


Figure 3. Simplified model of forces which are acting at the wellhead datum.

first transformed to force and bending moment components at the interface between the BOP and the wellhead. A local model of the well-head can subsequently be applied. Clearly, a more comprehensive model which comprises both the wellhead and the BOP can also be applied if this is required e.g. based on relative flexibility concerns.

An example of a measurement sequence for the two riser angle components is shown in Figure 4(a). A level plot of the histogram which represents the relative time the angular process spends in each square block is shown in Figure 4(b). It is found that a bivariate Gaussian model provides an adequate analytical model for the histogram.

In Figure 5, a number of projection planes for the angular process are indicated by straight lines. This will serve for the purpose of estimating the fatigue damage contributions from different directions. The cycle histogram can be established for each of these directions and subsequently the corresponding contribution to the well-head fatigue damage can be established.

2.3 *Comparison between full-scale measurements and numerical simulations*

By computing the resulting total angle for each of the blocks in Figure 4(b), a "one-dimensional" cycle distribution can be established for the angle range. The result is shown in Figure 6.

The frequency distribution of the response process components is also of significant interest. The response spectral densities for the total angle are shown in Figure 7 (a), (b) and (c) for three consecutive hours. It is seen that for the first two hours the frequency distribution is quite similar with two main peaks within two distinctive frequency

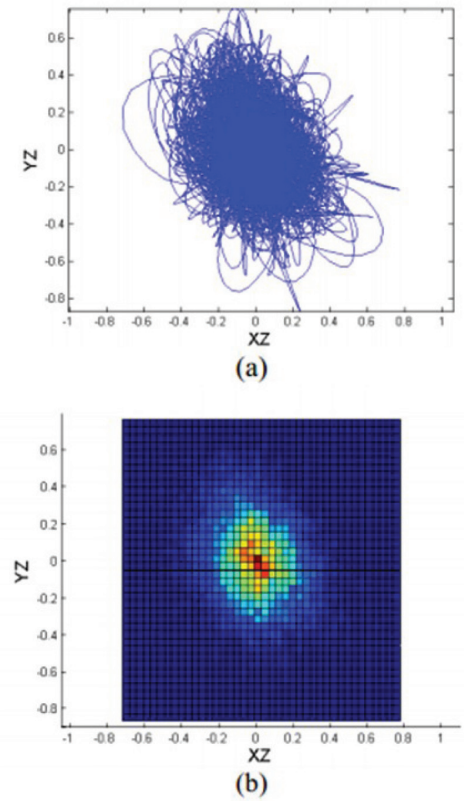


Figure 4. Angular response distribution.

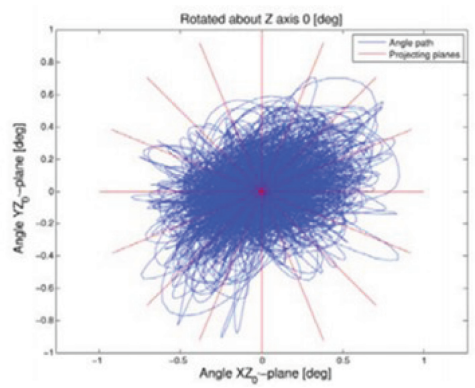


Figure 5. Projection planes for registration of angular response.

intervals. However, for the third hour there is a pronounced shift with the main peak being located at very low frequencies while the secondary small peak is located within the same frequency band as the main peak of the first two hours.

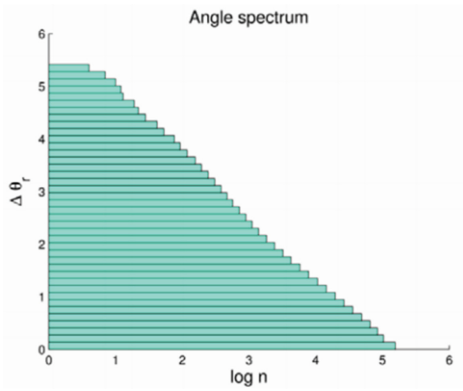


Figure 6. Histogram of angular cycles based on full-scale measurements.

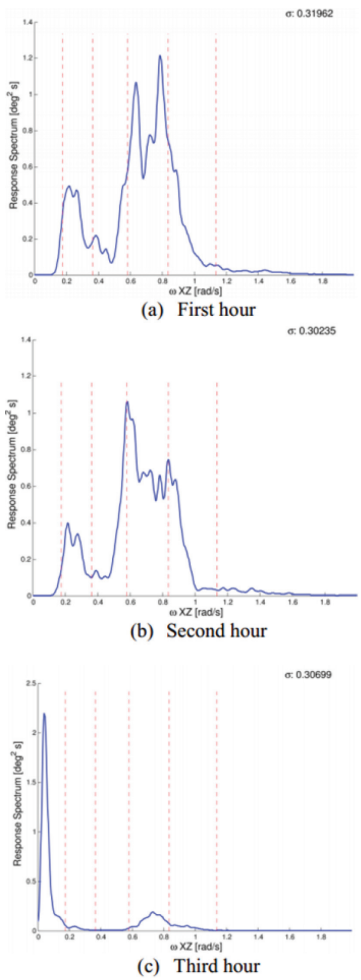


Figure 7. Spectral densities based on three consecutive one-hour periods of full-scale measurements.

The long-term distribution of angular cycles which is based on numerical simulations by application of the computer program Riflex, Marintek (1995) is shown in Figure 8. A fitted Weibull distribution is also shown. It is seen that there is a cut-off at a certain angle range (i.e. the very high amplitudes with a low number of cycles are missing as compared to the results in Figure 6).

This is more clearly seen by comparing the cycle distributions corresponding to Figure 6 and Figure 8 in the same graph, see Figure 9. The deviation for the highest cycle ranges are clearly observed. As the number of cycles within this range is very low, this is an indication that low-frequency response energy (e.g. due to slow-drift motion) is missing in the simulations.

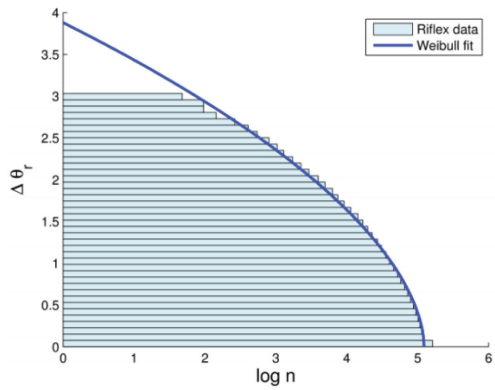


Figure 8. Histogram of angular cycles based on numerical simulations. Fitted Weibull distribution shown as blue line.

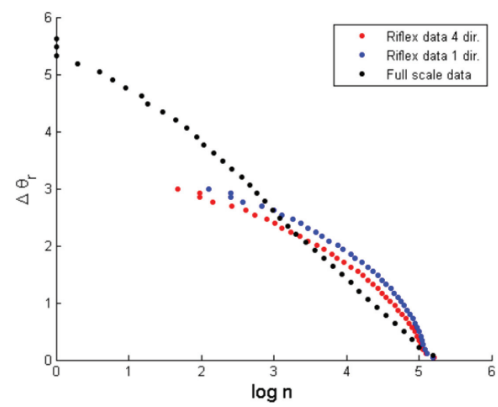


Figure 9. Comparison between long-term cycle distributions of riser angle which are estimated from measurements (black dots) versus numerical calculations (blue and red dots).

In order to investigate this in more detail, the computed response spectral densities are shown in Figure 10 for the two respective angular components. There are two-peaks in the spectral density also for this case for the case that the so-called Torsethaugen spectral model is applied. As observed, there is no response at very low-frequencies, which is due to slow-drift motion not being included in the analyses.

A more compact comparison between measured and calculated response is achieved by comparing the standard deviation of the angular response. The results in Figure 11 provide as comparison as a function of the mean heading direction. The straight horizontal lines correspond to the measured response with the middle line corresponding to the mean value and the upper and lower lines represent the 95 percent confidence interval.

For the computed response, a number of different cases are considered. These differ with respect to the type of wave spectral density that is applied

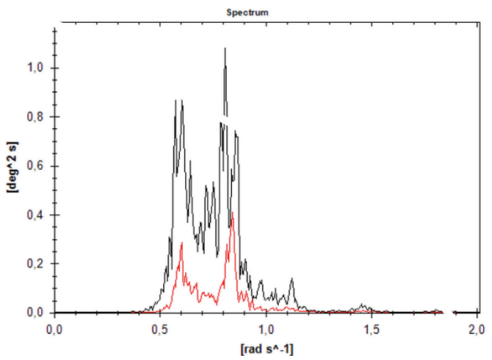


Figure 10. Computed response spectral densities based on numerical riser model.

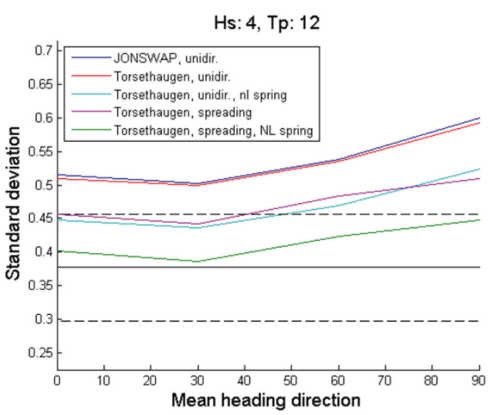


Figure 11. Comparison between angular standard deviations estimated from measurements versus numerical calculation model.

(i.e. Jonswap and Torsethaugen models), the wave spreading and the characteristic of the spring which represents the flex joint (i.e. a linear versus a nonlinear model is applied). It is found that the Torsethaugen model combined with unidirectional waves and a non-linear spring models gives good agreement. The same applies to the Torsethaugen model combined with wave spreading and a linear spring model.

2.4 *Comparison of measured and computed response for the case without low-frequency contribution*

A comparison between the cycle distributions for a measurement sequence without the low-frequency response component being present in the measurements is shown in Figure 12. A much better agreement is observed than for the results in Figure 9. The discrepancy in the high-amplitude range is now much less, and for the most relevant cycle amplitude range with respect to accumulation of fatigue damage the agreement is now extremely good.

Summarizing the findings from the comparison between full-scale measurements and the numerical simulations, the main observation is accordingly that the agreement is good provided proper models of the wave environment and the nonlinear structural behavior are applied.

However, the low-frequency response energy needs to be considered in more detail. The first step of such a study will be to include the slow-drift excitation in the numerical response analysis. In addition, the effect of low-frequency load energy caused by possible vessel motion induced by wind excitation should also be looked into.

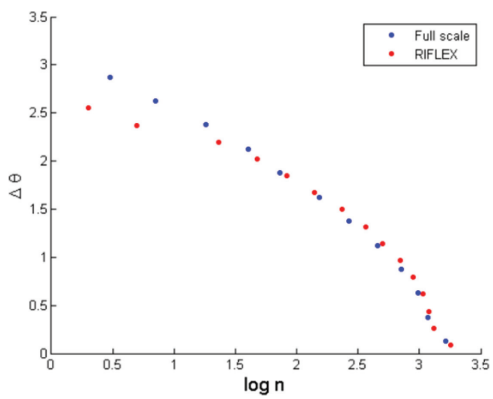


Figure 12. Comparison between short-term cycle distributions of riser angle which are estimated from measurements (blue dots) versus numerical calculations (red dots).

In addition, the reason that the measured low-frequency component is present only part of the time should be investigated in more detail by also looking at measurements of surface vessel motions. This will allow to decide whether this response component is due to top end motions or direct hydrodynamic loading on the riser itself.

3 MONITORING OF ICE-INDUCED STRAINS IN A SHIP HULL DUE TO ICE LOADING

The layout of the vessel KV Svalbard is shown in the uppermost part of Figure 13. The location of the strain sensors in the form of fiberoptic cables in the bow region are also shown in the same horizontal projection. The location of one of the fiberoptic cables on a vertical hull stiffener is also shown in the left middle photo, while the vessel itself is shown in the right middle photo. The route of the vessel through the waters around the Svalbard islands is shown on the map in the lowermost part of the figure.

An example of a time series showing the sequence of estimated ice load peaks (in kN/m) is given in Figure 14. The vertical arrows indicate the magnitude of each of the peaks.

Empirical short term cumulative distributions are shown in Figure 15 corresponding to four different measurement periods. It is observed that a bi-linear shape generally occurs for all the four periods. This implies that the standard types of analytical models will struggle to fit the data points adequately.

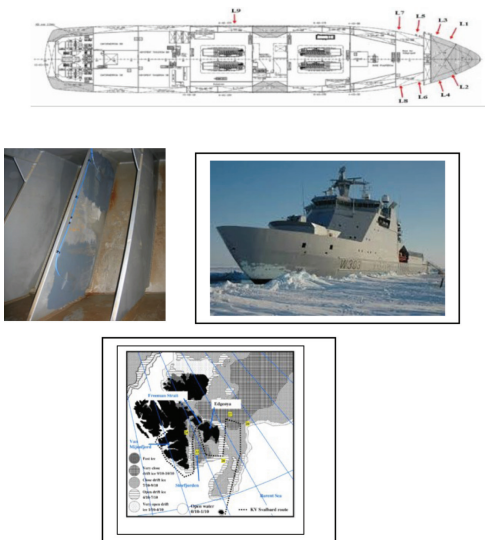


Figure 13. Fiberoptic cable instrumentation system for coast guard vessel KV Svalbard and expedition route.

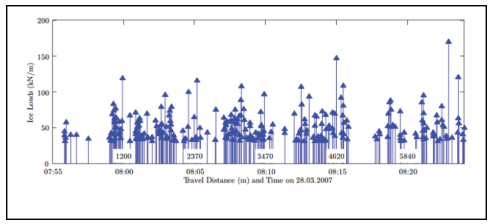


Figure 14. Example of estimated ice load peak sequence (magnitude in kN/m along vertical axis versus time along horizontal axis), Suyuthi (2013).

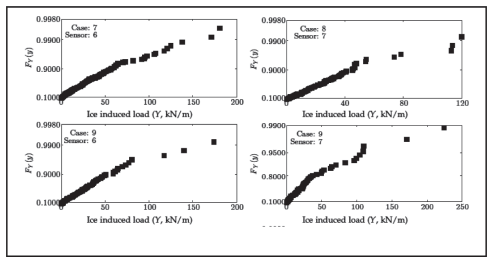


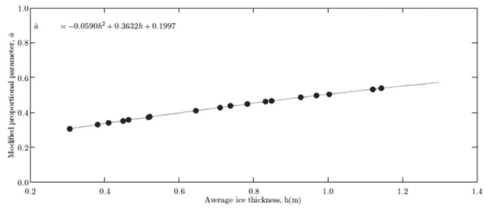
Figure 15. Empirical short-term cumulative distributions of load peak magnitudes (vertical axis) corresponding to four different measurement periods. Load level in kN/m along horizontal axis, Suyuthi (2013).

Still, the short-term distribution of the peaks is found to be well described by a three-parameter exponential distribution. This distribution was found to provide the best fit as compared to the Weibull and the Lognormal models. These latter distributions are frequently being applied in order to represent ice loading magnitudes. The conditional three-parameter model with the ice thickness (i.e. the "constant" h) as an indexing parameter is expressed as follows:

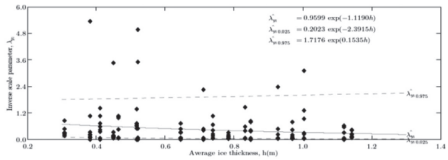
$$F_{Y|H}(y\,|\,h) = a(h)\left\{1-\exp\left(-\lambda_{y1}(h)y\right)\right\} + \left(1-a(h)\right)\left\{1-\exp\left(-\lambda_{y2}(h)y\right)\right\} \quad (1)$$

where $a(h)$ is a proportionality constant (i.e., "mixing parameter" for the two individual exponential distributions with inverse intensity parameters that are equal to $\lambda_{y1}(h)$ and $\lambda_{y2}(h)$, respectively.

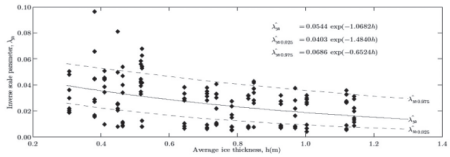
The variation of these three parameters as functions of the ice-thickness are shown in Figure 16. Both the mean curve and the upper and lower bounds which represent the respective 95% confidence intervals are shown. A significant scatter of



(a) Proportionality factor



(b) Inverse intensity parameter of first exponential model



(c) Inverse intensity parameter of second exponential model

Figure 16. Variation of the three parameters of the combined exponential models as functions of ice thickness (horizontal axis). (a) Proportionality factor (b) Inverse intensity parameter of first exponential model (c) Inverse intensity parameter of second exponential model.

the data points implies that the confidence intervals are rather wide.

The variation of the shape of the three-parameter distribution for a proportionality factor $a(h) = 0.5$ is illustrated by Figure 17. The first inverse intensity parameter varies between 0.2 and 1.2 whereas the second inverse intensity parameter varies between 0.02 and 0.12.

The procedure for prediction of the short-term extreme values for a given distribution of the load peaks can be summarized as follows: (i)The time history is divided into one minute intervals (ii)The maxima in each interval are identified (iii) These maxima form the basis for fitting an extreme value distribution of the Gumbel type.

For prediction of long-term extremes two different approaches are applied. These are referred to as the all peak amplitude approach and the m-nautical mile approach. For each of these two approaches three different analytical models are applied in order to study the sensitivity to these models.

The resulting cumulative distribution functions for the long-term extreme values are shown in Figure 18(a) for the "all peak amplitude approach" and in Figure 18(b) for the m-nautical

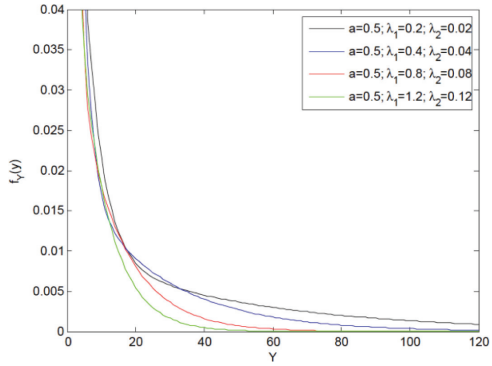
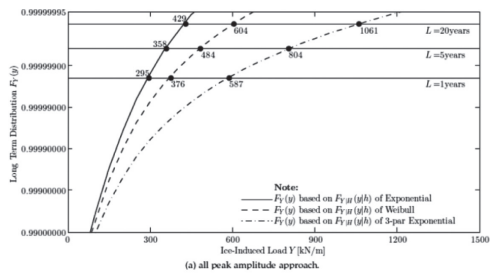
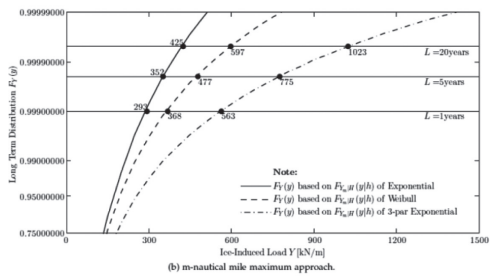


Figure 17. Variation in shape of three-parameter Weibull distribution for a proportionality factor of 0.5 Inverse intensity parameter of first exponential distribution varies between 0.2 and 1.2. Inverse intensity parameter of second exponential distribution varies between 0.02 and 0.12.



(a)All peak amplitudes are included



(b)Largest peaks during m nautical miles are included

Figure 18. Long-term extreme value distributions obtained by two different approaches: (a) All load peaks (b) Only the extreme peaks observed during a voyage of m nautical miles. Three different initial distributions are considered in each case: A. 1-parameter exponential (leftmost curves) B. Weibull distribution (middle curve) C. 3-parameter exponential distribution (rightmost curve).

mile approach. For both cases the rightmost curve corresponds to the three-parameter exponential distribution. The intersection between the distribution functions and the three different horizontal lines provide the values of the peak amplitudes

that correspond to return periods of 100 years (uppermost horizontal line), 10 years (middle horizontal line) and 1year (lowermost horizontal line).

It is clearly observed that for both cases the three-parameter exponential distribution gives the highest values. Furthermore, the percentwise difference between the predictions obtained by application of the two different approaches is quite modest.

Fatigue damage can also be estimated e.g. as being conditional on a specific (stationary) ice thickness, h. The unconditional damage is subsequently found by integration with respect to the ice thickness density.

The probabilistic model for the peak amplitudes will form the basis for calculation of the fatigue damage. Accordingly, the three-parameter exponential model will be highly relevant also for this case since the probabilities associated with the whole range of different peak levels are represented in an adequate way.

Additional parameters such as the vessel speed, v, can also be taken into account which results in a two-dimensional integration. Other types of effects, such as operational limits with respect to ice thickness or vessel speed can also be accommodated by introducing proper integration limits for these expressions.

The procedure for estimation of total fatigue damage (during a specified time interval length.) is illustrated in Figure 19.

An example of results for the computed fatigue damage is shown in Figure 20. The two parameters along the horizontal and vertical axis correspond the those for the long-term ice thickness distribution which is of the Gamma type. The figure shows the iso-contour lines for the fatigue damage levels. The level curves corresponding to increasing ice thickness are also shown. The reason that there is a peak for the fatigue damage values (and not a monotonous increase is that there is a vessel operation limit which here is assumed to be an ice thickness of 1 m.

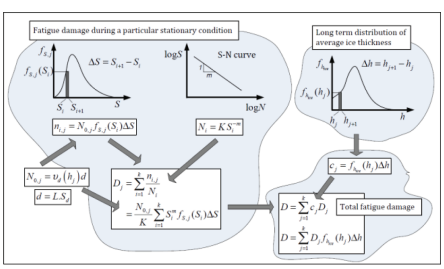


Figure 19. Illustration of steps which are associated with estimation of fatigue damage accumulation, Suyuthi (2013).

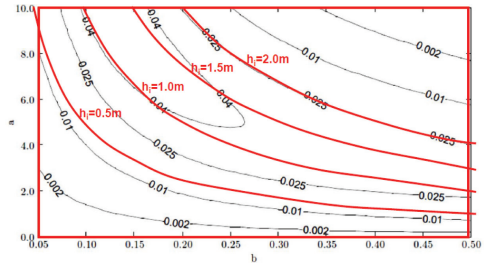


Figure 20. Iso-fatigue-damage contours and ice-thickness contours as functions of the two Gamma parameters (a and b) which define the ice-thickness distribution. Ice thickness operation limit is 1 m.

The fatigue limit state is controllable in the sense that regular inspection of the ship hull can be performed. Accordingly, estimation of the extreme value of the ice loading both within a short-term and long-term time horizon comes into focus in relation to the objective of the measurements. However, in relation to the implied learning process, improvement of fatigue design procedures is at least of equal importance.

4 CONCLUDING REMARKS

The role of structural response monitoring in relation to accumulation of more precise information for improvement of design has been a key topic in the present paper. Clearly, such response monitoring will also give information about the present condition of the structure once the measurements are combined with mechanical/numerical models in the light of acceptable threshold limits.

In general, measurements imply that more precise information becomes available which tends to reduce the level of uncertainty. In some cases, it is found that the numerical models which are applied for design purposes need to be updated. This leads to a reduction of the uncertainties related to the mechanical calculation models themselves.

In both cases, the measurements tend to improve the reliability level. In the latter case, the nominal value of the reliability level is improved by a reduction of the inherent model uncertainties (provided that they are included in the probabilistic representation).

For both examples of application, response monitoring may further serve as a decision support tool. Such decisions are related to specification of operation parameters as well as decommissioning of the structure or parts of the structure.

Regarding the mechanical limit states which are involved, the first case is mainly concerned with

the fatigue damage accumulation (also keeping in mind that direct information about presence of possible cracks is generally not available). The second case is more focused on the short- and long-term extreme values (still, the fatigue strength also needs to be verified, but inspection can be performed at regular intervals).

As a general observation it is found that instrumentation technology becomes increasingly advanced with time. The costs associated with instrumentation and monitoring systems also tend to be reduced. Monitoring and data acquisition are accordingly greatly facilitated and can be performed both on-line and off-line. Hence, the scope of application of such systems is expected to expand in the future. Application to vastly different types of structures is anticipate, which hopefully is also illustrated by the present paper.

However, a note of warning should clearly also be given: A number of potential failure modes (both of the mechanical type and other categories) are not covered by a particular instrumentation system, i.e. in the sense that no information about the parameters which are relevant are provided by the system. Hence, it should be ascertained that data which are relevant for the most important failure modes are provided by the measurements.

Altogether, the present paper has hopefully served to illustrate the benefit of response monitoring (i.e. structural health assessment) as a versatile tool within different areas of application.

ACKNOWLEDGEMENTS

The author is grateful to 4Subsea for access to the riser measurements and to DNV for access to the ship hull measurements. The contributions of the co-authors of the respective papers are also greatly acknowledged.

REFERENCES

Stange, I. 2013: "Comparison between Measured and Calculated Riser Response", Master thesis, Department of Marine Technology, NTNU, Trondheim, Norway.

Stange, I. and Leira, B.J. 2013: "A Comparison of Full-scale Measurements and Numerical Riser Response Simulation", Paper no. 11266, Proc. OMAE 2013, Nantes, France.

Marintek (2010): RIFLEX User and Theory Manuals, Trondheim, Norway.

Suyuthi, A. 2013: "Prediction of Extreme Loads and Fatigue Damage for a Ship Hull due to Ice Action", Phd thesis, Department of Marine Technology, NTNU, Report no. 2013:77, Trondheim, Norway.

Suyuthi, A., Leira, B.J. and Riska, 2012a: "Short term Extreme Statistics of Local Ice Loads on Sip Hulls", Cold Regions Science and Technology, Elsevier, Vol. 82, pp. 130–143.

Suyuthi, A., Leira, B.J. and Riska 2012b: "Statistics of Local Ice Load Peaks on Ship Hulls", Structural Safety, Elsevier, Vol. 40 (2013), pp. 1–10.

Suyuthi, A., Leira, B.J. and Riska 2013: "Long Term Extreme Statistics of Local Ice Loads on Ship Hulls", Submitted for publication in Cold Regions Science and Technology, Elsevier.

This page intentionally left blank

Uncertainty and sensitivity analysis

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparative analysis of rapid calculation methods for physical explosions of pressure vessels

R. Bubbico & B. Mazzarotta
Dipartimento Ingegneria Chimica Materiali Ambiente, Università di Roma "La Sapienza", Rome, Italy

ABSTRACT: A large number of correlations are available in the literature to estimate the overpressure profiles deriving from the physical explosion of vessels containing compressed gases. However, none of them is widely recognized as the most general and reliable, and in many cases the respective range of applicability is not always very clear. The paper presents a comparative analysis applying two of the most commonly used calculation procedures to a great number of study cases, in order to highlight the dependence of the results on the main input parameters: substance, size of the vessel and the operating conditions (P, T). The results were related to the operating variables and to the physical properties of the substances, in order to obtain guidelines about the use and the reliability of the rapid methods.

1 INTRODUCTION

A large number of correlations and calculation methods are available in the literature to estimate the overpressure profiles deriving from the physical explosion of vessels containing compressed gases. As a matter of fact the physical phenomenon, consisting in the sudden expansion of the gas, released in ambient air, is rather complex, and involves many variables dependent on the physical properties of the gas, the characteristics of the vessel, the operating conditions before the explosion occurs, and the modality of the explosion. An accurate estimate of the main parameters of interest (such as peak overpressure and impulse) would require an equally accurate modeling of the explosion, which may be difficult to be obtained even using Computational Fluid Dynamics (CFD) which is a rather demanding technique, in terms of expertise of the analyst and computational complexity. Accordingly, in several process and safety engineering applications a detailed approach (e.g CFD) may be unsuitable, especially in preliminary risk analyses, where the assessment of the effect zones for a great number of potential hazard sources is required. In such cases the estimates of the explosion parameters are carried out using simplified models, which are based on hypotheses that, on one hand, make calculations easier and faster but, on the other hand, make the results more uncertain. In fact, a number of simplified models are available, but none of them is widely recognized as general and reliable, and in many cases the respective range of applicability is not always very clear.

The aim of the present paper is to compare the pressure profiles generated by a gas explosion, calculated according to the two most widely used rapid methods for different substances, volumes and operating conditions. The attention will be focused on the predictions of peak overpressure in the middle-far range, taking into account that, in the short range, its values generally largely exceeds the thresholds of human lethality and of vessel collapse, which can be estimated around 0.3 bars.

2 SIMPLIFIED GAS EXPLOSION MODELS

In this paragraph the main features of Baker's (Baker et al., 1983) and Prugh's (Prugh, 1988) models are briefly recalled: they are the two probably most common models used in risk analysis to predict the pressure profiles generated by a gas explosion.

2.1 *Baker's model*

Baker derived the model for pressure vessel bursts based on small scale experiments (Baker et al., 1983); in the present work reference will be made to the "basic" version (AIChE/CCPS, 1994).

The energy of explosion is calculated by means of the Brode equation (Brode, 1959): this expression determines the energy required to raise the pressure of the gas at constant volume from atmospheric pressure, P_0, to the initial, or burst, pressure, P_1:

$$E = \frac{\left(P_1 - P_0\right) \cdot V}{\gamma - 1} \tag{1}$$

where: E = energy (J); P_1 = initial pressure of the expanding gas (Pa); P_0 = final (ambient) pressure

of the expanding gas (Pa); V = gas initial total volume (m^3); γ= gas heat capacity ratio, C_p/C_v (–).

However, in a real explosion, the gas behaves differently from Brode's assumption, finally reaching an equilibrium condition after an irreversible expansion from an initial volume at the burst pressure P_1 to a final (different) volume at ambient pressure P_0. Moreover, the expansion energy of the gas is partly dissipated in other phenomena accompanying the explosion, such as in vessel deformation and rupture, in vessel fragments projection, in heat dispersion, etc., which may account up to 50% of the total internal energy of the system. Despite these considerations, the energy released during a gas explosion is often calculated based on the Brode equation (AIChE/CCPS, 2000), possibly introducing some correction coefficients (Crowl and Louvar, 2002).

Most pressure gas vessel explosions happen close to the ground, where shock wave reflection occurs, increasing the intensity of the shock wave: in order to account for this phenomenon, the calculated explosion energy has to be doubled.

Once estimated the explosion energy, the peak overpressure at a given distance can be derived from generalized graphs, where the normalized overpressure as a function of the non-dimensional distance is reported. The non dimensional distance is calculated using the Sachs scaling law (AIChE/CCPS, 1999):

$$\bar{R} = r \cdot \left(\frac{P_0}{E} \right)^{\left(\frac{1}{3}\right)} \tag{2}$$

where: r = absolute distance (m); $\bar{R}$ = scaled distance (–).

Applying this method in the near field, i.e. close to the vessel surface, the calculated overpressures may results higher than the burst pressure, which is physically impossible. This inconvenience can be solved using a modified procedure for $\bar{R} < 2$ (Baker et al., 1983): this will introduce a discontinuity in the overpressure values calculated at $\bar{R} = 2$.

2.2 *Prugh's model*

Prugh's method (Prugh, 1988) estimates the explosion energy assuming an isothermal expansion of an ideal gas (Brown, 1985):

$$E = \frac{V}{V_R} \cdot \frac{P_1}{P_R} \cdot R \cdot T_1 \cdot \ln\left(\frac{P_1}{P_0} \right) \tag{3}$$

where: R = ideal gas constant (8314 J/kmol K); V = initial volume of the compressed gas (m^3); P_R = pressure at standard conditions (101300 Pa); V_R = volume of 1 kmol of gas at standard conditions (0.022414 m^3).

Then, the calculated energy is converted in an equivalent amount of TNT, which is used to estimate shock wave effects, using the TNT equivalency method. This is based on the Hopkinson's law as scaling method to evaluate the blast pressure profile as a function of the normalized distance (AIChE/CCPS, 1994).

The estimate of the explosion energy suffers from the same type of inconvenience of Brode's equation, and the analogy of the explosion of a pressurized gas vessel to a TNT one appears improper in the near field, since the vessel cannot be regarded as a point source. In this case, the correction method uses a virtual distance from the explosion center (Petes, 1971), to fictitiously move the explosion centre with respect to the surface of the expanding gas. The maximum overpressure of the shock wave, i.e. that at the contact surface between the initial expanding gas sphere and the air, is evaluated as (Baker et al., 1983; Prugh, 1988):

$$P_b = P_s \left[1 - \frac{3.5(\gamma - 1)(P_s - 1)}{\sqrt{\left(\frac{\gamma T_1}{M} \right)(1 + 5.9 P_s)}} \right]^{-2\frac{\gamma}{\gamma - 1}} \tag{4}$$

where: M = molecular weight (kg/kmol); T = absolute temperature of the expanding gas (K); P_b = blast pressure (Pa); P_s = pressure at vessel surface (Pa).

The virtual distance is then obtained by subtracting the geometrical distance between the centre and the external surface of the vessel (expanding gas initial surface), from the distance calculated by the TNT model to get the P_s overpressure. The proper distance to be used in the TNT equivalency method (AIChE/CCPS, 2000), is obtained adding the actual geometrical distance to the virtual distance.

$$Z = \frac{r}{W^{\left(\frac{1}{3}\right)}} \tag{5}$$

where: Z = scaled distance (m/kg$_{TNT}^{1/3}$); r = absolute distance (m); W = TNT equivalent mass (kg).

3 MODEL'S ANALYSIS

The focus of the present work is on the peak overpressure profile generated by the explosion of a vessel containing a pressurized gas. To this end, the previous models are applied to a number of study cases, changing the values of the parameters appearing in the model equations and comparing the calculated peak overpressure profiles.

Most attention will be devoted to the behavior of the models in the far range: in fact, in the near range, peak overpressure values generally greatly exceed the threshold values for damages to humans and structures (30 kPa).

3.1 *Parameters of interest*

The models summarized in the previous paragraph, contains different variables, related to the physical properties of the gases, the operating and ambient conditions, and the volume of the vessel.

The physical properties of the gas used in the calculations are the gas heat capacity ratio and the molecular weight: the substances listed in Table 1 were selected to cover a wide range of both variables.

Heat capacity ratio slightly depends on both pressure and temperature: data available for air (Cramer, 1993) show that γ variations are negligible in the temperature range –20/+50°C, while the influence of the pressure is more important. In fact, γ value increases from 1.402 to 1.57 increasing the pressure from 1 to 100 bars, at ambient temperature.

The operating conditions of a pressure vessel may vary considerably depending on its service. Storage vessels operate at ambient temperature, and at different pressure, based on the destination of the gas and the size of the vessels: the highest pressures are adopted for the smallest containers (e.g. gas cylinders). In the present work, the vessel size will vary from 0.5 to 200 m^3, the operating pressure from 2 to 200 bar, and the temperature from –10 to +40°C: as "reference" case as a 10 m^3 cylindrical vessel at 20°C is assumed.

3.2 *Influence of the physical properties of the gas*

In Baker's model the explosion energy is a function of the heat capacity ratio according to Brode equation (1) while, in Prugh's one, it does not depend on the physical properties of the stored gas, according to Brown equation (3). Figure 1 compares the results obtained applying the two equations to the reference case, assuming different gases. For low values of the blast pressure (up to around 20 bar) Brown's estimates of the explosion energy are lower than Brode's one, but the opposite occurs at higher pressures (20–50 bar, depending on the gas).

Table 1. Physical properties of the selected gases.

Substance	Heat capacity ratio at ambient conditions	Molecular weight (kg/kmol)
Air	1.402	29
Ethylene	1.22	28
Hydrogen	1.41	2
Hydrogen chloride	1.41	36.5
Nitrogen	1.41	28

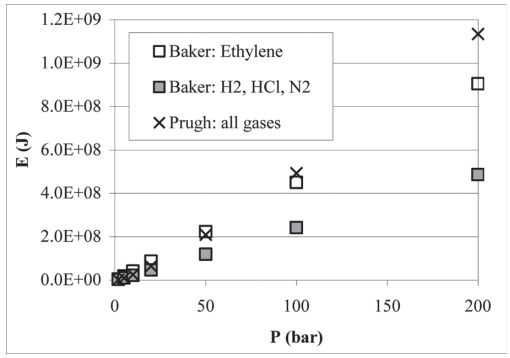


Figure 1. Explosion energy for a 10 m^3 vessel at 20°C, according to Brode's and Brown's equations.

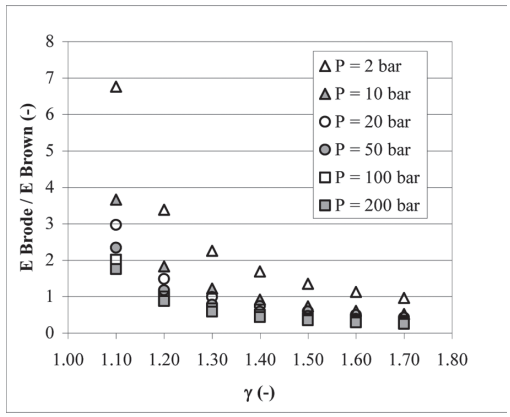


Figure 2. Ratio of the explosion energies for a 10 m^3 vessel at 20°C, according to Brode's and Brown's equations, vs. the gas heat capacity ratio.

In Brode's equation, which is used in Baker's model, larger values of the heat capacity ratio result in lower explosion energies. As highlighted before, since larger values of the heat capacity ratio correspond to increasing pressures, from this point of view, the direct influence of the burst pressure on the explosion energy in the Baker's model is somehow counterbalanced by the variability of γ, and this explains the slower increase of the explosion energy with respect to that calculated with the Brown equation.

Figure 2 shows the trend of the ratios between the energy of explosions calculated with the Brode and with the Brown equations (1) and (3) as a

function of the heat capacity ratio, in the range 1.1–1.7.

It can be noticed that for low values of γ, the Brode equation calculates higher explosion energies with respect to the Brown equation, while the opposite is true at high γ values. The ratio of the explosion energies, as defined above, increases noticeably by decreasing the blast pressure.

Figure 3 compares the explosion energy calculated with Brode equation (1), for air, either assuming a constant heat capacity ratio at the value corresponding to 1 bar (γ= 1.402), and then taking into account its dependency on the pressure (Cramer, 1993): the values at the burst pressures have been used in the calculations. It can be noticed that assuming the constant, ambient-pressure (low) value of the heat capacity ratio, may result in a overestimation of the explosion energy. However, Figure 3 emphasizes the influence of this parameter, since calculations should be more properly carried out with a suitable pressure averaged γ value, and not just based on its initial (high) value. Furthermore, taking into account that, according to the procedure of Baker, in case of explosion occurring close to the ground, the explosion energy calculated with the Brode's equation should be almost doubled to account for shock wave reflection, before being inserted in Baker's model, it is apparent that the heat capacity ratio deserves great attention and the use of a correct estimate of its value is highly recommended, especially at high burst pressures. However, peak overpressure profiles depend not only on the explosion energy, but also on the relationship between this energy, the generated overpressure and the scaled and actual distances. From this point of view, the estimates based on Baker's model (multiplying the explosion energy calculated with Brode equation by 2, to account for ground effects) appear to be only slightly sensible to the change of γ with the pressure, up to P values around 50 bar.

Figure 4 shows the peak overpressure profiles calculated at P = 200 bar: at this higher burst pressure, assuming the constant ambient pressure γ value (1.402) will give rise to higher peak overpressures than using the γ value at 200 bar (estimated as 1.719, according to Cramer, 1993). Figure 4 also shows the peak overpressure profiles calculated according to Prugh's model.

In agreement with the definition of the explosion energy, in this case no difference is observed between the curves calculated with the heat capacity ratios relevant to atmospheric or high pressure. From Figure 4 it can be also noticed that, despite the higher values of the explosion energy calculated by Brown's equation with respect to Brode's one (see Fig. 1), at high pressure, the peak overpressure profiles obtained according to Prugh's model fall below those of Baker's model, even if the differences decrease with increasing the actual distance r from the vessel. However, from this point of view, it should be remarked that, in the common practice, when applying Prugh's model, the energy values calculated with Brown equation (3) are not corrected to account for ground effects, even when the explosion source is located close to the ground, as for storage vessels (e.g. see the worked example of Prugh's model application in AIChE/CCPS, 2000). However, this procedure appears questionable, since shock wave reflection should be taken into consideration even in this case. The calculations according to Prugh's model were then repeated, multiplying by 2 the explosion energy calculated with Brown equation: Figure 5 compares the obtained results with the previous ones, assuming the heat capacity ratio at ambient pressure. It can be noticed that multiplying by 2 the explosion

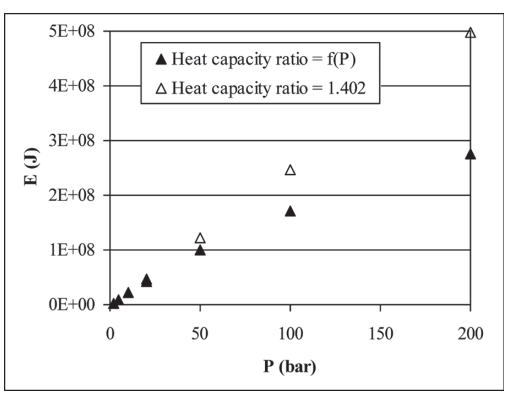


Figure 3. Explosion energy for a 10 m^3 vessel at 20°C, containing air according to Brode equation model.

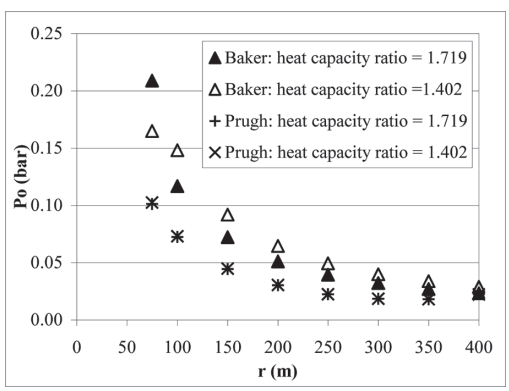


Figure 4. Overpressure profiles at 200 bar and 20°C for a 10 m^3 vessel containing air, according to Baker's and Prugh's models.

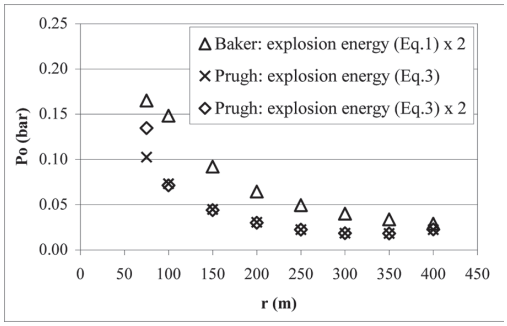


Figure 5. Overpressure profiles at 200 bar and 20°C for a 10 m^3 vessel containing air, according to Baker's and Prugh's models.; the heat capacity ratio was assumed $\gamma = 1.402$.

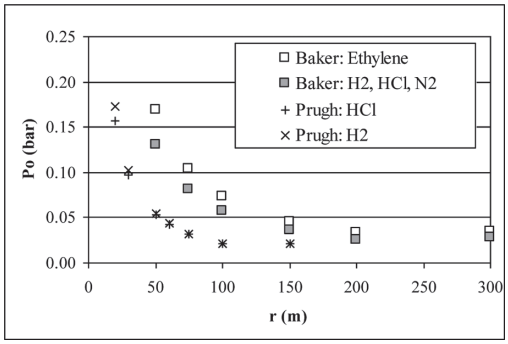


Figure 6. Overpressure profiles for a 10 m^3 vessel at 20°C and 20 bar, according to Baker's and Prugh's models.

energy value in the Prugh's model produced effects only in the near field, while the peak overpressure profiles does not change for $r > 100$ m. In any case, the overpressure values predicted according to Prugh's model still fall below those obtained using Baker's model, which appears to generally give more conservative results.

The influence of the physical properties of the substances can be better investigated by comparing the results obtained with different substances. Figures 6 and 7 compare the overpressure profiles obtained with Baker's and Prugh's models for the examined gases at pressure of 20 and 200 bar.

These substances have been adopted to cover a wide range of variability of both the heat capacity ratio and the molecular weight (see Table 1). In all cases the calculations were carried out based on the heat capacity ratio at ambient conditions; for Prugh's model the value deriving from Brown's equation (3) was used. Over all the investigated blast pressure ranges, the overpressure profiles calculated according to Baker's model remain

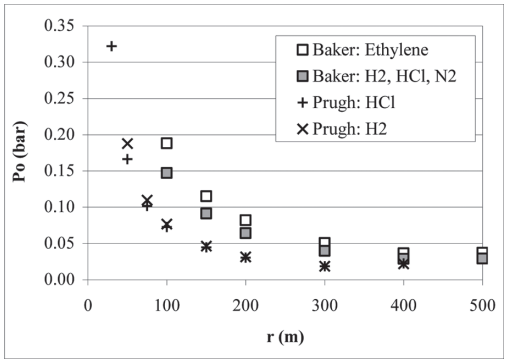


Figure 7. Overpressure profiles for a 10 m^3 vessel at 20°C and 200 bar, according to Baker's and Prugh's models.

always above those calculated according to Prugh's model, and the curves become closer as distance increases, and peak overpressure decreases. In other terms, at larger distances from the explosion source the choice of the model does not matter so much. Furthermore, the absolute distance between the peak overpressure curves increases with increasing the burst pressure value.

The differences observed among the results obtained from Baker's model for the different gases depend on the heat capacity ratio of the substance involved in the explosion, and the influence of this parameter appears noticeable, regardless of the narrow range of variation examined (1.22–1.41): γ values closer to the unity give rise to much higher values of the explosion energy, based on Brode's eq. (1) and, hence, to higher peak overpressure values, at fixed distance. Conversely, the influence of the physical properties of the substance appears much less remarkable for Prugh's model, where, together with the heat capacity ratio, also the molecular weight appears in the calculation of the pressure at the vessel surface, P_s, according to equation (4).

Figures 8 and 9 show the trend of P_s as a function of the heat capacity ratio and of the molecular weight of the gas, respectively.

It can be noticed that the influence of the heat capacity ratio on the pressure at the vessel surface is remarkable, especially at low γvalues and at high pressure: the value of P_s increases as the heat capacity ratio gets closer to the unity. The influence of the molecular weight of the gas on the pressure at the vessel surface appears even more remarkable, over the range of M values (2–58 kg/kmol) reported in Figure 9. By decreasing the molecular weight of the gas involved in the explosion, the value of P_s greatly increases, and, as already observed for the influence of the heat capacity ratio, the effect increases as the blast pressure increases.

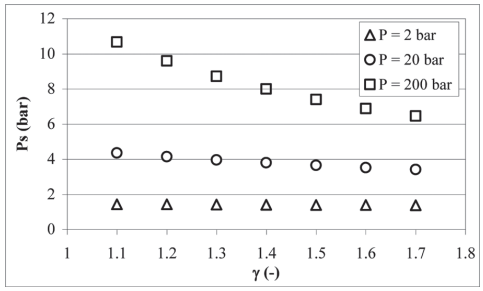


Figure 8. Trend of the pressure at the vessel surface vs. the heat capacity ratio for a 10 m^3 vessel at 20°C, containing a gas with molecular weight 28 kg/kmol.

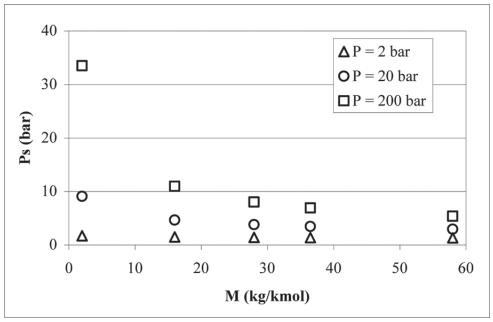


Figure 9. Trend of the pressure at the vessel surface vs. the molecular weight for a 10 m^3 vessel at 20°C, containing a gas with heat capacity ratio 1.4.

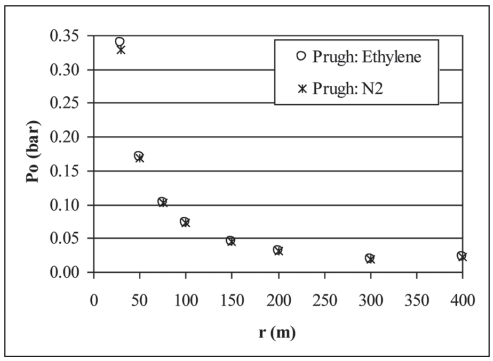


Figure 10. Overpressure profiles for a 10 m^3 vessel at 20°C according to Prugh's model: burst pressure 200 bar.

The actual influence of the heat capacity ratio and of the molecular weight of the gas on the overpressure profiles calculated with Prugh's model is shown in Figures 10 and 11: Figure 10 compares the results obtained for substance with the same molecular weight, but different heat capacity ratios,

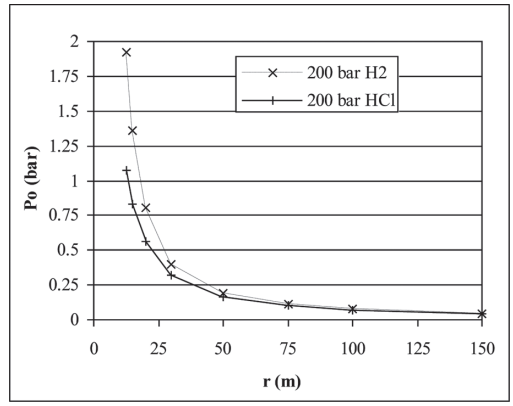


Figure 11. Overpressure profiles for a 10 m^3 vessel at 20°C according to Prugh's model: burst pressure 200 bar.

while Figure 11 compares those for substances with the same heat capacity ratio, but different molecular weight.

According to Prugh's model the influence of the heat capacity ratio seems negligible, even if, moving closer to the explosion centre, peak overpressure values are slightly higher for the substance with γ value closer to the unity. When reference is made to substances with different molecular weight, in the examined range 2–36.5 kg/kmol, (where the former refers to hydrogen and the latter to hydrogen chloride) the peak overpressure profile does not change appreciably. However, as the distance from the explosion decreases, higher peak overpressure values are observed for the substance with smaller molecular weight; this effect is more visible at high blast pressures. The influence of the molecular weight of the substance is more evident when applying Prugh's model in the near field, as shown in Figure 11.

3.3 *Influence of the vessel size*

The calculations of the overpressure profiles according to Baker's and Prugh's were repeated for differently sized vessels, namely 0.5 and 200 m^3. Increasing the vessel volume correspondingly increase the explosion energy for both models (eqs. 1 and 3), which linearly depends on this variable; an increase in peak overpressure also occurs, but for this parameter, the trend is less immediate than for explosion energy.

Figure 12 shows the results according to Baker's model, for vessels containing ethylene. A discontinuity can be observed in the curves, at low distance from the explosion, which is due to the varying adjustment factor for the overpressure for cylindrical vessels (Baker et al., 1975), which is a function

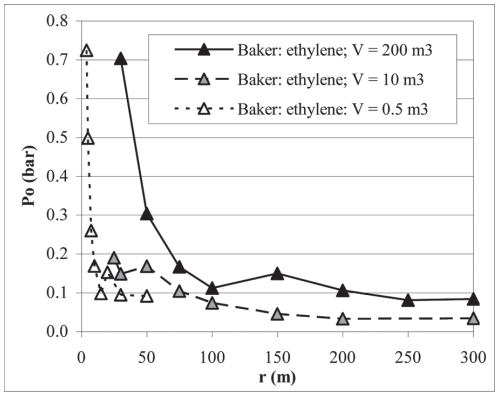


Figure 12. Overpressure profiles at 20°C according to Baker's model: burst pressure 20 bar.

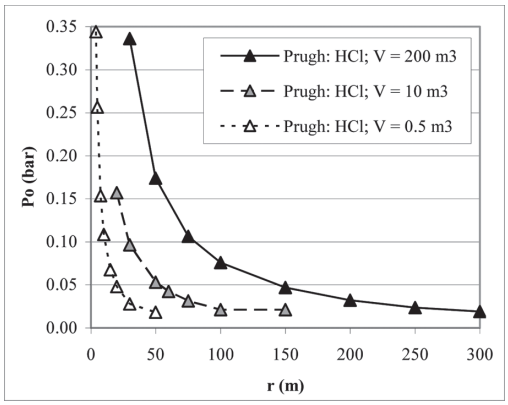


Figure 13. Overpressure profiles at 20°C according to Prugh's model: burst pressure 20 bar.

of $\overline{R}$. All the presented calculations were carried out for $\overline{R} > 2$; nevertheless, at $\overline{R} < 3.5$ the multiplier changes from 1.6, to 1.4 (in all previous graphs the reported values refer to $\overline{R} > 3.5$ and, therefore, no discontinuity is shown).

At 50 m from the explosion, where the same, lower, multiplier value holds for all vessels, the peak overpressures increase by a factor around 1.8 for each 20 time increase of the volume (from 0.5 to 10, and from 10 to 200 m^3).

Figure 13 shows the peak overpressure profiles calculated under the same operating conditions according to Prugh's model. At 50 m from the explosion the peak overpressures increase by a factor around 3 for each 20 time increase of the volume (from 0.5 to 10, and from 10 to 200 m^3), exhibiting a much greater dependence of the peak overpressure on the vessel volume, with respect to Baker's model.

3.4 *Influence of the temperature*

The results from Baker's model are not influenced by the temperature, since this variable does not appear in the calculations of the explosion energy, nor in those of peak pressure profiles. On the contrary, Prugh's model estimates are dependent on the temperature, which appears both in the estimate of the explosion energy and in the calculations of the maximum overpressure of the shock wave, according to equations (3) and (4).

Figure 14 compares the values of the explosion energy, calculated with Brown's equation, for the 10 m^3 vessel at different temperatures; the examined range includes usual ambient temperatures (–10/+40°C) and some higher values which may occur in process vessels. It can be noticed that the explosion energy calculated according to the Brown equation (3) appears remarkably influenced by this variable: by increasing the ambient temperature from –10°C to +40°C, the explosion energy increases, by a factor equal to 1.19; by further increasing the temperature, at 300°C, the explosion energy is almost double than at ambient temperature. As already shown in Figure 1, the explosion energy values calculated by the Brown equation do not depend on the selected gas.

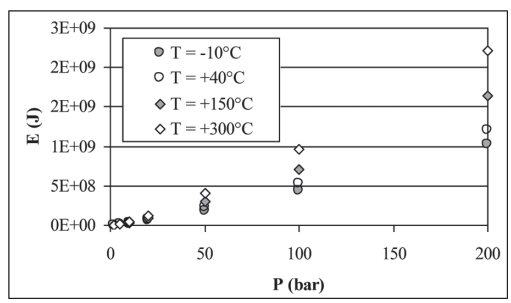


Figure 14. Explosion energy for a 10 m^3 vessel, according to Brown equation.

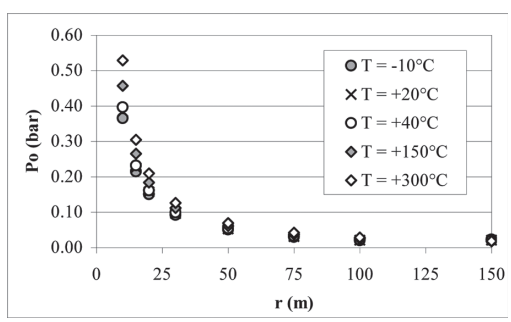


Figure 15. Overpressure profiles according to Prugh's model for a 10 m^3 vessel containing HCl: burst pressure 20 bar.

The overpressure profiles calculated for the explosion of a 10 m^3 vessel containing HCl at 20 bar and at different temperatures, according to Prugh's model are compared in Figure 15. The curves relevant to higher temperatures give rise to higher values of the peak overpressure: the influence appears remarkable in the near field, while at large distances (above 100 m, with reference to the examined study case) all the overpressure profiles almost collapse on the same curve, independently of the temperature.

4 DISCUSSION

Both the models analyzed are based on simplifying hypotheses concerning the estimation of the explosion energy, which, on one side, speed up calculations, but, on the other side, do not allow to properly simulate the involved phenomena. As a matter of fact, the explosion energy values estimated according to Brode's and Brown's equations may be remarkably different: the gas heat capacity ratio greatly affects the explosion energy calculated by the Brode equation, while, according to the Brown equation, no physical property of the gas enters in the explosion energy calculation. Therefore, greater uncertainty exists in the estimates based on Brode equation, taking into account that the difference $(\gamma - 1)$ at the denominator of eq.(1) is very small. Moreover, most of the available values of the heat capacity ratio are given at ambient temperature and atmospheric pressure: the influence of the pressure is not negligible, and may decrease the estimated explosion energy, especially at high burst pressure. Further uncertainty affects also the value of the explosion energy to be inserted in the expressions for estimating the peak overpressure profiles: following Baker's method, the value calculated from Brode equation should be doubled to account for ground effects, while this correction is not reported for Prugh's method.

Both methods cannot be safely extrapolated in the near field, and both require some "adjustment" procedure: using Baker's method, a discontinuity will occur, not only at the scaled distance $\overline{R} = 2$, limit for the near field zone, but also at $\overline{R} = 3.5$, due to a multiplier factor to be used for cylindrical vessels, which change its value from 1.6 to 1.4 at $\overline{R} = 3.5$ (AIChE/CCPS, 2000). On the contrary, Prugh's method makes use of a virtual distance, to properly adjust the distance from the explosion centre, and no discontinuity is observed in the peak overpressure profiles. Nevertheless, in the near field, the estimates obtained applying both methods likely suffer from greater uncertainty; on the other hand, it should be honestly admitted that, in the near field, peak overpressure values often largely exceed the damage thresholds of interest, and, therefore, most interest is devoted to the estimates in the far field. Different overpressure profiles have been obtained by simulating the same study cases with Baker's and Prugh models, even at distances exceeding the "near field" as defined above. In all cases, the estimates according to Baker's model give rise to higher values of the peak overpressure, at any given distance, with respect to Prugh's one. This difference does not derive from the multiplying factor of 2 used for the explosion energy in Baker's model, since, applying the same correction in Prugh's model, peak overpressure values slightly increase only in the near field.

Taking into account that the peak overpressure profiles are generally used to estimate damage distances when carrying out consequence analysis, using Baker's model will give conservative results.

The physical properties of the involved gases affect the overpressure profiles: higher heat capacity ratio results in lower peak overpressure values, in agreement with the influence of this parameter on the explosion energy. In Prugh's model, the involved physical properties (heat capacity ratio and molecular weight of the gas) exhibit a limited influence on the results, with respect to Baker's model. However, a decrease of the heat capacity ratio and of the molecular weight results in higher peak overpressures, especially in the near field and at high burst pressure.

For both models, increasing the vessel volume will linearly increase the explosion energy, but the effects on the peak overpressure profiles are something different, especially at moderate distance from the explosion, since, as usual, in the very far field all the peak overpressure profiles converge to almost a single curve. Close to the vessel (but not properly in the "near" field), Prugh's model appears much more sensitive to the vessel size than Baker's one. As a rough "rule of thumb" increasing 20 times the volume of the vessel will double the peak overpressure values according to Baker's model and will triplicate those estimated with Prugh's model.

The operating temperature does not affect the results of Baker's model, while the values calculated with Prugh's model increase with increasing the temperature. Accordingly, when the temperature is well above ambient values, the use of Prugh model may be preferred, to obtain conservative estimates.

5 CONCLUSIONS

The obtained results allowed to draw some considerations concerning the most commonly used models for estimating the overpressure profiles originated by the physical explosion of vessels containing compressed gases and their dependency on the

physical properties of the gas and some operating parameters. Their estimates suffer from some uncertainties, implicit in the models, concerning the way the explosion energy is calculated, and the near field is modeled. Baker's model appears to give conservative estimates, and may be preferred in most cases, but requires particular attention in the selection of the proper heat capacity ratio; Prugh's model is less influenced by the physical properties of the gas, but more sensitive to the temperature, and may be preferred for high temperature vessels. In the far range all the estimated peak overpressure profiles converge, and the differences become negligible.

REFERENCES

AIChE/CCPS, 1994. *Guidelines for evaluating the characteristics of vapor cloud explosions, flash fires, and BLEVEs*. New York: AIChE.

AIChE/CCPS, 1999. *Guidelines for Consequence Analysis of Chemical Releases*. New York: AIChE.

AIChE/CCPS, 2000. Guidelines For Chemical Process Quantitative Risk Analysis, 2nd ed. New York: AIChE.

Baker W.E., Cox P.A., Westine P.S., Kulesz J.J., Strehlow R.A., 1983. *Explosion hazards and evaluation*. New York: Elsevier.

Brode H.L. 1959. Blast wave from a spherical charge. *Phys. Fluids* 2, 217.

Cramer O. 1993. The variation of the specific heat ratio and the speed of sound in air with temperature, pressure, humidity and CO_2 concentration. *J. Acoust. Soc. Am.* 93 (5), 2510.

Crowl D.A, Louvar J.F., 2002. *Chemical Process Safety—Fundamentals With Applications*, 2nd edition. Upper Saddle River: Prentice Hall.

Prugh R.W., 1988. *Quantitative Evaluation of BLEVE Hazards.* 22nd Loss Prevention Symp. New Orleans: AIChE.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A study of determination of the design accidental fire load based on the quantitative Fire Risk Assessment with the treatment of uncertainty

B. Chu & D. Chang
Korea Advanced Institute of Science and Technology, Daejoen, Korea

ABSTRACT: This study proposed the new methodology for determining the Design Accidental Load (DAL) fire for further structural response analysis based on the probabilistic risk assessment with treatment of uncertainty. Although the probabilistic risk assessment procedure is regarded as the most rational and sophisticated method for determination of DAL fire, it is always subject to various uncertainty. There are three main sources of uncertainty: assumptions and simplifications, selection of representative scenarios, and probabilistic and statistical approaches. To increase the confidence of results and reduce the risk of making wrong decision, inherent uncertainty should be suitably treated and gives additional information about uncertainty. Latin Hypercube Sampling (LHS) technique is used throughout the procedure to select representative scenarios and cover the full extent of the parameter for treating uncertainty. The confidence interval and error factor are introduced to define probability distributions of parameters. With the proposed methodology, distribution of fire exceedance plots was obtained and instructed average and variance of DAL. With these additional information, the confidence in the results increased and the risk of making wrong decision was reduced.

1 INTRODUCTION

Offshore installations, which are operated in extreme marine environment, are essentially threatened by the various hazards to cause harms: injury or death of humans, damage to asset, degradation of the physical and biological environment, and interruption of oil and gas production and disruption of business (Spouge 1999).

There are four main hazards: ship collision, dropped objects, fire, and explosion. Specially, the topsides of the offshore platform, which treats combustible oil and gas, are always exposed hydrocarbon fire hazards bring out a high consequence disaster. Moreover, damages from fire accidents have increasingly been astronomical in accordance with the growing scale and complexity of the recent plants, as seen in the Deepwater Horizon incident.

In this situation, a concept of "Design Accidental Loads (DAL)" is introduced to ensure safety of offshore installations. The purpose of identifying and assessing accidental loads is to verify that accidents do not cause risks exceeding defined criteria for design of structures (ABS 2013, DNV 2010).

DAL is determined by Quantitative Fire Risk Assessment (FRA) as a rational and rigorous method for the risk estimation. The FRA uses a systematic analysis to quantify risks, which are expressed as a combination of frequency and consequences, and to provide input to a decision-making process. Consequently, it has made great advances in recent decades thanks to plentiful theoretical investigations and experiments.

FABIG (2010) proposes the approach for determining the DAL fire based on FRA with Computational Fluid Dynamics (CFD) and calculating temperature and strain in structure. This procedure is divided into two sections as shown in Figure 1. The main output from section 1 is the exceedance

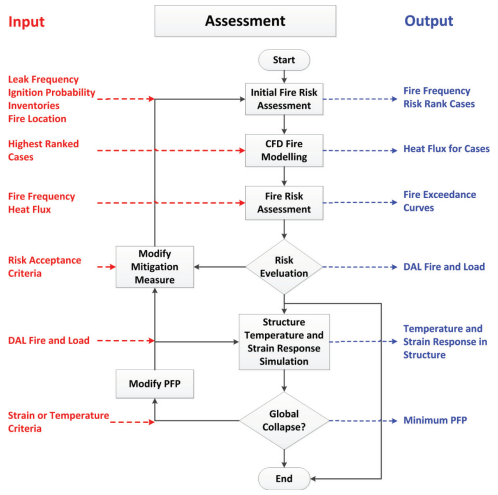


Figure 1. Schematic flow diagram of probabilistic fire load procedure.

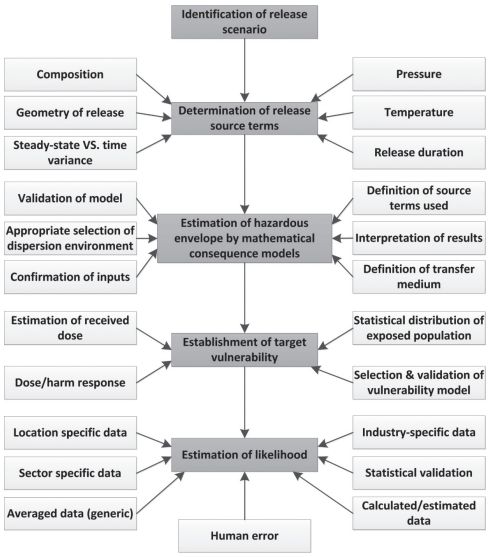


Figure 2. Sources of uncertainty in risk assessment.

curve and the DAL fire which is used as input in the structural response calculations.

Even though the FRA has made much advance in recent decades, most types of them have overlooked inherent uncertainty. HSE (2006) defines several sources of uncertainty in the FRA for hydrocarbon fire hazards as shown in Figure 2. They proposed inaccuracy and incompleteness from selecting representative scenarios and considered conservative assumptions to deal with uncertainty in the consequence and frequency estimation.

This study presents the uncertainty of the probabilistic fire load procedure of FABIG Technical Note 11. The main limitations of the procedure are described as sources of the uncertainty. A case study is also performed to involve uncertainty of the procedure. This study only covers section 1 of the procedure.

2 MAIN SOURCES OF UNCERTAINTY IN THE PROBABILISTIC FIRE LOAD PROCEDURE

As the first step of determining fire load, the initial fire risk assessment is performed to assign risk ranking to potential cases by combining leak frequency, ignition probability, segment inventories and fire types. Representative cases with the highest potential risk are selected for further detailed consequence analysis.

Within representative leak cases, fire scenarios to be modelled are selected. For the further consequence estimation with CFD, the detailed numerical data (e.g., hole size, wind direction, wind speed etc.) is needed as input and assumptions in the analysis. It is obvious that considering more scenarios will make the measured risks more accurate. However, since the scenario is the sequential combination of numerous parameters, it is absolutely impossible to model the total number of cases and possibilities due to time constraints. Accordingly, analysts have a challenge to select the limited number of parameters, which have a vital influences on the risks, and scenarios, which represent possible events. This work, despite of its significance to the risk assessment, offers serious causes of uncertainty due to incompleteness of selecting major parameters and credible scenarios.

Especially, selecting representative values of leak size is the most crucial part in the selection of scenario selection. Hydrocarbon fire scenarios begin with a leak and estimated risks are effected most by selecting initial leak sizes. Although the selection of leak sizes is one of the biggest uncertain part causing inaccuracy in the FRA, there is no definite basis and criterion for choosing representative values. Typically, median values within the range of leak size which is qualitatively categorized are selected as input parameters for the further analysis.

In the FRA, consequence of the credible scenarios is modeled by CFD simulations to predict fire profiles and damages. Although precision of CFD simulations largely depends on the ability of simulators, the numerical algorithm of CFD methods for the offshore fire consequences has been advanced enough to show accurate solutions comparing the experimental data (Paik et al., 2010). Thus, this type of uncertainty is so small and can be ignored in the QRA for hydrocarbon fire risks. However, one thing that is certain is that CFD results should be valid when the each of the credible scenarios is well defined.

Fire frequency in the FRA is expressed by a combination of leak frequency and ignition probability. Quantification of frequency is fundamentally based on probabilistic and statistical approach using historical records and statistical data for calculating fire frequency. The main benefits of this approach are making the analysis relatively simple and providing objective criteria from previous experiences for solving problems.

Use of statistical value means selecting an average value as an input variable and ignoring the details in each case. For instance, leak frequency of the target segment may differ from the statistical average value, but it is difficult to consider a specific factor about the detailed difference between them.

The obvious problem of probabilistic and statistical approach is that the approach comprehensively overlooks inaccuracy and unsuitability included in most of statistical data. This type of uncertainty would propagate throughout the analysis and be a main source which makes the measured risk insecure and unconfident.

Especially, offshore hydrocarbon fire accidents are typically high consequence and low frequency disasters. Zio and Aven (2013) emphasized that this type of accidents was typically accompanied by uncertainty from a scarcity of empirical and statistical information data compared with its occurrence.

This uncertainty can arise from following sources (Spouge 1999): *small number of events* which may contribute to the incredibility of the derived frequency from distorted statistics; *incomplete recording of events* due to omission and loss of event data; *inadequate screening of events* due to wrongly eliminating or leaving events; *inaccurate measures of exposure* arising from screening and underreporting of data on accident events; *frequency trends* in accordance with safety improvements and changing related standards; and *inapplicability of frequency data* due to overlooking difference of the collected age and installations. In the case of the FRA with respect to new systems or/and historically rare events, this uncertainty is much larger due to highly limited information and should be treated in suitable ways.

Fire exceedance plot as main output of the FRA is established by combining consequence and frequency analysis results as shown in Figure 3. The DAL fire of the target system is obtained on the x-axis for a given acceptance criteria. The criteria used for selecting the DAL fire are largely dependent on the social, economical and cultural factors (Zio and Aven 2013). Therefore, the DAL fire varies according to criteria analyst chooses.

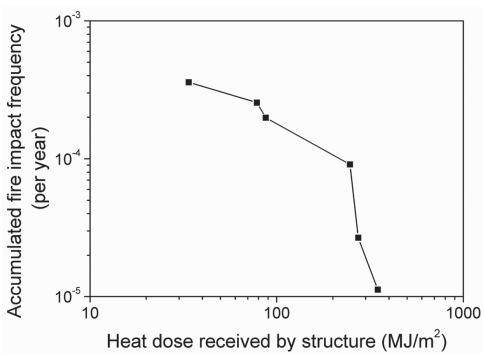


Figure 3. Fire exceedance plot.

3 TREATMENT OF UNCERTAINTYY

In the previous section, we investigated main sources of uncertainty in the probabilistic fire load procedure. There are many parameters to be used for the risk assessment. Each parameter is uncertain and can be expressed by probability distributions. For instance, when leak size distributions are represented by uniform distribution with specific ranges. Representative values are randomly selected in accordance with their distributions. These sets of values compose the sets of representative scenarios and are also used as input for simulating time-dependent leak rate profile and radiation intensity of fire.

Another concern is inherent uncertainty in the statistical data used in frequency analysis. They should be expressed by intervals, not one value, which involve information about uncertainty. This interval, which is called a confidence range, has the maximum and minimum value with statistical average value. The both sides of end points are determined by error factors of average value. For example, in the lognormal distribution, if the target segment has 4.691×10^{-2} of a median value and 10 of an error factor for 1 kg/s of leak rate, confidence range is from 4.691×10^{-3} to 4.691×10^{-1}. Other frequencies and probabilities can be also presented as confidence ranges. And events likelihood can be analytically calculated by statistical theory depending on their dependency such as leak frequency, ignition probability, and conditional probability of failure cases. Estimated confidence range of events likelihood can be used interval form between the minimum and maximum value, or randomly sampled from lognormal distribution function.

4 CASE STUDY

4.1 *Case definition*

The target system is divided into two isolatable segments by ESD valves. Inventory conditions within an isolatable section are identical. In the event of a leak, only the inventory in an isolatable section is assumed to be available if the ESD valves close as intended. The isolatable segments and major gas inventories are listed in Table 1.

4.2 *Selection of leak size*

Leak size is categorized into three different ranges which are small, medium, and large. The defined ranges vary with characteristics of the segment including inventory conditions and facility characteristics.

Table 1. Isolatable segments.

Item	Case 1	Case 2
Case name	LP	HP
Leak medium	Gas	Gas
Pressure, bar	10	50
Temperature, K	300	300
Molecular weight, kg/kmole	16.04	16.04
Ratio of specific gas	1.328	1.463
Inventory of gas in segment, kg	558	1342

Table 2. Initial leak rate.

Leak category	Small	Medium	Large
Leak rate range, kg/s	0.1~2	2~15	> 15
Representative initial rates, kg/s	0.5	5	20

The Latin Hypercube Sampling (LHS) technique is employed to extract random values from each uniform distribution of leak rate range, and each sampling iteration forms a set of representative scenarios. For the target system, this iteration is repeated 100 times, and 100 sets of representative scenarios are randomly produced for estimating 100 different exceedance plots.

4.3 *Fire load modelling*

Fire load is estimated by following values listed in Table 3 (Scandpower 2004).

With above values, heat dose is governed by the leak rate variation. It is assumed that ESD and blowdown work normally for all leak cases.

4.4 *Frequency analysis*

Estimating fire frequency should include information of uncertainty. A lognormal distribution is allocated for describing uncertainty of fire frequency. Table 4 shows detailed information about fire frequency for Case 2. From these distributions, 100 values of fire frequency are obtained using the LHS technique and assigned to 100 set of representative scenarios.

It is assumed that impact probabilities such as fire duration, leak direction, and fire size are 1 for all leak cases.

4.5 *Risk assessment: fire exceedance plot*

The fire exceedance plots are established by combining heat dose and end event frequency. Each set of representative scenarios from the LHS technique makes different fire exceedance plots as shown in Figure 4.

Table 3. Incident heat fluxes for jet fire.

	For leak rates m > 2kg/s	For leak rates m > 0.1kg/s
Local peak heat load, kW/m2	350	250
Global average heat load, kW/m2	0	100

Table 4. Incident heat fluxes for jet fire.

Leak size category	Small	Medium	Large
Best-estimate value, per year	1.12E-5	6..44E-5	1.07E-4
Medium value, per year	3.59E-6	2.06E-5	3.43E-5
Lower confidence limit, per year	2.99E-7	1.71E-6	2.86E-6
Upper confidence limit, per year	4.31E-5	2.47E-4	4.11E-4
Error factor	12	12	12

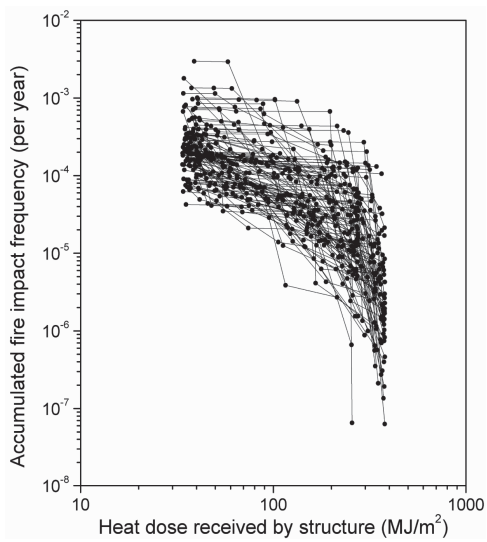


Figure 4. Fire exceedance plots with treatment of uncertainty.

5 CONCLUSION

The main sources of uncertainty in the probabilistic fire load procedure were discussed in this study. Parameter uncertainty can be expressed by probability distributions and treated by LHS sampling technique. 100 different exceedance plots were obtained over the sets of representative scenarios. Theses plots indicated the inaccuracy and discredit of previous DAL procedure, which had used only one fire exceedance plot.

Distribution of fire exceedance plots on the x-axis came from selection of different leak sizes in each set of representative scenarios. On the other hand, distribution of fire exceedance plots on the y-axis included information of uncertainty in fire frequency analysis. As a result, different fire exceedance plots involved information about uncertainty of the probabilistic fire load procedure. However, to cover the full extent of parameters, much more scenarios should be generated and simulated. In this situation, the non-CFD model was only qualified for the consequence analysis due to simple input and output.

ACKNOWLEDGEMENTS

This research was supported by a grant from the LNG Plant R&D Center funded by the Ministry of Land, Infrastructure and Transport of the Korean government.

REFERENCES

ABS, 2013. Accidental Load Analysis and Design for Offshore Structures. *Guidance Notes.* Huston: American Bureau of Shipping.

DNV, 2010. Design Against Accidental Loads. *Recommended Practice DNV-RP-C204*. Høvik: Det Norske Veritas.

FABIG, 2010. Fire Loading and Structural Response. *FABIG Technical Note 11*. Berkshire: The Steel Construction Institute.

HSE, 2006. Guidance on Risk Assessment for Offshore Installations. *HSE Information sheet*. Bootle: Health and Safety Executive.

Paik, J.K., Kim, B.J., Seo, J.K., Kim, S.H., Jang, Y.S., Kim, G.S., Woo, J.H., Kim, Y.S., Chun, M.J., Shin, Y.S., Czujko, J., 2010. CFD simulations of gas explosion and fire actions. *Ships and Offshore Structures*, 5(1): 3–12.

Scandpower, 2004. Guidelines for the Protection of Pressurised System Exposed to Fire. *Scandpower Technical Report*. Kjeller: Risk Management AS.

Spouge, J., 1999. A Guide to Quantitative Risk Assessment for Offshore Installations. *DNV Report*. Aberdeen: The Centre for Marine and Petroleum Technology.

Zio, E., Aven, T., 2013. Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks. *Process Safety and Environmental Protection*, 91(1–2): 31–45.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Sobol's sensitivity analysis of stability problems of steel beams

Z. Kala & J. Kala
Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT: The presented article reviews Sobol's sensitivity analysis of the effects of initial imperfections on the load carrying capacity of pin-ended steel I-beams subjected to bending. Failure due to lateral-torsional buckling occurs prior to the attainment of the full in-plane carrying capacity if these elements are not properly braced against lateral deflection and twisting. The load carrying capacity was evaluated using SHELL finite elements and non-linear computational methods of the ANSYS programme. The load carrying capacity is an output random quantity dependent on input random imperfections. The effect of residual stress was also taken into consideration. Latin Hypercube Sampling Method was used for sampling simulations.

1 INTRODUCTION

Majority of thin-walled beams are slender and have open section shapes. I-beams loaded in flexure have much higher strength and stiffness in the plane of the major axis, i.e., plane in which the loads are applied, than in the plane of the minor axis. Failure of the beam, due to lateral buckling of the compression flange, occurs if the I-beam is not supported in the lateral direction, i.e. perpendicular to the plane of bending, and the flexural load reaches its critical limit. The top of the I-beam is in compression, and the bottom is in tension. The cross section twists in torsion during lateral buckling of the compression flange. Failure then occurs due to bending or torsion rather than direct compression of the beam.

Generally, beams have many imperfections (geometrical and material), which can decrease its load carrying capacity. The article studies the influence of initial geometrical and material imperfections on the static load carrying capacity. Imperfections are generally random, quantifiable in a statistical sense with certain probability distributions. Non-linear analyses were performed using the finite element method of the ANSYS programme. Most of the input imperfections were measured. The Latin Hypercube Sampling method (McKey et al. 1979, Iman et al. 1980) was then employed for the computation of their random realizations using their histograms (Kala et al. 2009). Residual stresses, which influence the variability of the load carrying capacity with its random variability, were taken into consideration in the computational model. Sobol's sensitivity analysis (Sobol 1993, Saltelli et al. 2004) was employed in the study.

2 COMPUTATIONAL MODEL

2.1 *Shell finite elements and meshing*

The web and flanges of the beam were meshed in the programme ANSYS using shell elements SHELL 181, see Figure 1. Shell elements can typically be used for slender beams with negligible thickness compared to its length and width. Deflections of the nodes in the web of profile IPE 20 in the direction perpendicular to web were fixed at the edge of the loaded beam. On the lower flange of this edge, deflections in the direction perpendicular to the flange were also fixed. The upper flange was left free.

2.2 *Non-linear computational methods*

The Euler method based on proportional loading was applied in combination with the Newton-

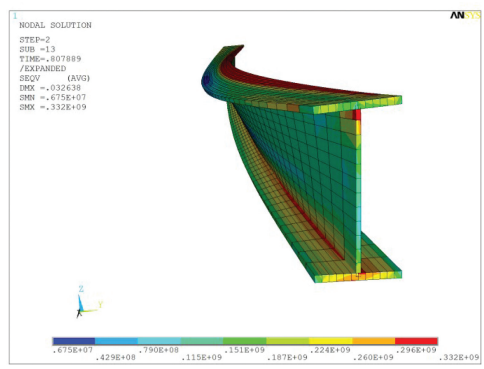


Figure 1. Lateral beam buckling of the shell model.

Raphson method for the geometrical and material non-linear FEM analysis (Kala & Kala 2010). The load carrying capacity was determined as the loading constant at which the determinant of incremental stiffness matrix K_t of the structure approaches zero with certain accuracy. Automatic control of the loading step was used with the Euler method as an accuracy of 0.1% was required for the determination of the load carrying capacity. Bilinear kinematic material strengthening was assumed. Furthermore, it was assumed that initial plastification of the steel occurs when Mises stress exceeds the yield strength.

3 INITIAL IMPERFECTIONS

3.1 *Geometric imperfections*

The statistical characteristics of the sectional height h, sectional width b, web thickness t_1, and flange thickness t_2 of profile IPE 220 were considered according to (Kala et al. 2009). The upper and the lower flange thicknesses were considered as one random quantity t_2. The upper and lower flange heights were also considered as one random quantity b. These suppositions are correct, due to the strong correlation between the geometrical characteristics of the upper and lower flanges (Kala et al. 2009). A more exact model would require that the geometrical characteristics of the upper and lower flange are considered with correlation according to (Kala et al. 2009).

Initial lateral deflection and twisting of the element axis was modelled in the form of a half sine curve, see Figure 1. Amplitudes of initial lateral deflection e_0 and initial twisting φ_0 were considered as two statistically independent quantities. It is different from the approach in which the initial geometrical imperfections are assumed to follow the shape of the first eigenmode pertaining to lateral-torsional buckling, which is conservative but do not necessarily correspond with real imperfections that would be observed during experimental research. The amplitude e_0 of initial axial deflection was introduced as a random quantity with a Gauss density function. It was assumed that 95% of the realizations of random imperfection e_0 of the beam of profile IPE 220 lay within the tolerance limit 0.15% of the beam length L acc. to the European standard EN 10034.

3.2 *Material characteristics*

The presented study utilizes experimentally obtained results of material and geometrical characteristics of steel products produced by a dominant Czech producer. The analysis of the strength characteristics of plates were published, for e.g., in (Strauss et al. 2006, Kala et al. 2009). The statistical characteristics of yield strength of hot-rolled IPE members were considered acc. to results published in (Melcher et al. 2004). The yield strength is a basic strength characteristic, which is fundamentally limited by the ultimate limit state in the case of short or lateral braced beams.

Histograms of yield strength values obtained from experimental research are the basic source of input data of a series of reliability analysis; see for e.g., (Kala 2010, Kala 2012, Kala & Kala 2012, Kala & Kala 2013, Kala 2013). Young's modulus E was considered acc. to results of experimental research to have a Gaussian distribution with mean value 210 GPa and standard deviation 12.6 GPa (Soares 1988).

3.3 *Residual stress*

In hot-rolled steel members unsteady cross-sectional cooling down occurs after hot rolling. Cooling down occurs more rapidly at the flange edge and at the middle of the web. The primary tendency is the stabilization of volume changes during shrinkage.

The subsequent slower cooling down and shrinkage of thermally more exposed internal cross-sectional parts in the contact regions of the flanges and web results in compressive stress in the previously cooled down and volume stabilized regions. Shrinkage stress arises at the flange edge and in the web middle. Redistribution of these primary technology states of stress components can continue due to loading and unloading of the beam.

Residual stress was considered with mean value 70 MPa, standard deviation 20 MPa and triangular distribution on the flanges and web acc. to (Kala and Kala 2010), see Figure 2.

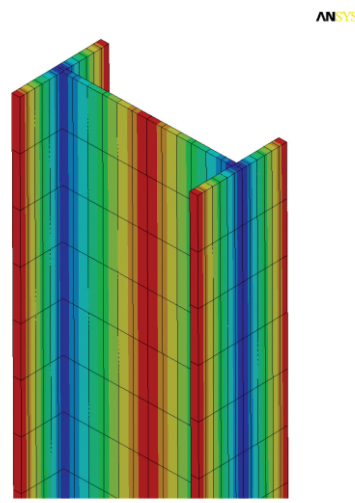


Figure 2. Model of residual stress.

Table 1. Input random quantities.

No.	Name	Symbol	Mean value	Std. deviation
1.	Sectional height	h^*	220.2 mm	0.975 mm
2.	Sectional width	b^*	110.5 mm	1.093 mm
3.	Web thickness	t_1	5.9 mm	0.247 mm
4.	Flange thickness	t_2	9.2 mm	0.421 mm
5.	Initial deflection	e_0	0	2.265 mm
6.	Initial twist	φ_0	0	0.51°
7.	Yield strength	f_y	297.3 MPa	16.8 MPa
8.	Young's modulus	E	210 GPa	12.6 MPa
9.	Residual stress	rs	70 MPa	20 MPa

*Histogram; **Gauss probability density function.

3.4 *Input random quantities*

Input random quantities were considered with histograms or Gauss density functions. All the input characteristics, which are clearly listed in Table 1, are statistically independent.

4 SENSITIVITY ANALYSIS

4.1 *What is sensitivity analysis*

Within the scope of modelling, sensitivity analysis means different things to different people, see for e.g. (Arwade et al. 2010, Mang et al. 2009, Kala 2011, Gottvald & Kala 2012). With the development of new concepts of reliability analysis, these procedures can contribute to a qualitative improvement of structural reliability analysis. Reliability of steel structures is dependent on the variance of input imperfections. In structural engineering, results of sensitivity analysis can be used for the optimization of control activities during production, which are aimed at lowering the variance of studied quantities.

4.2 *Sampling based methods*

Sampling based methods for sensitivity analysis are used to generate and explore mappings from uncertain analysis inputs to analysis results (Saltelli et al. 2004). If inputs values X_i are known unambiguously, then Y can be determined and presented as the unique outcome of the analysis. However, in majority of cases there is uncertainty with respect to the choice of appropriate values of inputs X_i, resulting in uncertainty in the value of Y (Saltelli et al. 2004). Uncertainty in inputs X_i and its associated effect on Y presents two closely related questions, i.e.: What is the uncertainty in Y, given the uncertainty in X_i? How important are the individual elements of X_i with respect to the uncertainty in Y? Attempts to answer these two questions are typically referred to as uncertainty analysis and sensitivity analysis, respectively.

4.3 *Sobol's sensitivity analysis*

Ilja M. Sobol, a mathematician, worked out the coherent concept of sensitivity analysis, which enables the analysis of the influence of arbitrary subgroups of input factors (doubles, triples, etc.) on a monitored output (Sobol 1993). Sobol's first order sensitivity index may be written as:

$$S_i = \frac{V\left(E\left(Y|X_i\right)\right)}{V\left(Y\right)} \tag{1}$$

S_i is a measure of the first order (for e.g. additive) effect (the so-called main effect) of X_i on the model output Y. The second order sensitivity index S_{ij} is the interaction term (2) between factors X_i, X_j, which captures that part of the response of Y to X_i, X_j that cannot be written as a superposition of the separate effects due to X_j and X_j:

$$S_{ij} = \frac{V\left(E\left(Y|X_i, X_j\right)\right)}{V\left(Y\right)} - S_i - S_j \tag{2}$$

Other Sobol's sensitivity indices enabling the quantification of higher order interactions may be expressed similarly. The sum of all sensitivity indices must be equal to 1:

$$\sum_i S_i + \sum_i \sum_{j>i} S_{ij} + \sum_i \sum_{j>i} \sum_{k>j} S_{ijk} + \cdots + S_{123\ldots M} = 1 \tag{3}$$

Sobol's sensitivity analysis of the influence of input imperfections (random inputs X_i from Table 1) on the load carrying capacity (random output Y) was performed in the presented study.

5 SENSITIVITY ANALYSIS RESULTS

The Latin Hypercube Sampling (LHS) method was used for the evaluation of sensitivity indices (McKey et al. 1979, Iman et al. 1980). The model output Y is the load carrying capacity evaluated in each simulation run of the LHS method. The conditional random arithmetical mean was evaluated for 330 simulation runs. The variance was also calculated for 330 simulation runs. All input random imperfections were considered as random quantities for the evaluation of the variance V(Y) of the load carrying capacity. 9000 simulation runs were applied. The second-order sensitivity indices S_{ij} were calculated analogously. The influence of imperfections on the load carrying capacity changes with increasing slenderness of the beam. Non-dimensional slenderness can be calculated acc. to EUROCODE 3 as:

$$\overline{\lambda}_{LT} = \sqrt{\frac{W_{pl,y} f_{y,n}}{M_{cr,n}}} \tag{4}$$

where $W_{pl,y}$ = 285.4 mm^3 is the nominal plastic sectional modulus of the cross section of profile IPE220, $f_{y,n}$ = 235 MPa is the nominal value of yield strength, and $M_{cr,n}$ is the elastic critical moment of a bilaterally hinged beam. A beam of length L = 2.96 m was considered. The non-dimensional slenderness calculated acc. to (4) is 0.8. Results of Sobol's sensitivity analysis are presented in Figure 3. It is possible to determine initial imperfections that can be fixed or simplified.

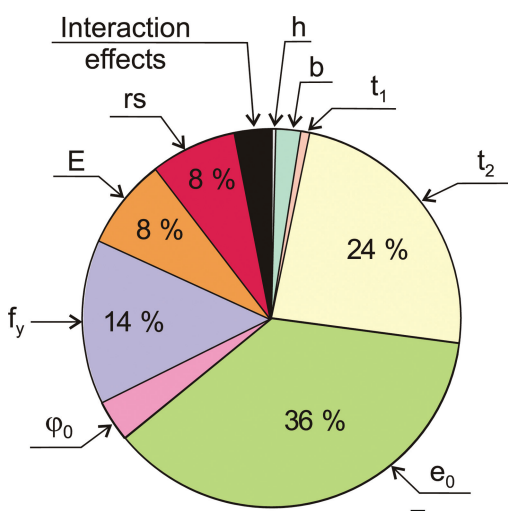


Figure 3. Sensitivity analysis results for $\overline{\lambda}_{LT}$ = 0.8.

6 CONCLUSION

The presented paper reviews bending stability problems of a simply supported hot-rolled I-beam with equal end moments. Obtained results of sensitivity analysis show that the load carrying capacity is most sensitive to the variability of the amplitude of initial deflection e_0. The variance of the load carrying capacity is minimal when e_0 is fixed (frozen), i.e. considered a constant quantity. Other crucial quantities include the flange thickness t_2, yield strength f_y, and residual stress rs. The variability of these imperfections can be influenced positively by manufacturing technologies. The variability of the amplitude of initial twist φ_0 has relatively little influence on the load carrying capacity. Therefore change in its variance does not affect the variance of the load carrying capacity significantly. The variance of this quantity need not be monitored so closely during manufacturing of hot-rolled steel beams. Furthermore, the tolerance standards do not state too strict rules for the adherence of its limits. Young's modulus is an example of an imperfection whose variability is insensitive to changes in technology.

The article was elaborated within the framework of projects of GAČR 14-17997S and VG20132015109.

REFERENCES

Arwade, S.R. & Moradi, M. & Louhghalam, A. 2010. Variance decomposition and global sensitivity for structural systems. *Engineering Structures* 32(1): 1–10.

Gottvald, J. & Kala, Z. 2012. Sensitivity analysis of tangential digging forces of the bucket wheel excavator SchRs 1320 for different terraces. *Journal of Civil Engineering and Management* 18(5): 609–620.

Iman, R.C. & Conover, W.J. 1980. Small sample sensitivity analysis techniques for computer models with an application to risk assessment. *Communications in Statistics—Theory and Methods* 9(17): 1749–1842.

Kala, Z. & Melcher, J. & Puklický, L. 2009. Material and geometrical characteristics of structural steels based on statistical analysis of metallurgical products. *Journal of Civil Engineering and Management* 15(3): 299–307.

Kala Z. & Kala J. 2010. Variance-based sensitivity analysis of stability problems of steel structures. *International Conference on Modelling and Simulation 2010; Proc. intern. conf., Prague, 22–25 June 2010*, Czech Republic.

Kala, Z. 2010. Sensitivity analysis in advanced building industry. *Procedia—Social and Behavioral Sciences* 2(6): 7682–7683. doi:10.1016/j.sbspro.2010.05.177.

Kala, Z. 2011. Sensitivity analysis of steel plane frames with initial imperfections. *Engineering Structures* 33(8): 2342–2349.

Kala, Z. 2012. Geometrically non-linear finite element reliability analysis of steel plane frames with initial imperfections. *Journal of Civil Engineering and Management* 18(1): 81–90.

Kala, Z. & Kala, J. 2013. Uncertainty and sensitivity analysis of beam stability problems using shell finite elements and nonlinear computational approach. *Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures—Proceedings of the 11th International Conference on Structural Safety and Reliability, ICOSSAR 2013*; *Proc. intern. conf. New York,16–20 June 2013*, USA.

Kala, Z. 2013. Elastic lateral-torsional buckling of simply supported hot-rolled steel I-beams with random imperfections. *Procedia Engineering* 57: 504–514. doi:10.1016/j.proeng.2013.04.065.

Mang, H.A. & Höfinger, G. & Jia, X. 2011. On the interdependency of primary and initial secondary equilibrium paths in sensitivity analysis of elastic structures. *Computer Methods in Applied Mechanics and Engineering* 200(13–16): 1558–1567.

Melcher, J. & Kala, Z. & Holický, M. & Fajkus, M. & Rozlívka, L. 2004. Design characteristics of structural steels based on statistical analysis of metallurgical products. *Journal of Constructional Steel Research* 60(3–5): 795–808. doi:10.1016/S0143-974X(03)00144-5.

McKey, M.D. & Conover, W.J. & Beckman, R.J. 1979. A comparison of the three methods of selecting values of input variables in the analysis of output from a computer code. *Technometrics* 21(2): 239–245.

Saltelli, A. & Chan, K. & Scott, E.M. 2004. *Sensitivity analysis*. Wiley series in probability and statistics, New York: John Wiley and Sons. 475 p.

Soares, G.C. 1988. Uncertainty modelling in plate buckling. *Structural Safety* 5(1): 17–34.

Sobol, I.M. 1993. Sensitivity analysis for non-linear mathematical models. Mathematical Modelling and Computational Experiment 1: 407–414; Translated from Russian: I.M. Sobol'. 1990. Sensitivity estimates for nonlinear mathematical models, *Matematicheskoe Modelirovanie* 2: 112–118.

Strauss, A. & Kala, Z. & Bergmeister, K. & Hoffmann, S. & Novák, D. 2006. "Technologische Eigenschaften von Stählen im europäischen Vergleich" [Comparison of technological characteristics of European steels]. *Stahlbau* 75(1): 55–60.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Quantitative vs. qualitative treatment of uncertain assumptions in risk assessment

C. Berner & R. Flage
University of Stavanger, Stavanger, Norway

ABSTRACT: The results of quantitative risk assessments are conditional on the background knowledge that the assessments are based on, including phenomenological understanding, models, data and expert statements used, as well as assumptions made. Risk indices established in the risk assessment may have a more or less solid foundation, depending for example on the validity of assumptions made. Poor models, lack of data or simplistic assumptions are potential sources of uncertainty in a risk assessment. In the present paper, we review both quantitative and semi-quantitative methods to treat such uncertainties. We then analyse different situations faced when performing a risk assessment, considering beliefs about assumption deviation, sensitivity of the risk index, and the overall strength of knowledge involved. We conclude that there is a need to balance the use of the different approaches, and to this end we present some recommendations and guidance on how perform this balancing.

1 INTRODUCTION

When performing a risk assessment a number of assumptions are typically made. In a risk assessment of an offshore oil and gas producing platform, assumptions may for example relate to:

- the number of personnel on board the platform and the distribution of these between different parts of the platform;
- the impact energy that the platform will be able to withstand in the event of a ship collision; or
- the blowout rate in case of an uncontrolled blowout.

See Vinnem (2007) for details regarding risk assessment of offshore risk assessments. The results of the risk assessment are then conditional on these assumptions holding true, and do not reflect the possibility that, in reality, the conditions may deviate from what has been assumed.

The combined set of assumptions underlying a quantitative risk assessment may be summarized in an appendix to the risk assessment report, perhaps with a comment that it is important to be aware that the results and conclusions are only valid so long as the assumptions are valid. Other times assumptions are further highlighted by including a sensitivity analysis, giving an understanding and possibly a ranking of which assumptions are most important. Assumptions might hide uncertainties Aven (2010), and it is therefore important that they are treated and communicated in a suitable manner.

A risk assessment less reliant on assumptions is always preferable. Relying too heavily on assumptions could in some cases place undesirable restrictions on carrying out a specific activity, creating situations where a strong focus on fulfilment of the assumptions is required to secure the validity of the risk analysis. Ideally, any uncertain condition should be accounted for using some representation of uncertainty; however, the solution is often rather to make conservative assumptions, making the results more robust but at the same time not properly reflecting uncertainties.

Still, some assumptions are always required to establish the basis of either quantitative or qualitative risk assessments. In the present paper we consider the following setting: An unknown quantity Y is defined denoting some aspect of loss, for example the number of fatalities. A probabilistic risk index R in the form of the (possibly normalised) expected value of Y is defined, linking the expected value of Y with some other unknown quantity X. That is, conditional on X we have:

$$R(X) = cE[Y|X,K].$$

and conditional on $X = x_0$ we have

$$R(x_0) = cE[Y|X = x_0,K].$$

where c is a normalising constant and K is the background knowledge that the risk index is based on, including phenomenological knowledge, models, data, expert statements and assumptions. The

class of risk indices included in the above definition includes probabilities of specific events (e.g. individual risk, IR, defined as the probability of death for a randomly selected person in a population), frequencies (e.g. fatal accident rate, FAR, defined as the expected number of fatalities per 10^8 exposed hours) and the probability/frequency distribution of Y (e.g. f-N curve, defined as the frequency of events with N or more fatalities, here taking $N = Y =$ number of fatalities). For a comprehensive overview of risk measures/indices for loss of life and economic damage, including those mentioned above, see Jonkman et al. (2003); see also Vinnem (2007) for such indices in the context of offshore risk assessment in particular.

In any given risk assessment there will be a number of assumptions; more or less explicitly stated. In this paper we first simplify and focus on a single assumption that may be formulated as $X = x_0$ for some fixed value x_0. Later we will discuss the effect of several assumptions. Examples of assumptions made in offshore risk assessments are:

- "The blowout potential is 80 kg/s" (i.e. $X = x_0 = 80$, where X is the blowout rate).
- "The number of immediate fatalities for a blowout given immediate ignition is 1" (i.e. $X = x_0 = 1$, where X is the number of immediate fatalities following a blowout when an immediate ignition occurs).
- "The jacket structure will withstand a ship energy of 9 MJ" (i.e. $X = x_0 = 9$, where X is the resistance of the structure).
- "A gas leakage will be detected within 30 seconds" (i.e. $X = x_0 = 30$, where X is the detection time a leakage).
- "The gas concentration is assumed to be reduced by 50% each 8 meters away from the leakage point" (i.e. $X = x_0 = G(u,v) = u(1/2)^{v/8}$, where X is the gas concentration at a point v meters from a leakage source and u the gas concentration at the leakage point).

The last assumption in the list above involves a model G of gas dispersion, and in effect states that the model error $\Delta G(u,v) = G(u,v) - X$ is 0. The implication is that there is no need to consider model output uncertainty, i.e. uncertainty on the value of the model error. The terms model error and model output uncertainty is here used as defined by Aven & Zio (2013).

The assumptions made may be more or less reasonable, i.e. there may be more or less uncertainty about whether the condition (assumption) $X = x_0$ holds true. This uncertainty can in principle be handled quantitatively, perhaps most obviously using the law of total expectation but also using various non-probabilistic representations of uncertainty, such as interval or imprecise probability, possibility theory and evidence theory; see e.g. Aven et al. (2014). In practice both these approaches may be prohibitively difficult to carry out, due to a large number of assumptions leading to high dimensionality of X and hence a high workload involved in establishing its joint distribution, and/or because the background knowledge K on which to base the quantification of uncertainty about X is poor.

An alternative approach is to report the risk index without any quantitative integration of uncertainty related to potential deviation from $X = x_0$, and then perform a qualitative assessment of the strength of knowledge that the resulting risk index is based on. An example is the qualitative classification scheme suggested by Flage & Aven (2009) where a crude categorisation of strength of knowledge and risk index sensitivity is performed with respect to so-called 'uncertainty factors', including assumptions, models and data. Looking at these two aspects combined gives an impression of how important (critical) the factor is. This information can be used either to direct further analysis efforts, or it may be communicated to the decision-maker together with the results of the quantitative risk assessment, in particular the values of the relevant risk indices, so that the decision-maker is informed about the basis of the assessment. The result is a semi-quantitative approach to risk assessment, entailing a quantitative representation of uncertainty, typically probability, supplemented by a qualitative characterization of the background knowledge K. The purpose of the qualitative characterization is to capture aspects beyond what can be transformed into and expressed in quantitative form. A more formalised semi-quantitative approach is based on the concept of 'assumption deviation risk' (Aven, 2013b), where the risk related to deviations from the assumptions made is assessed quantitatively, along with a qualitative assessment of the background knowledge.

In the present paper we review of the following methods to treat uncertainty related to the condition (assumption) $X = x_0$:

1. Quantitative treatment of uncertainty
   a. Law of total expectation
   b. Interval probability
2. Semi-quantitative treatment of uncertainty
   a. Crude strength-of-knowledge and sensitivity categorisation
   b. Assumption deviation risk

The gas leakage assumption listed above is used as an example throughout the review, to highlight ideas. We then perform an analysis of different situations faced when performing a risk assessment, considering beliefs about deviation from x_0, the sensitivity of $R(x_0)$ with respect to x_0, and the

overall strength of knowledge on which to base an uncertainty quantification of X. The result is some recommendations and guidance on how to balance the use of the approaches mentioned above.

The approach to risk analysis considered in the present paper may be referred to as predictive Bayesian, which is based on the following principles (Aven, 2012 p. 49–50):

- 'Focus is placed on quantities Y expressing states of the "world", i.e. quantities of the physical reality or the nature, that are unknown at the time of the analysis but will, if the system being analysed is actually implemented, take some value in the future, and possibly become known. We refer to these quantities as *observable* quantities. […]
- The observable quantities are predicted.
- Uncertainties related to what values the observable quantities will take is expressed by means of knowledge-based probabilities $P(\cdot|K)$. This uncertainty is *epistemic*, i.e. the result of lack of knowledge.
- Models in a risk analysis context are deterministic functions linking (observable) quantities on different levels of detail. The models are simplified representations of the world.'

This type of analysis constitutes a form of level 1 purely epistemic uncertainty propagation approach. Hence we do not consider a level 2 aleatory/epistemic uncertainty propagation approach (e.g. the probability of frequency approach); see Aven et al. (2014, p. 59–78) for a detailed description of the meaning of a level 1 or level 2 uncertainty propagation approach. Furthermore, we leave out of the consideration the goodness of the risk index $R(X)$, i.e. to what extent the index appropriately characterises risk. Of course, having a well-founded uncertainty characterisation of X may be less important if $R(X)$ represents a poor characterisation of risk.

The issue of uncertainties related to the background knowledge of probabilities is addressed also by Mosleh & Bier (1996). They refer to a subjective probability $P(A|X)$ expressing the probability of the event A given a set of conditions X, and argue that for such a setting the concept of 'uncertainty about probabilities' is meaningful in the sense that $P(A|X)$, being a function of X, is uncertain (since X is uncertain, $P(A|X)$ is a random variable). Accordingly there is uncertainty about the random probability $P(A|X)$. They also describe taking the expectation of $P(A|X)$ to obtain the unconditional probability $P(A)$ which, as they describe, according to a subjective probability interpretation is not uncertain. In the present paper we start from an initial conditional probability assignment $P(A|X = x_0)$ and, looking at different analysis situations, discuss how to handle the potential for having deviations from the condition (assumption) $X = x_0$.

The remainder of the paper is organised as follows: In Section 2 and 3 we present quantitative and semi-quantitative treatment of uncertainty, respectively. In Section 4 we analyse and discuss these in light of different analysis situations, as described above. Section 5 concludes.

2 QUANTITATIVE TREATMENT

2.1 *Law of total expectation*

The risk index unconditional on X (but still conditional on K) can in principle be obtained using the law of total expectation as follows:

$$R = E\left[R(X) \mid K\right] = \int R(x)\,dF(x \mid K). \quad (1)$$

where $F(x|K) = P(X \leq x|K)$. Ideally, all uncertain quantities involved in the risk analysis should be handled this way, as it constitutes a coherent integration of the uncertainty description of X into the risk index, which then incorporates and reflects uncertainty about X.

However, introducing a new probability (distribution) typically introduces new assumptions and, more generally, a more or less strong background knowledge on which the new probability is based. Again focusing on the situation where such an assumption can be formulated as $Z = z_0$ for some unknown quantity Z, and the distribution above instead becomes $F(x|z_0, \mathrm{K}) = P(X \leq x|Z = z_0, \mathrm{K})$. If the background knowledge of the distribution is poor and the distribution is sensitive to changes in z_0, then much may not be gained by the type of integration described above, as the sensitivity with respect to z_0 to greater or lesser extent carries over to the resulting risk index $E[R(X)|z_0, K]$.

Consider the example of the gas detection time and suppose that the analysts establish a discretised probability distribution on the following possible values of X: 5, 15, 30, 60, 90; with associated probabilities 0.05, 0.35, 0.40, 0.04, 0.01. Then the integration with $R(X)$ is straightforward; however, the basis for this distribution could be more or less arbitrary. It could for example be based on an assumption saying that all gas detectors function perfectly, i.e. $Z = z_0 = 1$, where Z is the availability of the gas detectors. The probability distribution then does not reflect the possibility that the gas detectors in the area of the leakage do not function at the time of the leakage.

2.2 *Interval or imprecise probability*

Alternative approaches for representing uncertainty have been proposed, including those based on interval or imprecise probability, possibility

theory and evidence theory (e.g. Aven et al., 2014). It is argued that these approaches provide a more adequate treatment of uncertainty in situations of poor knowledge on the phenomena and scenarios studied in the risk assessment.

Here we focus on interval or imprecise probability. The term imprecise probability brings together a variety of different theories (Coolen et al., 2010). It refers to a generalization of probability theory where the uncertainty related to an event A is represented using a lower probability $\underline{P}(A)$ and an upper probability $\overline{P}(A)$, $0 \leq P(A) \leq \overline{P}(A) \leq 1$, rather than a single-valued probability $P(A)$. Subjective probabilities are expressions of degrees of belief, and so this does not mean that the true value of the probability is in the interval $[\underline{P}(A), \overline{P}(A)]$, as no such true value exists. It rather means that the person asked to assign the probability is not able or willing to precisely assign a single-valued probability $P(A)$.

Arguably it may be no easier to assign a well-founded probability interval than an exact probability. Suppose for example that we have assigned a well-founded unconditional probability distribution $F(x|Z, K)$, but have problems assigning a probability distribution of Z (to integrate with F using the law of total probability), where Z is known to take a value in the interval $[z_{min}, z_{max}]$. Then we may at least obtain a set of distributions $F(x|z, K)$ generated by z ranging in the interval $[z_{min}, z_{max}]$; or, equivalently, probability intervals $[P(A|z_{min}), P(A|z_{max})]$ (assuming that $P(A|z)$ is increasing in z) for events A determined by the outcome of Z. Such an approach could, of course, lead to rather wide intervals.

In the gas detection time example, suppose that the analysis group makes the judgement that a detection time longer than 120 seconds is so unlikely that this eventuality can be ignored. They are not willing, however, to make any further judgements about the time to detection. In an interval or imprecise probability setting this leads to a p-box for $F(x|z_0, K)$ bounded above by the distribution $\overline{F}(x \mid z_0, K) = 1$ and below by $\underline{F}(x \mid z_0, K) = 0$ for all x in the interval [0, 120]. This corresponds to ultimately assigning $[R(0), R(120)]$ as an interval for the risk index. An important underlying assumption that is introduced by this distribution is that the detection time will not exceed 120 seconds, i.e. $Z = X_{max} = z_0 = 120$.

3 SEMI-QUANTITATIVE TREATMENT

3.1 *Crude strength-of-knowledge and sensitivity categorisations*

A semi-quantitative approach entails a belief that the full scope of uncertainty and risk is not transformable into a quantitative format, using probability or another measure of uncertainty. On this basis, 'uncertainty factors' that are 'hidden' in the background knowledge K of the subjective probabilities are identified and assessed in a qualitative way. The identification and assessment is made using simple criteria to categorize the strength of the knowledge that supports the probabilistic analysis, as well as the sensitivity of the resulting risk indices. For example, the background knowledge is classified as weak if one or more of these conditions are true (Flage & Aven, 2009):

- The assumptions made represent strong simplifications
- Data are not available, or are unreliable
  There is lack of agreement/consensus among experts
- The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions.

On the other hand, if all of the following conditions are met, the knowledge is classified as strong (Flage & Aven, 2009):

- The assumptions made are seen as very reasonable
- Much reliable data are available
- There is broad agreement/consensus among experts
- The phenomena involved are well understood; the models used are known to give predictions with the required accuracy.

Cases in-between are classified as corresponding to moderate strength of knowledge. In addition a crude classification is made of the sensitivity of the risk index with respect to the uncertainty factors. For example, the sensitivity may be classified as follows (Flage & Aven, 2009):

- High: Relatively small changes in base case values needed to bring about altered conclusions (e.g. exceedance of risk acceptance criterion)
- Moderate: Relatively large changes in base case values needed to bring about altered conclusions
- Low: Unrealistically large changes in base case values needed to bring about altered conclusions

Returning to the example of the gas detection time assumption, suppose that the following assessments are made for the criteria described above:

There is manufacturer test data available on the availability of the gas detectors; however, there is no field data on neither automatic nor manual detection from the platform in question. There is broad agreement among the analysts performing the risk assessment that 30 seconds is a 'representative' detection time, but it is also acknowledged

that the detection time could easily exceed this number, at least to some extent. The phenomenon gas dispersion is well understood and Computational Fluid Dynamics (CFD) modelling is used in the risk analysis; however, the modelling is based on a 'representative' gas leakage scenario, chosen from a range of possible scenarios.

Detection is a barrier function that enters early in the event sequence of a process accident scenario; it will hence be among the first branching events of a corresponding event tree and so its performance will significantly influence the process accident risk model. Moreover, process accidents are characteristically found to be the dominating risk contributor in Quantitative Risk Assessments (QRAs) of offshore oil and gas producing platforms.

Based on the above, both the strength of knowledge and sensitivity of the detection time assumption are classified as moderate, leading to an overall moderate importance (criticality) of this assumption.

3.2 *Assumption deviation risk*

The concept of assumption deviation risk was coined by Aven (2013b) and refers to the risk related to the (assumption) deviation $X - x_0$. To assess this risk, Aven (2013b) recommends highlighting:

- The magnitude of the deviation
- The (subjective) probability of the magnitude to occur
- The effect of the change on the consequences C addressed in the risk assessment
- An overall judgment of the strength of the background knowledge of this triplet risk assessment is to be conducted

Different magnitudes of deviation may be considered, and the probability of these to occur could for example be assessed in terms of

$$p(d|z_0, K) = P(|X - x_0| > d| z_0, K),$$

for different values of d. Furthermore, the effect of such deviations could be studied in a sensitivity analysis of $R(x_0)$ with respect to x_0 over the range $[x_0 - d, x_0 + d]$. Finally, the strength of the background knowledge could be assessed with reference to the criteria in Section 3.1. The last point is important, as there are two cases where a deviation between X and x_0 would not be surprising, namely if:

- $p(d|y_0, K)$ is moderate or high, which would be the case if the spread of F is moderate or high; or
- $p(d|y_0, K)$ is low, but the strength of knowledge is considered moderate or low.

Table 1. Assumption deviation risk assessment of gas detection time.

Magnitude of deviation d	0 sec	30 sec	90 sec
Probability of deviation $\tilde{p}(d \mid z_0, K)$	0.2	0.05	Negl.
Effect on consequences $[R(x_0 + d) - R(x_0)]/R(x_0)$	–	+ 2%	+ 5%

In the gas detection time assumption example main concern is with deviations of the detection time upwards of $x_0 = 30$, and hence focus may be placed on

$$\tilde{p}(d \mid z_0, K) = P(X - x_0 > d \mid z_0, K).$$

In accordance with the recommendations above, an assumption deviation risk assessment may take the form as illustrated in Table 1. According to this table the analysts assign a probability 0.2 of having a detection time in excess of 30 seconds and a probability 0.05 of having a detection time in excess of 60 seconds. They also judge that the probability of having a detection time in excess of 90 seconds is negligible, i.e. that such an event is so unlikely that it can be ignored. Just as for the interval/imprecise probability distribution in Section 2.2, the probability distribution in Table 1 introduces an assumption that the detection time will not exceed 120 seconds, i.e. that $Z = X_{max} = z_0 = 120$. In addition to the elements of the assumption deviation risk assessments reflected in Table 1, the recommendations above prescribe an overall judgment of the strength of the background knowledge of the assumption deviation risk assessment. Such an assessment could be performed according to the strength-of-knowledge criteria presented in Section 3.1, and should address inter alia the basis for the judgement of a negligible probability of having a gas detection time in excess of 120 seconds (i.e. a deviation of 90 seconds).

4 DISCUSSION

The methods described in Section 2 and 3 can be used to treat uncertainties and reflect strength of knowledge in a quantitative risk assessment setting. Considering, as described in Section 1, the necessity to balance the desire for coherent quantitative uncertainty characterisation with practical limitations, there is a need for some guidance on when the different methods may be appropriate. In this section we perform an analysis of different settings faced when making assumptions in a risk assessment, and provide some guidance on how to

balance the use of the different methods reviewed in the previous sections. The characteristics of the different settings are summarised in Table 2.

Settings I and II are both characterised by a low degree of belief in deviation from x_0 and a risk index that is not sensitive with respect to x_0. In setting I, as the background knowledge is strong it would be possible to establish a well-founded probability distribution for X; however, since the analyst is confident in the deviation/sensitivity assessment due to the strong background knowledge, he/she could as a simplification resort to simply report $R(x_0)$ to characterise the risk level. The assumption $X = x_0$ of course still needs to be documented in the risk assessment, but it is not highlighted as critical when presenting the results to the decision-maker. If the assumption nonetheless turns out not to hold true, and this contributes to an accident, we experience a surprising extreme event relative to present knowledge/beliefs. This is one way to define black swan type of events (Aven, 2013a); such events require other risk assessment methods than those reviewed here, and are hence out of scope of the present paper.

In setting II the deviation/sensitivity classification remains low/low; however, this judgement is based on a moderate or weak background knowledge. The analyst acknowledges that deviations from x_0 could still occur due to circumstances not considered by the analyst. This is important to be aware of in the subsequent risk evaluation; however, since the basis for a quantification of this uncertainty would not be strong, the analyst could chose instead to highlight a qualitative strength-of-knowledge assessment as described in Section 3.1 when presenting the results to the decision-maker. The guidelines just described related to settings I and II are summarised in Table 3.

Table 2. Settings faced when making assumptions in a risk assessment.

Belief in deviation from assumption	Sensitivity of risk index wrt x_0	Strength of knowledge	
		Strong	Moderate/ weak
Low	Low	Setting I	Setting II
	Moderate/ high	Setting III	Setting IV
Moderate/ high	Low	Setting III	Setting IV
	Moderate/ high	Setting V	Setting VI

Settings V and VI are characterised by a moderate or high degree of belief in deviation from x_0, as well as moderate or high sensitivity of $R(x_0)$ with respect to x_0. Then there is a need to both characterise uncertainty related to X in a more comprehensive manner, as well as to integrate this uncertainty characterisation with the risk index $R(X)$ in a coherent manner. This necessitates a quantitative approach to uncertainty representation.

In setting V the background knowledge on which to base a quantitative uncertainty representation of X is strong; hence a well-founded probability distribution $F(x|z_0, K)$ may be established, which can be integrated with $R(X)$ according to Equation (1). Since the background knowledge is strong, the assumption $Z = z_0$ (Section 2.1) on which F is conditional is non-critical and does not need to be highlighted.

In setting VI the background knowledge on which to base a quantitative uncertainty representation of X is moderate or weak. It may still be possible to establish a probability distribution $F(x|z_0, K)$; however, such a distribution will be based on more or less reasonable assumptions, and so the risk index $E[R(X)|z_0, K]$ resulting from an integration according to Equation (1) needs to be supplemented by an assumption deviation risk assessment of the assumption $Z = z_0$. This could be achieved by reporting of (interval) probabilities

$$q(d|w_0, K) = P(|Z - z_0| > d|W = w_0, K)$$

for different values of d corresponding to different magnitudes of deviation; combined with highlighting of a qualitative strength of knowledge assessment of the background knowledge of the probability $q(d|w_0, K)$, including any new

Table 3. Guidance on treatment of uncertainty related to deviation from assumptions in settings I and II.

Belief in deviation from x_0	Sensitivity of $R(x_0)$ wrt x_0	Strength of knowledge	
		Strong	Moderate/weak
Low	Low	Report $R(x_0)$ List the assumption $X = x_0$ as non-critical	Report $R(x_0)$ Highlight qualitative strength-of-knowledge assessment of assumption $X = x_0$

Table 4. Guidance on treatment of uncertainty related to deviation from assumptions in settings V and VI.

Belief in deviation from x_0	Sensitivity of $R(x_0)$ wrt x_0	Strength of knowledge	
		Strong	Moderate/weak
Moderate/ high	Moderate/ high	Assign $F(x\|z_0, K)$ and determine $E[R(x)\|z_0, K]$ wrt F using law of total expectation List assumption $Z = z_0$ as non-critical	Assign and determine $E[R(x)\|z_0, K]$ wrt F using law of total expectation Highlight assumption deviation risk assessment for assumption $Z = z_0$, based on probability or interval/imprecise probability OR Assign interval/imprecise probability distribution on X and determine resulting interval for $E[R(X)\|K]$

Table 5. Guidance on treatment of uncertainty related to deviation from assumptions in settings III and IV.

Belief in deviation from x_0	Sensitivity of $R(x_0)$ wrt x_0	Strength of knowledge	
		Strong	Moderate/weak
Low	Moderate/ high	Report $R(x_0)$ Highlight assumption deviation risk assessment for assumption $X = x_0$, based on probability OR See Table 4	Report $R(x_0)$ Highlight assumption deviation risk assessment for assumption $X = x_0$, based on probability or interval/ imprecise probability OR See Table 4
Moderate/ high	Low		

assumption $W = w_0$ introduced for some unknown quantity W that q depends on.

Alternatively, the lack of knowledge could be reflected quantitatively by assigning an interval/ imprecise probability distribution on X, leading to an interval for the resulting risk index. The guidelines just described related to settings V and VI are summarised in Table 4.

Settings III and IV are characterised by conditions between settings I/II and settings V/VI; i.e. either by a low degree of belief in deviation from x_0 combined with a moderate or high sensitivity of $R(x_0)$ with respect to x_0, or vice versa.

If the frame conditions of the risk assessment are such that there is an expectation for or are resources available to perform a more detailed assessment, then the guidelines given for settings V and VI apply to settings III and IV, respectively. Otherwise an assumption deviation risk assessment should be performed; in setting III based on probability as the background knowledge is strong; in setting IV possibly based on interval/imprecise probability to reflect that the background knowledge is only moderate or weak. These guidelines for settings III and IV are summarised in Table 5.

The guidelines presented in Table 5 rely on two central premises. Firstly, the more important an assumption is, the more effort should be expended on characterising uncertainty and effect related to potential deviation. Six levels of importance are distinguished, corresponding to the settings I-VI. Secondly, the methods reviewed are associated with an increasing level of effort, ranging from low for the qualitative assessment as described in Section 3.1, through moderate for assumption deviation risk assessment as described in Section 3.2, to high for the establishment of a full (interval/imprecise) probability distribution on X as described in Section 2. The presented guidelines couple the different settings with different (combinations of) methods, in an attempt to balance the desire for coherent quantitative uncertainty characterisation with practical limitations.

5 CONCLUSION

Making assumptions are an inevitable aspect of performing risk assessments. The assumptions may be more or less reasonable, i.e. there may be more or less uncertainty about whether the conditions these specify hold true. In principle, this uncertainty can be handled quantitatively, but in practice, this may be prohibitively difficult due to a large number of assumptions and hence a high workload associated with establishing the required

probability distributions; and/or the background knowledge on which to base the quantification may be poor. Alternatively, a semi-quantitative approach can be taken, based on a combination of quantitative descriptions and qualitative methods.

In the present paper we review various quantitative and semi-quantitative methods. These are associated with different levels of effort and, based on the premise that the more important an assumption is the more effort should be expended on characterising uncertainty and effect related to potential deviation, we conclude that there is a need to balance the use of the different methods. We distinguish six different settings arising from different levels of beliefs about deviation from an assumption, sensitivity of the relevant risk index with respect to changes in the assumption, and overall strength of knowledge on which to base uncertainty quantification. These different settings are then coupled with different (combinations of) methods, in an attempt to balance the desire for coherent quantitative uncertainty characterisation with practical limitations. The resulting recommendations are summarised in Table 3, Table 4 and Table 5 in Section 4.

ACKNOWLEDGEMENTS

The work has been partly funded by the PETROMAKS2 programme of the Research Council of Norway. The financial support is gratefully acknowledged.

REFERENCES

Aven, T., Zio, E., Baraldi, P., & Flage, R. (2014). *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods*. John Wiley & Sons.

Aven, T. (2013a). On the meaning of a black swan in a risk con text. *Safety science*, 57, 44–51.

Aven, T. (2013b). Practical implications of the new risk perspectives. *Reliability Engineering & System Safety*, 115, 136–145.

Aven, T., (2012). *Foundations of Risk Analysis*. 2 Edition. Wiley.

Aven, T. (2010). On how to define, understand and describe risk. *Reliability Engineering & System Safety*, 95(6), 623–631.

Coolen, F., Troffaes, M. and Augustin, T. (2010). Imprecise Probability, *International Encyclopedia of Statistical Science*, Springer.

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability & Risk Analysis: Theory & Application*, 2(13), 9–18.

Jonkman, S.N., van Gelder, P.H.A.J.M. & Vrijling, J.K. 2003. An overview of quantitative risk measures for loss of life and economic damage. *Journal of Hazardous Materials* 99(1): 1–30.

Mosleh, A & Bier, VM 1996. Uncertainty about Probability: A Reconciliation with the Subjectivist Viewpoint. IEEE Transaction on Systems, Man, and Cybernetics—Part A: *Systems and Humans* 26(3): 303–310.

Vinnem, J.E. (2007). *Offshore risk assessment: principles, modelling and applications of QRA studies*. Springer.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Comparison of uncertainty models of impact of teleinformation devices reliability on information quality

M. Stawowy
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: This research is a continuation of previous work related to the determination of Information Quality (IQ) for different systems. IQ is it a top level of evaluation of this information. IQ is depends on: accessibility, actual value, completeness, credibility, flexibility, form, meaning over time, relevance, reliability, selectivity, validity. But many researchers believed reliability of the teleinformation devices (the IT devices) is one of the main components of IQ. I would like to present a new approach for estimating the IQ with specific regard on reliability of the IT devices. This approach is based on modelling uncertainties. For this purpose, I used two known methods and compare it. Estimate IQ using the method Certainty Factor (CF) and Dempster-Shafer (DS) method.

1 INTRODUCTION

The reliability of data communication elements is an important constituent part on the quality of transferred information (IQ). It may be stated that IQ consists of: accessibility, actual value, completeness, credibility, flexibility, form, meaning over time, relevance, reliability, selectivity, validity (Olaisen 1990, MITIQ). All the above components of IQ tend to be encumbered by some uncertainty. Whether associated with measurement or caused by the unreliability of equipment or software. Hence, the proposal to determine IQ using uncertainty modelling. There are several major methods of uncertainty modelling. The best known are Bayes networks based on conditional probability, the theory mathematical evidence based on the Dempster-Shafer theory, the method making use of the Certainty Factor (CF) created by Buchanan, Shortliffe for the MYCIN expert system, the theory of fuzzy sets or the theory of rough sets.

This paper presents and compares methods: basing on the theory of mathematical evidence (Dempster 1967, Shafer 1976) (DS) and using the certainty factor of a hypothesis (Shortliffe & Buchanan 1984, Heckerman 1992, Stawowy 2013) (CF) to evaluate the information quality. Uncertainty models of impact of teleinformation devices reliability on information quality. These methods was chosen because make possible modelling uncertainty on the basis of values from various sources. Usually, known publications talking about statistical models like Vinay & Khelil & Suri 2010 or Weng & Vespa 2011. Presented work by Raghunathan 1999 was similar but not used presented in this article method and not compared it.

2 MODELLING UNCERTAINTY

The first part of this chapter specifies the dependencies used to calculate the values of the CF. It results from the variable directions of development of this method.

2.1 *Modelling the certainty factor of a hypothesis*

The formal simplified description of the certainty factor is as follows:

$$CF_{(s)} = MB_{(s)} - MD_{(s)} \tag{1}$$

where *CF*—certainty factor; *MB*—reflection of knowledge, that is measure of belief; *MD*—reflection of ignorance, that is measure of disbelief; *s*—hypothesis based on some information.

It is important to remember that:

$$MB \to [0,1]; MD \to [0,1] \; then \; CF \in [-1,1] \tag{2}$$

So, as it results from formula 2 the result of the calculations should fit within the range from –1 to 1. The value of 1 will indicate the highest IQ.

A model using the CF can be presented in the form of a graph where the nodes are the hypotheses and the branches are the certainty factors of the hypotheses. A sample model has been presented in Figure 1.

The whole begins from observation nodes (e1, e2), the node of hypothesis h1, which in fact becomes an observation in the further step of calculations, appears subsequently. The following

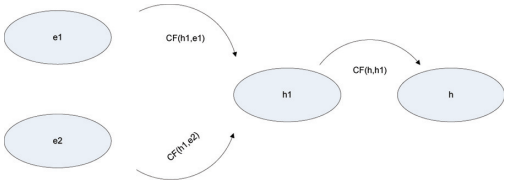


Figure 1. Sample CF model. Prepared by the author.

dependence has been used for calculation of parallel CFs (Heckerman 1992):

$$CF_{(h1,e1,e2)} = \begin{cases} CF_{(h1,e1)} + CF_{(h1,e2)} - CF_{(h1,e1)} \cdot CF_{(h1,e2)}, CF_{(h1,e1)}\ and\ CF_{(h1,e2)} \geq 0 \\ \dfrac{CF_{(h1,e1)} + CF_{(h1,e2)}}{1 - \min(\left|CF_{(h1,e1)}\right|;\left|CF_{(h1,e2)}\right|)}, \qquad CF_{(h1,e1)} \cdot CF_{(h1,e2)} < 0 \\ CF_{(h1,e1)} + CF_{(h1,e2)} + CF_{(h1,e1)} \cdot CF_{(h1,e2)}, CF_{(h1,e1)}\ and\ CF_{(h1,e2)} < 0 \end{cases} \tag{3}$$

The following dependence has been used for calculation of serial CFs (Heckerman 1992):

$$CF_{(h,h1,e1,e2)} = CF_{(h1,e2,e1)} \cdot CF_{(h,h1)} \tag{4}$$

Using formulas 3 and 4 the graph can folded down to a single branch with two nodes and the CF of this branch will be the sought value of the certainty factor of a hypothesis. We assume that such CF coefficient is the measure of information quality IQ. In this work only formula 3 was used because model was only parallel (Shortliffe & Buchanan 1984, Heckerman 1992, Stawowy 2013).

2.2 *Modelling uncertainty using the theory of mathematical evidence*

The theory of evidence assumes that it is possible to conduct a synthesis of information for particular elementary measures of probability. Information can be synthesised even if it is contradictory or comes from various sources (Dempster 1967, Shafer 1976). Such synthesis can be described by the following formula:

$$m_3(C) = \frac{\sum_{A_i \cap B_j = C} m_1(A_i) m_2(B_j)}{1 - \sum_{A_i \cap B_j = O} m_1(A_i) m_2(B_j)} \tag{5}$$

where *A, B and C*—sources of observations represent subsets of set Θ; m_1 *and* m_2—sets of masses; m_3—new set of mass.

This synthesis is called the Dempster combination rule (Dempster 1967).

The belief mass (called as *basic belief assignment* BBA) is defined as follows:

$$\begin{aligned} &m: 2^{\Theta} \rightarrow [0,1] \\ &m[\varnothing] = 0 \\ &\sum_{A \subseteq \Theta} m(A) = 1 \end{aligned} \tag{6}$$

Belief marked in brief Bel ∈ [0,1] measures the strength of acquired observations supporting the belief on the authenticity of the examined set of hypotheses.

$$Bel(A) = \sum_{B \subseteq A} m(B) \tag{7}$$

Plausibility designated in brief as Pl ∈ [0,1] determines how much the belief on authenticity A is limited by supporting evidence ¬A.

$$\begin{aligned} &Pl(A) = \sum_{B \cap A \neq 0} m(B) \\ &Pl(A) = 1 - Bel(\neg A) \end{aligned} \tag{8}$$

The combination rule affects the belief function and it can presented in such a way:

$$Bel1 \oplus Bel2(A) = \sum_{B \subseteq A} m_1 \oplus m_2(A) \tag{9}$$

Assume was that Bel is the measure of information quality IQ.

3 MODEL OF INFORMATION QUALITY OF A SELECTED DATA COMMUNICATION SYSTEM

Most often found is the data communication system based on TCP/IP (Transmission Control Protocol/ Internet Protocol) as well as IEEE 802 (Institute of Electrical and Electronics Engineers) protocols. By relying on the model of ISO OSI (International Organization for Standardization Open Systems Interconnection) the model of such a system can be presented in a manner shown in Figure 2.

Apart from normal damage of constituent elements of such a data communication system, data can also be damaged in spite of the fact that the recipient of this fails to notice. The possible causes are: imperfection of protection with CRC code (Cyclic Redundancy Check) in the layer of data links, incorrect configuration of transmission in the network layer e.g.: improperly set TTL (Time To Live) field in the IP protocol or unauthorised change of data.

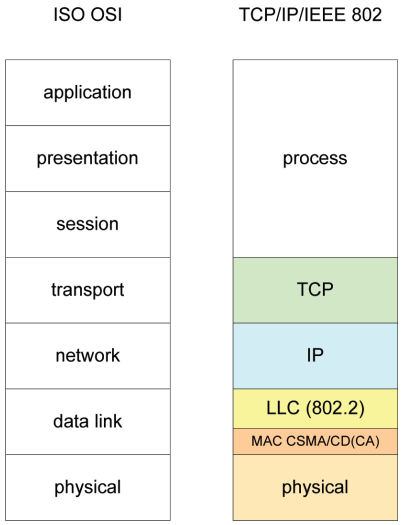


Figure 2. Model of a data communication system of TCP/IP as well as IEEE 802 protocols as compared to the model of ISO OSI. Prepared by the author based on International standards.

Values of all IQ components tend to be encumbered by some uncertainty. Whether associated with measurement or caused by the unreliability of equipment or software. Hence, the proposal to determine IQ using uncertainty modelling. The theory of mathematical evidence based on the Dempster-Shafer theory (DS) as well as the method of making use of the Certainty Factor (CF) created by Buchanan, Shortliffe for the MYCIN expert system have been applied here. These methods make it possible to model uncertainty on the basis of premises from various sources.

A model of information quality based on the CF or DS model may consist of one final hypothesis:

h—correctly provided data.

Observations can be as follows:

e1—correct transmission,
e2—data link layer errors (e.g.: imperfection of CRC,
e3—damage of transmission connection,
e4—damage of network control devices,
e5—damage or defective software,
e6—network layer errors (IP protocol),
e7—transport layer errors (TCP protocol).

3.1 *Modelling information quality of a selected data communication system by means of the certainty factor of a hypothesis*

The previous chapter describes two methods of uncertainty modelling. In the example concerned both can be used to evaluate the information quality (IQ). Using CF-based uncertainty modelling the graph may be presented as in Figure 3 and the value of particular CF presented as in Table 1. Values is not real but near real. Used for method demonstration only.

Calculated IQ using CF-based uncertainty modelling IQ(CF) was about 0,984.

Another step was the simulation. A special program has been written in order to conduct the simulation. This program uses standard normal distributions. The distributions have been used as multiply for all input values and limited with a range of values that may be accepted by the CF according to formula 2. The number of repetitions of the simulation amounted to 10000. The result of the simulation is presented in Figure 4. There is a density function of CF values after simulation.

3.2 *Modelling information quality of a selected data communication system using mathematical evidence*

Information from various sources can be synthesised using the theory of mathematical evidence. It has been described with formula 5.

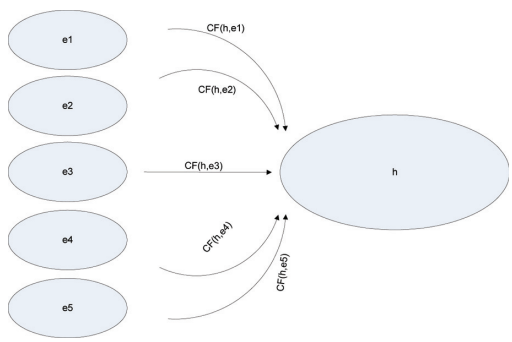


Figure 3. CF model graph. Prepared by the author.

Table 1. Assignment of particular CF values. Prepared by the author.

h
CF(h,e1) = 0.998
CF(h,e2) = $-0.2 * 10^{-2}$
CF(h,e3) = $-0.1 * 10^{-2}$
CF(h,e4) = $-0.1 * 10^{-2}$
CF(h,e5) = $-0.1 * 10^{-2}$
CF(h,e6) = $-0.1 * 10^{-2}$
CF(h,e7) = $-0.1 * 10^{-2}$

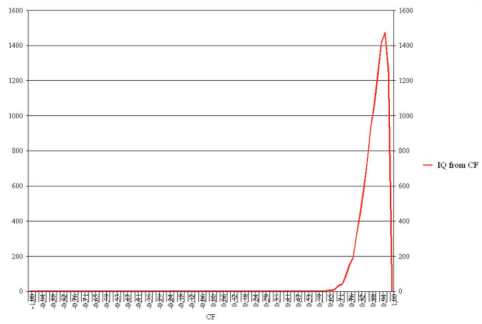


Figure 4. Result of CF model simulation. Result of operation of a program written by the author of the article.

Table 2. Observation Ze1. Prepared by the author.

	m_2 ({e1})	m_2 (Θ)
m_1 (Θ)	m_3 ({e1})	m_3 (Θ)

Table 3. Observation Ze2. Prepared by the author.

	m_4 ({e3, e4, e5})	m_4 (Θ)
m_3 ({e1})	m_5 ({Ø})	m_5 ({e1})
m_3 (Θ)	m_5 ({e3, e4, e5})	m_5 (Θ)

Table 4. Observation Ze3. Prepared by the author.

	m_6({e2, e3, e4, e5, e6, e7})	m_6 (Θ)
m_5 ({Ø})	m_7 ({Ø})	m_7 ({Ø})
m_5 ({e3, e4, e5})	m_7 ({e3, e4, e5})	m_7 ({e3, e4, e5})
m_5 ({e1})	m_7 ({Ø})	m_7 ({e1})
m_5 (Θ)	m_7 ({e2, e3, e4, e5, e6, e7})	m_7 (Θ)

Let's define the three observations of effects on the basis of observation of causes.

Ze1—correct transmission, (e1),
Ze2—data failed to reach destination (e3, e4, e5),
Ze3—data reached destination, but are incorrect (e2, e3, e4, e5, e6, e7).

Tables 2–4 present the subsequent stages of the analysis of observation of effects.

Θ = {e1, e2, e3, e4, e5, e6, e7}

m_1 (Θ) = 1
m_2 ({e1}) = 0.998 (10)
m_2 (Θ) = 0.002

m_4 ({e3, e4, e5}) = 0.003 (11)
m_4 (Θ) = 0.997

m_6 ({e2, e3, e4, e5, e6, e7}) = 0.007 (12)
m_6 (Θ) = 0.993

Bel (e1) = m7 (e1) (13)

If we assume that Bel (e1) = IQ is a result of calculations using the theory of mathematical evidence modelling, it is only slightly different from the result of modelling of the certainty factor of a hypothesis. However, the simulation may show that they differ only by the coefficient. Calculated IQ(DS) was about 0,998.

3.3 *Comparison of results of simulation of both methods*

Simulations was prepared like simulations CF in 3.1 chapter but for both models. During the simulations the values from both methods seem to be similar. After the completion of the simulation for different values of observations one can recognise that both

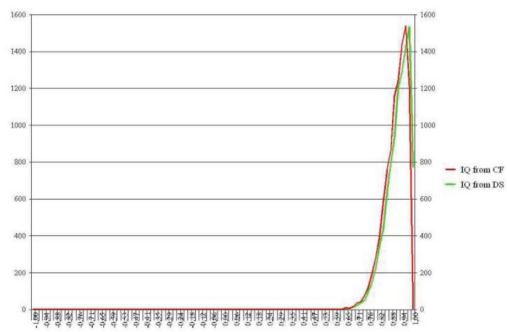


Figure 5. Result of simulation of DS and CF model. Result of operation of a program written by the author of the article.

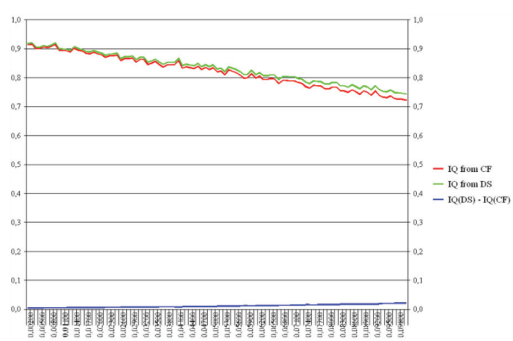


Figure 6. Result of simulation of DS and CF model e3 from 0,001 to 0,1 for DS and minus values for CF. Result of operation of a program written by the author of the article.

results are very similar (Fig. 5). The conclusion is that both methods are suitable for determination of information quality to an equal extent.

The next step was comparison of the simulations of IQ(CF) and IQ(DS) for the parameters of reliability of the elements of the sample system. Those elements were observations: e3, e4 and e5.

A simulation was carried out for e3, e4 and e5 variables in the range from 0.001 up to 0.1. The result has been presented in Figures 6, 7 and 8. There is values of IQ(CF), IQ(DS) and difference from it for different values of three observations: e3, e4 and e5. These observations are defined on the begin of this chapter and are related to reliability (Meeker, Stawowy 2010).

The CF method has greater dynamics, since the result may vary from –1 to 1, also on the simulation graph IQ (CF) changes faster than IQ (DS). Differences IQ (DS) – IQ (CF) take the form of a straight line. This means that the values IQ (DS) and IQ (CF) differ only by a constant factor.

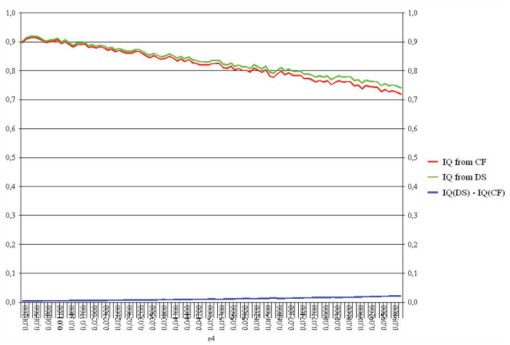


Figure 7. Result of simulation of DS and CF model e4 from 0,001 to 0,1 for DS and minus values for CF. Result of operation of a program written by the author of the article.

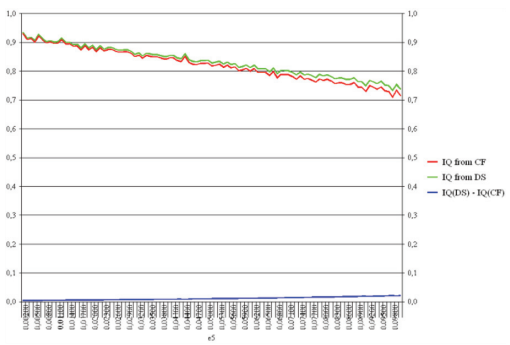


Figure 8. Result of simulation of DS and CF model e5 from 0,001 to 0,1 for DS and minus values for CF. Result of operation of a program written by the author of the article.

4 SUMMARY

This paper presents the method of determination of information quality (IQ) on the basis of reliability of the components of a data communication system using two different methods. The first was based on uncertainty modelling with the use of the certainty factor of a hypothesis, the other using the theory of mathematical evidence. Both methods have given a similar result. Difference is very small and it is result of different range of final values. Range of final value of IQ(DS) is [0,1] and IQ(DS) is [–1,1]. On the basis of the results, it can be concluded that the two methods give similar results and can be used to modelling the IQ.

Also a simulation of the example has been made using normal distributions along with a simulation comparing both methods.

REFERENCES

Dempster A.P. 1967. Upper and lower probabilities inducted by a multi-valued mapping. *The Annals of Mathematical Statistics* 38, 1967, 325–339. USA.

Heckerman D. 1992. The certainty-factor model. In S. Shapiro, editor, *Encyclopedia of Artificial Intelligence, Second Edition*, pages 131–138. New York: Wiley.

International standards ISO/IEC. *www.iso.org*. 2382–25.

Meeker, W. Q., Escobar L. 1998. Statistical methods for reliability data. US and Canada: John Wiley & Sons Inc.

MITIQ MIT Information Quality Program. 2014. *http://mitiq.mit.edu*.

Olaisen, J. 1990. Information quality factors and the cognitive authority of electronic information. Wormell, I. (Ed.), *Information Quality: definitions and dimensions*, London: Taylor Graham.

Raghunathan, S. 1999. Impact of information quality and decision-maker quality on decision quality: a theoretical model and simulation analysis. *Decision Support Systems* 26 1999. 275–286. Dallas.

Shafer, G. 1976. A mathematical theory of evidence. *Princeton University Press.* Princeton.

Shortliffe, E.H. & Buchanan, B.G. 1984. Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. USA & Canada: Addison-Wesley Publishing Co., Inc.

Stawowy, M. 2010. Reliability of data obtained from video systems of traffic surveillance. *Archives of Transport System Telematics,* ISSN 1899-8208. vol. 3, iss. 3, 2010: 46–51. Katowice.

Stawowy, M. 2013. Wyznaczanie jakości informacji w telematyce autostradowej. *Prace naukowe—Transport* ISSN 1230-9265. 92/2013: 221–229. Warszawa.

Vinay, S. & Khelil, A. & Suri, N. 2010. Quality of information in wireless sensor networks: A survey. *International Conference on Information Quality 2010*. Germany.

Weng, Ning, I. Li, & Vespa, L. 2011. Information quality model and optimization for 802.15. 4-based wireless sensor networks. *Journal of Network and Computer Applications* 34.6 (2011): 1773–1783. USA.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Sensitivity analysis of geological parameters having impact on nuclear waste deep geological repository safety

J. Chudoba
Technical University of Liberec, Liberec, Czech Republic

ABSTRACT: When evaluating nuclear waste DGR safety it is necessary to confirm its safety in a long run and above all its safety towards the biosphere. With the aid of geologists a model of the Melechov Massif was elaborated and described with the use of geological and hydrogeological parameters. The paper results showed that ground water flow and transport of substances within the area (3D geometry) were the first ones to be determined. The Flow123D SW (Brezina 2012) was used for the determination. The resulting outcome represents a determination of transported substances concentration depending on time and its "function" is shown graphically or in the map form. The disadvantage of the model is the fact that all the input parameters were set deterministically. The problem is being solved using the sensitivity analysis.

1 INTRODUCTION

In the Czech Republic, there are two nuclear power plants: Dukovany and Temelin (with 6 blocks) producing highly-active nuclear waste. The waste has to be handled in a long run well to guarantee it will not be misused anytime anyway and—in the same time—to minimize risks for biotopes. Preparation-work and the future realization of such a Safe Nuclear Waste DGR has been carried by the Deep Geological Repository Authority of the Czech Republic (SURAO)—www.surao.cz.

The basic concept of the nuclear waste depository is described in the report: "The Reference Project of a Nuclear Waste DGR in a hypothetical locality and its Actualization" (Vokal 2011, Mandik 1999). The idea is that nuclear waste will be deposited in granite massive underground in the depth of about 500 m (in the Czech Republic). Now, suitable localities (that have been selected) are being checked and pass through for a detailed geological and hydrogeological research. The own building of such a DGR (Deep Geological Repository) is forecasted for the year 2040. The hot issue of nuclear waste DGR represents of course a complex problem—combined with THMC processes (thermo-hydro-mechanical and chemical processes).

Calculations on ground water flow and on dissolved substances transport are based on a hypothetical locality in the Melechov Massive. The locality is not determined for the a.m. DGR but a detailed geological and hydrological research had been carried there in the past. To calculate ground water flow and substances transport we used the SW Flow123D—https://dev.nti.tul.cz/trac/flow123d (Brezina 2012) The main advantage of the SW is that it processes data on flow and transport parameters on the 3D area, which is divided into 2D and 3D elements. The resulting output of a task on the flow is the determination of velocity and a direction of the flow and the determination of volume of a substance coming over the walls of the elements. Analogously, the resulting output of a task on the substance transport is the determination of a dissolved substance concentration (volume activity) depending on time in individual elements.

The paper deals with an analysis of critical radioactive substances transport out of a nuclear waste DGR. A 3D model of the area was designed and it is described with 37 000 elements (where the 2D elements represent fissure and the 3D elements represent the massive). The task on flow and substances transport was calculated with the SW Flow123D (Brezina 2012). The geological and hydrogeological parameters at the input corresponded with the geological and hydrogeological research, which had been carried out there in the Melechov massive in the past (Rukavickova 2008, Maryska 2010). The Melechov Model contains the following parameters:

- Hydraulic conductivity of rocks and fissures.
- Porosity of rocks and fissures zones.
- Fissures opening.

The substances transport is described with a real model containing the following:

- Time-variable radioactive substances release out of the near/far field border. Results on quantity of the released radioactive substances were

detected using the SW GoldSim—www.goldsim.com (GoldSim). All of the critical isotopes according to were covered.
– Radioactive Degradation of Substances
– Sorption Parameters K_d and Diffusion Coefficients D_e of transported radionuclides

The model did not consider the maximal dissolution of a substance in the water as the quantity of released radioactive substances is about 2 g/yr maximally. The output of the task is the determination of the substance concentration [ng/m^3] recalculated in volume activity [Bq/m^3] in individual elements—based on time. A special stress is put on the ground elements where radioactive substances penetrate into biotopes. To calculate the "received" dose [μSv] we chose a scenario based on a presumption that a human was drinking water from the ground (of the area) in the quantity of 0.002 [m^3/day].

A sensitivity analysis of the model was designed with a parameter change. The analysis is for finding parameters that have the most impact on the concentration change of the selected elements—mainly the ground ones. The following parameters were changed: hydraulic connectivity of rocks and fissures, rocks porosity, opening of fissures and—for each of the transported substances its sorption K_d. The changes describe changed hydrogeological conditions of the researched area in a long run. The output of the sensitivity analysis is a table where all of the stated parameters are shown, those which have the most impact on the increased concentration of substances on the ground elements.

The paper extends case studies issued before with the following:

– Time-variable feature of released isotopes.
– Radioactive degradation of substances.
– Implementation of sorption and diffusion coefficients.
– Calculation for more substances.
– Results re-calculation of received dose [μSv] for the selected scenario.

2 DESCRIPTION OF THE LOCALITY AND INPUT DATA OF THE MODEL

The designed model of the DGR is situated in the locality of the Melechov Massive located about 150 km to the Southeast from Prague.

In order to perform the desired analysis, a mathematical mesh was formed describing the massif of Melechov. The mesh covers the area of about 10 000 × 10 000 × 1300 m. The model mesh was created basing on geologic data, listed in (Rukavickova 2008, Maryska 2010). The suggested model contains a few vertical and horizontal rift fissures and 40 types of materials displaying different physical characteristics, such as hydraulic conductivity for example.

For the Melechov Massive—the geometry was prepared first. Then we generated a calculation mesh of the system. We used software Flow123D For the calculation of simulating task. The mesh contains in total 7174 nodes and 37 069 elements. There are 2140 ground elements, where a transport of radiation into the biosphere can happen. The challenge was to specify (make more accurate) the distribution function of concentrations in the elements of the area. (Chudoba 2012).

A geological research had been carried in the area in the past. The results of the research helped to set types of rocks, the location of fissures and to determine their hydraulic conductivity. Later, the following was discovered:

– Its geological structure—porous massif or fractural zones of the rock.
– Types of rocks there—granit of *melechov* type, granit of *kout* type, granit of *Lipnice* type, gneiss.

Then we considered different physical features of the environment according to the depth analysis of the area for the depths of 75, 150, 400, 600, 800, and more than 800 m. Input details of hydraulic conductivity for a particular type of a rock and fissures are stated in Table 1. To set the boundary condition, three basic parts of boundaries were stated within the simulated area. The Boundary condition and hydraulic conductivity in the

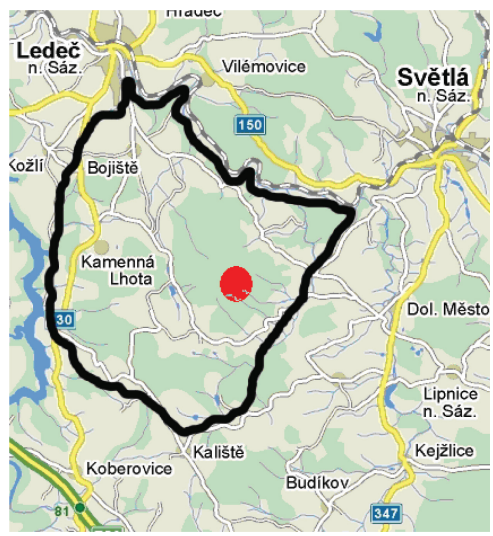


Figure 1. Map of area hypothetical DGR.

Table 1. Hydraulic conductivity of particular type of rock and rifts.

Hydraulic conductivity [mm/year]				
Deep to [m]	Melechov type	Kout type	Lipnice type	Gneiss
Type of rock				
75	18000	5400	1800	360
150	2880	860	288	57.6
400	288	43	28.8	5.76
600	28.8	8.6	2.88	0.36
800	5.4	1.53	0.54	0.072
>800	1.08	0.324	0.12	0.012
Deep to [m]	Without specification of rock		Deep to [m]	Without specification of rock
Vertical rifts				
75	14400		600	3600
150	7200		800	1800
400	7200		>800	720
Deep to [m]	Melechov type	Kout type	Lipnice type	Gneiss
Horizontal rifts				
150	72000	36000	36000	18000

Table 2. Sorption parameters K_d and diffusion coefficients De and the maximal dissolution of substances.

Substances	K_d [m³/kg]	D_e [m²/s]	Dissolution [mol·m³]
C14	0.0005	5,0E-15	Unlimited
Cl36	0	8,00E-15	Unlimited
Ni59	0.01	2,80E-14	
Se79	0.0005	4,00E-14	2.59E-6
Mo93	0.0005	1,00E-15	1.0E-3
I129	0	8,00E-15	Unlimited
Cs135	0.01	9,00E-13	Unlimited
Ra226	0.01	3,70E-14	1.2E-1

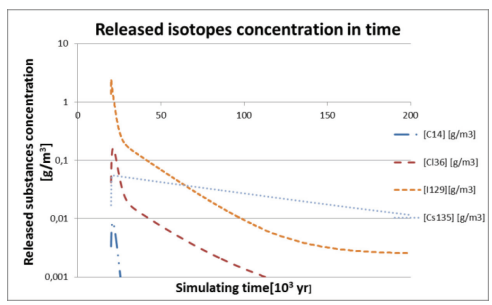


Figure 2. Quantity of released isotopes in time.

individual parts within the simulated massif were calibrated to:

– The piezometric height in the upper layer of the model area at the level of underground water.
– 1% of rain level deeper than 800 m under the ground.

Sorption Parameters K_d and Diffusion Coefficients D_e of substances were taken from a reference project (Vokal 2011). The values of those parameters are stated in the Table 2.

Another input into the model was substance quantity released from the near to the far field in time. A conservative case was considered—that was the container damage in the time of 20 000 years. A concrete plug is considered to be around the container with a bentonite package preventing immediate contamination of ground water. The calculation of the quantity of released substances was done through the simulation SW GoldSim. Figure 2 shows a graph describing critical isotopes release in time. Calculations of different variants of container damage were done in the analysis. Those scenarios were less conservative and that is why they are not mentioned here.

3 BASIC MODEL RESULTS

A model analysis, which was performed using the SW Flow123D (Brezina 2012), helped to determine the state of concentration (a volume activity) in time for all the elements used in the calculated mesh. We supposed the zero concentration of isotopes within the area at the beginning of the simulation. The DGR (Surao) in the calculated

mesh was modeled in the way that an element was withdrawn and a non-zero concentration on the walls of the withdrawn element was entered. Thanks to the element withdrawal it is possible to model variable-in-time quantity of released radioactive substances.

For modelling purposes the simulated time was 200 000 years with a damage of all the containers containing spent nuclear fuel set on 20 000 years. The time (20 000 years) represented quite a pessimistic forecast, more optimistic forecasts were also modeled (those ones also considered quite a different character of containers damage—e.g. the Weibull Distribution).

The input parameters of the model are stated in the Chapter 2 (the definition of the area geometry, hydraulic conductivity and porosity of rocks and fissures zones, fissures openings, substances sorption parameters, diffusion coefficient, released volumes of substances in time). These parameters are analyzed (in the view of the model sensitivity and supposing the same calculated mesh but different input parameters—e.g. those of hydraulic conductivity or porosity) in the Chapter 4.

Progress (state) of volume activities of ground water (Bq/m^3) in time was found for all the elements in the calculated mesh within the task. In total 2000 elements with non-zero concentration were recorded (from the total amount of 37 000) and from those elements the following ones were analyzed in a more detailed way:

– Elements that were found on the surface of the area where isotopes penetrated biotopes (out of the geosphere). There were 2140 surface elements within the area. In the paper, results for 1 element are presented. The element with the most volume activity of isotopes. Results of other elements are stated v (Chudoba 2014).

  Elements that formed the main transport line out of the DGR onto the surface of the area of the maximal recorded volume activity. The main transport line is formed with 10 elements.
– Elements that were found near the surface of the area (forming a layer at more than 400 m above the sea level), that could turn into surface elements (due to denudation) in future.

Within the task volume activity graphs were designed for each of the elements (in time). Another outputs of the task were maps showing substances concentration at the given sea level. Results obtained (for all the isotopes) were used in radioactive dose calculations. To determine the dose, the scenario of 1 m^3 ground water drunk by a human being a year had been chosen. Based on that scenario ingestion factors were found (SKB 2002) and were stated for all the critical radionuclides shown in Table 3.

Table 3. The ingestion factor for the critical isotopes, the maximal recorded volume activity on the surface element and the dose calculated basing on the given scenario.

Isotope	Ingestion factor [Sv/Bq]	Max. volume activity [Bq/m^3]	Dose [μSv/m^3]
C14	5,80E-10	30000	17,4
Cl36	9,30E-10	9500	8,8
I129	1,10E-07	540	59,4
Cs135	2,00E-09	700	1,4
Ra226	2,80E-07	85	23,8
		Sum	110,8

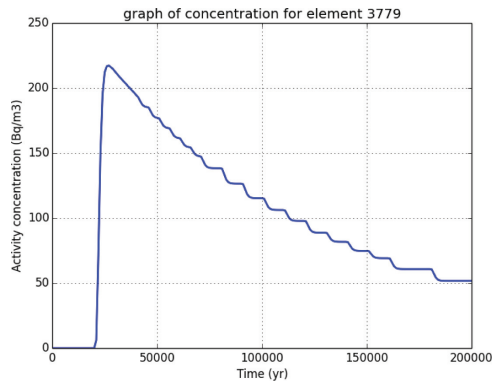


Figure 3. Volume activities of I129 on the surface element in time.

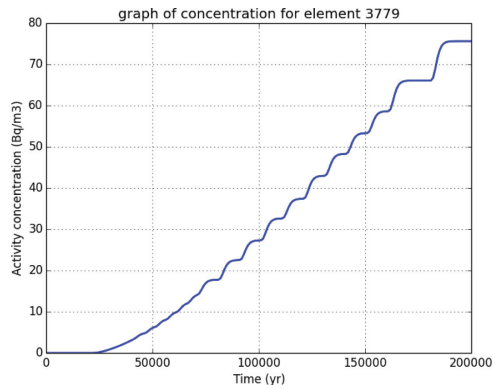


Figure 4. Volume activities of and Ra226 on the surface element in time.

In Figures 3 and 4 there are volume activity graphs for the critical isotopes for one surface element (the one of the maximal activity) in time. It is quite clear, that the released quantity of isotopes and the activity of elements on the surface are strongly dependent on

the simulated time, the half-life and the course of its release out of the near/far field borders.

The crucial impact on the total radioactive dose (after the containers damage) had the I129, which did not absorb, with unlimited dissolution and with a too long half-life (15.7 Myr). Another disadvantage is its immediate release out of the damaged container—resulting in the worst possible situation where all the containers are damaged at once in the given simulated time. The total dose therefore is not dependent on the time of the damage of all the containers—only a shift of the maximal activity towards the maximum is shown in the graph. Using the Weibull Distribution to describe the containers life-time it is necessary to consider the value of β.parameter. The similar problems are with I C14 with shorter half-life time and that absorbs very little. The both isotopes penetrate into biotopes and into food-chain too easily—increasing that way their potential perilousness.

Another of the elements that has a crucial impact on the total dose is the Ra226, arisen with radioactive degradation of uranium matrix—with a short half-life (1600 years) the released quantity is increasing with natural degradation of safety barriers and a large mass of U238 concentrated in a small volume of the DGR.

In Table 3 there are shown the maximal volume activities of isotopes on the surface element of the maximal volume activity in the given simulated time. The total dose received by a human with the given scenario (1 m^3 of ground water drunk a year) is calculated out of the volume activities. The other isotopes (not mentioned in Table 3) have lower impact on the given scenario—less 1 μSv. The total dose on other elements is lower (as it is shown in Fig. 4).

The map of volume activity was designed (pls. see Fig. 5) in a similar way. The map shows the surface area with volume activity of isotopes. It is clear that a substance reaches only a small part of the modeled area and that is why it is not necessary to extend the modelled area. Similar maps were designed for cuts of a given sea-levels. The cuts can be used to model denudation of the area in future.

The SW GoldSim (GoldSim) does not provide calculations of ground water flow. Knowing the preference line—1D geometry or cut geometry—2D area could be connected using components of physical relations and the resulting concentration of a substance (in the area) could be calculated. "Cell Pathway"—representing a mix chemical reactor and "Pipe Pathway"—representing chemical colony—belong among those basic components.

The transport module (knowing flow among components) is for the transport of more substances calculating: variable-in-time quantity released on the near/far filed border, sorption

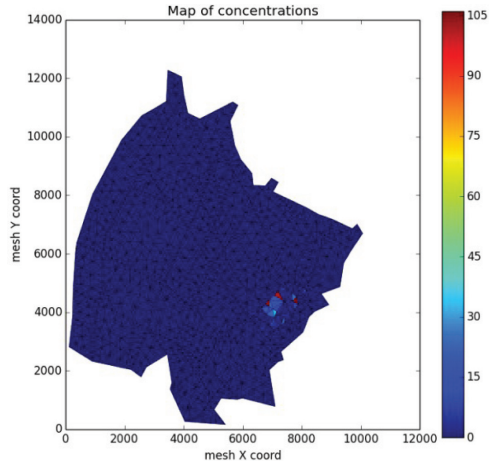


Figure 5. Map of volume activity (Bq/m^3) I 129 on surface elements in the simulated time of 50 000 years.

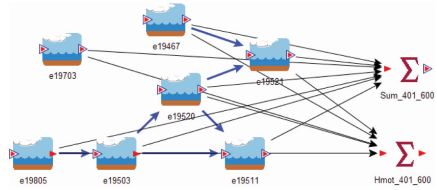


Figure 6. A sample of a modeled part designed using the SW GoldSim.

parameters, radioactive degradation, diffusion coefficient and the maximal dissolution of a substance in ground water.

The task model of flow and transport described at the beginning of the Chapter 2 (using the SW Flow123D) was also analyzed using the SW GoldSim. Geometry of the area was chosen basing on elements with non-zero concentration of a substance—they represented the input data for the model using the SW GoldSim. The Complexity of the Conversion was due to the fact that the elements entered using the SW Flow123D were of the tetrahedron shape and that is why the conversion of overflows between walls in the flow task was so complex. A sample of a part of the model for a few elements near the DGR is shown in the Figure 6. Both tasks reached quality—correspondence in model results.

4 SENSITIVITY ANALYSIS THROUGH PARAMETER CHANGE

Sensitivity Analysis through Parameter Change is based on a comparison of substance concentration

between the Reference Task and the Task with Changed Input Parameters (Chudoba 2010, Chudoba 2014). The basic parameters that are changed are the following:

- Hydraulic conductivity of fissures and rocks that was changed as follows: 0,1; 0,2; 0,5; 2; 5 and 10 multiple of the former value calculated for every type of rock or fissure. There are 38 types of rocks within the area, which represented 228 tasks in total.
- Fissures openings (14 types of openings in total) that were changed in 0,5 and 2 multiple of the former value, which represented 28 tasks in total.
- Porosity that was changed from the former value of 0,5 for 0,25 and 0,75 (mainly fissure zones and the surface area); the former value of 0,05 was changed for 0,02 and 0,10; the former value of 0,01 was changed for 0,005 and 0,02, which represented 76 tasks (38 × 2) in total.
- Sorption parameters of substances were changed as follows: 0,1; 0,5; 2 and 10 multiple of the former value (only for absorbing substances), which represented 4 tasks in total.

Those changes were made for all the isotopes of a higher radioactive dose (more than 1 μSv) in the basic model, which were: C14, Cl36, I129, Cs135 and Ra226. Each of them had to be evaluated individually due to their different half-life, different character of their release out of the near/far field and different absorption properties.

The designed tasks of transport with changed parameters were calculated using the SW Flow123D (Brezina 2012). The resulting concentrations (volume activities Bq/m^3) were analysed and tasks where the change of an input parameter caused the strongest response, i.e. an increase of substance concentration (volume activity) on selected elements were found, afterwards. Similar elements to those of the basic task could be included:

- Elements on the surface of the area, where a substance penetrates out of the geosphere into biotopes. Results for one element (the one of the biggest volume activity of isotopes) are stated in the paper. Results for the other elements are stated in (Chudoba 2014).
- Elements forming the main transport line out of the DGR up to the surface of the area with the maximal volume activity. The main transport line is composed of 10 elements.
- Elements at the selected (or higher) sea level. Those elements could describe penetration of a substance out of the geosphere into the biosphere taking into account the rock denudation.
- Elements that are found in a particular part of the modelled area with (supposing) a higher concentration of people.
- One crucial element could be analysed (e.g. a surface element of the maximal detected concentration or an element supposed in the area of a higher concentration of people).

The SW Flow 123D compares the substance concentration (activity) between the Reference Task and the Task with changed input parameters. A list of tasks of the strongest impact on the substance concentration change in the selected area is in fact the result of the SW analysis. The supposed "RATE" of the evaluation of particular tasks differences is the sum of the concentrations found on surface elements in the simulated time (all of the simulated time/s/). The surface elements were selected because of radioactive substances penetration out of the geosphere into biotopes.

The rate was "fixed" as we supposed that: (1) all the simulated time/s/ were of the same "weight"—the simulated time entry was done in an equidistant way, (2) elements were of the similar volume. That presumption was met, there was no "over-density" of any part of the area reflected on the calculated net. The total simulated time was 200 000 years and the results were recorded into the input files every 1000 years.

The resulting volume activities on selected elements were compared with the Reference Task and are stated in Table 4.

Table 4. Sensitivity analysis results.

	C14	Cl36	I129	Cs135	Ra226
The reference task, sum of activities [kBq/m^3]	16 950	3 400	148	1 850	1 450
Change parameters					
Rock near the DGR, hydraulic conductivity 0,1x	3.49x	3.46x	3.49x	3.42x	3.13x
Hornina blízko úložiště, vodivost 0,2x	2.25x	2.24x	2.26x	2.23x	2.10x
Rock near the surface, hydraulic conductivity 2x	2.07x	2.08x	2.08x	2.08x	2.08x
Hornina u povrchu, vodivost 5x	3.90x	3.91x	3.91x	3.92x	3.93x
Hornina u povrchu, vodivost 10x	4.86x	4.86x	4.86x	4.87x	4.88x

It is clear (from the results stated in the Table 4) that the strongest impact on the substance concentration increase in the surface area was caused by:

– Decrease of hydraulic conductivity in the surroundings of the DGR (with the types of rocks 9517, 9617), where the preference like is represented by a fissure system and where contamination is not diluted anyway. That is why concentration near the surface is increased (as dilution of concentration happens on the surface).
– Increase of hydraulic conductivity near the surface of the area (with the types of rocks 9112, 9212 and 9317), where transported substances are spread into greater "near the surface" area, due to higher hydraulic conductivity.
– Decrease of sorption coefficient K_d with substances of a higher sorption parameter. According the results, the sorption parameter has a strong impact on the substances transport in the surroundings of the DGR—having also an impact on the total weight (mass) of substances released out of the near/far field. The weight (mass) of the released substances could have an crucial impact on concentration (volume activity) on surface elements.

5 CONCLUSION

A complex task describing a substances-transport out of the DGR onto the surface of/within the area was presented in the paper. Our model covered a real area that had passed through a geological and hydrological research in the precedent years. The area was described by a geometry that included the basic geological types of rocks and the location of a fissures-net. The geological "situation" is described with: (1) hydraulic conductivity, (2) rock(s) porosity and (3) openings of fissures. The other input parameters were: (1) substance quantity released out of the near/far field border in the surroundings of the DGR, (2) sorption and diffusion coefficients of particular isotopes released out of the near/far field of the DGR.

A calculation net was designed for the area. Substance Flow and Substance Transport was calculated with the use of the SW Flow123D. The results of the transport task were verified with the use of the SW GoldSim afterwards.

The radioactive dose was calculated from the obtained substances concentrations (volume activities) of isotopes (in every element of the calculated net). The selected scenario supposed a human being who drinks 1 m^3 of ground water a year. The maximal dose on some surface elements was 110 μSv/year. That did not reach the limit of 3 mSv/year.

A sensitivity analysis was done through a parameter change in the model. Parameters of hydraulic conductivity, porosity, opening of fissures and sorption parameters were changed for every critical isotope and the impact of such a change on resulting concentration (volume activity) on surface elements was observed.

ACKNOWLEDGMENTS

The contribution was supported financially by the Faculty of Mechatronics, Informatics and Interdisciplinary Studies of the Technical University of Liberec.

REFERENCES

Brezina, J. et al. 2012, *Flow123d version 1.7.0 Documentation of file formats and brief user manual*. https://dev.nti.tul.cz/trac/flow123d/wiki/UserDoc.

Chudoba, J. 2011, Advances in Safety and Risk Mangement In Ch. Bérenguer & A. Graff (eds), *Modelling of dynamical dependability by using stochastic processes*.

Chudoba, J. 2012, 11th International Probabilistic Safety Assessment and Management Conference and The Annual European Safety and Reliability Conference. *Modelling of transport of radioactive substances from underground storage with uncertainties of geological parameters*.

Chudoba, J. 2014, Manuál k software Flow123D verze 1.6.6, http://www.nti.tul.cz/cz/Software/RiskFlow123d.

GoldSim, www.goldsim.org.

Mandik, F. 1999, *Referenční project hlubinného úložiště*, http://www.rawra.cz/cze/content/search?SearchText=referen%C4%8Dn%C3%AD+projekt.

Maryska, J et al. (2010), *Modelování transportních procesů v horninovém prostředí*, Technical University of Liberec, Czech Republic, ISBN 978-80-7372-571-6.

Rukavickova, L et al. 2008, *Příprava vstupních geologických dat pro matematické modelování transport a geochemické interakce v horizonut stovek tisíců let*, ČGS Praha Czech Republic.

SKB R-02-28 2002, *Nuclide documentation. Element specific parameter values used in the biospheric models of the safety assessments SR 97 and SAFE*, http://www.skb.se/Templates/Standard____17139.aspx.

SURAO (Deep Geological Repository Authority of the Czech Republic)—www.surao.cz.

Vokal, A. et al 2011, *The Reference Project of a Nuclear Waste DGR in a hypothetical locality and its Actualization (Aktualizace referenčního projektu hlubinného úložiště radioaktivních odpadů v hypotetické lokalitě)*, www.surao.cz (unpubl.).

This page intentionally left blank

Processes reliability and safety modelling

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

An impact of the operators and passengers behavior on the airport's security screening reliability

A. Kierzkowski & T. Kisiel
Wrocław University of Technology, Wrocław, Poland

ABSTRACT: The authors have developed a simulation model of the airport's security screening counters in terms of the impact of the behavioral characteristics of the operators and passengers on the reliability of the system. Intentionally been omitted reliability of technical objects, due to the fact, that the authors attempt to determine, where the failures occur during daily (reliable) functioning of the security screening system. The simulation model was developed to estimate the above-mentioned aspects for any configuration of counters with a wide ability to editing a method of conducting screening for given assumptions.

The developed model enabled the execution of simulation experiments for the counters with different capacities of contained areas in single security screening lane. In the next step was possible to determine the probability density function for the effectiveness of the process in the hourly period of time.

1 INTRODUCTION

1.1 *Legal requirements*

Bearing in mind the necessity to ensure a high level of security for air transport system, international law regulates, inter alia, the procedures relating to the control of the flow of passengers and luggage at the airport. The main law responsible for maintaining the level of security of air transport in Poland is the Regulation of the Minister of Transport, Construction and Maritime Economy of 31 July 2012 on the National Civil Aviation Security Program (Dz. U., 2012), referring to regulations (EU, 2010; EC, 2008; EC, 2009), setting out detailed procedures, the enforcement of which is the duty of the manager of the airport. Airports designate appropriate zones designed for the movements of passengers, baggage and the performance of the necessary ground handling processes:

- airside, with limited access,
- security restricted area, which is a part of the airside area and in which are also used other aviation security standards (for example, part of the airport designated for the movement of passenger flows after security control, part of an airport appointed for the movement of baggage flows subjected to security control, aprons while passengers boarding or luggage servicing),
- critical part of the restricted area, defined for airports, which employ at least 40 people with access cards to the restricted area. For critical part of the restricted area is included:
  - part of the airport where occur a passengers and luggage flow after the security control,
- separated area, which is a part of restricted area and designate an area separated from another area. This area has its application even to the departure hall, in order to separate the flows of passengers from Schengen and Non-Schengen zone.
- landside, which means that part of the airport, which does not belong to airside.

1.2 *Security screening*

Airport managing body shall designate boundaries between each zones clearly to differentiate by physical barriers that prevent access by unauthorized persons. Access to the restricted area is performed by security control system via counters with special devices able to detect potentially dangerous items. Before screening, passengers are required to prepare the cabin baggage to control and put outer garment to suitably cuvette in the area reserved for this purpose. Operator can also ask the passenger to insert additional garment into cuvettes, depending on the probability of occurrence of potential causes to occur the error to pass through the detectors

It is important that from cabin baggage is the need to remove large electronic devices, whose density can significantly affect the results obtained from the x-ray. These devices are subject to a separate inspection. Separate screening are also subject to fluids, which possibilities of transportation are regulated by the European Commission Regulation No 246/2013 (EU, 2013).

The next steps in the process are parallel baggage and passenger control. Screening of passengers can be carried out using:

– metal detectors,
– manual control,
– security scanners,
– devices for detection trace amounts of explosives combined with manual metal detectors,
– dogs to detect explosives in combined with manual control.

Screening of passengers can be carried out using:

– x-ray,
– manual control,
– explosives detection systems,
– dogs to detect explosives in combined with manual control.

Sniffer dogs and equipment for the detection of trace amounts of explosives may be used only as a supplementary means of screening during periods of increased risk. Control of passenger and baggage ends with a positive result only in case when the operator of the process is able to recognize clearly that the requirements of the screening process were provided. Any incorrect indication of control equipment must be diagnosed and eliminated. Otherwise, the passenger or luggage is subjected to re-inspection or decision is taken to refuse passenger from boarding the aircraft.

After completion of the screening process, passengers and their cabin baggage are protected from baseless intervention until departure of the aircraft, unless it would be "contamination" the passenger or luggage (contact with the passenger, luggage, which was not subjected to security checks). The algorithm of daily conducting security screening at the Wrocław Airport presents Figure 1.

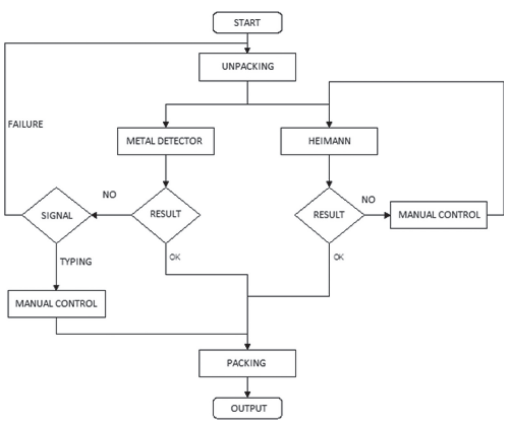


Figure 1. Scheme of security screening process.

1.3 *Modeling of security screening—literature review*

Modeling of ground handling services at airports is of interest to a wide group of scientists. In the literature can be found completely different approach. This is connected with numbers of different input variables and the diversity of the objectives to be attained.

There are several main directions of research. Very highly developed is the field of safety. Models in this area may even support in the development of technologies and procedures by assessing the impact of the implemented security technology (Akgun et al., 2010; Babu, et al., 2006; Chawdhry, 2009). Noteworthy are the models that in addition to the need to ensure the safety, indicate the need to minimize the inconvenience for the passenger (Gkritza et al., 2006).

Very well developed is also area of operational planning and design. Although for queuing systems are a variety of models for determining basic indicators—described in the literature as the queuing theory (Cooper, 1981). However, for complex processes, such as those at the airport are developed various models for engaging the wider analysis. From the old times, the models relate to the multicriterion analysis of passenger flows (Eilon et al., 1973). The issue of shortening the waiting time in queues with minimal use of resources was also discussed a long time ago and repeatedly (Baron et al., 1974; Manataki and Zagfros, 2010; Bevilacqua and Ciarapica, 2010). There are also a lot of models for allocating the appropriate number of resources (Roanes-Lozano et al., 2004; Solak et al., 2009).

The authors of this paper indicate how random is the flow of passengers through the security screening and show it in terms of reliability, to draw attention to the need for a wider analysis, particularly in regional airports, which due to low passenger traffic, often based on the basic characteristics. For the development of the simulation model the functioning of security checkpoints were used (Werbinska-Wojciechowska et al., 2013; Magott et al., 2009). The authors want to implement a Petri nets in further work (Kowalski, 2011). Today, many articles discuss the application of fuzzy logic for modeling complex systems (Vališ, 2014). In this work will also be taken into account reliability of the technical system (Magott et al., 2009; Plewa, 2009) and aspects of vulnerability (Vališ, 2012). Will be developed dependence functioning of the systems, as in (Vališ, 2012).

2 PROBLEM BACKGROUND

Knowledge of the procedures allows to forecast the basic efficiency characteristics of the carried

process. Theoretical estimates, which may take into account even the reliability of technical system, are purely illustrative. Security screening system is a system with relation machine-operator-environment in which, besides the basic characteristics of the reliability of technical system—causing the failures, are also failures, generated by the operators and the environment. Assuming the environment as a passengers of air transport system, can be seen a close relationship to the functioning of the line operator-environment-efficiency.

Airports, in the process of planning the necessary number of lanes to perform the assigned tasks, are often based on the primary statistical indicator—the arithmetic mean. However, in the case of non-uniform intensity of passengers notifications at a time, is really important a temporary efficiency of the process, which should ensure certain assumptions especially at the time of the increased flow of passengers (peak hours).

Passengers differ from each other in many categories. One of the important factors for the length of the performance of specific tasks in the next stages of the process, is the experience of traveling by air transport. Lack of knowledge of procedures significantly increases the time of service. The length of service time affects even the flight target. Another length of service is characterized by passengers of business flights (usually a low number of subjects to screening) and the other, for passengers of charter flights or low-cost (a large number of items subject to screening). This implies, that the process is stochastic. Time characteristics are presented later in this article.

3 DEVELOPED SIMULATION MODEL

3.1 *Assumptions*

The simulation model was developed by mapping procedure applicable in Wroclaw Airport. In the model, it has been assumed names of areas, in which take place specific tasks, as in Figure 2.

The passenger shall be notified to a queue common to all air operations. In the next step, depending on the availability of capacity of the unloading areas may move to an entry area. Because the simulation model applies to the double security screening counter (common metal detector for two lanes), entry area divides the input stream into two independent streams (*ELS*—entry left stream, *ERS*—entry right stream) and allocating passengers in one of them. The capacity for *ELS* stream is equal to:

$$C_{ELS} = C_{UA1} + C_{FU1} + C_{BAA1} \tag{1}$$

where C_{UA1} = capacity of UNLOADING AREA A1, C_{FU1} = capacity of FINAL UNLOADING 1 and C_{BAA1} = capacity of BUFFER AREA A1. Capacity for C_{ERS} is similar to C_{ELS}, but uses areas intended for the right stream. For both streams, capacity of some areas are deterministic and are equal:

$$C_{FU1} = C_{FU2} = 1 \tag{2}$$

$$C_{BAA1} = C_{BAA2} = 2 \tag{3}$$

The user put to the system the capacity of the entry area (C_{ELS}, C_{ERS}). Thus, indirectly determines the capacity of C_{UA1} and C_{UA2}, which can be determined after the transformation for example equation (1) for the left stream.

Passenger allocation to the appropriate entry stream is done on the basis of the shortest queue. In the case of absence of available place in both unloading areas, passenger is waiting for the available space to proceed to the unloading area. After passenger proceed to one of the streams of entry area, is respectively identified as a passenger of the left or right stream ($P_{LS_{(i)}}$—passenger of left stream, $P_{RS_{(i)}}$—passenger of right stream). Time

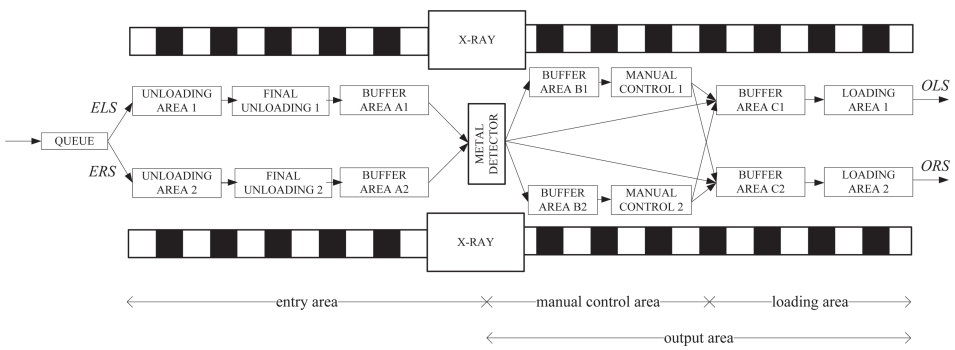


Figure 2. Structure of security screening counter.

of entry to unloading area ($t_{UAent_{(i)}} = t_{current}$) is recorded as a local label for each passenger, where $t_{current}$ = actual time of simulation. A passenger in this area received an information about the procedure and began to unload items on the conveyor, moving toward the final unloading area. Unloading time ($t_{1stunl_{(i)}}$) is a random variable of function $f_{(t_{1stunl})}$ (see Table 1). Flow of the *ELS* and *ERS* is based on the FIFO strategy.

A duration of the process ($t_{finunl_{(i)}}$) is determined by a random variable of function $f_{(t_{finunl})}$ (see Table 1). When the unloading process is completed, the passenger enters the buffer area (A1 or A2, depending on the side of the stream). Opportunity to enter the buffer area is therefore dependent on the availability of the capacity in the buffer area and when the equation (4) is true.

$$t_{current} - (t_{UAent(i)} + t_{UAwait(i)}) \geq t_{1stunl_{(i)}} + t_{finunl_{(i)}} \quad (4)$$

where: $t_{current}$ = current time of simulation, $t_{UAwait_{(i)}}$ = time when a passenger completed the process started in unloading area and had to wait for the input to the buffer area, due to the limited capacity. The algorithm for the entry area is shown in Figure 3.

Pass through a metal detector depends on the way from the three conditions. The first one concerns the separation between subsequent entrances. It is related to the functioning of a technical object, which indicates the possibility of entering the next passenger. Separation time is assumed as $t_{sep} = 2s$ (1st condition). Further conditions relate to the capacity of control area and receiving items area.

Passengers entering the metal detector from *ELS*, belong to the *OLS* (output left stream). Similarly, *ERS* passengers, upon entering the metal detector belong to the *ORS* (output right stream). Considering the *ELS*, the passenger of this stream can proceed to the metal detector, if the number of $P_{LS_{(i)}}$ in *OLS* is less than the capacity of the *OLS* (2nd condition):

$$\sum P_{OLS_{(i)}} < C_{OLS} \quad (5)$$

where, as passenger $P_{OLS_{(i)}}$ assumes the passenger $P_{LS_{(i)}}$ who has entered to the metal detector and are still in the system,

$$C_{OLS} = C_{BAC1} + C_{LA1} \quad (6)$$

where C_{BAC1}=capacity of buffer area 1, C_{LA1}=capacity of loading area 1. Capacity for C_{ORS} is similar to C_{OLS}, but uses areas intended for the right stream. For both streams, capacity of buffer area is deterministic and is equal:

$$C_{BAC1} = C_{BAC2} = 2 \quad (7)$$

This is related to the construction of the actual position of the test in Wroclaw Airport, where the loading area precedes the area separated from the

Table 1. Probability density function for specific tasks.

Task	Sign	Probability density function	Statistic test
First unloading	t_{1stunl}	$f(t_{1stunl}) = \frac{t_{1stunl}^{3,42}}{13,74^{4,42} \cdot \Gamma(4.42)} e^{-\frac{t_{1stunl}}{13,74}}$	0,4711
Final unloading	t_{finunl}	$f(t_{finunl}) = \frac{e^{-\frac{23,62}{t_{finunl}-0,94}}}{23,62 \cdot \Gamma(2,02) \cdot \left(\frac{t_{finunl}-0,94}{23,62}\right)^{3,02}}$	0,5786
Manual control	t_{mcont}	$f(t_{mcont}) = \frac{(t_{mcont}-16,95)^6}{2,13^7 \cdot \Gamma(7)} \cdot e^{-\frac{t_{mcont}-16,95}{2,13}}$	0,4041
Waiting for items	t_{wfi}	$f(t_{wfi}) = \frac{1}{B(0,67;2,56)} \cdot \frac{(t_{wfi}-2,93)^{-0,33} \cdot (139,10-t_{wfi})^{1,56}}{136,17^{2,23}}$	0,6551
Loading time	t_{load}	$f(t_{load}) = \frac{2,01}{23,62} \cdot \left(\frac{t_{load}-0,94}{23,62}\right)^{1,01} e^{-\left(\frac{t_{load}-0,94}{23,62}\right)^{2,01}}$	0,5768

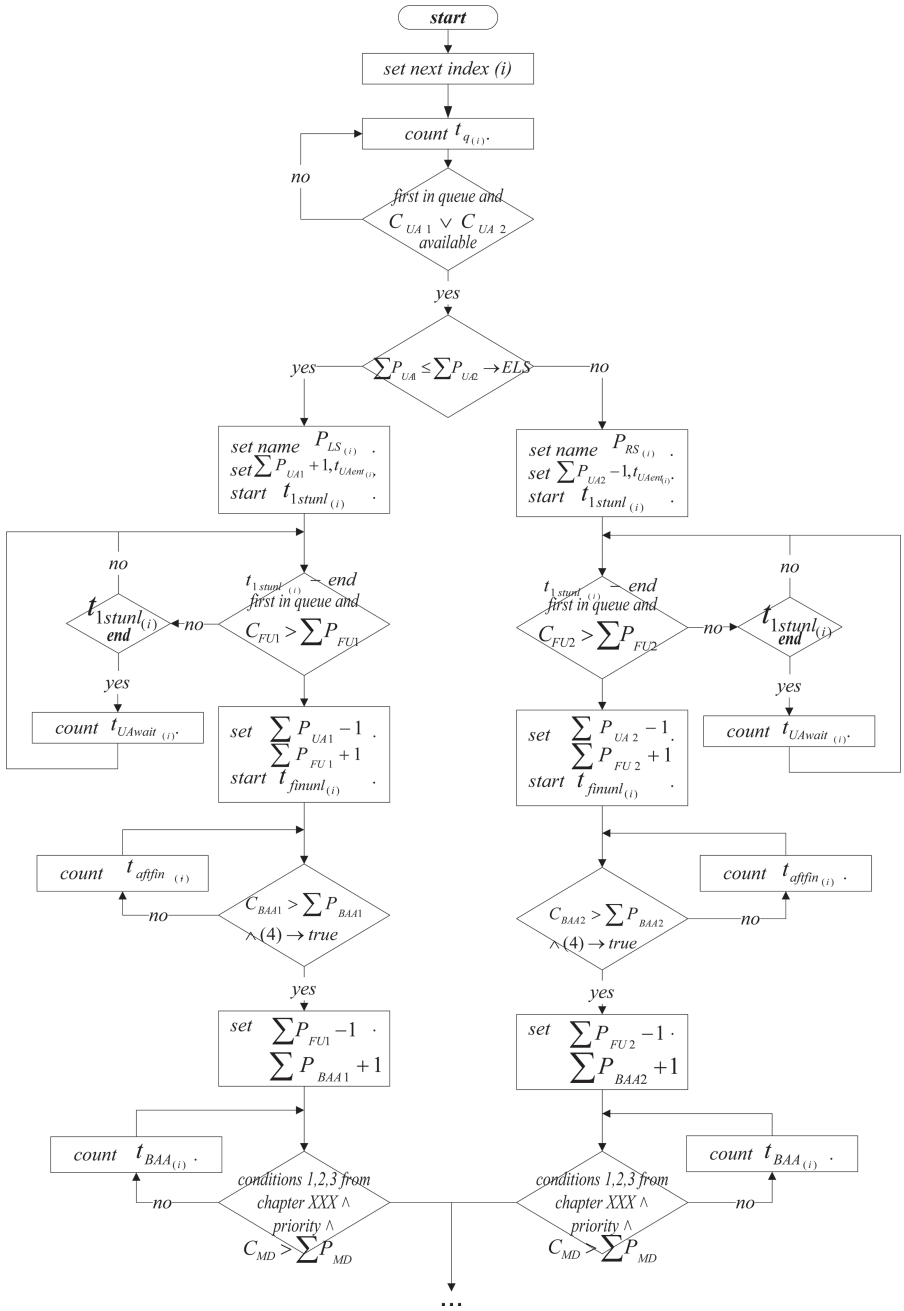


Figure 3. The algorithm for the entry area.

conveyor, used as a buffer area to increase the efficiency of the process.

Passenger flow strategy assumes assignment of two operators (both genders) for manual control of passengers. Passengers passing through the metal detector can be selected for manual control randomly or if has prohibited items. The intensity of the designation to the control is λ_c = 0,24 and was determined experimentally at the airport. The intensity of the direct flow

into the buffer area C is therefore is λ_{nc} = 0,76. Advantage of the double lanes counters in relation to the one lane counters is the fact that in the case of picking a passenger to manual control, the passenger flow is not suspended, because of the availability of the second operator conducting the process.

It is also possible to allocate buffer areas when the next passenger was directed to the same operator at the same time. Therefore, the third

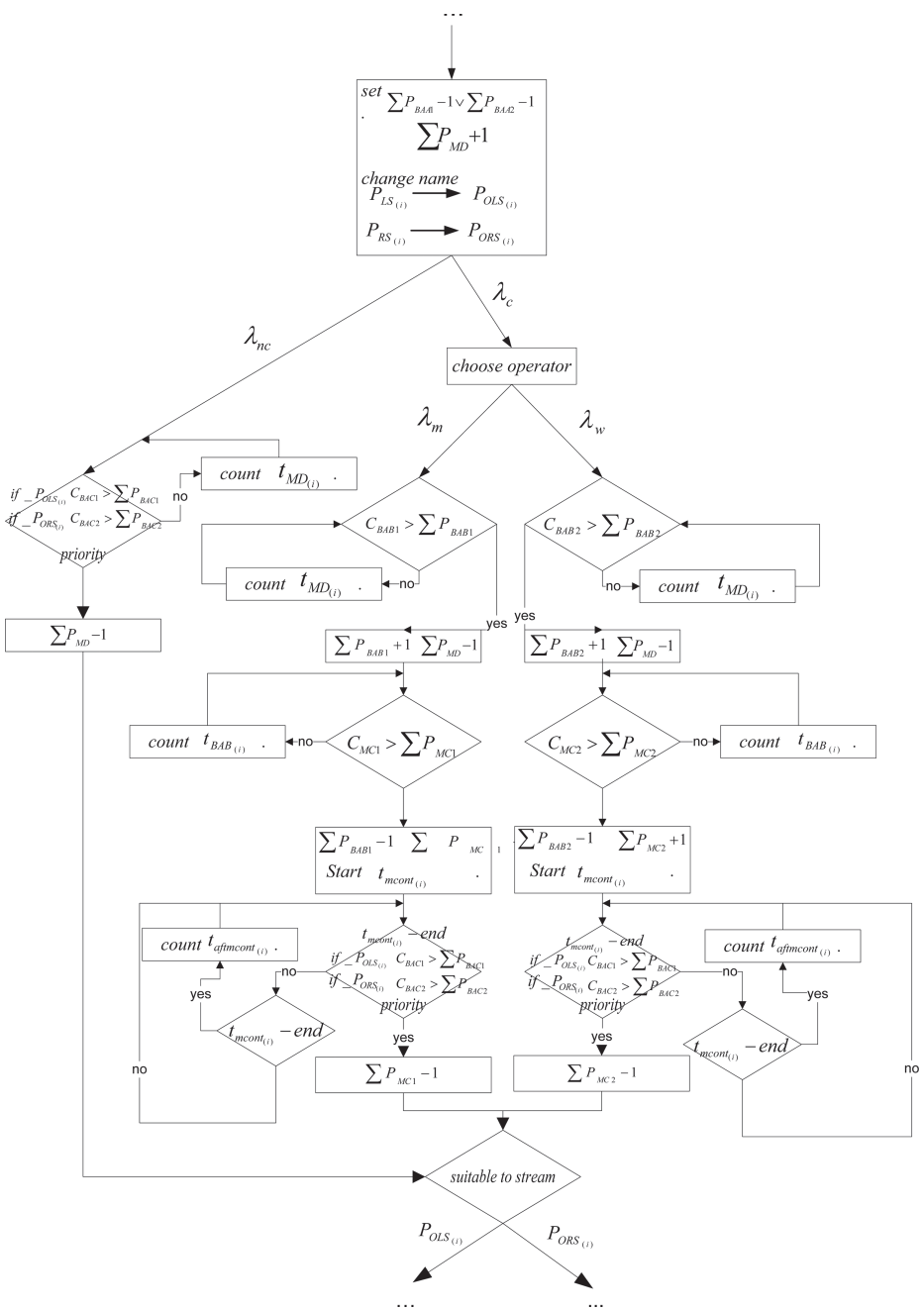


Figure 4. The algorithm for the manual control area.

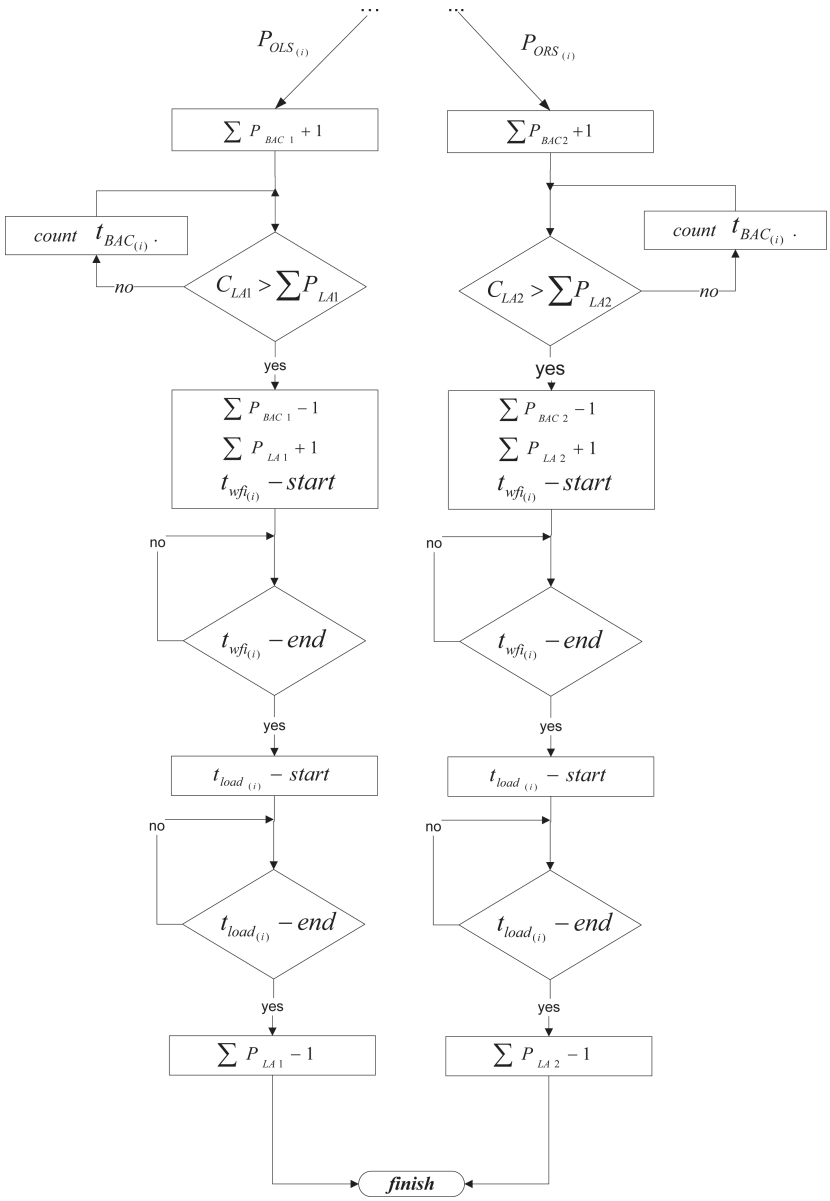


Figure 5. The algorithm for the loading area.

condition (3rd condition) for the possibility of entering the metal detector is to meet the equation (8), which says that at least, one operator must be available (9) and neither of the buffer areas can't be overloaded (10). Overloading too many passengers in the control area may adversely affect the proper conduct of control in terms of safety.

$$MD_{entconIII} = OP_{av} \wedge BA_{nov} \tag{8}$$

and:

$$OP_{av} = \left(\sum P_{MC1} = 0\right) \vee \left(\sum P_{MC2} = 0\right) \tag{9}$$

$$BA_{nov} = \sum P_{BAB1} < C_{BAB1} \vee \sum P_{BAB2} < C_{BAB2} \tag{10}$$

where: $\sum P_{MC1}$ = sum of total passengers inside manual control 1, $\sum P_{MC2}$ = sum of total passengers inside manual control 2, $\sum P_{BAB1}$ = sum of total pas-

sengers inside buffer area B1, $\sum P_{BAB2}$ = sum of total passengers inside buffer area B2, C_{BAB1} = capacity of buffer area B1, C_{BAB2} = capacity of buffer area B2. In described model the capacity are equal to:, $C_{BAB1} = C_{BAB2} = 1$.

Selected for manual control passenger is directed to an buffer area B for the same type process operator. Operator selection intensity was assumed as $\lambda_m = \lambda_w = 0{,}5$, where λ_m is a man and λ_w is a women. Entrance to the manual control 1 or 2 is possible if the area is available. Since the operator can control only one person at a time, capacity was taken as $C_{MC1} = C_{MC2} = 1$. Manual control time ($t_{mcont_{(i)}}$) is a random variable of function $f_{(t_{mcont_i})}$ (see Table 1). The algorithm for the control area is shown in Figure 4.

The next step is to proceed to the output area. Passengers after manual inspection or passing directly from the metal detector, enter the buffer area C1 or C2 (depending on flow stream) if there is a free capacity. Priority gets the passenger who came earlier to the output area. Buffer areas C are designed for waiting for the free capacity in the loading area 1 or 2. Capacity of buffer areas C have been assumed according to the actual system $C_{BAC1} = C_{BAC2} = 2$. Capacity of loading area 1 and 2 can be changed depending on a simulation scenario.

In the loading area there are two different variables assigned to the passenger. The first of these ($t_{wfi_{(i)}}$), determines how long passenger have to wait for items and is a random variable of function $f_{(t_{wfi})}$ (see Table 1). The second ($t_{load_{(i)}}$) is a random variable of function $f_{(t_{load})}$ (see Table 1). and determines the time of items loading. The sum of these two variables allows to leave the system by the passenger. The algorithm for the loading area is shown in Figure 5.

In summary, the total time a passenger in the system is equal:

$$\begin{aligned} t_{paxinsys_{(i)}} &= t_{q(i)} + t_{q\backslash stunl_{(i)}} + t_{UAwait_{(i)}} \\ &+ t_{finunl_{(i)}} + t_{aftfin_{(i)}} + t_{BAA_{(i)}} \\ &+ t_{MD_{(i)}} + t_{BAB_{(i)}} + t_{mcont_{(i)}} + t_{aftmcont_{(i)}} \\ &+ t_{BAC_{(i)}} + t_{wfi_{(i)}} + t_{load_{(i)}} \end{aligned} \tag{11}$$

where: $t_{q_{(i)}}$, $t_{UAwait_{(i)}}$, $t_{aftfin_{(i)}}$, $t_{BAA_{(i)}}$, $t_{MD_{(i)}}$, $t_{BAB_{(i)}}$, $t_{aftmcont_{(i)}}$, $t_{BAC_{(i)}}$ depend on the time of service and intensity of notification previous passengers and shall be designated during the simulation.

These values represent in the order as above: time in the queue to the system, the waiting time between the end of the initial unloading and the start of the final, waiting to enter the buffer area A after completion of final unloading, time in buffer area A, the waiting time at the output of the metal detector, the time in the buffer area B, the time in the buffer area C.

As input has been appointed times in subsequent steps in the process for $\alpha = 0{,}05$ (Table 1). For all the random variables are no grounds for rejecting the hypothesis of compliant empirical distributions with given theoretical (test statistics below 1.36).

3.1.1 *Results*

The model allows to determine the capacity in accordance with the specified input parameters. Capacity of entry area has been established as follows: $C_{ELS} = C_{ERS} \in \{3,4,5,6,7\}$. As input variables has also been established capacity of the loading area $C_{OLS} = C_{ORS} \in \{3,4,5,6,7\}$. Table 2 presents obtained mean capacity values for the screening process.

It should be noted that the currently functioning system of security screening in configuration 4×4 at Wrocław Airport obtain capacity of passenger flows through the metal detector at the level of 230-240PAX per hour. The developed simulation model reported a value of passenger stream flow at the level of 237PAX per hour. In order to achieve higher capacity, it is necessary to expand the entry area and/or expand the loading area after screening. From the obtained results, is clearly seen that expansion only of volume of the area to prepare for security checks will not increase the intensity of passenger flows. The key for Wroclaw Airport was to obtain capacity at the level of 300PAX/h This value may be achieved for $C_{ELS} = C_{ERS} = 6$ and $C_{OLS} = C_{ORS} = 5$.

However, while planning the allocation of resources to sustain the process, it should be brought into account some risk that the intended capacity will not be reached. If there will not be selected adequate spare of capacity, especially during the peak hours, the system can generate failures and be unreliable. The simulation model allows forecasting of counters capacity for selected intervals and counter's configuration (Fig. 6), which

Table 2. The average capacity depending on the size of the areas.

Loading area capacity	3	220	215	213	205	187
	4	279	270	259	237	190
	5	322	309	279	238	190
	6	345	318	280	238	190
	7	360	324	283	238	191
		7	6	5	4	3
		Entry area capacity				

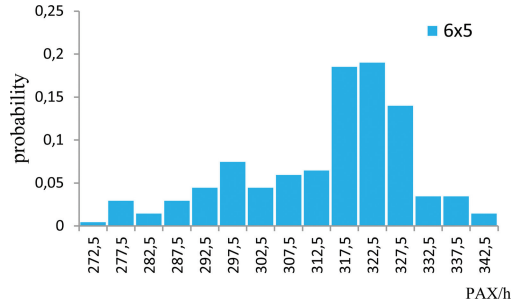


Figure 6. Probability of achieving a different capacity for 6×5 configuration.

Table 3. Verified values for the different configurations.

Loading area capacity	3	NO	216	NO	NO
	4	273	254	235	NO
	5	307	286	239	NO
	6	316	287	242	NO
		6	5	4	3
			Entry area capacity		

gives a greater understanding of the functioning of the process. There are also many other factors that could affect the reliability of the system in key moments of increased level of intensity of passenger flows (e.g. triggering radioactivity signal), which will be taken into account during further development.

3.2 *Model verification*

Model verification was carried out at Wroclaw Airport (PLW) on a sample of about 1000 PAX for each of the tested configuration. Due to the need to maintain high efficiency of the screening process in PLW, were verified only certain configurations, which are presented in Table 3. In the table as the value of NO was determined configurations that have not been verified.

Chi-square test at a significance level $\alpha = 0{,}05$ was verified hypotheses about the consistency of data obtained in the simulation model and observed in the PLW. The value of statistics $\chi^2_{0,05} = 16{,}919$, which proves the consistency of data in the simulation model with empirical data.

Verified were also times between subsequent notifications of passengers to the metal detector of security screening received in the simulation model and those observed in a functioning system. Results (after the split into time intervals) are presented in Figure 7. On significance level $\alpha = 0.05$ was verified compliance of distribution.

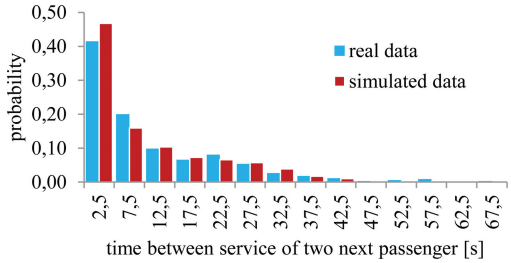


Figure 7. Verification of times between service of two next passenger.

Kolmogorov Smirnov statistic is equal $\lambda_k = 1{,}18$, whereas the limit value, obtained from the tables is equal $\lambda_{0,05} = 1{,}36$. This proves the compatibility of empirical data with simulation.

4 CONCLUSION

The paper presents a model of security screening, which allows the determination of the intensity of passenger flows at the selected input parameters. The advantage is versatility, which allows you to use it at any airport. However, it is necessary to insert the input data.

Further works are directed to the dependence of the system on subsequent factors affecting the reliability and an indication of the proper configuration of security checkpoints at a certain limited area available at Wroclaw Airport. Developed will also be an algorithm that will create a schedule for the operation of security checkpoints for a given timetable.

ACKNOWLEDGMENTS

The project is co-financed by the National Research and Development Centre under the Applied Research Program. This publication presents the results of research conducted in the project: “Model of logistical support for the functioning of the Wrocław Airport” realized by the Wrocław University of Technology and Wrocław Airport consortium.

REFERENCES

Babu, V.L.L., Batta, R., Lin, L., 2006. Passenger grouping under constant threat probability in an airport security system. *European Journal of Operational Research* 168 (2), 633–644.

Bevilacqua, M., Ciarapica, F.E., 2010. Analysis of check-in procedure using simulation: a case study. In: IEEE Int. Conf. Industrial Engineering and Engineering Management (IEEM), pp. 1621–1625.

Chawdhry, P.K., 2009. Risk modeling and simulation of airport passenger departures process. In: Winter Simulation Conference, pp. 2820–2831.

Cooper, R.B., 1981, *Introduction to queueing theory*. Second edition., New York: Elsevier North Holland,

Dz.U., 2012, poz. 912, The Regulation of the Minister of Transport, Construction and Maritime Economy of 31 July 2012 on the National Civil Aviation Security Program. Journal of Laws of the Republic of Poland 2012 Item 912.

Eilon, S., Mathewson, S., 1973. A simulation study for the design of an air terminal building. *IEEE Transactions on Systems, Man and Cybernetics* 3 (4), 308–317.

EC, 2008, Commision Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

EC, 2009, Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council.

EU, 2010, Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security.

EU, 2013, Commission Regulation (EU) No 246/2013 of 19 March 2013 amending Regulation (EU) No 185/2010 as regards the screening of liquids, aerosols and gels at EU airports.

Gkritza, K., Niemeier, D., Mannering, F., 2006, Airport Security Screenning and changing passenger satisfaction: An exploratory assessment, *Journal of Air Transport Management*, 12(5), 213–219.

Kowalski, M., Magott, J., Nowakowski, T., Werbinska-Wojciechowska, S., 2011, Analysis of transportation system with the use of Petri nets. *Eksploatacja i Niezawodnosc—Maintenance and Reliability*, Issue: 1, pp.: 48–62.

Magott, J., Nowakowski, T., Skrobanek, P., Werbinska, S., 2009, Analysis of possibilities of timing dependencies modeling-Example of logistic support system. Safety, reliability and risk analysis: theory, methods and applications. Vol. 2, eds. Sebastian Martorell, C. Guedes Soares, Julie Barnett. Boca Raton: CRC Press; Taylor & Francis, pp. 1055–1063.

Manataki, I.E., Zografos, K.G., 2010. Assessing airport terminal performance using a system dynamics model. *Journal of Air Transport Management* 16 (2), 86–93.

Nowakowski T., Werbińka S., 2009, On problems of multicomponent system maintenance modelling. *International Journal of Automation and Computing*, vol. 6, nr 4, pp. 364–378.

Plewa, M., 2009, Assessment of influence of products' reliability on remanufacturing processes, *International Journal of Performability Engineering* 5 (5) PP. 463–470.

Roanes-Lozano, E., Laita, L.M., Roanes-Macas, E., 2004. An accelerated-time simulation of departing passengers' flow in airport terminals. Mathematics and Computers in Simulation 67 (1–2), 163–172.

Solak, S., Clarke, J.-P.B., Johnson, E.L., 2009. Airport terminal capacity planning. *Transportation Research* Part B: Methodological 43 (6), 659–676.

Vališ, D.; Koucký, M.; Žák, L., 2012, On approaches for non-direct determination of system deterioration. *Eksploatacja i Niezawodnosc—Maintenance and Reliability*, vol. 14, no. 1, p. 33–41.

Vališ, D.; Vintr, Z.; Malach, J., 2012, Selected aspects of physical structures vulnerability—state-of-the-art. Eksploatacja i Niezawodnosc—*Maintenance and Reliability*, vol. 14, no. 3, p. 189–194.

Vališ, D.; Pietrucha-Urbanik, K., 2014, Utilization of diffusion processes and fuzzy logic for vulnerability assessment. Eksploatacja i Niezawodnosc—*Maintenance and Reliability*, vol. 16, no. 1, p. 48–55.

Werbinska-Wojciechowska, S., 2013, Time resource problem in logistics systems dependability modelling. *Eksploatacja i Niezawodnosc—Maintenance and Reliability*, Issue: 4 pp.: 427–433.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk analysis of the point on aging aircraft structure

M. Woch
Airworthiness Division, Air Force Institute of Technology, Warsaw, Poland

ABSTRACT: For complex systems, such as aircraft, the implementation of prognostic and health management techniques can effectively improve system performance. This paper presents some recent results of research on risk assessment for aircraft structures and intendeds to show the procedures of reliability calculations of the point of aircraft PZL-130 ORLIK TC II structure as an object under investigation. In this paper, the ways to determine failure rate and failure probability at the location on interest, which may be influenced by a different type of mission profile, have been presented. The goal of this paper was to answer the question of when inspections should be carried out depending on different types of missions. A technical risk management approach was applied to relieve the inventory problem to the highest degree possible, while ensuring safety.

1 INTRODUCTION

Typically, when one thinks of aging aircraft, safety is what comes to mind. However, another important aspect is readiness—that is the aircraft has to be available and reliable when needed. PZL-130 ORLIK TC II is a Polish two seat training aircraft designed by PZL Warszawa-Okecie. This aircraft was designed for basic and advanced training primarily for military pilot candidates. Constructed mostly of the 2024-T4 aluminium alloy, Orlik was design according to safe-life design procedures. Today Orlik is being called upon to last longer under more severe conditions. Consequently, the current tools of structural analysis must go beyond the specifics of strength, durability, fracture mechanics and into the realm of probabilities. The question became how to realize a huge cost-avoidance (acquiring Orlik TC-II aircraft earlier and more rapidly than planned) while ensuring safety and maintaining readiness (Koucky & Valis 2007). To address this dilemma a technical risk management approach was devised to relieve the inventory problem to the highest degree possible, while ensuring safety (Valis et al. 2012, Valis and Vintr 2007b). Risk-based approaches and tools have been widely adopted by the aircraft communities, especially by the military, to ensure aircraft availability and to reduce cost while maintaining structural safety.

Some work on reliability analysis has been already completed e.g. (Woch 2013) however there is lack of complete risk analysis for the aircraft Orlik.

The paper has been intended to present the procedures of reliability calculations of the point of aircraft structure as an object under investigation (Valis et al. 2012). In this paper the ways how to determine failure rate and failure probability of all points, which may be influenced by a mission profile, have been presented. The goal of this paper is also to answer to the question of when inspections should be carried out on demand types of missions.

Presented mathematical model is implemented in the computer program PRobability Of Fracture (PROF) and widely used at United State Air Force (Babish 2010, Iyyer and Kittur 2002, Gallagher et al. 2005, Berens et al. 1998, among others). National Research Council Canada (Liao et al. 2003, Liao et al. 2011) are using a similar mathematical approach, which is implemented at ProDTA (PRObabilistic Damage Tolerance Analysis) software. However, ProDTA uses different numerical integration subroutines, and is enhanced with Monte Carlo simulation on crack growth modelling.

2 METHODOLOGY

For every critical location in the aircraft structure failure is defined either as having a crack larger than a pre-defined size or encountering a stress cycle at a crack with smaller size that produces a stress intensity factor that exceeds the fracture toughness (Miedlar et al. 2005, Valis and Vintr 2006a, Valis and Vintr 2006b).

Pre-defined size a_{cr} is defined as the size that corresponds to the mean fracture toughness $\overline{K_{IC}}$ and the average stress (63% percentile) per flight $\overline{\sigma}$:

$$a_{cr} = g^{-1}\left(\frac{\overline{K_{IC}}}{\overline{\sigma}}\right) \tag{1}$$

where g^{-1} is the inverse of the function (2).

The defining relation between stress intensity factor K, stress σ, and crack size a is expressed as

$$K/\sigma = \sqrt{\pi a}\beta(a) = g(a) \tag{2}$$

2.1 *Failure rates and failure probabilities*

Failure rate function $\lambda(t)$ (Bedford and Cooke 2001, Koucky et al. 2009, Valis and Vintr 2007a) is defined as the limit, if it exists, of the ratio of the conditional probability that the instant of time, T, of a failure of an item falls within a given time interval $(t, t+\Delta)$ and the length of this interval, Δt, when Δt leads to zero, given that the item is in an up state at the beginning of the time interval, which can be described as (3).

$$\lambda(t) = \lim_{\Delta \to 0} \frac{P\{T \le t + \Delta \mid T > t\}}{\Delta} \tag{3}$$

If T has a density $f(t)$ and the distribution $F(t)$, it can be writen:

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{4}$$

Given the failure rate, the life distribution can be calculated by the equation:

$$F(t) = 1 - e^{-\int_0^t \lambda(x)dx} \tag{5}$$

This analysis assumes there are two primary failure rates for fracture at the location ($\lambda(t) = \lambda_1(t) + \lambda_2(t)$) Damage tolerance is lost and the aircraft is unsafe when a crack reaches the predefined size ($\lambda_1(t)$) or cracks smaller than a_{cr} encounter an exceptionally large stress and the materialâĂŹs fracture toughness is exceeded ($\lambda_2(t)$).

2.1.1 *Slow crack growth*

Probability that crack size can exceed the predefined size a_{cr} can be described by (Miedlar, Berens, Hovey, Boehnlein, & Loomis 2005):

$$F_{\mathrm{Lcr}}(t) = 1 - F_A(a^*(t_{cr} - t)) \tag{6}$$

where $F_A(a)$ is the distribution function of crack length at the start of the interval; $a^*(t)$ is the crack size, which correspond to the time to failure; t_{cr} is the time, when crack size will reach the predefining size a_{cr}.

The first failure rate, associated with cracks growing to a_{cr} is then given by:

$$\lambda_1(t) = \frac{f_{\mathrm{Lcr}}(t)}{1 - F_{\mathrm{Lcr}}(t)} \tag{7}$$

2.1.2 *Sudden fracture due to an unusually large load during a flight*

Fracture occurs when an applied stress procedures a stress intensity factor which exceeds the fracture toughness for the crack. Probability Of Fracture (POF) can be calculated as: $POF = P\{\sigma \ge \sigma_{cr}\}$. Critical value of stress can be calculated form (2) as $\sigma_{cr} = K_{Ic}/\beta(a)\sqrt{\pi a}$. Distribution of maximum stress peak in a flight can be model by Gumbel distribution function $H(\sigma)$.

From the distributions of three random variables, the probability that a peak load will cause a failure during a flight at time t for cracks that are less than a_{cr} is a double integral over crack size and fracture toughness, and can be described by:

$$POF(t) = \int_0^{\infty}\int_0^{a_{cr}} \widehat{H}(\sigma_{cr}(a,k_c)) f_A(a;t)da \cdot f_{K_{Ic}}(k_c)dk_c \tag{8}$$

where $\widehat{H}(\sigma) = 1 - H(\sigma)$ is the exceedance probability for the peak load per flight; $f_A(a;t)$ is the density of the flaw size distribution at time interval t; $f_{K_{Ic}}(k_c)$ is the density for fracture toughness.

The failure rate due to a large stress can then be approximated by (Vintr et al. 2012, Vintr and Valis 2012):

$$\lambda_2(t) = \frac{POF(t)}{t_f} \tag{9}$$

where t_f is the length of a flight.

The overall failure probability for one point on the structure can be calculated from equation (5).

2.2 *Crack size distributions*

The initiating crack size distribution either comes from an equivalent initial flaw size characterization or is inferred from the sizes of cracks that are detected during inspections of the location. This analysis assumes that detected cracks will be repaired. The proportion of cracks that is detected and repaired depends on the $POD(a)$ function of the NonDestructive Inspection (NDI) system.

$$POD(a) = POI \cdot \int_0^a \frac{1}{x\sigma\sqrt{2\pi}} \cdot \exp\left[-\frac{(\ln(x) - \mu)^2}{2\sigma^2}\right] dx \forall a > a_{\min} \tag{10}$$

where POI—probability of the inspection or nondestructive testing performed conformity with the approved documentation; $a_{\min}$ = the minimum detectable crack size; $e^{\mu} = a_{50}$ = the median detectable crack size; σ = scale parameter.

The cumulative crack size distribution after all inspections F_{af} can be calulated by:

$$F_{af}(a) = P \cdot F_r(a) + \int_0^a (1 - POD(x)) f_{bf}(x) dx \qquad (11)$$

where $P = \int_0^\infty POD(a) f_{bf}(a) da$ is the percentage of details that will be repaired after cracks are detected; $F_r(a)$ = equivalent repair crack size distribution; f_{bf} = probability density of the crack size distribution at a location immediately before an inspection.

3 NUMERICAL CALCULATION

In this section we will briefly show the required input parameters in order to perform risk analysis calculation. Preliminary analysis conducted with the use of finite element methods (Leski et al. 2008) in order to obtain the region of the points placement were performed. To perform further calculations the crack of main spar web in bottom part, right wing between ribs No. 5 and 6, below the hole for cables have been chosen.

3.1 *Distribution of plane-strain fracture toughness*

The parameter K_{IC} characterizes the resistance of a material to fracture in the presence of a sharp crack under severe tensile constraints. To determine the mean and standard deviation of K_{IC} 11 RTC samples, made of aluminium alloy 2024-T4 in the L-T reference directions were tested (Lisiecki & Bochenek 2013).

Results are presented in Table 1 where K_Q is the provisional value of K_{IC}.

The obtained mean value of plane-strain fracture toughness was $\mu(K_{IC}) = 36.75$ MPa$\sqrt{\text{m}}$ and standard deviation was $\sigma(K_{IC}) = 0.25$ MPa$\sqrt{\text{m}}$, in accordance with the standard (ISO-12737 2010).

Table 1. RTC samples (Lisiecki et al. 2013).

Samples	$K_Q(MPa\sqrt{m})$
1	37.4558
2	37.2230
3	36.8735
4	37.9447
5	36.5824
6	36.2398
7	36.3771
8	38.0453
9	37.1710
10	36.8731
11	36.8671

3.2 *Relation between stress intensity factor, stress, and crack size*

Relation between stress intensity factor, stress, and crack size, which is described as (2) was obtained from the damage tolerance analysis. Calculations were performed with the use of finite element methods; Patran and Nastran software, which are the world's most widely used pre/post-processing software. The results of calculations are listed in Table 2.

3.3 *Maximum stress distribution*

The distribution of maximum stress peak in a flight is modeled in terms of a Gumbel distribution of extreme values.

Based on 19 different types of missions, which were performed in order to obtain the average profile of 200 simulated flight hours (Leski & Dragan 2010), we obtained the following distribution, mathematically represented as:

$$H(\sigma) = e^{-\exp\frac{-(\sigma-84.8)}{10.43}} \qquad (12)$$

Another simulation was performed in order to obtain the distribution for which the construction suffers high stress cycles. The following distribution was obtained:

$$H(\sigma) = e^{-\exp\frac{-(\sigma-118.5)}{21.2}} \qquad (13)$$

The results of calculations of both simulations are showed on the Figure 1. The length of a average flight was designated as $t_f = 42$ min.

3.4 *Inspection capability*

Inspections are performed using the eddy-current testing, which was based on the electromagnetic

Table 2. Relation between stress intensity factor, stress, and crack size.

a (mm)	$K/\sigma\left(\sqrt{mm}\right)$
0.125	0.7100
0.25	1.0810
0.5	2.3529
1	2.0426
2	2.7799
4	3.3078
6	4.2088
8	5.0155
10	5.7686

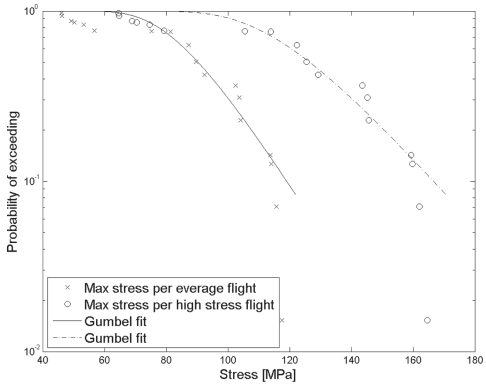


Figure 1. Distribution of maximum stress per flight.

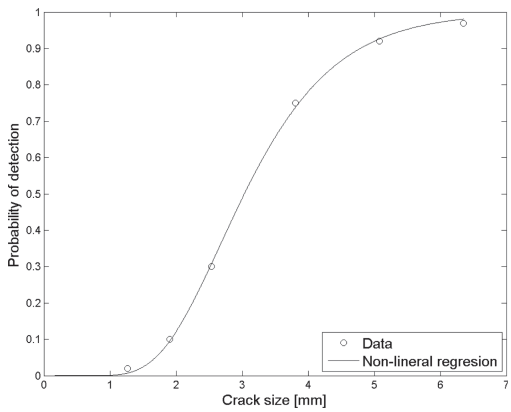


Figure 2. Probability of crack detections.

induction to detect flaws in conductive materials. In order to obtain the proper fitting (Fig. 2) to the cumulative lognormal equation (10) nonlinear fitting procedure based on Levenberg-Marquardt algorithm has been used. Parameters used for further calculations are as follows: POI = 1; $a_{min} = 0$; $a_{50} = 3.03$ mm $\sigma = 0.35$.

The lacking input data for the calculations were mainly adopted from literature (Miedlar et al. 2005, Valis and Pokora 2014).

3.5 *Failure rates and failure probabilities*

The numerical calculation of failure rates and failure probabilities were calculated using the computer program PRobability Of Fracture (PROF) which is based on a deterministic damage tolerance approach and uses the methodology described above.

Because of different types of missions, two separate analyses had to be performed. After calculations we obtained the following results of failure rate and failure probability, presented in Figures 3 and 4.

The challenge for this contribution was how long to leave this aircraft in service without inspections. In order to calculate intervals between inspections several analyses were performed. Finally, we obtained the results of calculations shown in the

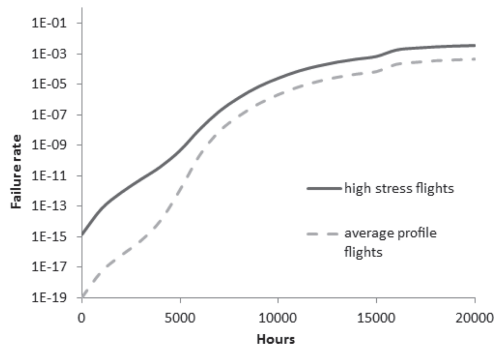


Figure 3. Failure rate.

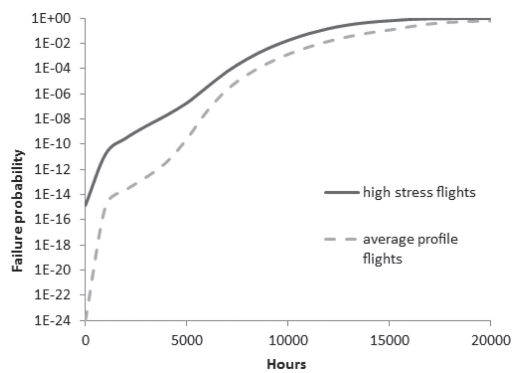


Figure 4. Failure probability.

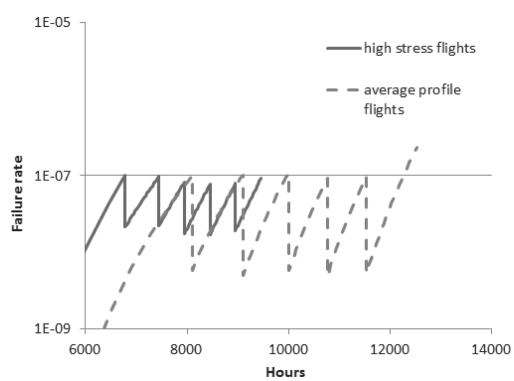


Figure 5. Failure probability.

Table 3. Inspection times for average profile flights.

#	Intervals (hour)	Time (hour)
1	8100	8100
2	1000	9100
3	900	10000
4	760	10760
5	770	11530
6	1000	12530

Table 4. Inspection times for high stress flights.

#	Intervals (hour)	Time (hour)
1	6780	6780
2	670	7450
3	500	7950
4	500	8450
5	500	8950
6	500	9450

Figure 5, listed in Tables 3 and 4. Two different curves represented the different types of missions.

3.6 *Conclusion*

A brief review of the Record of Airworthiness Risk Management (Liao M. & G. 2012) process shows that risk assessment is becoming a very important tool for managing aircraft airworthiness. For complex structural systems, both qualitative and quantitative risk assessments are needed to support decision-making.

In accordance with (MIL-STD-882E 2012, MILSTD-1530C 2005) a probability of catastrophic failure at or below 10^{-7} per flight $\lambda(t)$ for the aircraft structure is considered adequate to ensure safety for long-term military operations. Probabilities of catastrophic failure exceeding 10^{-5} per flight for the aircraft structure should be considered unacceptable. When the probability of failure is between these two limits, consideration should be given to mitigation of risk through inspection, repair, operational restrictions, modification, or replacement (Koucky et al. 2009, Valis and Vintr 2007a).

The challenge set for this contribution was how long to leave this aircraft in service without inspections. In order to guarantee safety and maintain readiness, the following times to perform the inspections, as is shown on the Figure 5 and presented in Tables 3 and 4, were suggested.

This example demonstrate how risk analyses might be used as one more source of information in evaluating inspection intervals. Although not shown in this paper, a similar analysis has been performed for different points and for multiple points. In that case, however, different types of input parameters have been chosen (Valis and Zak 2014, Valis and Krzak 2014).

REFERENCES

Babish, C. (2010). Application of risk & reliability analysis for fatigue cracking in F-16 aircraft structure. Technical report, 2010 F-16 ASIP.

Bedford, T. & R. Cooke (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Pressn.

Berens, A., J. West, & A. Trego (1998). Risk assessment of fatigue cracks in corroded lap joints. *Fatigue in the Presence of Corrosion*.

Gallagher, J., C. Babish, & J. Malas (2005). *Damage Tolerant Risk Analysis Techniques for Evaluating the Structural Integrity of Aircraft Structures*. Proceedings of the 11th international conference on fracture, Turin, Italy.

ISO-12737 (2010). Metallic materials—determination of plane-strain fracture toughness. INTERNATIONAL STANDARD.

Iyyer, N. & M. Kittur (2002). Corrosion assessment of wing fold transmissions of a fleet fighter/attack aircraft. *2002 USAF Aircraft Structural Integrity Program Conference*.

Koucky, M. & D. Valis (2007). Reliability of sequential system with restricted number of renewals. *Risk, Reliability and Social Safety ESREL*.

Koucky, M., D. Valis, & Z. Vintr (2009). Contribution to highly reliable itemsÂt' reliability assessment. *Reliability, Risk and Safety: Theory and Applications (Proceedings of the European Safety and Reliability Conference, ESREL 2009)*.

Leski, A. & K. Dragan (2010). *Wyznaczenie sekwencji obci-azen do proby zmĂŹczeniowej samolotu PZL-130* Orlik TC-II Etap I âĂŞ wyznaczenie reprezentatywnej sekwencji zlozonej z zarejestrowanych lotow badawczych, SPRAWOZDANIE Nr 152/31/2010. Warsaw, Poland: Air Force Institute of Technology.

Leski, A., S. Klimaszewski, P. Barszcz, L. Jarzebinski, & T. Wolf (2008). *Okreslenie miejsc krytycznych w strukturze wybranego typu statku powietrznego ze wzgledu na za-grozenie uszkodzeniem zmeczeniowym, SPRAWOZDANIE Nr 137/31/2008*. Warsaw, Poland: Air Force Institute of Technology.

Liao, M., Y. Bombardier, & G. Renaud (2011). Monte Carlo simulation based probabilistic risk analyses for aircraft structures containing msd/med. *The Aircraft Airworthiness and Sustainment (AA&S) Conference*.

Liao, M., D. Forsyth, & N. Bellinger (2003). Risk assessment of corrosion maintenance actions in aircraft structure. *2003 USAF Aircraft Structural Integrity Program Conference*.

Liao M., B.Y. & R.G. (2012). Probabilistic risk analysis for aircraft structures with limited in-service damages. *28TH International Congress of The Aeronautical Sciences*.

Lisiecki, J. & D. Bochenek (2013). *Raport z badanian odpornosci na pekanie, Raport z badan nr 5/13*. Warsaw, Poland: Air Force Institute of Technology.

Miedlar, P., A. Berens, P. Hovey, T. Boehnlein, & J. Loomis (2005). *PRoF v3 PRobability Of Fracture Aging Aircraft Risk Analysis Update*. Dayton: University of Dayton.

MIL-STD-1530C (2005). *AIRCRAFT STRUCTURAL INTEGRITY PROGRAM (ASIP)*. DEPARTMENT OF DEFENSE STANDARD PRACTICE.

MIL-STD-882E (2012). *SYSTEM SAFETY*. DEPARTMENT OF DEFENSE STANDARD PRACTICE.

Valis, D., M. Koucky, & L. Zak (2012). On approaches for non-direct determination of system deterioration. *Eksploatacja i Niezawodnosc—Maintenance and Reliability 14*, 33–41.

Valis, D. & A. Krzak (2014). Selected safety aspects of polymer composites with natural fibres. *European Safety and Reliability Conference ESREL (in prep.)*.

Valis, D. & O. Pokora (2014). Application of selected diffusion processes on system state assessment. *European Safety and Reliability Conference ESREL (in prep.)*.

Valis, D. & Z. Vintr (2006a). Dependability of mechatronics systems in military vehicle design. *Safety and Reliability for Managing Risk âĂŞ Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006)*.

Valis, D. & Z. Vintr (2006b). Vehicle maintenance process optimisation using life cycle costs data and reliability-centred maintenance. *Proceedings of the First International Conference on Maintenance Engineering*.

Valis, D. & Z. Vintr (2007a). Aircraft gun reliability modelling. *Risk, Reliability and Societal Safety âĂŞ Proceedings of the European Safety and Reliability Conference ESREL 2007*.

Valis, D. & Z. Vintr (2007b). Modeling and analysis of the reliability of systems with one-shot items. *Proceedings of Annual Reliability & Maintainability Symposium*.

Valis, D., Z. Vintr, & J. Malach (2012). Selected aspects of physical structures vulnerability âĂŞ state-of-the-art. *Eksploatacja i Niezawodnosc—Maintenance and Reliability 14*, 189–194.

Valis, D. & L. Zak (2014). Contribution to oil data assessment for system condition determination. *European Safety and Reliability Conference ESREL (in prep.)*.

Vintr, Z. & D. Valis (2012). A tool for decision making in k-out-of-n system maintenance. *Applied Mechanics and Materials 110–116*, 5257–5264.

Vintr, Z., D. Valis, & J. Malach (2012). Attack tree-based evaluation of physical protection systems vulnerability. *Proceedings—46th Annual IEEE International Carnahan Conference on Security Technology*, 59–65.

Woch, M. (2013). *Analiza ryzyka (Risk Analysis) dla punktow kontrolnych (Control Points—CP) struktury nosnej samolotu PZL-130 TC-II Orlik, METODYKA BADAN MB-17/31/2013*. Warsaw, Poland: Air Force Institute of Technology.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk assessment of a bulk cryogenic tank: Beyond the Leak-Before-Break criterion

M. Compare & L. Legnani
Aramis Srl, Milan, Italy

M. Buldrini
Nier Ingegneria, Bologna, Italy

G. Sansavini
ETHZ, Zurich, Switzerland

E. Zio
Ecole Centrale Paris and Supelec, Paris, France
Politecnico di Milano, Milan, Italy

L. Beretta
SOL Group, Monza, Italy

ABSTRACT: The increase in the size and production capacity of air separation plants has boosted the need of developing methodologies to properly assess the risk related to major releases of liquefied gas. In this respect, the Leak-Before-Break (LBB) assessment is currently adopted to demonstrate the safety of the structures containing liquefied gas, under the assumption that the tank is always operated in nominal conditions. This assumption is questioned in this paper, which proposes a new methodology for the assessment of the risks related to cryogenic tank catastrophic rupture. The methodology provides a comprehensive understanding of the issues associated to the worst case rupture scenario: from the investigation of the causes of the undesirable operating conditions up to the analysis of the associated structural consequences, within a probabilistic framework.

1 INTRODUCTION

The increase in the size and production capacity of air separation plants, has led to a growing capacity of cryogenic liquid storage installations at production sites. Therefore, considering the potential hazards associated with liquid products has become a fundamental issue to address, together with the estimation of the effects of a major release of liquid on the local environment, and the development of preventive measures.

Nowadays, evaluating the structural safety of the cryogenic tanks by critically examining the integrity of new or existing constructions is a common practice. To do this, non-destructive testing methods for flaws detection are usually performed, whereas acceptability criteria for the revealed flaws have been defined in standards of the sector. In this respect, a typical approach to demonstrate the safety of a structure containing defects is to design it under the Leak-Before-Break (LBB) criterion; the scope is to guarantee that in nominal operating conditions the stress conditions inside the structure are such that the growth of flaws leaves time for a stable leak of the liquefied gas preceding the occurrence of a sudden disruptive break of the structure. Thus, a leakage of fluid through a crack can be detected before it reaches a critical dimension; this allows preventing catastrophic liquefied gas releases.

In practice, the LBB design criterion is based on setting two critical values for the crack length: l_C and l_L. The former represents the maximum length that prevents the tank from experiencing a catastrophic rupture; the latter represents the minimum length to have a fluid leakage. To meet the LBB criterion, the designers have to prove that $l_L < l_C$ with a suitable margin: in this case, a fluid leakage is detected before the catastrophic failure. In particular, the analysis is conducted at the most risky vessel sections, i.e, the sections with extreme loading conditions and poorest material properties.

However, the traditional LBB approach suffers from the limitation of considering the tank

behavior in nominal operating conditions, only. Indeed, it is also interesting to analyze the worst case rupture scenario, which, for the structure under study, coincides with the tank catastrophic rupture, caused by potential malfunctions of the control system or the safety devices.

In this context, the paper proposes a new approach to the assessment of the risks related to the catastrophic rupture of a flat bottom cryogenic tank containing Liquefied Oxygen (LOX). The rupture is considered catastrophic if it leads to an uncontrollable nearly-instantaneous release of the entire liquefied gas content. The assessment aims at reaching a comprehensive understanding of the problems related to the tank rupture, from the investigation of the causes of abnormal operating conditions up to the analysis of the associated structural consequences, within a probabilistic framework.

The proposed procedure consists of two parts. In the first part, Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) guide the investigation of the storage system in order to identify the critical events that may evolve in dangerous scenarios affecting the structural safety of the tank, together with the associated occurrence frequencies. This part of the study also includes sensitivity and uncertainty analysis, which allow improving the robustness of the results. In the second part, structural analyses based on Finite Element Methods (FEM) are performed to investigate the behavior of the tank in both ordinary and abnormal operating conditions. In particular, the abnormal conditions are those in which the vessel is under exceptional stresses, due to the critical scenarios identified by FMEA and FTA. The combination of FMEA, FTA and FEM structural analyses allows identifying and assessing the stress conditions which may lead to a catastrophic rupture of the tank. The main outcome of such an analysis is a list of recommendations such as the installation of protective equipment and instrumentation, definition of a strategy for equipment inspection and testing, identification of the components for which a re-design may be convenient, etc. This allows reducing the occurrence of large releases of cryogenic fluids, by providing useful guidelines to the engineers directly involved in the design, installation, operation and maintenance of bulk cryogenic liquid storage systems.

2 CASE STUDY

The methodology is illustrated by way of a real case study concerning a LOX flat bottom cryogenic tank, owned by SOL Group and sited in Frankfurt. The analysis focuses on the cryogenic tank and all the pieces of equipment connected to it. This is compliant to the definition of tank given by EIGA IGC Doc. 127/13/E(EIGA 2013):

"the total fixed assembly of liquid storage tank(s) integrated with other equipment, such as pumps, filling equipment, pressure build-up vaporizers, controls and other related ancillary equipment that are connected to it."

The cryogenic tank is made up of two different structures: the internal vessel, which is designed to contain the cryogenic liquid, and the outer casing, which contains the insulating material that ensures a correct storage of the liquefied gas. The inner tank, with capacity of 2000 m^3, is made of stainless steel A240-304; this material is capable of withstanding cryogenic temperatures of the liquefied oxygen, which is stored at −183 °C, at nearly atmospheric pressure (−0.0022 bar < P < 0.095 bar). The outer casing, made of A283 grC, is not designed to withstand low temperatures, as it is not wetted by liquefied oxygen in normal operations.

Both vessels are connected to a number of components which allow performing the liquefied oxygen load and unload operations, and guarantee that the operating pressure, temperature and level conditions are close to the corresponding design values.

The tank is usually filled with the liquefied oxygen from the liquefaction unit, although sometimes it can be stocked up with liquid from tanker track. The unloading operation is performed by means of cryogenic pumps, which fill the tanker tracks for final distribution. A drain system is also installed on the inner vessel to allow the complete removal of the stored liquid in emergency conditions.

The annular space delimited between the inner and outer vessels is intended to ensure a thermal insulation. To this aim, it is filled up with perlite, an amorphous volcanic glass with high insulating characteristics and light weight. Moreover, to guarantee a better insulation quality, the annular space is also continuously flushed with nitrogen, which allows keeping the insulation in a dry state. The nitrogen flow is provided by nozzles located at the inner vessel bottom, and is released in proximity of the top of the tank.

Table 1 and Table 2 summarize the material properties and the operating conditions of the inner vessel and the annular space, respectively.

The operating conditions are controlled by two redundant systems: an equipment installed to regulate the value of the parameters during normal operations, and a set of safety devices to prevent the occurrence of dangerous conditions in the tanks, when regulating system fails. In addition, the vessels are provided with detectors and alarms, which go off when measured parameters assume unexpected values.

Table 1. Material properties.

	Oxygen	Nitrogen
Content in air	21 Vol%	78.1 Vol%
Gas density (1.013 bar, 15°C)	1.36 kg/m^3	1.19 kg/m^3
Boiling temperature (1.013 bar)	–183°C	–196°C
Liquid density (1.013 bar, boil T)	1.14 kg/l	0.8 kg/l

Table 2. Operating conditions for the LOX storage system.

	Inner tank	Annular space
	Oxygen	Nitrogen
Temperature	–183°C	+20°C
Vapor space press max	+0.095 bar	+0.01 bar
Max negative pressure	–0.0022 bar	–0.0022 bar
Max level	14.32 m	

3 A NOVEL APPROACH TO RISK ASSESSMENT OF A CRYOGENIC TANK

The risk associated to the catastrophic rupture of the cryogenic storage system described above has been studied by applying a novel and comprehensive approach, which can be summarized in the following three steps:

1. FMEA and FTA. These traditional techniques of risk analysis allow identifying the critical events that may lead to dangerous scenarios affecting the structural safety of the tank, and estimating the associated occurrence frequencies.
2. Uncertainty and sensitivity analyses, which are performed to assess the robustness of the results obtained from the previous step.
3. Structural analyses, performed to evaluate the severity of the consequences of the tank rupture both in ordinary operating conditions and in the critical scenarios identified by FMEA and FTA.

In the following Sections, the different steps are detailed, and the corresponding results commented.

3.1 *Identification of critical events dangerous for the structural safety of the cryogenic tank*

3.1.1 *Procedure*

In the first step of the procedure, a FMEA study is performed, whose core is to go over all the potential component failure modes, identify the consequent losses of system functionalities and configure the resulting outcomes from the accidental scenarios; a qualitative evaluation of the criticality of the failure modes is also given by the analysts in terms of severity of consequences and likelihood of occurrence. These two latter attributes, severity and likelihood, are the entries of a criticality matrix, which allows assessing whether the failure modes are critical and violate the safety requirements.

This analysis has supported a full understanding of the system at hand, and its main outcomes have been:

- The functions implemented by the system;
- The items involved in performing these functions;
- The consequence of each loss of function. This information is used for the identification of the most severe events in relation to the tank integrity, to be further investigated;
- The identification of the most critical elements of the system, whose malfunctions can affect the integrity of the tank or the success of functions that concur in assuring the structural integrity;
- The identification of the failure modes and failure rates associated to the critical items;
- The detection means of the different failure modes;
- The redundancies of the system, listed in the fields "compensatory measures" and "remarks".

Once the critical events have been identified, a quantitative FTA has been carried out to estimate the occurrence frequencies of the undesired events.

3.1.2 *Results*

The functioning of the storage system has been analyzed with respect to eight main functions:

1. Inner tank pressure regulation;
2. Inner tank pressure safety control;
3. Inner tank level safety control;
4. Liquid extraction;
5. Liquid introduction;
6. Insulation;
7. Annular space pressure safety control;
8. Oxygen containment.

The FMEA has shown that the safety related functions are the most critical among the eight above. This is an expected result, as safety related functions are involved in mitigating or compensating conditions potentially dangerous for the tank integrity. In this respect, Table 3 shows the critical functions and the subsystems involved in their implementations.

Table 3. Critical functions and related subsystems.

Functions	Associated subsystems
Inner tank pressure Safety control	Pressure safety valve PSV4001 Pressure safety valve PSV4002
Inner tank level Safety control	Differential pressure level meter LT/LI4002 Differential pressure level meter LT/LI4003 Level switch LSHH/LSH4004
Annular space pressure Safety control	Pressure safety valve PSV4003 Pressure safety vent PSE4001

Finally, the procedure has allowed to identify four critical events and their occurrence frequencies:

- TOP event 1: overpressure in the inner tank (pressure > 95 mbar), as consequence of the malfunction of the pressure safety subsystems;
- TOP event 2: under pressure (i.e., vacuum) in the inner tank (pressure < –2.2 mbar), as consequence of the malfunction of the pressure safety subsystems;
- TOP event 3: extreme liquid level in the inner tank (level > 14.32 m), as consequence of the malfunction of the level safety subsystems;
- TOP event 4: overpressure in the annular space (pressure > 10 mbar), as consequence of the malfunction of the pressure safety subsystems.

The failure frequencies of the four critical events, at time $t = 20$ years are listed in Table 4. In particular, these values refer to two different settings:

1. The Pressure Safety Valves (PSV) installed on the tank to protect the structure against overpressures are periodically inspected, with a period of 4 years;
2. PSV are not inspected.

In this respect, notice that the regular inspection and maintenance of the pressure safety devices is not mandatory for the typology of tank under analysis, since the particular vessel is not required to comply with the Pressure Equipment Directive (97/23/EC).

The two different work hypotheses yield two values of occurrence frequencies. In fact, the inspection interval enters the quantification of the availability of dormant devices such as the safety valves degradation (Zio 2007). In particular, from Table 3 it emerges that even when the PSV are not periodically inspected, the frequencies of the four top events have very small values (smaller than 10^{-7} y^{-1}). The small values of these frequencies are due to the fact that long sequences of failure events have to occur to get the top event; in addition, as illustrated in Table 3, there is redundancy of safety control devices.

Table 4. Occurrence frequencies of critical events.

	Failure frequency events/year	
	PSV inspected	PSV not inspected
TOP event 1	8.76 e-12	7.86 e-10
TOP event 2	3.64 e-10	3.27 e-8
TOP event 3	8.30 e-9	7.93 e-8
TOP event 4	1.85 e-10	1.68 e-8

On the other side, from Table 4 it also emerges that when the PSV are regularly maintained, then the occurrence frequencies of the top events decrease significantly. Therefore, a periodic inspection of the PSVs is highly recommended for any generic flat bottom cryogenic tank, even if not mandatory.

3.2 *Robustness of the results*

Importance, uncertainty and sensitivity analyses have been performed in order to investigate the robustness of the results. In particular, these additional analyses have been carried out for every critical event, with a twofold scope:

1. Identifying the component failures or basic events which most influence the event occurrence frequency. This allows to identify the system weaknesses, and provides guidelines for effective actions for system improvements;
2. Estimating the uncertainty on the critical event occurrence frequencies, which comes from the lack of precise knowledge about the failure model parameters.

3.2.1 *Importance analysis*

Generally speaking, Importance Measures (IMs) aim at quantifying the contribution of components or basic events to the considered measure of system performance, which can be the system reliability, unreliability, unavailability or risk, depending on the application (Zio 2007; Baraldi et al. 2009). Information about the importance of the components constituting a system with respect to its safety and availability is of great practical aid: the identification of the components which mostly determine the overall system behaviour allows identifying system vulnerabilities and the most effective actions for the system improvement.

Different IMs have been proposed in literature, which allow investigating different system features. In particular, the Birnbaum IM expresses the contribution to system reliability of the reliability of the various system components (Baraldi et al.

2013). In details, components for which a variation in the reliability results in the largest variation of the system reliability have the highest importance. Thus, a reduction in the occurrence probability of the most important events is expected to result in a reduction of the occurrence probability of the TOP event.

With reference to the analysed case study, the Birnbaum IM have been computed for each basic event constituting the Fault Trees of the four investigated critical events. This has allowed to identify the most important basic events, and thus the improvement actions with the highest priority.

The results of the analysis can be summarized as follows:

- The failure of the inner tank pressure Safety Valves greatly influences two out of four critical events (TOP event 1 and TOP event 2). Then, improving the reliability of these items is expected to lead to a great improvement in system reliability;
- Redundancy in the monitoring system of the control valves in the inner tank pressure would significantly reduce the occurrence probability of the critical TOP event 1;
- A good control during the operation of tank filling and emptying is recommended in order to reduce the probability of occurrence of the critical TOP events 2 and 3;
- The failure of the Pressure Control Valves PCV9039 (i.e., the valves regulating the nitrogen purging into the annular space between the inner and outer vessels) greatly influences the occurrence of the critical TOP event 4.

An uncertainty analysis has been performed in order to assess the robustness of the results of the importance analyses. In fact, the importance measures depend on the values of the failure probabilities of the components of the storage system, which are uncertain. Thus, the results of the importance analysis need to be checked against the variability due to the uncertainty in the model input parameters. To do this, uncertainty in the occurrence probabilities of the most important basic events has been considered by uniform distributions with lower and upper bounds provided by SOL experts. The analysis has highlighted that the uncertainties in the occurrence probabilities of the basic events do not impact on the ranking of the most important causes identified for each TOP event: thus, the results discussed above can be considered robust.

3.2.2 *Uncertainty and sensitivity analysis*

As mentioned in Section 3.1.1, FTA has been performed to calculate the occurrence probabilities of the four critical events identified by the FMEA study.

In general, FTA allows resolving a TOP event into the combination of single primary events, which contribute to its realization. Then, the probability of the TOP event is computed as function of the probabilities of the basic events. However, in practice it is often difficult to evaluate the exact probability values of the primary events, which are affected by uncertainties. These latter need to be propagated through the Fault Tree model to assess the variability in the Top event failure probability due to the variability in the probability values of the basic events.

Two different analysis have been carried out, both based on Monte Carlo (MC) method:

- Sensitivity analysis to identifying the contribution of the various basic events to the uncertainty in the TOP event.
- Uncertainty analysis to propagate the uncertainties from the basic events up to the TOP events.

The results of the sensitivity analysis have shown that the estimations of the probabilities of the critical events are significantly influenced by the uncertainties in the failure probability values of the PSVs, human errors and uncontrolled filling and emptying operations. Then, improving the knowledge about the occurrence probability values of the identified events would reduce the uncertainty in the overall system reliability.

Once the most influent basic events have been identified, MC sampling technique has allowed to estimate the probability distribution expressing the variability in the probability of occurrence of every TOP event considered. Such distributions have shown that the values of the occurrence probability calculated without uncertainty, are always near to the values of the distributions associated to highest probability (distributions modes). However, the occurrence probability reference values are located toward the low values of the probability distributions. This finding entails that disregarding the uncertainty in the top event probability values does not lead to conservative results, and thus highlights the importance of giving due account to the uncertainty in reliability assessments.

3.3 *Structural analysis*

The Finite Element Method (FEM) has been used to perform the structural analysis to demonstrate the LBB criterion in both nominal and deviated conditions. FEM is a numerical technique for resolving complex problems, widely used in structural mechanics. The structural system to be studied is modeled by a set of finite elements interconnected at points, called nodes, that are organized in a mesh. The analysis provides the stresses and displacements, in each single element of the

mesh. Therefore, the FEM methodology allows to identify the most stressed portions of the analyzed object.

For the case under study, the flat bottom tank has been modeled with a mesh of 262919 elements and 264267 nodes. The FEM analyses have been performed considering the tank behavior both in nominal operating conditions and in conditions of extreme loads, caused by the occurrence of the critical events identified by the previous failure analyses. The loads in ordinary conditions and the material strength have been set according to SOL internal documents.

As expected, the analysis performed in ordinary conditions has shown that the tank is not subjected to excessive stresses and strains when everything operates normally: both Von Mises stresses and displacements are smaller than the maximum allowable limit set by the designers. Moreover, the analysis has highlighted the weakness of the structure in correspondence of the conjunction between the wall and the dome of the inner vessel. This is due to the fact that the stresses concentrated in this portion of the structure are very high, as exemplified in Figure 1 which shows the stress level in the inner tank under external pressure, in nominal conditions.

Analyses relevant to the critical scenarios have been carried out with the purpose of identifying the extreme values of pressure (TOP event 1, 2 and 4) and liquid level (TOP event 3) that leads to the rupture of the tank structure. The resulting values are summarized in Table 5.

In particular, no value is reported for TOP event 3, corresponding to the scenario of tank overfilling. Indeed, the analysis has shown that the criticality of such scenario is not due to the hydrostatic pressure of the liquid, but to the overpressure generated by the pumps that introduce the LOX in the vessel. Therefore, the TOP events 3 is analyzed similarly to TOP event 1 (i.e., overpressure in the inner tank).

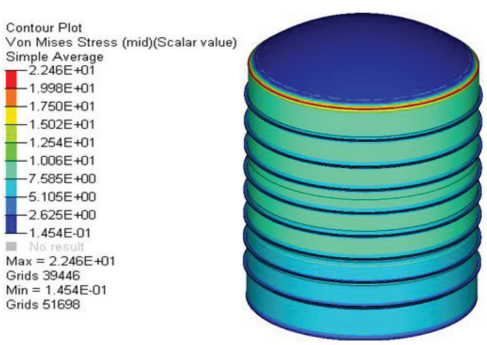


Figure 1. Von Mises stresses in the internal vessel under external ordinary pressure.

Table 5. Extreme loads that lead to tank rupture.

	Parameter	Max value
TOP event 1	Pressure inner tank	187.5 mbar
TOP event 2	Pressure inner tank	–175 mbar
TOP event 3	Level in inner tank	_
TOP event 4	Pressure annular space	1610 mbar

The values listed in Table 5 are expected to be reached gradually, with a slow variation in the level and pressure values. This operating condition makes reasonable to assume that if cracks appear on the metal surfaces, then they slowly propagate. In these conditions, the detection of the leak is possible before the sudden rupture of the tank. In details, the analyses have highlighted that TOP events 1, 2 and 3 lead to the rupture of the inner tank, whereas TOP event 4 generates failure on the outer casing. In the first case, the LOX penetrates into the annular space and ice forms on the outer casing; this can be visually detected. In the latter case, when the external vessel breaks, there is a release of perlite in the air, which, again, is easily detectable.

As in ordinary conditions, the loads corresponding to TOP events 1, 2 and 3 show that the weak section of the storage system lies in correspondence of the conjunction between the wall and the dome of the inner vessel. TOP event 4, instead, particularly stresses the surface of the vertical wall.

The results are compliant with the adopted manufacturing standards; in fact, quoting EIGA IGC Doc 127/13:

"The need to prevent a rupture by overpressure at the bottom of the inner tank is identified in the various available codes. API 650 talks of a frangible joint between the roof and the shell and gives it as a possible purchaser requirement. API 620, instead, establishes a link between the sizing of the anchorage straps and the design of the roof to shell junction. Finally, BS 7777 explicitly states that the weakest point of the structure shall not be at the bottom and present it as a further increase in safety".

3.4 *Conclusions*

The present study has been performed with the aim of evaluating the risks related to the catastrophic rupture of a flat bottom cryogenic tank containing liquefied gas. To do this, the cryogenic storage system has been deeply investigated in order to identify all the critical events that may evolve in dangerous scenarios affecting the structural safety of the cryogenic tank, together with their associated occurrence probabilities.

Four critical events have been identified, whose occurrence frequencies are very low. It has also emerged that regular inspections of PSVs yield a significant reduction in the occurrence frequencies of the top events.

The robustness of the risk analysis results has been checked by means of sensitivity and uncertainty analysis.

The structural behavior of the flat bottom tank has been analyzed both in ordinary operating conditions and in case of exceptional loads, due to the occurrence of the individuated TOP events, with the aim of assessing whether the identified scenarios produce loads that may lead to the rupture of the analyzed vessel.

As expected, the analysis performed in ordinary conditions has shown that the tank is not subjected to excessive stresses and strains. The analyses under the conditions brought by the critical events have allowed:

- Estimating the load conditions that lead to the rupture of the tank structure.
- Checking that there is a release of LOX or perlite when such load values are reached. This entails that both the failures of the inner and outer vessels can be detected.
- Verifying that an explosion of the tank can be regarded as improbable, due to the slow variation in level and pressure.

Finally, the structural analysis has also highlighted, in both ordinary and extreme conditions, the structure weakness in correspondence of the conjunction between the wall and the dome of the inner vessel, except for TOP event 4. This is compliant with the recommendations of the design codes API 620, API 650 and BS 7777, which require to design the vessels in such a way to ensure that the weakest point of the inner tank is not at the bottom cylindrical seam, but at the top of the vessel (EIGA 2013).

REFERENCES

API 620. Design and Construction of Large, Welded, Low-pressure Storage Tank. American Petroleum Institute. API Publishing Services. Washington DC.

API 650. Welded Steel Tanks for Oil Storage. American Petroleum Institute. API Publishing Services. Washington DC.

Baraldi P., Compare M., Zio E. 2013. Component ranking by Birnbaum importance in presence of epistemic uncertainty in failure event probabilities. *IEEE Transactions on Reliability 62(1)*:37–48.

Baraldi, P., Zio, E., Compare, M. 2009. A method for ranking components importance in presence of epistemic uncertainties. *Journal of Loss Prevention in the Process Industries 22(5)*:582–592.

BS 7777. Flat bottomed, vertical, cylindrical storage tank for low temperature service. British Standard Institute. London. United Kingdom.

BS 7910:2005. Guide to methods for assessing the acceptability of flaws in metallic structures. British Standard Institute. London. United Kingdom.

EIGA. 2013. IGC Doc 127/13/E. Bulk liquid oxygen, nitrogen and argon storage systems at production sites. Bruxelles.

Zio, E. 2009. Computational Methods for Reliability and Risk Analysis. *Series in Quality, Reliability and Engineering Statistics Vol 14*. *World Scientific*. Singapore.

Zio, E. 2007. An Introduction to the Basics of Reliability and Risk Analysis. *Series in Quality, Reliability and Engineering Statistics Vol 13. World Scientific.* Singapore.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Modeling of a degradation path set with a Gamma process mixture—application to a maintenance decision rule

Edith Grall-Maës, Antoine Grall & Pierre Beauseroy
ICD-LM2S, Université de Technologie de Troyes, UMR 6281 CNRS, Troyes, France

ABSTRACT: A maintenance decision rule is considered for deteriorating systems executing successive working cycles and which can be inspected from time to time. A novel method is proposed to exploit jointly degradation measurements originating from a set of identical spare parts and maintenance practices for making a degradation prognosis. The systems experience different degradation processes depending on operational conditions, and assumed to be Gamma processes. The aim is to cluster the degradation paths in classes corresponding to the different operational conditions in order to group properly the data for the estimation of degradation process parameters. A model of Gamma process mixture is considered and an expectation-minimization approach is proposed to estimate the unknown parameters. The feasibility of the method is shown on simulated cases. Prognosis results obtained with the proposed method are compared with results obtained with basic strategies (considering each system alone or all systems together).

1 INTRODUCTION

In practice, most of the manufacturing systems have to execute successive jobs or working cycles. Some units or devices in the systems are deteriorating with usage. Wear or cumulative degradation can lead to failure with production downtimes or loss of quality of the end product. A relevant maintenance decision making ails to ensure balance between preventive planned maintenance and corrective one. In various situations different maintenance practices and different sets of spare parts procured from several suppliers have an impact on the degradation process.

This paper considers the case of a dynamic maintenance decision rule based on the remaining useful lifetime of the considered device or item. To estimate the Remaining Useful Lifetime (RUL) of a deteriorating system it is necessary to be able to model its deterioration in order to predict when the deterioration leads to a failure i.e. when it reaches a given threshold. To perform this RUL prognosis one generally relies on measurements of the degradation level and on a degradation model which is assumed to describe the degradation evolution in time (Si, Wang, Hu, & Zhou 2011, Nystad, Gola, & Hulsund 2012). For example, in the case of a metal pipe corrosion, the thickness provides a deterioration measure.

The Gamma process is widely used for degradation models when deterioration is non decreasing and gradual (Van Noortwijk 2009). This process is defined by a set of parameters, in particular the shape and scale parameters in the case of an homogeneous process. These parameters are usually unknown and must be estimated in order to perform prognosis. Obviously the reliability of prediction is directly related to the estimation precision. Most of the time, in operational conditions the amount of measurement is very limited. So when a set of similar systems is available, one can use the data coming from all the systems in the set to estimate the model parameters. The expected gain of using all measurements together is to improve the estimator precision (reduction of its variance for example).

By considering all systems as a single one while estimating the model parameters it is assumed that the degradation process model is the same for all systems. In most cases, the degradation process depends also on operating conditions that may be partially unknown. In the pipe corrosion example, the evolution of the pipe thickness depends on the used metal but it also depends on the characteristics of the fluid carried by the pipe (liquid/gaz, temperature, pressure …) and on the location (air/ground/underwater …) and on the environmental conditions of the pipe (temperature, humidity …).

In this paper, we consider that we have a limited amount of data from different systems. Each system has one operating condition among an unknown finite number. For each operating condition the degradation process is assumed to be ruled

by a Gamma process model. The aim is to estimate the parameters of these Gamma processes in order to predict their RUL for maintenance decision making purpose.

We propose a method to cluster the observed systems in classes, in order to estimate properly the Gamma process parameters. In order to tackle the hypothesis of a number of operating conditions, a model of Gamma process mixture is introduced. An expectation-minimization algorithm is considered to estimate the parameters of each process in the mixture model.

The problem is formalized in section 2. Then in section 3, the mixture model and the expectation-minimization algorithm (Ambroise & Govaert 1998) (Hu & Sung 2006) are presented to determine the clusters. In section 4, the considered prognosis is described and a maintenance decision rule is proposed. The maintenance policy assessment is used for comparing the prognosis values obtained according to different strategies of the Gamma process parameter estimation. In section 5, results on simulated data are presented and analyzed.

2 PROBLEM FORMULATION

This section first gives a description of the problem and notations and ends with a brief recall about the Gamma process.

2.1 *General aim*

The data we consider originates from N components which are inspected randomly. More precisely each component is inspected opportunistically e.g. when the system is stopped or between two production batches. It is assumed the time interval between two successive inspections is random and uniformly distributed between two bounds a and b. Each component is associated to a path describing its degradation process realizations. At a given time, each path $p_n, (n = 1, \ldots, N)$ is composed of $|p_n|$ observations $l_{n,i}$ with $i = 1..|p_n|$. The observation $l_{n,i}$ is characterized by the inspection time $t_{n,i}$, and the observed deterioration level $x_{n,i} = x(t_{n,i}) \in \Omega_x \subset \mathcal{R}$. Then $p_n = \{l_{n,i} = (t_{n,i}, x_{n,i})\}_{i=1..|p_n|}$.

We suppose that the observation set can be divided into K unknown clusters $C_k, (k = 1, \ldots, K)$. In practice, each cluster would correspond to an operating condition. Each cluster represents a deterioration process characterized by some unknown parameter vector belonging to the parameter set $\Theta = \{\theta_k\}_{k=1}^{K}$. Besides, the latent membership, or cluster labels of paths are denoted by $\mathbf{z} = \{z_n\}_{n=1}^{N}$ where $z_n = k$ means that the path p_n belongs to the cluster k. A set of cluster labels defines a partition of all paths. Obviously, for a given path n, all observations $l_{n,i}, (i = 1, \ldots, |p_n|)$ belong to the same cluster.

The aim is to determine the latent cluster label for each observation and jointly the parameter vector of each process. Afterwards this parameter vector can be used for remaining lifetime prognosis and maintenance decision-making. Each component is supposed "failed" as soon as its deterioration level crosses a threshold S hereafter referred as "failure limit".

In this paper the chosen model for the deterioration processes is the Gamma process, parameterized by 3 parameters, a, b and u described in section 2.2. The increments, given by $x(t_{n,i}) - x(t_{n,i-1})$ with $t_{n,0} = 0$ and $x(0) = 0$, are independent. Their density distribution in the cluster k depends on the time and on the parameter θ_k, and can be written as

$$f_k\left(x(t_{n,i}) - x(t_{n,i-1}) \mid t_{n,i}, t_{n,i-1}, \theta_k\right).$$

In the following, for simplicity we will use the notation $f_k(\Delta x_{n,i} \mid \theta_k)$. It has to be noticed that the density distributions of all the degradation increments are not the same because the increments are usually all different and/or the process may be not stationary.

The objective is to find out the unknown cluster labels $\{z_n\}_{n=1}^{N}$ and consequently the distribution parameter set $\theta = \{\theta_k\}_{k=1}^{K}$, such that paths in the same cluster originate from a process model with the same parameters.

The relevance of a partition described by $\mathbf{z}$ and a parameter set θ can be measured using the log-likelihood given by

$$l(\mathbf{z}, \theta) = \sum_{n=1}^{N} \sum_{i=1}^{|p_n|} logf_{z_n}(\Delta x_{n,i} \mid \theta_{z_n}) \quad (1)$$

2.2 *Gamma process*

2.2.1 *Definition*

Mathematically, the Gamma process is defined as follows: let $A(t)$ be a non-decreasing, right-continuous, real-valued function for $t \geq 0$, with $A(0) = 0$. The Gamma process with shape function $A(t)$ and scale parameter $b > 0$ is a continuous-time stochastic process $\{X(t), t \geq 0\}$ such that:

- $X(0) = 0$ with probability one;
- $\{X(t), t \geq 0\}$ is a stochastic process with independent increments;
- $\Delta_{s,t}X = X(t) - X(s)$ follows the Gamma distribution $\Gamma(A(t) - A(s), b)$ for $0 \leq s < t$

where the Gamma distribution is characterized by the p.d.f written as:

$$f_{u,v}(x) = \frac{v^u}{\Gamma(u)} x^{u-1} e^{-vx} \mathbb{I}_{(0,\infty)}(x) \quad (2)$$

with $u > 0$ the shape parameter, $v > 0$ the scale parameter, $\mathbb{I}_{(0,\infty)}(x)$ the indicator function and $\Gamma(x)$ the Gamma function.

The definition of the Gamma process leads to two straightforward properties:

- $\{X(t), t \geq 0\}$ is a non-decreasing process.
- For all $t \geq 0$, the expectation value and the variance of $X(t)$ could be written as:

$$\mathrm{E}(X(t)) = \frac{A(t)}{b} \quad \mathrm{Var}(X(t)) = \frac{A(t)}{b^2} \quad (3)$$

An homogeneous Gamma process corresponds to a particular case with $A(t) = at, (a > 0)$. In this case, $X(t) - X(s)$ follows the Gamma distribution $\Gamma(a(t-s), b)$, which means that the increments of the process depend only on the time increments $t - s$.

In the degradation modeling framework, a non-homogeneous Gamma process defined by $A(t) = at^u$, $(a > 0, u > 0)$ is often considered. Thus the process is described by three parameters: a, b, and u. In this case, $X(t) - X(s)$ follows the Gamma distribution $\Gamma(a(t^u - s^u), b)$.

2.2.2 *Parameter estimation*

Two methods are often mentioned for the parameter estimation of the Gamma process: the moments estimation and the maximum likelihood estimation (Cinlar, Osman, & Bazant 1977). The maximum likelihood estimator is asymptotically unbiased, which means the estimates converge to the true values as the number of observations increases as: $N \to \infty$. On the other hand, the moments approach leads to simpler formulae of the estimator. It is more straightforward to implement and the computation time is much reduced compared with the maximum likelihood method.

3 PROCESS CLUSTERING

The proposed approach is based on the computation of mixture models using the Expectation-Maximization (EM) algorithm (Dempster, Laird, & Rubin 1977). Beside, side information is considered according to (Shental, Bar-Hillel, Hertz, & Weinshall 2003).

3.1 *Related work*

The EM algorithm is an iterative method that produces a set of parameters that locally maximizes the log-likelihood of a given sample, starting from an arbitrary set of parameters. It is often used to estimate the unknown parameters of a mixture model of K p.d.f. f_k given by:

$$f(x \mid \theta) = \sum_{k=1}^{K} \alpha_k f_k(x \mid \theta_k)$$

where α_k is the probability of class k and $f_k(x \mid \theta_k)$ the a posteriori probability of class k.

Furthermore the procedure we use is based on the work of Shental et al. (Shental, Bar-Hillel, Hertz, & Weinshall 2003) which describes an EM procedure for a Gaussian mixture model and for handling positive constraints, indicating that some observations arise from the same source. The data set is assumed to be a set of chunklets, and each chunklet is a set of points that originate from the same source. Alternating E steps and M steps leads to the estimation of the probability of each class, and the parameters (mean and variance) of each Gaussian class. The solution can be considered as a soft partition.

3.2 *Proposed method*

The problem we deal with, in comparison with the problem considered in (Shental, Bar-Hillel, Hertz, & Weinshall 2003), has to lead to a hard partition. Then we add an intermediate classification step between the E and M steps. This has been suggested in (Celeux & Govaert 1992, Celeux & Govaert 1995) in a hard classification problem using mixture models without constraints.

In comparison with the problem considered in (Shental, Bar-Hillel, Hertz, & Weinshall 2003), there is another main difference. The model is not a Gaussian mixture model and especially the degradation increments have different density distributions. The density distributions of all the degradation increments would be the same only in the case of homogeneous Gamma process, and of regularly sampled paths.

Thus, we have proposed an algorithm based on the mixture models for the problem of statistical process clustering with the two following properties. On the one hand, it takes into account that observations in a same path belong to a same class, and on the other hand it takes into account that a hard classification is searched.

The E step at iteration m consists in calculating an estimation of the *a posteriori* probability for each observation using the parameters $\theta^{(m-1)} = (a^{(m-1)}, b^{(m-1)}, u^{(m-1)})$. The posterior probability $c_{nk}^{(m)}$ at iteration m that the path n belongs to class k, given p_n and the parameter $\theta^{(m-1)}$ writes according to

$$c_{nk}^{(m)} = p(z_n = k \mid p_n, \theta^{(m-1)}) = \frac{\alpha_k^{(m-1)} \prod_{i=1}^{|p_n|} f_k(\Delta x_{n,i} \mid \theta_k^{(m-1)})}{\sum_{r=1}^{K} \alpha_r^{(m-1)} \prod_{i=1}^{|p_n|} f_r(\Delta x_{n,i} \mid \theta_k^{(m-1)})} \quad (4)$$

with

$$f_k(\Delta x_{n,i} \mid (a_k, b_k, u_k)) \sim \Gamma(a_k (t_{n,i}^{u_k} - t_{n,i-1}^{u_k}), b_k)$$

The expectation of the log-likelihood over all possible assignments which comply the given constraints is given by:

$$E(l(\mathbf{z}, \theta)) = \sum_{k=1}^{K} \sum_{n=1}^{N} log \alpha_k p(z_n = k \mid p_n, \theta_k^{(m-1)}) + \sum_{k=1}^{K} \sum_{n=1}^{N} \sum_{i=1}^{|p_n|} log f(\Delta x_{n,i} \mid k, \theta_k) p \times (z_n = k \mid p_n, \theta_k^{(m-1)})$$

The M step at iteration m consists in computing the parameters $\alpha_k^{(m)}$, and $\theta^{(m)}$ that maximize the expected log-likelihood found on the E step. The parameter $\alpha_k^{(m)}$ is given by

$$\alpha_k^{(m)} = \frac{1}{N} \sum_{n=1}^{N} (z_n^{(m)} = k) \quad (5)$$

and the parameters $(a^{(m)}, b^{(m)}, u^{(m)})$ are determined by maximization of the log-likelihood.

Then the algorithm is the following one.

- Initialize the parameter set $\theta^{(0)}$
- Repeat until $l(\mathbf{z}^{(m)}, \theta^{(m)}) - l(\mathbf{z}^{(m-1)}, \theta^{(m-1)}) < \in$
  - compute $c_{nk}^{(m)}$ for each path n and each class k using relation (4)
  - determine the partition $\mathbf{z}^{(m)}$: choose $z_n^{(m)} = k$ corresponding to the largest value $c_{nk}^{(m)}$
  - determine the parameter vector $\theta^{(m)}$ that maximizes $l(\mathbf{z}^{(m)}, \theta^{(m)})$
  - compute the new value of the probability $\alpha_k^{(m)}$ for each class k using relation (5).

4 MAINTENANCE DECISION RULE

The proposed maintenance decision rule aims at controlling the risk of failure while having the longest life cycle as possible. It is based on the remaining useful lifetime of the considered item or system. When a maintenance action is planned, the actual operation occurs after a minimum delay time τ which corresponds to a maintenance setup time. During the delay time, the system still operates and deteriorates. Hence a failure can occur between the decision time and the onset of the maintenance action. After maintenance operation, the component is replaced and the system is supposed to be as good as new.

Let S be the failure or tolerance threshold and let p_n be the path for the n-th monitored device. The last observed degradation level is $x_{n,|p_n|}$ at time $t_{n,|p_n|}$. The class label for the path is z_n and is associated to a set of Gamma process parameters $\theta_{z_n} = (a_{z_n}, b_{z_n}, u_{z_n})$. Assuming the last degradation level is smaller than the failure threshold, i.e. $x_{n,|p_n|} < S$, then the remaining useful lifetime from time $t_{n,|p_n|}$ is a random variable $RUL_{\theta_{z_n}}(S, t_{n,|p_n|}) = \inf\{t > t_{n,|p_n|} \text{ s.t. } X_t \geq S\}$ and $\sigma_{n,\theta_{z_n}}(S) = t_{n,|p_n|} + \mathrm{RUL}_{\theta_{z_n}}(S, t_{n,|p_n|})$ is the first passage time of the failure level S.

The survival function of the first passage time $\sigma_{n,\theta_{z_n}}(S)$ given the last observed degradation level can be obtained from the Gamma process with parameters θ_{z_n} by:

$$\begin{aligned} &\mathbb{P}(\sigma_{n,\theta_{z_n}}(S) > t \mid t_{n,|p_n|}, x_{n,|p_n|}) \\ &= \mathbb{P}(X(t) \leq S \mid t_{n,|p_n|}, x_{n,|p_n|}) \\ &= \mathbb{P}(\Delta X_{t_{n,|p_n|},t}) \leq S - x_{n,|p_n|} \mid X(t_{n,|p_n|}) = x_{n,|p_n|}) \\ &= \overline{F}_{a_{z_n}(t^{u_{z_n}} - (t_{n,|p_n|})^{u_{z_n}}), b_{z_n}}(S - x_{n,|p_n|}) \end{aligned} \quad (6)$$

It is assumed that the system can be inspected every ΔT unit of time, where ΔT is a uniformly distributed random variable such that $a \leq \Delta T \leq b$.

For a given accepted upper limit $\in$ of the probability of failure, the following three-steps decision rule is considered:

Step1: Data acquisition and classification—no decision about maintenance can be taken until a first classification is available;

Step 2: The results of classification are considered for maintenance decision making. At inspection time t and considering the delay time τ
- if $\mathbb{P}(\Delta X_{t,t+\tau+b}) \geq S - x \mid X(t) = x) \geq \in$ with the estimated parameters θ_{z_n} of the Gamma process then plan to replace the component by a new one at the inspection time between $t + \tau$ and $t + \tau + b$.
- else wait for the next inspection.

Step 3: If the system is failed, replace it correctively by a new one.

For each path n, two quantities are considered for the policy assessment: the life cycle duration (time until preventive replacement or failure) and the type of replacement (preventive or corrective). In the case of simulated data, it is possible to derive the empirical the mean life cycle duration by class $\hat{T}$ and the empirical probability of failure $\hat{P}_f$.

5 RESULTS

Simulations have been done considering two situations. For both of them, there are 3 classes, each class with 12 paths. The time increments are within an uniform distribution between 4.75 and 5.25. Parameters for both situations are given in Table 1. The failure threshold s has been chosen equal to 500. The value ϵ to threshold the predicted probability has been chosen equal to 0.5.

The mean theoretical evolution respectively for situation 1 and situation 2 is described in Figure 1a and Figure 2a. In situation 2, the classes are more similar than in situation 1: at each instant the mean values for 2 different classes are closer than in situation 1. However the standard deviations are the same for both situations.

Table 1. Parameters—situations 1 and 2.

	Class 1	Class 2	Class 3
Situation 1			
a	28.41	20.00	16.0
b	1.14	1.00	0.94
u	0.8	0.8	0.8
Situation 2			
a	28.41	25.31	22.22
b	1.14	1.12	1.11
u	0.8	0.8	0.8

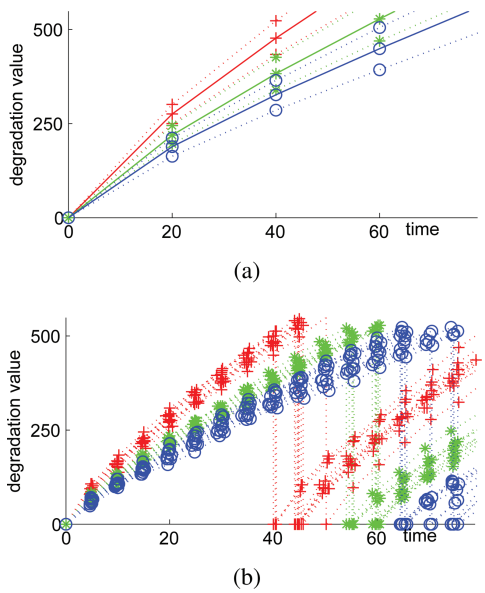


Figure 1. Evolution of degradation value in situation 1 (a) mean evolution using the theoretical parameters (b) example of simulated data.

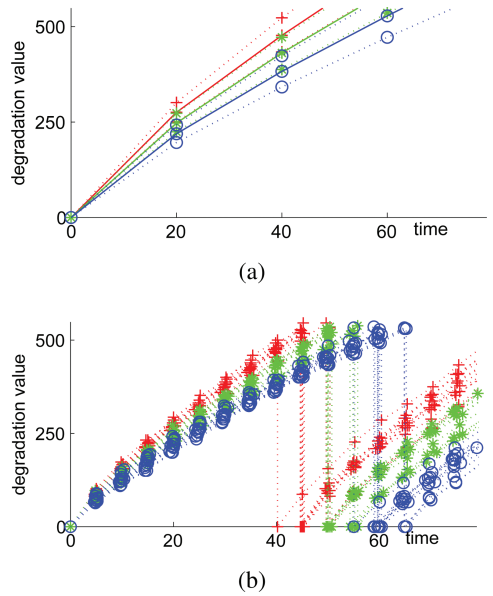


Figure 2. Evolution of degradation value in situation 2 (a) mean evolution using the theoretical parameters (b) example of simulated data.

Example of simulated data respectively corresponding to situation 1 and situation 2 are given in Figure 1b and Figure 2b.

Since we are in a case of simulated data, it is possible to compare the results obtained from the residual lifetime prognosis using the proposed approach with other classical approaches. The considered approaches are the following:

- theoretical clustering process: the real set of parameters Θ and the real class labels $\mathbf{z}$ are used;
- without clustering process (or 1-class): the estimated parameters using all the data are used;
- path case: a parameter set is estimated for each path using the available observations at the inspection time of the considered path;
- estimated 3-class clustering process: the available observations at the inspection time are used to determine jointly the class of each path ($\tilde{\mathbf{z}}$) and the parameter set of each class ($\tilde{\Theta}$).

The mean evolution of the Gamma process obtained with the estimated parameters in the three later cases is given is Figure 3, for situation 1, and an estimation done at time $t = 20$, meaning that approximatively 4 observations are available for each path. Similar illustrations are given on Figure 4, for situation 1, and an estimation done at time $t = 60$, and on Figures 5 and 6, for situation 2, and an estimation done at time $t = 20$ and $t = 60$ respectively.

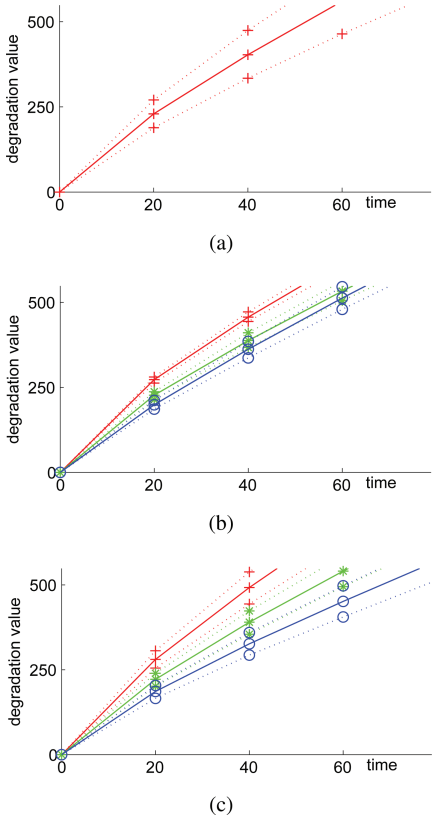


Figure 3. Evolution of the mean degradation value in situation 1 for (a) the estimated parameters with 1 class (b) the estimated parameters for each system (c) the estimated parameters with 3 classes. Each color corresponds to an estimated class. Estimation is done at $t = 20$.

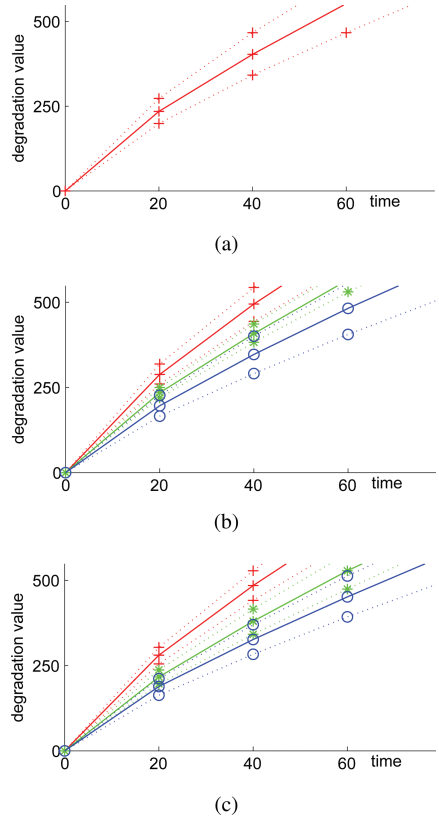


Figure 4. Evolution of the mean degradation value in situation 1 for (a) the estimated parameters with 1 class (b) the estimated parameters for each system (c) the estimated parameters with 3 classes. Each color corresponds to an estimated class. Estimation is done at $t = 60$.

As expected, the estimation is better when more observations are available. This is mainly the case when the estimation is done using only the observations of the considered path (path case). In the case of a clustering process, the estimation is better when more observations are available. This is particularly the case when the classes are more similar (situation 2 versus situation 1).

The estimated parameters have been used for the maintenance decision rule described in section 4. The delay time τ has been considered equal to 19 (approximatively equal to $4 * \Delta t$).

The simulation has been repeated for 500 path sets. The empirical probability of failure $\hat{P}_f$ and the empirical mean life cycle duration by class $\hat{T}$ are given in Table 2(a) and (b) for situation 1, with simulations done between $t = 0$ and $t = 100$. Similar results are given in Table 3 for situation 2 with simulations done between $t = 0$ and $t = 100$, and in Table 4 for situation 2 with simulations done between $t = 0$ and $t = 60$.

These tables show that grouping all the observations in a single set (1 class case) leads to very poor results. In both situations (1 and 2) one can observe that the ageing law estimated parameters correspond to an average behavior of all systems with a larger variance to fit the scatter of the different measurements. This leads to underestimate the degradation level when the degradation is rapid (class 1). As a consequence, less preventive maintenance operations are scheduled and more failures occur. On the contrary, the systems that experience slower ageing (class 3) gives low degradation measurements that lead to overestimate their residual life time, leading to more predictive maintenance and reducing the lifetime of the systems. For class 2, the model is more accurate and the results are acceptable.

Compared to the theoretical case, the strategy that consists to estimate the parameter for each path gives results that show an increase of corrective maintenance frequency (Tables 2a, 3a and 4a).

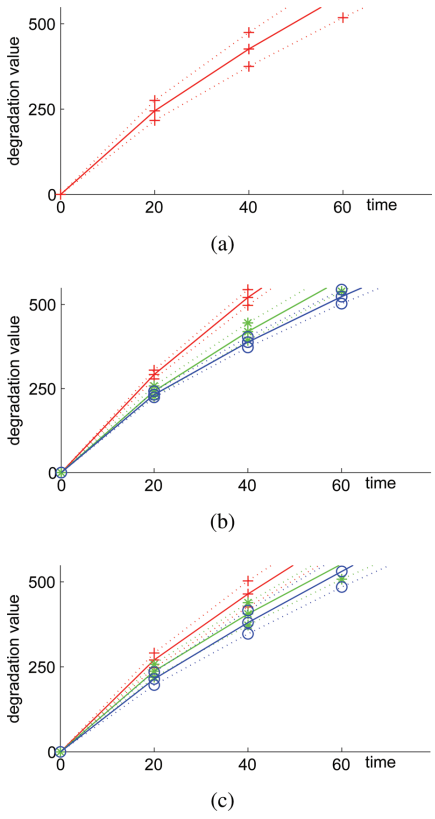


Figure 5. Evolution of the mean degradation value in situation 2 for (a) the estimated parameters with 1 class (b) the estimated parameters for each system (c) the estimated parameters with 3 classes. Each color corresponds to an estimated class. Estimation is done at $t = 20$.

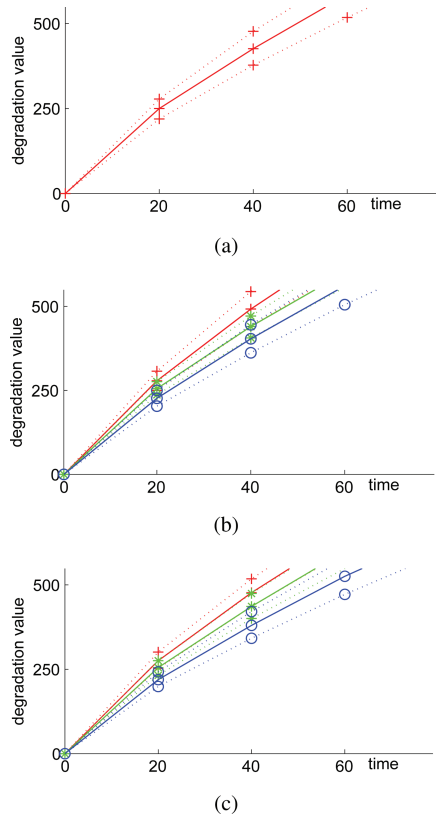


Figure 6. Evolution of the mean degradation value in situation 2 for (a) the estimated parameters with 1 class (b) the estimated parameters for each system (c) the estimated parameters with 3 classes. Each color corresponds to an estimated class. Estimation is done at $t = 60$.

This is due to the estimation which can not be good when the number of samples is too small. Thus, the estimated remaining useful life has a large variance. Consequently early conditional repairs occurs quite often and the mean lifetime is reduced (Tables 2b, 3b and 4b). Comparing results of Table 3a with Table 4a, it can be seen that the probability of corrective maintenance decreases when the study interval increases.

Considering the proposed approach, the results are much closer from the theoretical ones. The frequency of corrective maintenance is significantly reduced while maintaining a long mean life cycle duration.

In situation 2 these observations are a little less obvious which is normal because the deterioration processes of all systems are much similar, thus the one class strategy is not so bad even if it is by far not as pertinent as the proposed approach.

As expected, results obtained with the "estimated 3-class clustering process case" and the "path case" get closer to the theoretical results when the study interval increases. For the "estimated 3-class clustering process case" the results also improve when the classes are more different, since it is easier to class the process and then the parameters are

Table 2. (a) percentage of corrective maintenance actions and (b) mean life cycle duration, for situation 1 estimated on $t = [0,100]$.

Class	1	2	3
(a)			
Theor	11.6714	14.7849	18.0398
1 class	85.3571	7.6793	0.1905
1 path	19.0714	20.6911	25.3568
3-class	13.2143	18.5459	19.0138
(b)			
Theor	39.8248	53.1625	66.0175
1 class	42.1431	52.1480	60.5106
1 path	39.4928	52.4370	65.6941
3-class	39.5378	52.8110	65.5926

Table 3. (a) percentage of corrective maintenance actions and (b) mean life cycle duration for situation 2 estimated on $t = [0,100]$.

Class	1	2	3
(a)			
Theor	12.8674	12.6401	15.3450
1 class	52.7500	12.7940	0.5505
1 path	20.2094	19.0294	21.6030
3-class	18.6551	15.3006	15.8254
(b)			
Theor	39.8414	45.6487	53.2246
1 class	41.4780	45.6200	49.7411
1 path	39.4922	45.2358	52.5088
3-class	39.6503	45.2083	52.5085

Table 4. (a) percentage of corrective maintenance actions and (b) mean life cycle duration for situation 2 estimated on $t = [0,60]$.

Class	1	2	3
(a)			
Theor	12.8674	12.7704	15.9420
1 class	51.5972	13.0278	0.6253
1 path	24.1681	23.0727	23.4006
3-class	21.4365	18.0810	17.0701
(b)			
theor	39.8172	45.6530	53.2923
1 class	41.3753	45.5999	50.1807
1 path	39.3184	45.0541	52.5418
3-class	39.3772	45.0188	52.6360

better estimated if the path are correctly clustered. Then the clustering is a crucial step for estimating the Gamma process parameters that are used in any maintenance decision rule.

6 CONCLUSION

In this paper, a method is proposed for jointly clustering Gamma processes and estimating the Gamma process parameters, using degradation measurements on different systems. It is assumed that there are a number of operational conditions leading to different degradation processes. The aim is then to use the estimated parameters in a maintenance decision rule.

The proposed method consists in considering a mixture of Gamma process models. It allows to cluster the degradation paths in classes corresponding to the different degradation trends and to estimate the Gamma process parameters. It uses an expectation-minimization approach that takes into consideration that all measurements in a same path belong to the same class.

Estimating the Gamma process model parameters using only one system leads to poor results due to the limited number of samples. On the contrary, estimating the Gamma process model parameters considering only one Gamma process leads to poor results due tothe mixture of systems with different degradation trends.

Simulations have been done and demonstrate the feasibility of the method. They have shown that grouping paths originating from the same process allows to decrease the probability of failure while keeping a good mean life cycle duration in comparison with the two basic strategies (all paths in one class, one class per path).

The simulations have been done considering that the number of classes is known. A method for choosing the number of classes is currently being studied.

In a real case where the observations do not fit perfectly to Gamma process, a strategy consisting of increasing the number of classes with the number of observations could be considered. At the beginning it is not possible to distinguish different process so all the observations can be merged. On the contrary, when the time tends to infinity, it is feasible to consider one process per system.

REFERENCES

Ambroise, C. & G. Govaert (1998). Convergence of an EM-type algorithm for spatial clustering. *Pattern Recognition Letters 19*, 919–927.

Celeux, G. & G. Govaert (1992). A classification EM algorithm for clustering and two stochastic versions. *Computational statistics & Data analysis 14*(3), 315–332.

Celeux, G. & G. Govaert (1995). Gaussian parcimonious clustering models. *Pattern Recognition 28*, 781–793.

Cinlar, E., E. Osman, & Z.P. Bazant (1977). Stochastic process for extrapolating concrete creep. *Journal of the Engineering Mechanics Division 103*(6), 1069–1088.

Dempster, A.P., N.M. Laird, & D.B. Rubin (1977). Maximum likelihood from incomplete data via the em algorithm. *Journal of the Royal Statistical Society, Series B 39*(1), 1–38.

Hu, T. & S.Y. Sung (2006). A hybrid EM approach to spatial clustering. *Computational Statistics & Data Analysis 50*, 1188–1205.

Nystad, B.H., G. Gola, & J. Hulsund (2012, July 3–5). Lifetime models for remaining useful life estimation with randomly distributed failure thresholds. In *Proc. of First European Conference of the Prognostics and Health Management Society 2012*, Dresden, Germany, pp. 141–147.

Shental, N., A. Bar-Hillel, T. Hertz, & D. Weinshall (2003, August 21–24). Computing gaussian mixture models with EM using side-information. In *Proc. of the 20th International Conference on Machine Learning*, Washington DC, USA. Citeseer.

Si, X.-S., W. Wang, C.-H. Hu, & D.-H. Zhou (2011). Remaining useful life estimation—a review on the statistical data driven approaches. *European Journal of Operational Research 213*(1), 1–14.

Van Noortwijk, J. (2009). A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety 94*(1), 2–21.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Reliability of the delivery in the last 100 meters

K. Lewandowski
Wrocław Univeristy of Technology, Wrocław, Poland

ABSTRACT: The article presents the dependence of reliability of delivery in the last 100 meters, dependent on technical and organizational conditions when the car is stopped. The paper presents boundary conditions for the modeling deliveries in city logistics based on a study of real 900 sales points. This paper describes five specific cases deliveries in the last 100 meters, when the car is stopped.

1 INTRODUCTION

In common understanding the supply issues are analyzed primarily typical topics:

– arrangement of warehouses,
– routing directions for vehicles using various methods such as the task of a Salesman, ants algorithm, the method of the shortest paths in the network, the minimum spanning tree, zoning and other service areas.
– choice sequence transport to customers, using for example rule CRM, customer ratings, etc.

The presentation of the above issues concern the transport to the client, but rather in its close to.

The last phase of delivery-goods movement is recognized as a delivery time—Td.

From field research most of responders said that the maximal total time one operation of unloading and carrying gods to recipients is about 15 minutes (Lewandowski, K. et al, 2005) 56% less than 15 min. also in (Debauche W., 2007) 56% less than 15 min.

When we want to use this time to modeling of delivery process, we should check this from the point of view a efficiency a technical and organizational conditions of carrier equipment.

Meanwhile, the study made real conditions of delivery to the customer at the center of the city on the basis of 900 sales points indicates that it is wrong.

These studies reveal very different values to delivery time depending on several conditions governing. The article presents an analysis of five real cases to define the time of delivery tdo in modeling supply in city logistics.

2 PAPER REVIEW

In area of city logistics is very often use term delivery. The delivery process is a part of supply chain at the last link, from last warehouse to recipient. Here due to hard conditions for delivery vehicle, problems with stopping and obstacles with accessing time to city center, without possibility to stopping delivery vehicle in safety place for carrier and for other users of road traffic we can use term urban goods movement UGM (Debauche W. 2007), (Shimizu M. 2007) (Woudsma C. 2001). Urban goods movement UGM that is integrated modelling effort needed to address issues associated with congestion and air quality with respect to urban structure through land use transport interaction (Woudsma C. 2001).

Goods movement is the last phase of delivery process (Fig. 1).

The reliability of supply process mainly encompasses (Nowakowski, Werbińska 2007):

– delivery reliability—defined as the probability of in-full delivery being performed *without any delay with respect to the customer's specified time;*
– transport reliability—the probability of fault-free delivery being performed on time;

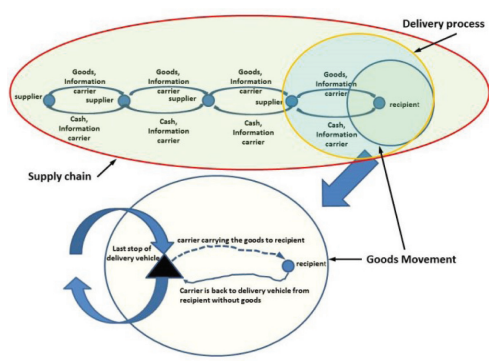


Figure 1. Place of goods movement in supply chain and delivery process (own work).

– reliability of logistic support infrastructure—which includes performance parameters of support personnel and support facilities (support and test equipment and support tools).

Reliability of the delivery process is regarded as the most important of the logistics processes with respect to potential losses (Nowakowski T. 2008).

There the service reliability for logistics networks is defined as (Nowakowski T. 2008):

$$Rd = P\,(Td < t0) \tag{1}$$

where:
Td—time of delivery,
*t*0—pre-specified time limit.

3 DEFINITION A PROBLEM

In this article is shown that delivery time Td is linked with technical and organizational conditions under unloading process and goods movement when the car is stopped. In this subject we analyze only influence of technical equipment of carrier to the pre-specified time limit *t*0. Is here proposition to calculation *t*0 where we don't add any influence of outside sources: road traffic, robbery, damage of cargo under unloading process and others.

4 BASE FOR RESULTS

Indicate the basis for determining the value of the delivery time tdo are the results of the supplies launched under the program DORED in the years 2004–2012 (Aniołowska A. et al, 2009), (Blaszyński M., 2011), (Gluz M., 2007), (Hałub A. et al., 2005), (Januszkiewicz R., 2007), (Jędra E., et al, 2007), (Kordas Ł., 2008), (Lewandowski, K. et al, 2005), (Lewandowski K., 2006), (Skoczylas I., 2007), (Stein S., 2011), (Wawrzyniak M., 2010), (Wędrak E., 2011), (Zachara R., 2006). During its course examined pond 900 sales points. The implementation of field studies conducted students of the Faculty of Mechanical Engineering Wrocław University of Technology in the framework of the thesis.

The results were based on studies in six cities: Wroclaw, Gdansk, Kępno, Opole and Jelenia Gora and Tourquay (UK) more than 900 points. The amounts of polls over time:

Gdańsk 2006-64,
Jelenia Gora, 2011-54,
Kępno 2010-50,
Opole 2006/2007-54,
Torquay (UK) 2007-70,
Wroclaw: 2004-135, 2004/2005-127, 2006/2007-229, 2008-16, 2008/2009-72, 2010-34

In addition, dozens of points has been studied based on the model developed by the author of the survey in Krakow. The results were publicly presented III Mobility Forum organized within the project Caravel/Civitas II. It was held in the Hall of the Portrait of the City of Kraków on 17 September 2007.

5 THE CONDITIONS THAT DETERMINE THE DELIVERY TIME TD

The main elements that determine the actual time of delivery is:

a. car type Rs:
   – Maximum payload/tare weight limit,
   – Whether it has a floor equal to over the entire width and length, this affects the whether it can use EUR pallet without demoulding, if you need the goods spread out on the vehicle,
b car equipment Ws
   – Is equipped with buildings inside the cargo space, if the shelf goods before delivery must be spread, if not, the goods can be loaded directly onto pallets as long as the floor is equal to over the entire width and length,
   – Is equipped with a self-unloading device, tail-lift or crane HDS,
c. the equipment driver unloading Wkpsr auxiliary equipment, platform trucks two or four wheels, etc.
d. the actual conditions of traveling to collect goods Fwrd:
   – Whether a dealer has its own place for the supply of goods,
   – If access to the site for delivery of goods is always ensured,
   – Whether the place of delivery for goods is not occupied by other vehicles,
   – Is a trading allows the use of pallets, ie whether its door openings are not too narrow for passing pallets 800 mm wide.
e. Equipment of recipient with the auxiliary unloading equipment, platform trucks two or four, etc. Wopsr
f. the size of the portion of delivery Wd.

Therefore can be saved the delivery time tdo depends on the aforementioned variables:

$$Td\{Rs, Ws, Wkpsr, Fwrd, Wopsr, Wd\} \tag{2}$$

Consider a hypothetical delivery of goods with a total mass of 250 kg.

6 CASES OF DELIVERY

6.1 *The primary method of delivery of the goods by the carrier when the vehicle is stopped is a hand delivery*

Ordered the load is usually in bulk packaging. Widely used in trade packs, boxes and bags for homogeneous goods in packages of individual (Fig. 2.):

- Sugar, flour and salt in a pack 1 kg, in packs of 10 kg;
- Drinks in baskets after 9.12 or 16 pieces, but with a mass of up to about 10–12 kg;
- Vegetables in bags and boxes weighing up to 10–15 kg, rarely are weight 25 kg, eg potatoes.

We assume that delivery truck gets a load in the form of packaging arranged in packets orders for each recipient. When the driveway to the next point need to add a delivery time of about 10 minutes to translate the load in the vehicle. This time can be added in the analysis of delivery to the next step. This situation occurs when to delivery is used cars that do not have a smooth floor of the load box over the entire width and length. The study 900 points were identified that 80% of deliveries were used cars without any self-unloading device. This way the load on the car without any hardware to self-unloading was observed in 55% of the surveyed points.



Figure 2. Delivery truck equipment with taillift with packages of cargo on pallets for each recipient. Own work.

In continuous operation which is cyclical and heavy reliance receiving cargo from a delivery truck to the store are applicable health and safety regulations 31. Rules of safety are given (Regulation 2000) (Act of Regulation 1997) on the general safety and health say:

a. for men:
   - 30 kg at continuous operation,
   - 50 kg casual work,
   - 30 kg to a height > 4 m,
   - 30 kg at a distance > 25 m.
b. for women:
   - 12 kg at continuous operation, 3 kg for pregnant women and breast-feeding,
   - 20 kg at a casual work (up to 4 times per hour during the work shift), 5 kg for pregnant women and breast-feeding.
c. In addition, it is unacceptable team moving objects at a distance greater than 25 m and a weight more than 500 kg and keep in mind that lifting and moving by one employee objects with a weight more than 50 kg is prohibited. (Regulation 2000) (Act of Regulation 1997).

As a result of more than 900 actual sales points established, in 49% of them delivery truck is staying up to 5 m. And 32% at a distance of 5 to 20 m, 19% of this distance is more than 20 m.

Therefore based on real tests can be assumed that the probability that the distance of the place of delivery to the receiving store is more than 5 meters, is:

$$\lambda l > 5 = \frac{\sum_1^n pol > 5}{\sum_1^n po} \tag{3}$$

which in the case the test results gives a value of:

$$\lambda l > 5 = 0{,}51 \tag{4}$$

Therefore it can be assumed that the distance of the point of delivery to the receiver is

$$l = 15\ m \tag{5}$$

Therefore it can be assumed that the duration of delivery time Td is:

$$Td = to1 + n * vpzl10\ kg * 1 + n * vp * 1 + n * to2 + tzd \tag{6}$$

where:
$to1$—the time of the carrier to the customer, checking invoices, an indication of the view loads in the store or in front of him, $to1 = 2$ min

n—number of complete cycles of cargo transfer from the car to the store, assuming that the mass delivery charge is 250 kg and the load is divided on the packaging of mass 10 kg, we get

$$n = \frac{md}{mlop} = \frac{250}{10} = 25 \tag{7}$$

$vpzl10\ kg$—the speed of the human walking distance with a load of 10 kg

$$vpzl10\ kg = 0{,}01\ min/m, \tag{8}$$

data obtained from observation
vp—a man walking distance speed without load

$$vp = 0{,}015\ min/m, \tag{9}$$

data obtained from observation
l—distance between the place of delivery to the point of receiving

$$l = 15\ m \tag{10}$$

$to2$—shutter load box car, retrieve the cargo, and the closure of the cargo box $to2 = 0.5$ min
tzd—time to close the door load box van after delivery of the last batch, checking documentation, the passage of the carrier to the cab driver, take a seat behind the steering wheel to check the next journey, setting driving directions, start the engine.

$$tzd = 3\ min \tag{11}$$

Therefore substituting into the formula we get that the duration of delivery time Td a mass 250 kg with only manual work is:

$$Td = 2 + 25 * 0{,}01 * 15 + 25 * 0{,}015 * 15 + 25 * 0{,}5 + 3 = 26{,}875\ min \tag{12}$$

If the weight of the load supply is higher, the time will be extended. Therefore the probability of keep delivery time is a reference a model delivery time, a priori, to the calculated on the basis of the real studies. Assuming that the probability of satisfactory delivery time deemed made as technical fitness amounts.

$$\lambda zadtd = \frac{t0}{Td} \tag{13}$$

Therefore (Fig. 3) keeping the delivery time Td recognized as delivered during the pre-specified time, the delivery time $t0$ with the probability recognition $\lambda zadtd \geq 0.75$ can be satisfied only for the supply of up to 200 kg, but not more than

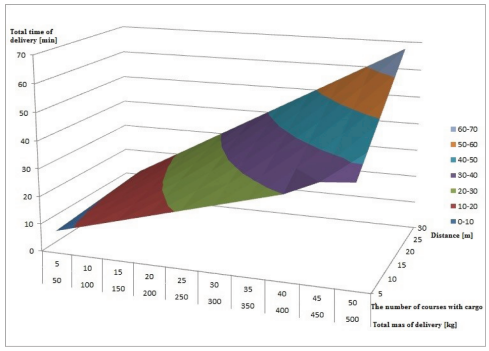


Figure 3. Graph calculation of keep delivery times as technical fitness, case 1. Own work.

10 meters from stopping place to delivery truck from the point of receipt of the delivery, store. Keep in mind that with the driveway to the next point receipt of the delivery may take longer time reloading. This is due to physical fatigue, so that the company's practice with a driver is with the loader. Such practices were observed only in 10% of 900 points.

The probability of recognition to provide delivery at the appointed time at the level of 0.75. In the opinion of owners of trade point the better situation is when who is now managers of logistics were first drivers supplying goods, and late occupied managerial position. Knowledge of reality situation at delivery is very important. According to their opinion, every day of the week are the other conditions of delivery, which also vary depending on the time of day. This is due to of traffic on the roads, and changes in pedestrian traffic on the sidewalks, which is supplied after delivery.

6.2 *We assume that delivery vehicle collected load in the form of packages on pallets of cargo*

Loading is done in such warehouse, and pallets are loads of packages in the form of homogeneous cargo that is on each pallet is the same type of goods, the carrier shall supply realizing completion delivery charge consecutively with each pallet individually (Fig. 4).

This manner the load on the car without is no equipment to self-unloading was observed in 23% of the surveyed points. This necessitates the adoption of that time $to2$—opening time load box on delivery vehicle, retrieve the cargo, and the closure of the cargo box is not $to2 = 0.5$ min, but is larger because is about $to2 = 1.5$ min, due to the additional time spent to choose the load to the contract and move the load box of the car.



Figure 4. View load box overloaded delivery vehicle with of homogeneous cargo (Main Road Transport Inspectorate, 2014).

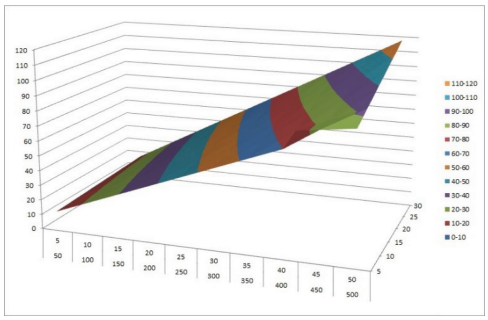


Figure 5. Graph calculation delivery times as technical fitness of, case 2. Own work.



Figure 6a. Carriers with hand truck on a street of Wroclaw. Own work.



Figure 6b. Carrier with hand truck in the street of London. Own work.

Thus (Fig. 5), keeping delivery times *Td* considered as delivered during the pre-specified time, the delivery time *t*0 with the probability of recognition $\lambda zadtd \geq 0.75$ can be satisfied only for the supply of up to 100 kg, but not more than 5 m from stopping place to delivery truck from the point of receipt of the delivery, store.

6.3 *We assume that delivery vehicle collected load in the form of packages on pallets of cargo*

Loading is done in such warehouse, and pallets are loads of packages in the form of homogeneous cargo that is on each pallet is the same type of goods, the carrier realizing supply uses a platform hand truck with a capacity of 150 kg (Figs. 6a and 6b).

This case of delivery was observed in 12% of the surveyed points. Assuming that one hand truck can put a load of 150 kg obtain that the number of cycles for delivery weight 250 kg is 2. This necessitates the adoption of that time *to*2—opening time load box car, retrieve the cargo, and the closure of the cargo box is not *to*2 = 0.5 min, but is larger because is about *to*2 = 4.5 min, due to the additional time spent to choose the load to the contract and move inside of load box of the delivery vehicle. There must also be additional time discharge of hand truck, then 2 * *to*2 = 9 min.

This results from the measurements at 5 points that indicated that the need for about 1.5 minutes load of 50 kg per 10 kg each pieces.

Assuming that one hand truck can put a load of 150 kg obtain that the number of cycles for delivery weight 250 kg is 2. This necessitates the adoption of that time *to*2—opening time load box car, retrieve the cargo, and the closure of the cargo box is not *to*2 = 0.5 min, but is larger because is about *to*2 = 4.5 min, due to the additional time spent to choose the load to the contract and move inside of load box of the delivery vehicle. There must also be additional time discharge of hand truck, then 2 * *to*2 = 9 min. This results from the measurements

at 5 points that indicated that the need for about 1.5 minutes load of 50 kg per 10 kg each pieces.

The formula for the delivery time take the form

$$Td = to1 + n * vjzl150\ kg * 1 + n * vjp * 1 + 2 * n * to2 + tzd \quad (14)$$

vjzl150kg—the speed of the man pushing a the truck with load 150 kg

$$vpzl10kg = 0{,}015\ min/m, \quad (15)$$

data obtained from observation

vjp—the speed of the person drawing an empty the truck

$$vp = 0{,}02\ min/m, \quad (16)$$

data obtained from observation

Thus (Fig. 7), keeping delivery times *Td* considered as delivered during the pre-specified time, the delivery time *t*0 with the probability recognition $\lambda zadtd \geq 0.75$ can be met for the supply of up to 150 kg, but not more than 10 meters from stopping place to delivery truck from the receipt of the delivery, store. Platform hand truck costs about 270 zł. Stability of such a truck is about 5 years. Thus, the monthly cost 4.5 zł per vehicle.

6.4 *We assume that delivery vehicle collected load in the form of packages on pallets of cargo*

Loading is done in such warehouse, and on pallets ie, each pallet is placed in packets for successive orders, the carrier realizing supply uses a mechanical device to self-unloading and hand forktruck for pallets, with or no self-propelled (Fig. 8 and 9). This necessitates the adoption of that time *to*2—opening time load box car, retrieve the cargo, and the closure of the cargo box is not *to*2 = 0.5 min, but is larger because is about *to*2 = 3.5 min.

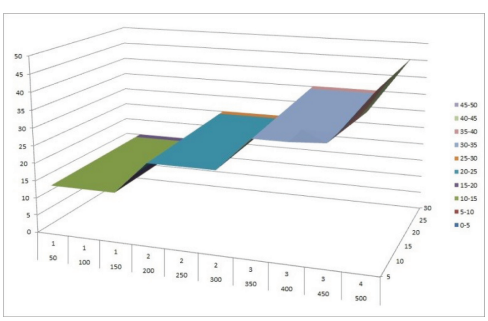


Figure 7. Graph calculation of delivery times as technical fitness of, case 3.



Figure 8. Light self-propelled hand pallet truck (Linde 2011).



Figure 9. Scene before store in Wrocław, Świdnicka street, when the carrier does not wait for unloading pallets. The recipient, store owner participate actively in the implementation of delivery. Own work.

In studies 900 points were identified that 10% of deliveries were used cars the equipment for self-unloading. In the middle of them has been found that the pallet is supplied to the interior of the store through the door and is involved in the unloading. If the carrier does not wait for unloading pallets, leaving realizing the delivery of the remaining points, and then doing reverse course collecting empty pallets.

Assuming that there is a pallet load of 550 kg obtain that number of pallets for delivery by weight 250 kg.

$$Td = to1 + n * vjzl250\ kg * l + n * vjp * l + n * to2 + tzd \quad (17)$$

vjzl250 kg—the speed of the man pushing a the truck with load 250 kg

$$vpzl10\ kg = 0{,}015\ min/m, \quad (18)$$

data obtained from observation

vjp—the speed of the person drawing an empty the truck

$$vjp = 0{,}025\ min/m, \tag{19}$$

data obtained from observation

Thus, keeping delivery times *Td* considered as delivered during the pre-specified time *t*0 the delivery time with the probability recognition $\lambda zadtd \geq 0.75$ can be fulfilled in order all shipments weighing up to 500 kg, but at a distance up to 30 meters from stopping place to delivery truck from the receipt of the delivery, store (Fig. 10).

With the use of equipment to self-unloading as lifting equipment is mandatory periodic inspection of the Office of Technical Inspection. Operation of this equipment without a valid certificate of technical test is punishable by a fine, an administrative and stopping the vehicle registration document. The vehicle is permanently associated with the device. Thus, if it is a taillift, it blocks the possibility of using a load box vehicle.

Price of hand pallet truck is about 1200 zł without self-propelled, and self-propelled about 7000 zł. Thus, the cost per month for 5 years is respectively 20 and 117 zł. The cost of using the side hopper is about 500 zł per month. In return, however, is to shorten the delivery time of delivery.

6.5 *We assume that delivery vehicle collected load in the form of packages on pallets of cargo*

Loading is done in such warehouse, and on pallets ie, each pallet is placed in packets for successive orders, the carrier realizing supply uses a mechanical device to self-unloading. Upon delivery to the stores it turns out that the pallet load will not enter the door stores, and the recipient, store owner, does not participate actively in the implementation of delivery, only controls. The carrier is obliged to charge transfer across the threshold of the store. It is related to the liability of the load (Fig. 11).

This necessitates the adoption of that time $to2 = 3.5$ min. Such cases were found in half of the 10% of the supply of 900 points, where they were used cars the equipment for self-unloading. Pallet is not supplied to the interior of the store through the door, because they are too narrow, store personnel not involved at unloading. In this situation, the carrier substitutes palette under the door of the store and brings the goods to the interior making it in the place indicated by the staff.

Then the formula for the delivery take the form

$$Td = to1 + n * vjzl250\ kg * l + n * vjp * l + n * to2 + tzd + troz\ palety \tag{20}$$

troz pallets—the pallet unloading time at the threshold of the store. Is the transfer distance of 5 m from the relationship can be used as for Case 1 (11).

Thus, keeping delivery times *Td* considered as delivered during the pre-specified time, the delivery time *t*0 with the probability recognition $\lambda zadtd \geq 0.75$ can be satisfied only for delivery to the 100 kg weight and distance of 5 meters from stopping place delivery truck from the receipt of the delivery store (Fig. 12).

If we want to calculate total delivery time, we should know what kind of vehicle we want to use. In centers of cities are use two main kinds of delivery vehicles. with maximal total mass to 3,5 ton:

– car equipment with buildings inside the cargo space, if the shelf goods before delivery must be spread, if not, the goods can be loaded directly onto pallets as long as the floor is equal to over the entire width and length,

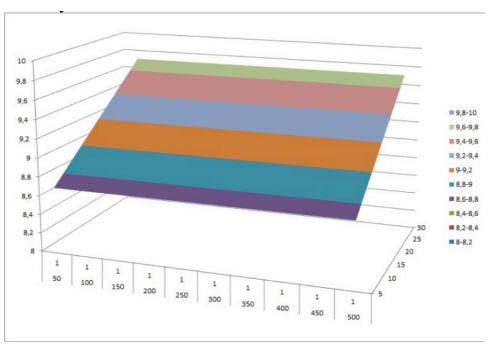


Figure 10. Graph calculation of delivery times as technical fitness of, case 4. Own work.



Figure 11. Pallet on the threshold of the storestore. Own work.

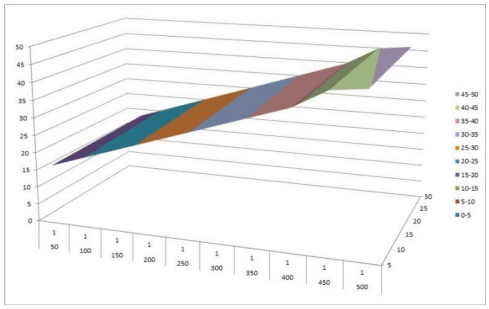


Figure 12. Graph calculation of delivery times as technical fitness, case 5. Own work.



Figure 13. Delivery vehicle equipment with buildings inside the cargo space (Femi 2014).

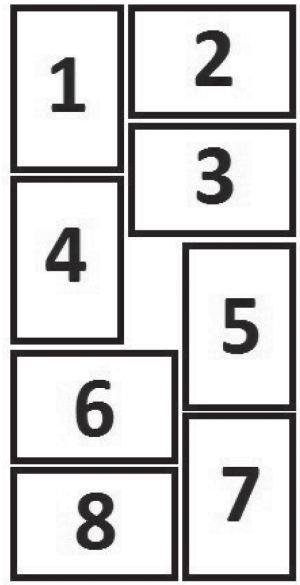


Figure 14. Location of pallets inside delivery vehicle unless than 3,5 tons (Equipment 2014).

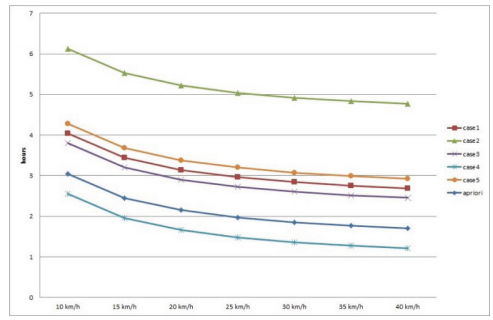


Figure 15. Time of delivery depends on cases of real situation of delivery and road speed. Own work.

– car with floor equal to over the entire width and length,
– isn't equipped with a self-unloading device,
– is equipped with a self-unloading device, taillift or crane HDS.

If we had a delivery car with a floor equal to over the entire width and length, they could carrying total 8 EUR pallets and taillift (Figs. 13 and 14).

We assume that delivery vehicle has do delivery for 5 points. This example is known from *Operations research*. Solution thus use insertion algorithms 1, 2, 3, 5, 4, 1 = 18 km.

We change parameters speed under road traffic, since 10 to 40 km/h, and ceases of delivery from case 1 to 5, all we compare to theoretical time of delivery $t0$ in trade point is 15 minutes.

$$\begin{Bmatrix} \infty & 2 & 4 & 7 & 3 \\ 2 & \infty & 4 & 5 & 7 \\ 8 & 4 & \infty & 7 & 3 \\ 5 & 9 & 2 & \infty & 7 \\ 4 & 8 & 1 & 4 & \infty \end{Bmatrix} \tag{21}$$

When will be change only case of delivery and speed of road traffic we can see that reliability of the delivery in the last 100 meters depends from

Table 1. Unloading times Td in each cases [min].

	Case 1	Case 2	Case 3	Case 4	Case 5
Best	8,125	13,125	14,175	8,7	16,825
Worst	67,5	117,5	45,2	9,7	45,95

a conditions of delivery vehicle and speed under road traffic (Fig. 15).

7 DISCUSSION

To calculate $t0$—pre-specified time we can use results of the shortest and longest time of unloading Td (Table 1).

To calculate a $t0$ time I suggest as the sum total of the products of the frequency of the cases examined (expressed in %) and half sum of the total time for the best and worst examined cases.

Thus this we have $t0$—pre-specified time limit.

$$t0 = 41{,}41 \text{ min} \approx 40 \text{ min}. \quad (22)$$

This values of pre-specified time limit is permitted for a maximum of 40 minutes if loading is observed in London city (London Councils 2014).

8 SUMMARY

Reliability of delivery in the last 100 meters depends on real type of delivery vehicle and from cases of real situation of delivery. The easiest and cheapest solution to keep pre-specified delivery time *t0* within 15 minutes and designated horizontal recognition of 0.75 is the purchase of a platform hand truck for 270 zł. The second opportunity to shorten the time of to provide supplies is to buy a pallet. It is more expensive, but significantly reduces the time to provide the goods. Therefore, to promote at use of auxiliary unloading devices in the course of delivery of supplies. Note, however, that the possibility of the use of pallets in the delivery of the goods may depend on the geometric store the recipient, if there's a narrow door opening. Better to provide planning delivery at the appointed time is that logistics managers are who were first drivers supplying goods, and later occupied managerial positions.

Research the real conditions the supply relationship should be considered as a basis for modeling and simulation. Because the one who wants to write a mathematical model should ask yourself whether creating a simulation model, which is a multi-program computer, creating a functional computer with a compatible sort of simulator, allowing the generation of system states modeled (Korzeń Z., 1998)—thus not associated with the reality but with the virtual city, eg. SIMCITY or model imitating the real operation processes/systems occurring in real-time (Hailala J., 1999), for example in Poznań. If you create mathematical notation only without testing reality it arises only theoretical simulation, which has no relation to reality, and therefore no practical application.

Article submitted data for calculation of $t0$—pre-specified time of supply in the real world.

REFERENCES

Act of Regulation 1997 of the Minister of Labour and Social Policy of 26 September 1997 on the general safety and health (1997) (pol.) Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy, *Dz. U. 1997 nr 129 poz. 844.*

Aniołowska A., Politowska M. (2009): The project organizational and technical delivery to the customer in the downtown area of the city: Study of organizational and technical supply customers in the downtown area of the city center logistics by the warehouse and distribution center. Analysis of organizational and technical units of cargo deliveries in the downtown area of the city of Wroclaw. Thesis. Wrocław University of Technology.

Blaszyński M. (2011): Analysis of organizational and technical units use in cargo deliveries in the downtown area of the city Jelenia Gora, Engineering Jobs. Wrocław University of Technology.

Debauche W. (2007). An investigation into the delivery of goods to the city centre of Liege, The 5th International Conference on City Logistics (11th—13th July 2007, Knossos Royal Village Hotel, Crete Island, Greece).

Equipment of vehicle to international transport—the essential question: 8 or 10 pallets, or maybe 9? (2014) (pol), Wyposażenie międzynarodówki—pytanie zasadnicze: 8 czy 10 palet, a może 9?, http://net4car.pl/wyposazenie-miedzynarodowki-pytanie-zasadnicze-8-czy-10-palet-a-moze-9.

FEMI Zakład Metalowy (2014): Installation inside cabin of delivery vehicles and trucks, (pol) Zabudowy samochodów dostawczych i ciężarowych, http://wyrobyzestali.com.plzakres_uslug/zabudowy_samocdow_dostawczych_i_cierarowych_o1.

Gluz M. (2007): The project organizational and technical delivery to clients in the downtown area of the city of Opole with the introduction of the use of the logistic management of urban transport infrastructure. Thesis, Wrocław University of Technology.

Hałub A., Kozłowska-Kempa J., Szawan E. (2005): Analysis of organizational and technical deliveries in the city center of Wroclaw, Thesis. Wrocław University of Technology, Award in the Transport Minister Jerzy Polaczek 16.12.2005r. For the best dissertation.

Heilala J. (1999), Use of simulation in manufacturing and logistics systems planning, *VTT Manufacturing Technology,* 1999.

Januszkiewicz R. (2007): Study of organizational and technical supply customers in the downtown area of the city center logistics warehouse and distribution center in Wrocław. Thesis. Wrocław University of Technology. Unanimously elected prize winner Logistics Forum Winncanton 27.03.2008r.

Jędra E., Mak M. (2007): The organizational and technical analysis of urban cargo transport units, Thesis, Wrocław University of Technology.

Kordas Ł. (2008): The problem of urban deliveries on the example of the market square in Wroclaw. Thesis, Wrocław University of Technology.

Korzeń Z (1998)., Logistic handling and warehousing systems, ILiM, Poznań 1998.

Kowalewski J. (2007): The project organizational—technical delivery to the customer in the downtown area of the city of Wroclaw, at the introduction of the use of the logistic management of urban transport infrastructure for example Ruska street. Thesis, Wrocław University of Technology.

Lewandowski, K.; Diug, I.; Lisek, A.; Okrent, K.; Soszycki, J.; Szawan, E.; Szepelak, T.; Ucinek, P.; Wakulski, P.; Zachara, R (2005): The pilot study of the program DORED, *Logistyka 2/2005r*.

Lewandowski K (2006). The project of road sign a unloading place for delivery vehicles*, Logistyka 2/2006r*.

Linde Material Handling (2011): Eurostar selects new Linde CiTi-Truck as rail side delivery solution for palletised goods, 25-Oct-2011,http://www.linde-mh.co.uk/en/country_site_uk/news_infoservices/news_info_services_details_1281.html.

London Councils, 2014: Loading and unloading, http://www.londoncouncils.gov.uk/policylobbying/transport/parkinginlondon/loadingandunloading.htm.

Main Road Transport Inspectorate (2014): Overloaded delivery vehicles, (pol). Główny Inspektorat Transportu Drogowego: Przeładowane „dostawczaki", 13/01/14, http://www.gitd.gov.pl/content/przeladowane-dostawczaki.

Nowakowski T., Werbińska S. (2007). *Problems of logistic system availability assessment. Wybrane Zagadnienia Logistyki Stosowanej, No. 4*, Oficyna Wydaw. TEXT, Kraków.

Nowakowski T. (2008): Problems of supply process reliability assessment at small and medium-sized enterprises, *Total Logistic Management No. 1 • 2008* • PP. 125–136.

Regulation 2000 of the Minister of Labour and Social Policy of 14 March 2000 on health and safety manual handling. OJ 2000 No. 26, item. 313 Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 14 marca 2000 r. w sprawie bezpieczeństwa i higieny pracy przy ręcznych pracach transportowych. *Dz. U. 2000 nr 26 poz. 313.*

Shimizu M., Hyodo T., Takebayashi H., Kuse H., Hagino Y. (2007): Study of delivery distribution in the central area by Tokyo metropolitan freight survey, The 5th International Conference on City Logistics (11th–13th July 2007, Knossos Royal Village Hotel, Crete Island, Greece).

Skoczylas I. (2007): Analysis of the supply system of the Market Hall in Wroclaw. Thesis, Wrocław University of Technology.

Stein S. (2011): The project organizational and technical deliveries to the customer in the downtown area of the city. Analysis of organizational-technical loading units use in the downtown area of the city Kępno. Thesis, Wrocław University of Technology.

Wawrzyniak M. (2010): The project organizational and technical deliveries to the customer in the downtown area of the city: Study of organizational and technical supply of customers in the downtown area of the city center logistics warehouse and distribution center. Thesis, Wrocław University of Technology.

Wędrak E. (2011): The project organizational and technical deliveries to the customer in the downtown area of the city of Wroclaw. Analysis of organizational-technical loading units use in the downtown area of the city of Wroclaw. Thesis, Wrocław University of Technology.

Woudsma C. (2001): Understanding the Movement of Goods, Not People: Issues, Evidence and Potential *Urban Studies, Vol. 38, No. 13,* 2439–2455, 2001.

Zachara R. (2006): Study of the organization of transport in the Gdańsk agglomeration, Thesis, Wrocław University of Technology.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Risk analytics within high-precision dental tool manufacturing: Multidimensional failure probabilities and validation

S. Bracke & M. Pospiech
Chair of Safety Engineering and Risk Management, University of Wuppertal, Wuppertal, Germany

ABSTRACT: Manufacturing processes of technically complex products require highly standardised methods to fulfil technical/customer specifications and minimise risks. One method for estimation of manufacturing risks is the univariate Process Capability Index (PCI). The determination of state-of-the-art PCI allows visualisation of risk with one indicator and failure probability regarding one product characteristic. Therefore the focus of the research work is the development of an approach to determine a multidimensional PCI (MPCI) as an analogon to the common, univariate PCI. The goal is the analysis of risks, the determination of risk indicator MPCI and failure probabilities with regard to complex manufacturing processes based on multivariate product characteristics. This paper presents a method for the determination of a multidimensional process capability index with the help of a case study 'dental drill'. The method considers the risk analysis of a set of functional important characteristics, the determination of a capability indicator as well as a failure probability.

ABBREVIATIONS

C1–4: Characteristic 1–4
C_p/C_{pk}: Process capability/(critical)
MPCI: Multidimensional process capability index
PPM: Parts per million
QCC: Quality control chart
SPC: Statistical Process Control
PCI: Process capability index
USL: Upper specification limit
LSL: Lower specification limit

1 INTRODUCTION

Manufacturing processes of technically complex products require highly standardised methods to fulfil technical and customer specifications. To accomplish the demanded specifications, various methods, which can be applied at different phases of the product life cycle, have been developed. One of these methods, within the manufacturing phase, is the Process Capability Index (PCI). The determination of the PCI allows the visualisation of risk with one indicator and failure probability with regard to a manufacturing process. State of the art is the univariate calculation of the PCI based on the analysis of one product characteristic. However risks of complex manufacturing processes generally depending on more than one product characteristic. The analysis of manufacturing processes and the attendant process optimisation actions leads to a reduced amount of production failures and therefore to a reduced manufacturing risk and reliable products.

With decreasing tolerances of demanded component characteristics, the medical technology is one of the major branches of industry, where industrial state-of-the-art methods mustn't be thus sufficient anymore. Furthermore, a basic requirement, especially regarding medical-technical products is the minimisation of product risks and therefore the optimisation of manufacturing processes. The multidimensional PCI is one possibility to verify manufacturing processes of medical-technical products. Previous researches exhibited the successful benefit of such multidimensional process capability indices (Goethals & Cho 2011, Tano & Vännman 2011). Nevertheless a general procedure for industrial manufacturers hasn't been developed yet.

This paper presents a method for the determination of a multidimensional process capability index with the help of a case study 'dental drill'. The method considers the risk analysis of a set of functional important characteristics and the determination of a capability indicator as well as a failure probability. The presented case study uses a synthetic data set with simulated data and tolerance regions. The characteristics of the synthetic data set are close to observed reality effects.

2 FOCUS AND GOAL OF THE RESEARCH WORK

The focus of the research work is the development of an approach to determine a Multidimensional PCI (MPCI) as an analogon to the common, univariate PCI. Precondition for the determination of

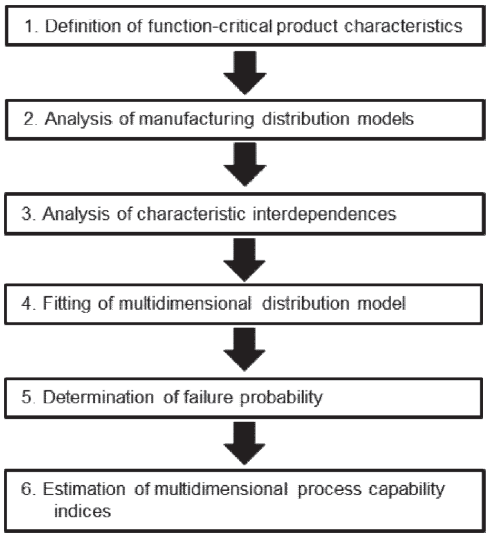


Figure 1. Overview of the approach for determination of Multivariate Process Capability Indices (MPCI).

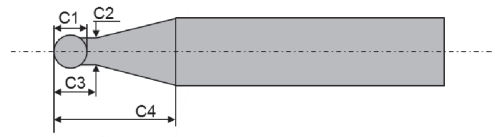


Figure 2. Important characteristics of a dental drill: head-diameter (C1), neck-diameter (C2), head-length (C3) and head-neck-length (C4).

Table 1. Comparison of the drill characteristics C1–C4 with their individual tolerance areas, nominal value and the estimated process parameters (statistical) $\hat{\mu}$ (mean) and $\hat{\sigma}$ (scattering) regarding the manufacturing process.

	Tolerances	Nominal value	$\hat{\mu}$	$\hat{\sigma}$
C1	0.8–0.85	0.80	0.840	0.01224
C2	0.53–0.73	0.63	0.646	0.00605
C3	1.65–1.95	1.75	1.821	0.01259
C4	7.5–8.5	8.00	7.934	0.10187

PCI or MPCI are capable measurement systems and machine tools (Pospiech et al. 2013).

The goal is the analysis of risks, determination of MPCI and failure probabilities of manufacturing processes based on multivariate product characteristics. Subsequently, it is possible to ensure optimised manufacturing processes. This paper focuses on one method for the calculation of multidimensional process capability index with an analogy to the state-of-the-art PCI. An overview of the developed method regarding the estimation of Multivariate Process Capability Indices (MPCI) is shown in Figure 1. The method steps are theoretically explained and applied within the case study in the following sections.

3 CASE STUDY DENTAL DRILL: FUNCTION-CRITICAL CHARACTERISTICS

It is very important to fulfil the customer's specifications within high precision manufacturing. The challenge is the fulfilment of the narrow characteristic tolerances. In the presented case study dental drill (Fig. 2), there are four important product characteristics defined (also step 1, Fig. 1): head-diameter (C1), neck-diameter (C2), head-length (C3) and head-neck-length (C4). If these drill characteristics are manufactured outside the required tolerance area, it has serious consequences on the dental drill application area: the dentist uses the drill unconsciously wrong and the patient-centered care—e.g. tooth therapy—is inefficient. The schematic drawing in Figure 2 outlines the four function-critical drill characteristics. It is assumed, that all four characteristics are normal distributed regarding the manufacturing process.

The shown characteristics are based on a real dental drill: For this paper the data set has to be synthesized. The tolerance areas of the drill characteristics as well as their expected normal distributions (step 2, Fig. 1) parameters regarding the manufacturing process are shown in Table 1. The assumption of the expected normal distribution model was verified and confirmed by a Kolmogorov-Smirnov conformance test (Sachs 2002).

4 STATE OF THE ART: PROCESS CAPABILITY INDEX (PCI)

The continuously analysis and control of the manufacturing process is the precondition for the obtaining of excellent products. The two established methods are quality control charts and the relayed process capability indices. Quality Control Charts (QCC) can be used without an exact knowledge of the characteristic distribution model and are useful in the analysis of manufacturing risks. QCCs show the mean and scattering of each product characteristic in relation to the given tolerance areas. Furthermore, alert and intervention limits can be adapted inside QCC, if needed. This method is an industrial standard, further explanations can be found in (Timischl 2002). It is possible

to gain additional information with the Process Capability Indices (PCI) by obtaining a determined distribution. This is also an industrial standard for univariate product characteristic analysis, but mainly used for normally distributed processes (Pfeifer 2002). Current technical literature gives also basic approaches for other fitted distribution models (Dietrich & Schulze 2009).

In general, process capability is divided into two perspectives: process capability and critical process capability: C_p represents the ratio between the given tolerance area and the manufacturing deviations whereas C_{pk} considers the position of the manufacturing's arithmetic mean inside the ratio. This method is mainly established for normal distributed processes. Equation 1 shows the determination of the process capability C_p hereas equation 2 describes the critical process capability C_{pk}.

$$\widehat{C_p} = \frac{USL - LSL}{6\hat{\sigma}} \tag{1}$$

$$\widehat{C_{pk}} = \min\left[\frac{USL - \hat{\mu}}{3\hat{\sigma}}; \frac{\hat{\mu} - LSL}{3\hat{\sigma}}\right] \tag{2}$$

As all characteristics are normally distributed, the process capability indices are determinable by using equation 3, which shows the density function of the normal distribution.

$$f(x,\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{3}$$

The abbreviations inside the shown equations are as follows:

USL = upper specification limit
LSL = lower specification limit
μ, $\hat{\mu}$ = mean (estimated)
σ, $\hat{\sigma}$ = standard deviation (estimated)

If the process capability index of one product characteristic is below a defined critical value—e.g. state-of-the-art value 1.33—a review of the production process should be done to improve the manufacturing steps and achieve higher capability indices. Depending on the industrial discipline there are also higher capability requirements such as $\widehat{Cp} > 2.0$ and $\widehat{C_{pk}} > 1.67$. An example for a normally distributed characteristic (drill characteristic C1 in Table 1) is shown in Figure 3.

The visualisation in Figure 3 shows, that the distribution model of C1 is not completely inside the tolerance area, therefore the related manufacturing process step has to be improved.

In case of risk analyses of technically complex manufacturing processes, possible interdependences

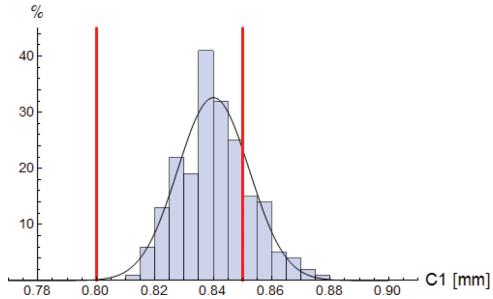


Figure 3. Classified data of C1 fitted with a normal distribution density function within the given tolerance area. The PCI C_p is the ratio between scattering and tolerance area, The PCI C_{pk} considers the mean of the density functions.

of different product characteristics have to be considered. Therefore, the correlation and regression analysis (step 3, Fig. 1) is the subsequent step and the base of operations for the multivariate PCI.

5 CORRELATIONS OF THE CHARACTERISTICS

State-of-the-art calculations for correlations analysis are based on Bravais-Pearson (precondition: bivariate normal distributed characteristics), Spearman and Kendall (rank based analysis; independent of characteristic distribution models), explanation in (Sachs 2002). The results of the application of these correlation analyses show the interdependences of the product characteristics (step 3, Fig. 1). For this case study Spearman correlation, shown in equation 4, was used.

$$r_s = \frac{\sum_{i=1}^{n}\left((R(x_i) - \overline{R(x)})(R(y_i) - \overline{R(y)})\right)}{\sqrt{\sum_{i=1}^{n}(R(x_i) - \overline{R(x)})^2 \sum_{i=1}^{n}(R(y_i) - \overline{R(y)})^2}} \tag{4}$$

Abbreviations:
$R(x_i)$ = rank of x_i
$\overline{R(x)}$ = mean rank of x
$R(y_i)$ = rank of y_i
$\overline{R(y)}$ = mean rank of y

The result of this formula can be between ± 1, where 1 means full positive correlation and −1 means full negative correlation. Values near 0 indicate that the data does not correlate. If there are correlations between the product characteristics, it has an impact regarding the analysed multidimensional tolerance area and therefore for the estimated failure probability (Fig. 3). Furthermore, it has an impact on the manufacturing process

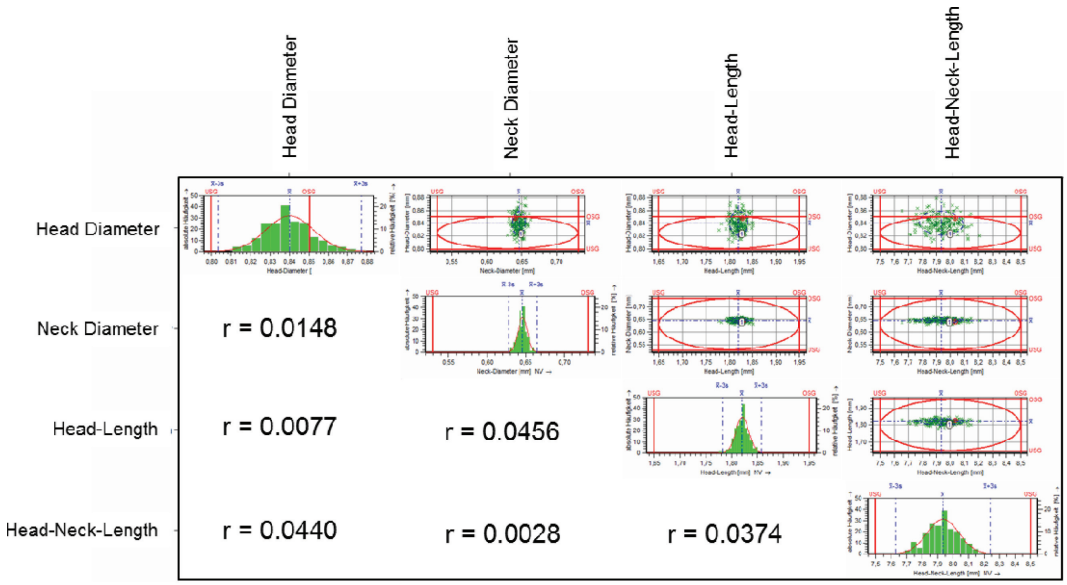


Figure 4. Comparision of the important dental drill characteristics and their correlation influences on each other determined with Spearman's rank correlation coefficient (schematic visualisation).

control. The results of the correlations analysis within the case study dental drill are shown within a correlation matrix in Figure 4. Rows and columns show the important characteristics of the dental drill (also Fig. 2); the crossing shows the fitted distribution models—based on measurement samples—of the proper manufacturing process steps. The graphics top right show the visualised correlations; the equations down left show the estimated correlation coefficients.

Obviously, the values of the estimated Spearman correlation coefficients equal nearly 0. That means that there are no detectable interdependences between the important dental drill characteristics. This leads also to non-depending tolerances zones. This is one precondition for the presented method of MPCI regarding the analysed multidimensional tolerance area.

6 MULTIDIMENSIONAL PROCESS ANALYSIS: DISTRIBUTION AND FAILURE PROBABILITY

As a matter of principle, there are two possible approaches to estimate a MPCI based on multidimensional analysis regarding to product characteristics:

a. Base of operations for the estimation of a MPCI is the fit of a multidimensional distribution model (Fig. 1, step 4), which is explained with the help of the case study in section 6.1. Afterwards, the ratio of the fitted distribution model and the multidimensional tolerance area leads to the failure probability (Fig. 1, step 5) and subsequently to the estimation of the MPCI (analogon C_{pk}; (section 6.2)). This approach is feasible regarding dependent or independent characteristics.
b. Base of operations is the individual estimation of the failure probabilities for each characteristic. Afterwards the composition of the failure probabilities in due consideration of Boolean algebra leads to a comprehensive product failure probability. Precondition is the independency of the analysed characteristics.

This paper focuses on the estimation of the MPCI using the first outlined approach by using multidimensional distribution models.

6.1 *Application of multidimensional distribution models within the case study*

The proper multidimensional distribution model depends on the distribution of the several analysed product characteristics (step 4, Fig. 1). Within the case study dental drill, the analysed important characteristics are normally distributed. If two (or more) characteristics are normally distributed their combination should be also normally distributed. Therefore, the multidimensional approach regarding normally distributed characteristics

can be used, equation 5 (Genz & Bretz 2009). The parameters of the distribution were estimated with the Maximum-Likelihood function (Sachs 2002).

$$f_x(x_1, \ldots, x_k) = \frac{1}{\sqrt{(2\pi)^k \mid \Sigma \mid}} \exp\left(-\frac{1}{2}(x-\mu)^T \Sigma^{-1} * (x-\mu) \right) \quad (5)$$

Abbreviations:
μ = mean vector
$\sum$ = covariance matrix

In comparison with equation 3, μ is a vector and σ a matrix ($\sum$ in (3)). The multinormal-distribution of two characteristics leads to a bivariate vector μ and a bivariate matrix $\sum$. It is possible to visualise this distribution together with the tolerance areas of each characteristic. The non-correlation is a basic condition regarding this approach: There is no impact based on characteristic interdependences. Within the analysed drill characteristics of the case study, there are no characteristic correlations (section 5). This leads to a tolerance zone in form of a rectangle. Otherwise the tolerance zone could be ellipse shaped, which would lead to a different integration form. An example of two dental drill characteristics C3 and C4 (Fig. 2), which are multinormal-distributed, within the resulting tolerance zone is shown in Figure 5.

The graphical interpretation of this example should indicate, that any calculation of separate C_p or C_{pk} should lead to a positive result. Furthermore, the combination of a two-dimensional normally-distributed approach allows the conclusion, that its peak is near to the centre of the tolerance area conducted by a small scattering. Another example is shown in Figure 6.

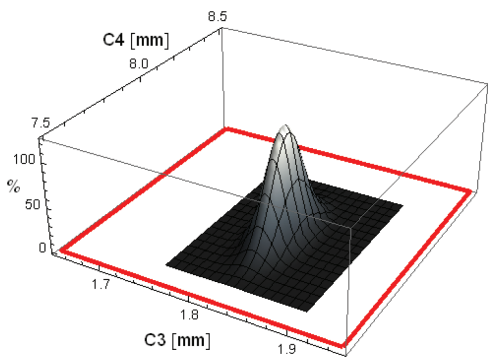


Figure 5. Combination of drill characteristics C3 and C4 (Fig. 2), visualised with the help of a two-dimensional normal distribution density function within the given tolerance area.

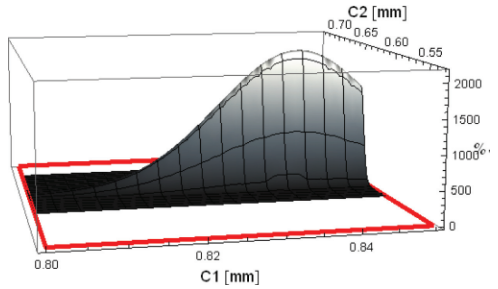


Figure 6. Combination of dental drill characteristics C1 and C2 (Fig. 2), shown with the help of a two-dimensional normal distribution density function within the given tolerance area.

The graphical interpretation shows that the multinormal-distribution of the characteristics C1 and C2 is not completely inside the tolerance area: C1 is located within the tolerance zone, contrary to C2. The application of this approach is also possible for more than two product characteristics: Within the case study, the dental drill has four important product characteristics (Fig. 2). The combination of C1–C4 leads two a four-dimensional normally distributed approach (based on eq. (5)), which obviously cannot be visualised.

6.2 *Failure probability based on multidimensional approaches*

Based on the fitted multidimensional density function, the calculation of the failure probability regarding the given tolerance areas is feasible (step 5, Fig. 1). The integration of the multidimensional density functions by using the tolerance areas as integral limits (equation 6) leads to the probability of manufactured products within the combined tolerance zone. The complement (equation 7) leads to the failure probability.

$$P_{IT} = \int_{x_1 LSL}^{x_1 USL} \int_{x_2 LSL}^{x_2 USL} \int_{x_3 LSL}^{x_3 USL} \int_{x_4 LSL}^{x_4 USL} f_x(x_1, x_2, x_3, x_4) = \int_{0.8}^{0.85} \int_{0.53}^{0.73} \int_{1.65}^{1.95} \int_{7.5}^{8.5} \frac{1}{\sqrt{(2\pi)^4 \mid \Sigma \mid}} \times \exp\left(-\frac{1}{2}(x-)^T \Sigma^{-1} * (x-\mu) \right) dx_1 dx_2 dx_3 dx_4 \quad (6)$$

$$P_F = 1 - P_{IT} \quad (7)$$

Abbreviations:
P_F = Probability failure
P_{IT} = Probability inside tolerance

Therefore, this approach is independent of the amount of combined variables and therefore

Table 2. Comparison of different combinations of the functional-important characteristics C1–C4 (multinormal-distributed).

	Integral of the tolerance zones	ppm
C1/C2	0.791243	208757
C3/C4	0.999999	1
C1/C2/C3/C4	0.791236	208764

independent of the graphical visualisation (Figs. 5 and 6). With regard to the shown case study, several integrals are presented in Table 2. The first two rows show the two-dimensional analysis of drill characteristic combinations C1/C2 and C3/C4. The third row shows the combination of all important drill characteristics C1–C4 with the goal of a comprehensive estimated Product Failure Probability. The probability is expressed in unit Parts Per Million (PPM), which is the base of operations regarding the estimation of the multidimensional process capability index MPCI (section 7).

7 LINK BETWEEN PPM AND C_{pk}

The next step for MPCI is the link between PPM and the common state-of-the-art one-dimensional capability index C_{pk} (section 4; also step 6, Fig. 1). Based on the ratio of process scattering and tolerance area (eq (1) and (2)), the determination of the failure probability is feasible (integration of (3) by using tolerance area as limits). Therefore, each one-dimensional C_{pk} value belongs to a failure probability PPM-value. The relationship between one-dimensional C_{pk} value and PPM value is shown in Figure 7.

In addition to the graphical visualisation, a non-linear regression has been calculated using the Equation 8.

$$y = \beta_0 \, exp \, (\beta_1 \exp(x)) \tag{8}$$

with $\beta_0 = 4.61153 * 10^7$ and $\beta_1 = -3.54913$.

The expression allows the direct conversion of an estimated failure probability into a C_{pk} value. Based on this conversion (direct link), the estimation of a multivariate process capability index MPCI is feasible: The estimation of the expected failure probability with regard to the combination of two or more important product characteristics is shown in section 6.2, Table 2.

The failure probability (unit [ppm]) of the multidimensional analysis leads now directly to the MPCI, as an analogon to the direct conversion of ppm into C_{pk} (Fig. 7 and eq. (6)): The results are

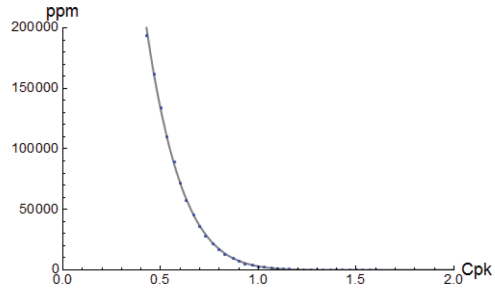


Figure 7. Non-linear regression of the relationship between failure probability ppm and C_{pk}.

Table 3. Expected failure probability (ppm) based on multidimensional process analysis and conversion into MPCI as an analogon to one-dimensional C_{pk} (Fig. 7) within the case study dental drill.

	ppm	MC_{pk}
C1/C2	208757	0,42
C3/C4	1	1,6
C1/C2/C3/C4	208764	0,42

shown in Table 3. E.g. the expected failure probability regarding the analysis of the four important dental drill characteristics C1–C4 (208764 ppm; Table 2) leads to a MPCI value of 0.42.

8 CONCLUSION

This paper outlines a method for multidimensional process analyses and the estimation of multidimensional process capability indices inside the manufacturing phase. The presented results were established within a case study 'dental drill' and were calculated due to simulated data. The procedure of this method was subdivided into three parts.

The first part was focussing on the manufacturing phase by analysing the data. Each characteristic is normal distributed and there are no interdependences between them. This leads to non-related tolerance zones. It was also shown, that within the case study three important dental drill characteristics (C2, C3 and C4) conformed to given tolerance specifications, whereas the important drill characteristic C1 led to non-conforming manufacturing results. The second part was focussing on advanced manufacturing analysis: Multidimensional analysis methods were visualised and possible interactions were explained. Therefore, the multinormal distri-

bution formula was used for several characteristic combinations and the expected failure probability by calculation of the integrals of these multinormal-distributions. The third and concluding part was the analogy of ppm and C_{pk}, which leads to a MPCI. With this linkage it is possible to determine a MPCI of the previous calculated integrals using the equation 6.

With the application of all three parts together, an approach for estimation of MPCI has been shown. With the help of this approach, the multivariate validation of a set of important product characteristics by using one capability index (therefore one risk indicator)—as an analogon to the univariate case—is feasible.

In this context it is important to underline the comparison between one-dimensional SPC methods (state-of-the-art) and the approach of Multidimensional Process Capability Indices (MPCI): For example QCC and PCI—as important parts of SPC—are included in this paper. The added value of the shown MPCI approach is the combination of known SPC methods to detect a risky manufacturing process. Subsequently, by choosing proper process improvement actions, it is possible, to ensure a reliable production process. The output of the method combination is the base of a MPCI. The MPCI enables the validation and supervising of a production line; furthermore the evaluation of the production process by the use of one risk indicator. The separate application of single SPC methods examines only excerpts of production aspects, such as a specific production process step or measurement process. Therefore, the presented approach of this paper extends the reliability of the whole production process.

The presented method will be implemented in future manufacturing process lines of different medical instruments. Furthermore, the mathematical formula will be improved by using different kinds of distribution models regarding different product characteristics (e.g. Weibull and Log-normal). Thus, future results should lead to a precise description of the manufacturing influences by multidimensional process capability indices.

ACKNOWLEDGEMENTS

The authors thank the project sponsor (Bundesministerium für Bildung und Forschung (BMBF); Projektträger Karlsruhe, Germany) for supporting this project. The authors also thank the cooperation partner (Burkhard Höchst, Hager & Meisinger GmbH, Neuss, Germany) for their support due to production information and measurement data as a basis for our research work.

REFERENCES

Dietrich, E. & Schulze, A., 2009. *Statistische Verfahren zur Maschinen- und Prozessqualifikation*. München: Hanser.

Genz A. & Bretz F., 2009. *Computation of Multivariate Normal and t Probabilities*. Berlin; Springer, 2009.

Goethals P.L. & Cho B.R., 2011 The Development of a Target-Focused Process Capability Index with Multiple Characteristics. In *Quality Reliability Engineering International* (27): 297–311, 2009.

Pfeifer, T., 2002. *Quality Management*. München: Hanser.

Pospiech, M., Michalski, J. & Bracke, S., 2013. *Multivariate manufacturing process validation: Risk minimisation within high-precision dental tool manufacturing*. In: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia, A.C.W.M. Vrouwenvelder: Safety, Reliability and Risk Analysis: Beyond the Horizon. Proceedings: ESREL 2013, European Safety and Reliability Association—ESRA.

Sachs, L., 2002. Applied statistics. Berlin: Springer, 2002.

Tano I. & Vännman K., 2011 Comparing Confidence Intervals for Multivariate Process Capability Indices. In *Quality Reliability Engineering International* (28) 481–495, 2011.

Timischl, W., 2002 *Qualitätssicherung. Statistische Methoden*. München: Hanser.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

A unified model of systems dependability and process continuity for complex supply chains

L.A. Bukowski
Academy of Business in Dąbrowa Górnicza, Poland

J. Feliks
AGH Academy of Science and Technology, Krakow, Poland

ABSTRACT: Nowadays the manufacturing and logistic systems, and especially global supply networks, become more and more complex, sophisticated and expensive. They operate in an environment of dynamic changes, disturbances, disruptions threats and uncertainty that is related to market behaviour. The typical methods of lean management, based on traditional policies, under this risky work conditions, are for those systems not sufficient and the rules of crises management are not efficient enough. The objective of this paper is to come up with a new unified concept of systems dependability and process continuity management for complex supply chains and especially for global supply networks. The core idea of the overall concept is based on the experiences gained in the area of so called dependable computing, as well as that in the field of the resilience engineering.

1 INTRODUCTION

The modern business activity, both real and virtual, meaning capital, is dynamically developing on the global scale. It involves, amongst others, a constant increase in complexity of the systems within which integrated business, production and service processes are realised, as well as the necessity of making key decisions based on imperfect knowledge, burdened with the uncertainty, incompleteness and ambiguity of the available information.

These complex systems also include modern supply chains, which are characterised by a topology of complicated networks realising particular functions consisting in moving goods in space and time, as well as their storage in an efficient and effective way, in the conditions of a changeable and uncertain environment and possible disturbances and threats. The rational management of these processes relies on logistics, an interdisciplinary domain concerned with efficient and effective coordination of flows (moving and storing) of material and immaterial resources (goods, people, transaction, and information connected with them) as a part of supply chains.

Ensuring a high level of quality for logistic services in global networks requires a continuous improvement process with particular consideration of safety and risk aspects. The most important trends in activities improving the modern supply chains include (Straube & Pfohl 2009):

- Improvement of supply networks' safety through decreasing their vulnerability to external threats connected with both acts of nature (natural disasters) and intentional acts of criminal or terrorist groups.
- Increasing the security of supply networks as well as their survivability and resilience in critical conditions.
- Strategic and complex approach to supply chain risk management, as a tool supporting key decision making in logistics.

A complex approach to the supply chains management, with particular emphasis on dependability of logistic systems and the continuity of the processes realised by them is, according to the authors, the key to the success of the actions mentioned above. The aim of this paper is to present a proposition of a unified model encompassing both of these aspects (systems dependability and process continuity) in a constituent and non-contradictory way, as bases for an effective and efficient supply chains management.

2 COMPLEX SUPPLY CHAINS—SYSTEMS APPROACH

Modern supply chains, particularly these of global range, are large scale systems, consisting of many subsystems, which often are autonomous distributed systems. Thus, from the point of

view of systems science they can be considered so-called systems of systems, which are a subject of a new branch of science—system of systems engineering.

System of Systems Engineering (SoSE) methodology is successfully used in U.S. Department of Defence applications, but is increasingly being applied to non-defence related problems such as architectural design of problems in transportation, healthcare, global communication networks, search and rescue, space exploration and many other domains. SoSE deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a system of systems capability greater than the sum of the capabilities of the constituent parts (Luzeaux et al. 2011). System of systems may deliver capabilities by combining multiple collaborative and autonomous-yet-interacting systems. The mix of systems may include existing, partially developed, and yet-to-be-designed independent systems.

SoSE differs from the classical engineering (engineering of a single system), and should include the following factors (Luzeaux et al. 2011):

- Larger scope and greater complexity of integration efforts,
- Collaborative and dynamic engineering,
- Engineering under the condition of uncertainty,
- Continuing architectural reconfiguration,
- Simultaneous modelling and simulation of emergent systems behaviour,
- Rigorous interface design and management.

The most important features characterizing the differences between the conventional approach to Systems Engineering (SE) and the approach of Systems of Systems Engineering (SoSE) were compiled in Table 1.

It clearly shows that the global supply chains which have:

- network structure of changeable boundaries, set-up with approximation methods (according to the "good enough" principle),
- manifold aims, resulting from the complexity of mutual relations of the chain's "links",
- emergent properties which cannot be predicted with traditional analytical methods, and
- a time-scale considered not as a part of a life cycle, but in the aspect of the continuity of action, can be qualified among Systems of Systems (SoS).

A simplified model of such a system of systems, exampled by a Complex Supply Chain (CSC) is represented in Figure 1.

The task of such system is to purposefully process material and non-material inputs into outputs. A system of systems consists of a structure (in case of CSC, an infrastructure of network character) and a process realised by it (supplying goods to consumers). In real operating conditions a system of systems is affected by common threats and atypical hazards. They can cause a failure of the structure of a system of systems and a disruption of the process the system is realizing. Since ensuring systems' reliability and the continuity of the processes realized by them is one of dependability engineering and resilience engineering tasks, both of these concepts will be discussed in a later part of this work.

Table 1. Comparing the system engineering and system of systems engineering attributes.

Nr.	Attribute	Systems engineering	System of systems engineering
1	Focus	Single complex system	Multiple integrated complex systems
2	Problem	Defined	Emergent
3	Objective	Optimization (best)	Satisfying (good enough)
4	Boundaries	Static (fixed)	Dynamic (variable)
5	Structure	Hierarchy	Network
6	Goal	Unitary	Pluralistic
7	Approach	Process related	Methodology related
8	Timeframe	Life cycle	Continuous
9	Design tools	Many	Few
10	Management standards	Few	Non

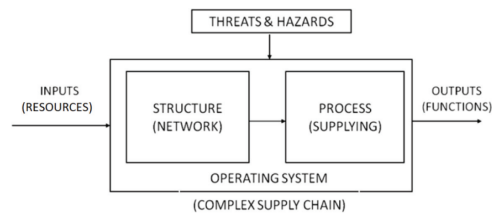


Figure 1. Simplified model of complex supply chain.

3 DEPENDABILITY ENGINEERING—CONCEPT OF FAULT-TOLERANT COMPUTING

There are two perspectives of defining dependability within the IEC Technical Committee 56: dependability as a system property and dependability as cumulative terms of quality. IEC defines dependability in both forms. One dependability description concerns collective forms (IEC 60300-1 (2003-06), IEC 60300-2 (2004)): "Dependability describes the availability performance and its influencing

factors: reliability performance, maintainability performance and maintenance support performance". Dependability is also defined according to IEC 60300-3-15 (2009) as "the ability of a system to perform as and when required to meet specific objectives under given conditions of use".

The contribution from the computer system group is represented in the Laprie's dependability tree. The authors developed the concept of fault-tolerant computing, based on the idea of dependable service delivering (Avizienis et al. 2004). In this work the dependability of a system is understood as the ability to deliver service that can justifiably be trusted. The service delivered by a system is its behaviour as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at the service interface. The function of a system is what the system is intended for, and is described by the system specification. Dependability is an integrative concept that consists of three parts: the attributes of, the means by, and the threats to which dependability is attained.

Dependability attributes:

- Availability—readiness for correct service;
- Reliability—continuity of correct service;
- Safety—absence of catastrophic consequences on the users and the environment;
- Confidentiality—absence of unauthorized disclosure of information;
- Integrity—absence of improper system state alterations;
- Maintainability—ability to undergo repairs and modifications.

Dependability means:

- Fault prevention how to prevent the occurrence or introduction of faults;
- Fault tolerance—how to deliver correct service in the presence of faults (e.g. Redundancy);
- Fault removal—how to reduce the number or severity of faults (e.g. Corrective or preventive maintenance);
- Fault forecasting—how to estimate the present number, the future incidence, and the likely consequences of faults.

Dependability threats:

- Faults
- Errors
- Failures

Security is the concurrent existence of:

- availability for authorized users only,
- confidentiality, and
- integrity with 'improper' meaning 'unauthorized'.

Correct service is delivered when the service implements the system function. A failure is an event that occurs when the delivered service deviates from correct service. A system may fail either because it does not comply with the specification, or because the specification did not adequately describe its function. A failure is a transition from correct service to incorrect service, i.e., to not implementing the system function. A transition from incorrect service to correct service is service restoration. The time interval during which incorrect service is delivered is a service outage. An error is that part of the system state that may cause a subsequent failure: a failure occurs when an error reaches the service interface and alters the service. A fault is the adjudged or hypothesized cause of an error. A fault is active when it produces an error, otherwise it is dormant. A system can fail in the different ways—failure modes.

A system consists of a set of interacting components, therefore the system state is the set of its component states. A fault originally causes an error within the state of its components. An error is detected if its presence in the system is indicated by an error message or error signal that originates within the system. Faults and their sources are very diverse.

The concept of fault-tolerant computing became very successful in the area of information technology and computer science, but was not general enough, to cover all types of technical systems, e.g. global production systems and logistics chains, especially in presence of the low frequent and unpredictable hazards.

4 RESILIENCE ENGINEERING—CONCEPT OF DISRUPTION-TOLERANT OPERATION

Resilience Engineering is the latest departure from the popular image in which the typical path to disaster is a single and major failure of a system component—very often the human. The understanding of how accidents happen has undergone a huge development over the last century (AMBER 2009). Accidents were initially viewed as the conclusion of a sequence of events, which involved "human errors" as causes or contributors. This is now being replaced by a systemic view in which accidents emerge from the complexity of people's activities in an organizational and technical context. These activities are typically focused on preventing accidents, but also involve other goals (e.g. effectiveness, throughput, productivity, efficiency, costs) which means that goal conflicts can arise, always under the pressure of limited resources (e.g. time, money, equipment). Accidents emerge from a confluence of conditions and occurrences that are usually associated with the pursuit of success,

but in this combination (each necessary but only jointly sufficient) able to trigger failure instead. The iceberg model proposes that there are a certain number of incidents for each accident, and a certain number of near misses for each incident, and a certain number of unsafe acts for each near miss. The average ratio used is 1 accident for 10 incidents for 30 near misses for 600 unsafe acts (1:10:30:600) (Hollnagel et al. 2006).

The idea of latent failures is an evolution and combination of ideas from preceding theories and models on accident causation, particularly the sequence-of-events model and man-made disasters theory. According to the latent failure model, disasters are characterized by a concatenation of several small failures and contributing events, rather than a single large failure. Multiple contributors are all necessary but individually insufficient for the disaster to occur (Dekker et al. 2008). Latent failures are decisions or other issues whose adverse consequences may lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defences. Some of the factors that serve as "triggers" may be active failures, technical faults, or atypical system states. According to the latent failure model, we understand of accident potential in terms of organizational processes, task and environmental conditions, individual unsafe acts, and failed defences. A safety-critical system is surrounded by defences-in-depth (as depicted by the various layers between hazards and the object or process to be protected in the figure). Defences are measures or mechanisms that protect against hazards or lessen the consequences of malfunctions or erroneous actions. None of these layers are perfect, however, and the "holes" in them represent those imperfections. According to the latent failure model, accidents happen when all of the layers are penetrated, and when all their imperfections or "holes" line up. Incidents happen when the accident progression is stopped by a layer of defence somewhere along the way. This idea is carried over from the earlier sequence-of-events model, as is the linear depiction of a failure progression.

The word resilience means the tendency or ability to spring back (bouncing back), and thus the ability of a body to recover its normal size and shape after being pushed or pulled out of shape, and general any ability to recover to normality after a disturbance. It means to being able to withstand shocks and deviations from the intended state and go back to a desirable or acceptable, state. The authors of ReSIST document (ReSIST 2009) concluded that a useful meaning to apply to resilience for current and future systems is ability to deliver, maintain and improve service when facing threats and evolutionary changes. Their concern is often one of balance, as they see excessive emphasis on static means for achieving safety, designed in response to accidents, while they see a need for a culture of self-awareness, learning how things really work in the organization (real processes may be very different from the designed procedures), taking advantage of the experience in dealing with anomalies, paying attention to the potential for unforeseen risks, fostering fresh views and criticism of an organization's own model of risk.

A limitation of maximum tolerable disturbance measures is that we may well be interested in characterizing how well a system rebounds from smaller disturbances. For instance, given a form of fault tolerance that allows for some degradation of service, we may then want to measure not just how far the system can be pushed before failing altogether, but the relationship between the size of disturbances and the degradation of performance.

Since for most systems of interest the resilient behavior is non-deterministic in practice, we are no longer interested in whether the system will rebound from a disturbance but in the probability of it successfully rebounding; or the distribution of the time needed for it to return to a desired state. Thus in fault-tolerant computing we talk about the "coverage" factor of a fault-tolerant mechanism, and we can talk about the distribution of the latency (time to detection) of a component fault or data error (Avizienis et al. 2004).

A concern in the resilience engineering literature is that measures of outcomes may lack predictive power: success in the past is no guarantee of success in the future). Thus a search for leading indicators that can be used to assess future resilience has begun. Leading indicators sets should be based on: Management commitment, Just culture, Learning culture, Opacity, Awareness, Preparedness and Flexibility. Examples of indicators related to preparedness is "crisis training beyond minimum requirements" and to management commitment is "percentage of overtime" (Avizienis et al. 2004). Another approach based on organizational resilience focuses on Commitment, Competence, and Cognizance—"three C's". Sometimes these three C's' are combined with "four P's": Principles, Policies, Procedures, and Practice (O'Rourke et al. 2007).

Sum up, one is simply the recognition of the multidimensionality of resilience. For instance, Westrum (Westrum 2006) writes: "Resilience is a family of related ideas, not a single thing. The various situations that we have sketched offer different levels of challenge, and may well be met by different organizational mechanisms. A resilient organization under Situation I will not necessarily be resilient under Situation II (these situations are defined as having different degrees of predictabil-

ity). Similarly, because an organization is good at recovery, this does not mean that the organization is good at foresight".

5 CONCEPT OF THE UNIFIED MODEL OF SYSTEMS DEPENDABILITY AND PROCESS CONTINUITY FOR COMPLEX SUPPLY CHAINS

The concepts discussed briefly in points 3 and 4 are different in many ways, but can be considered mutually complementary. However, as of yet, in spite of huge and constantly growing interest in the issue of resilience engineering (particularly in the field of logistics), there still is no complex quantitative model of resilience, compatible with other related fields of study (ex. dependability engineering). Thus, a proposition has appeared to build a resilience model on the basis of an analogy with the dependability model, in compliance with the specificity of the process perspective dominant in the resilience approach.

Dependability of the supply chains is understood as the ability to deliver correct service that is available and safe under normal (ordinary) work conditions in a given time interval.

Dependability (D) is also the 2-dimentional vector

$$D = \{AV, SA\} \quad (1)$$

with:

- Availability (AV):
  - Reliability (REL),
  - Maintainability (MAI),
  - Maintenance Support Performance (MSP),
- Safety (SA):
  - Absence of Critical Damages (ACD)—active actions,
  - Protecting the environment against the effects of any potential critical damages (PRO)—passive actions.

Resilience of the supply chains is the ability to assure the service delivery with an acceptable discontinuity under abnormal (uncommon, hazardous) working conditions and situations (e.g. disruptions, attacks, accidences, disasters).

So we understand resilience (R) as the 3-dimentional vector

$$R = \{SE, SU, RE\} \quad (2)$$

with:

- Security (SE)—protection of a system from malicious intent, is displayed by
  - Confidentiality (CON) of information to unauthorized users,
  - Integrity (INT)—impossibility of introducing changes into the system by unauthorized users, and
  - Accessibility (ACC) for authorized users only.
- Survivability (SU)—the capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents, is described by
  - Detectability (DET)—early threats recognition, supervision and monitoring,
  - Robustness (ROB)—resistance and redundancy,
  - Adaptability (ADA)—flexibility, agility, fault tolerance.
- Recovery (RE)—failure removal (restoration) in acceptable time and costs, is divided into
  - Susceptibility to repair (SUS) and
  - Availability of Repair Resources (ARR).

The framework for evaluation of technical systems dependability with the use of fuzzy logic and experts' knowledge was developed and published by authors in (Bukowski & Feliks 2011).

The resilience model proposed in this work is based on a typical course of a service delivering process, interrupted by an occurrence of a threat leading to a disruption of the process continuity. An example of such a course as a function of time is represented in Figure 2, on which three fundamental phases can be distinguished:

- A phase of normal work, interrupted only by slight disturbances and rare cases of more serious hazards, which were recognized sufficiently early and "parried" (thwarted), thanks to a properly functioning security system
- A phase of process continuity disruption, directly after an occurrence of a hazard, which has not been effectively blocked by the security system. During this phase, the system's survivability is its decisive feature, which is measured by the levels of performance: DPL and PPL, as well as time t_s
- A phase of process recovery to an acceptable level of APL performance after the continuity's disruption, characterized by time t_r.

After the removal of the effects of the process continuity disruption, a process of improvement can begin, consisting in an adaptation of the system to new working condition and a possible increase in the level of performance.

This model is algorithmically illustrated in Figure 3.

External sources of risk generate disruptions and hazards which encounter security barriers.

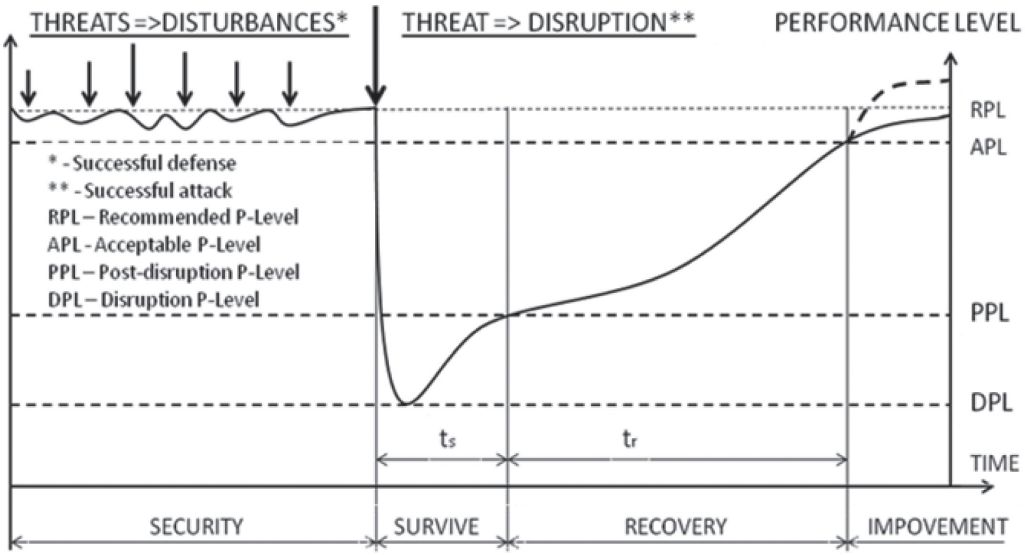


Figure 2. Typical disruption time history.

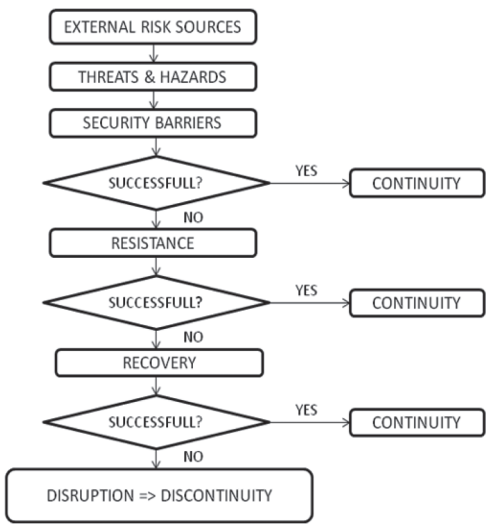


Figure 3. Disruption model flowchart.

Table 2. Comparing the dependability engineering and resilience engineering attributes.

Nr.	Attribute	Dependability engineering	Resilience engineering
1	Focus	System related	Process related
2	Desirable state	Availability	Continuity
3	Undesirable state	Fault	Interrupting
4	Undesirable event	Failure	Disruption
5	Activity after undesirable event	Renewal	Recovery
6	Desired abilities	Reliability robustness maintainability	Survivability resistance recoverability
7	Measures in time dimension	MTBF MTTFF MUT MDT	ETBD ETTFD ECT EDT

As long as these barriers fulfil their roles, the system realizes the required functions in a continuous way. If the barriers turn out to be insufficient to protect a given system, the system must defend itself with its internal resistance. In a case in which the resistance is too weak in relation to the working hazard (to absorb disruption impact and to withstand disruption shock), the system goes into the "recovery" state, which encompasses the stages of damage removing, as well as repair and restoration. If this stage also ends in failure, a total interruption of the process continuity will occur, resulting in the need of reengineering (redesign of structure and processes).

Basic characteristics of the accepted dependability and resilience models have been compiled in Table 2, together with the measures of the time indicators describing them quantitatively.

Thus, the MTBF (mean time between failures) indicator corresponds with ETBD (expected time between disruptions), the MTTFF (mean time to first failure) indicator corresponds with ETTFD (expected time to first disruptions), the MUT (mean up time) indicator corresponds with ECT (expected continuity time), while the MDT (mean down time) indicator corresponds with EDT (expected disruption time). Differences result mainly from the fact that while in the case of dependability the indicators are generally assessed through statistical methods, in the case of resilience, due to very infrequent events threatening to disrupt the process continuity, generally only expert methods are available. Such a method, with the use of artificial intelligence methods, is proposed by the authors of this paper.

The application of fuzzy sets theory in this case is reasonable because expert's knowledge can be used to build a suitable rule base (Bukowski & Feliks 2005). Expert knowledge on the impact of the various parameters on result is expressed in the form of "if … then" rules. The knowledge encoded in a rule base is derived from human experience and intuition as well as on the basis of theoretical and practical understanding of the properties of the studied object. The main task of this deduction system is to calculate the approximate value of the output variable based on the share of each rule from the rule base with an appropriate factor determining the "validity" of the rule. Fuzzy logic based systems are a kind of expert system built on a knowledge base that contains inference algorithms in the form of a rule base. What distinguishes fuzzy inference in terms of concept from conventional inference is the lack of an analytical description. The approximate inference mechanism transforms knowledge from the rule base into a non-fuzzy form. The non-fuzzy form of the result is obtained in the process of defuzzification. Defuzzification is interpreting the membership degrees of fuzzy sets into a real value. The correctness of selection of rules as well as the shape and ranges of the membership function is verified with a rules viewer and simulation. The rules viewer displays a roadmap of the whole fuzzy inference process.

The software WinFACT® (WinFACT—User Guide 2003) was used for building a system for evaluating resilience level. WinFACT® provides FLOP (Fuzzy Logic Operating Program) tools for creating and editing fuzzy inference systems or integrating our fuzzy systems into simulations with BORIS (Block Oriented Simulation). An example of the application of this idea is shown in the Figures 4 and 5.

The evaluation system of supply chain resilience is a hierarchical structure. In the first sequence the Security (SE), Survivability (SU) and Recovery (RE), were evaluated, and the information about them can be represented by the membership function of fuzzy system. Trapezium membership functions are associated with the numerical value RE, SU, SE. Each of these parameters was divided in to three categories—Low, Moderate and High from range 0 to 1. Level of resilience (R) is an output of

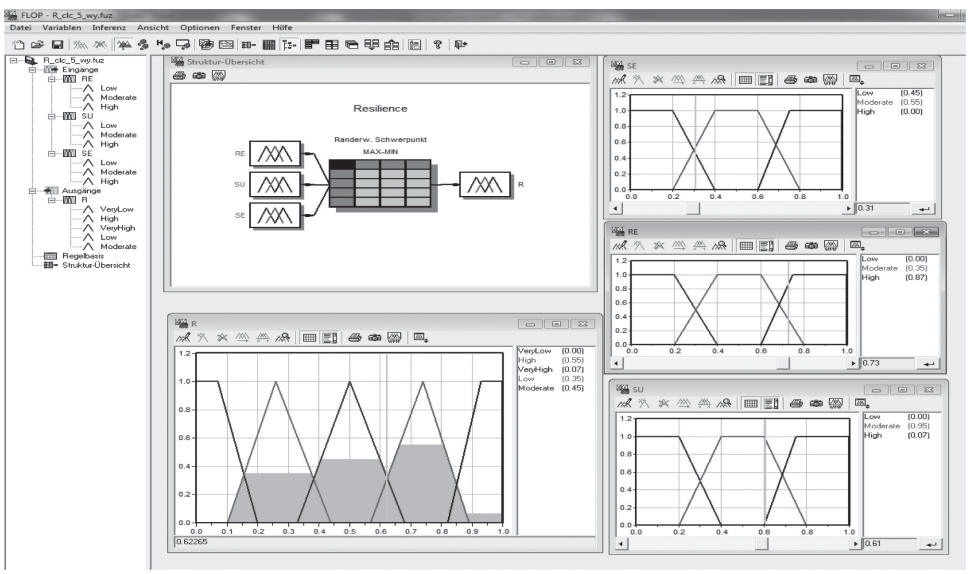


Figure 4. Screen shot of resilience fuzzy model.

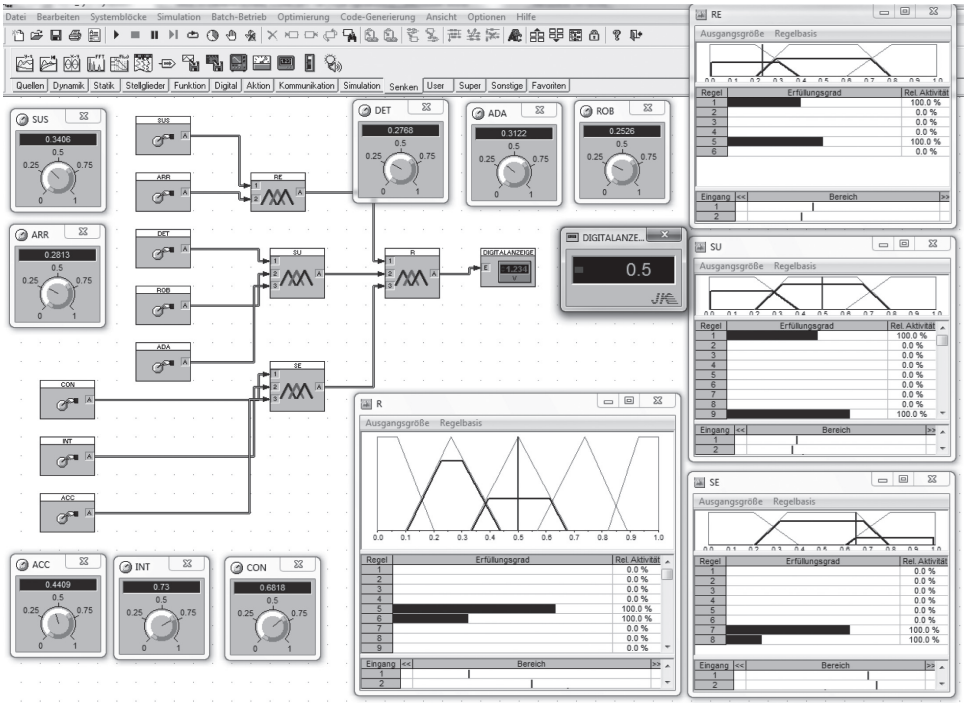


Figure 5. Screen shot of simulation fuzzy model.

this system and it is depends on the value of inputs and on the "knowledge" which is implemented in the rules base in a fuzzy system. In the case of using trapezoidal membership function models for linguistic variables, one may assume that that the measure of uncertainty in quantitative estimates is the angle of inclination of the sides of the. So slope of each input variables could be interpreted as an uncertainty of input parameter estimation.

6 CONCLUSIONS

The unified model of systems dependability and process resilience proposed in this paper is a universal, "shell" type tool, that can be applied to verifying and validating the vulnerability of complex systems, especially for complex supply chains.

Adapting this model to the needs of a particular type of system or a specific practical case requires the estimation of numerical values (or ranges) corresponding to each parameter class.

The measure of uncertainty in this model is the inclination angle of the triangles or trapezoids sides (the smaller the angle, the larger the uncertainty).

REFERENCES

AMBER 2009—Assessing, Measuring, and Benchmarking Resilience, FP7-216295.

Anderson, R. 2008. Security engineering. A guide to build dependable distributed systems, Wiley.

Aven, T. 2014. A new perspective on how to understand, assess and manage risk and the unforeseen, Reliability Engineering and System Safety 121(2014), 1–10.

Avizienis, A. et al. 2004. Basic concepts and taxonomy of dependable and secure computing, IEEE Trans. on Dependable and Secure Computing, 1(1):11–33.

Bukowski, L. & Feliks, J. 2005. Application of Fuzzy Sets in Evaluation of Failure Likelihood. Proceedings of the 18-th Int. Conference on Systems Engineering—Las Vegas, Nevada: 170–175.

Bukowski, L. & Feliks, J. 2011. Evaluation of Technical Systems Dependability with the Use of Fuzzy Logic and Experts' Knowledge, Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando (Florida), 07.2011, 285–290.

Dekker, S. et al. 2008. Resilience Engineering: New directions for measuring and maintaining safety in complex systems, Final Report December 2008.

DHS (U.S. Department of Homeland Security), 2006. National Infrastructure Protection Plan. Available online at: www.dhs.gov/nipp.

Herrera, I.A. & Hovden, J. 2008. The Leading indicators applied to maintenance in the framework of resilience engineering: A conceptual approach, 3rd Resilience Engineering Symposium, Antibes-Juan Les Pins, France, 2008.
Hollnagel, E. et al. 2006. Resilience Engineering. Concepts and Precepts, UK: Ashgate.
Luzeaux, D. et al. 2011. Complex System and Systems of Systems Engineering. ISTE Ltd and John Wiley & Sons Inc.
Natarajarathinam, M. et al. 2009. Managing supply chains in times of crisis: a review of literature and insights, International Journal of Physical Distribution and Logistics Management, 39(2009), 535–573.
O'Rourke, T.D. 2007. Critical Infrastructure, Interdependencies, and Resilience, The Bridge, National Academy of Engineering, Vol. 37, No. 1, Spring 2007.
ReSIST, 2009. Deliverable D39: Selected Current Practices.
Sanchis, R. et al. 2012. Identification and analysis of Disruptions: the first step to understand and measure Enterprise Resilience, Proceedings of the 6th International Conference on Industrial Engineering and Industrial Management, Vigo, July 18–20, 2012.
Sheffi, Y. & Rice Jr, J.B. 2005. A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Rev., 47(2005), 41–48.
Standard Risk Measures. An Overview of Standard Risk Measures in Practice. 2013, www.superratings.com.au.
Straube F. & Pfohl H.-Ch. 2009. Global Networks in an Era of Change. Environment, Security, Internationalization, People, Hamburg.
Waters, D. 2007. Supply chain risk management: vulnerability and resilience in logistics, Kogan Page Limited, London & Philadelphia.
Westrum, R. 2006. A Typology of Resilience Situations, in Resilience Engineering. Concepts and Precepts, Hollnagel, E. and all, UK: Ashgate, 2006.
WinFACT—User Guide, 2003.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Using quantitative stochastic model checking tool to increase safety and improve efficiency in production processes

L. Herbert
DTU Compute, The Technical University of Denmark, Lyngby, Denmark

Z.N.L. Hansen & P. Jacobsen
Department of Management Engineering, The Technical University of Denmark, Lyngby, Denmark

ABSTRACT: This paper shows how quantitative stochastic model checking can be employed in an evolutionary algorithm to automatically reconfigure a production process to improve the efficiency of production while observing freely defined safety constraints. Our approach is based on a formalized subset of the modelling language Business Process Modelling and Notation (BPMN). This language is extended with annotations, which capture the associated consumption of resources (e.g. time, cost or consumption of materials) and which allow for stocastic behaviour. We employ Probabilistic Temporal Logic (PCTL) to specify safety constraints and to determine the quatative properties of the workflow. We procced to present an evolutionary algorithm to search through possible reconfigurations of a production process to meet the required safety constraints while observing safety constraints specfied in PCTL. The ideas in this paper are implemented in SBOAT, a prototype software tool which is employed in a case study in the baked goods industry. Applied to the case study SBOAT is able to optimize a production process such that production time of baked goods is improved while safety constrints are observed, thereby reducing the costs associated with production faults while maintaining a defined level of safety.

1 INTRODUCTION

Historically, Frank Gilbreth is credited with developing the first method for documenting process flow (Gilbreth & Gilbreth 1921), and since then many different abstract representations of business processes have been proposed. Today, two modelling languages have come to dominate modern business process modelling: the *Business Process Model and Notation* (BPMN) language (Object Management Group 2011a) and the *Unified Modelling Language* (UML) (Object Management Group 2011b). Both of these are visual languages which has allowed them to be used by practitioners with little formal training. However, the rapid adoption and development of these languages has come at the expense of an imprecise and incomplete semantic definition, preventing analysis by formal means (Börger 2012, Recker, Indulska, Rosemann, & Green 2005).

1.1 *Efficiency gains in production processes*

Modern enterprises exist within complex networks which must adapt to constantly changing environments. The architecture of an enterprise is the organizing logic of the individual business processes which make up its operations (Ross, Weill, & Robertson 2006). For industries which create complex products or provide complex services, their strategy and business processes often exhibit a high degree of complexity. In these environments creating dependable, yet efficient, business processes poses a significant challenge. Requirements for process models can be divided into the following categories, although a specific requirement may belong in more than one category (Vergidis, Tiwari, & Majeed 2008):

- **Validation properties:** testing whether the business process behaves as expected in a given context; e.g., does this financial process comply with the Sarbanes–Oxley act?
- **Performance properties:** evaluating the ability to meet requirements for throughput times, service levels, and other quantitative factors; e.g., how long does it take to deliver a package?
- **Stochastic properties:** evaluating the probability of behaviour within the system; e.g., is there a greater than 98% chance the package will be delivered in three days?

The predominant approach to developing business processes is first to develop conceptual process models, which are used for development of

an implementation, typically involving a mix of automated and manual processes. There is substantial evidence (Gallaher & Kropp 2002, White, O'Connor, & Rowe 2004) that being able to determine such properties and their exact quantitative values early in their design phase can result in smoother integration, accurate provisioning to meet service level agreements, and significant cost savings. In particular, safety critical processes frequently combine the need for certainty that safety properties are not violated while simultaneously requiring a specific performance profile.

In this paper we present a mathematical approach to analysing production processes in order to optimise them for greater efficiency and safety. We do this by employing quantitative stochastic model checking. We show the practical applicability of this approach by applying our software tool SBOAT (*Stochastic BPMN Optimisation and Analysis Tool*), to an small example from the baked goods industry. Combined this approach provides a practical technique for business process architects a means to automatically test and redesign production processes according to given constraints (e.g. safety, cost, time).

1.2 *Related work*

In general by performing model checking to determine quantitative and qualitative properties of BPMN models, this work draws a comparison with a number of other BPMN analysis techniques outlined below. The selection of analyses discussed is not exhaustive, but covers the main approaches which have been widely referenced in the literature. They can broadly be defined as functional analyses, non-functional analyses and stochastic analyses.

In terms of the analysis of functional qualitative properties a wide range of approaches have been developed for BPMN. These are predominantly focused on the analysis limited sets of functional properties, such as proving the absence of deadlocks. The work of Ouyang et al. (Ouyang, Dumas, ter Hofstede, & van der Aalst 2006, Ouyang, Dumas, & Hofstede 2007) is the closest match to the type of translation approach taken in this paper. Here, translation of BPMN models is done directly into the web-services orientated Business Process Execution Language (BPEL) (Organization for the Advancement of Structured Information Standards (OASIS) 2007) by means of an algorithm similar to what is presented in this thesis. However, the approach by Ouyang et al. is intended to support simulation through execution of the BPEL services with all the limitations that a simulation approach entails. Limitations are for example that statistical simulation can explore some situations, but cannot observe all behaviours. Safety properties which guarantee that specific behaviour will always, or, can never, occur need to be evaluated under all possible situations which simply cannot be achieved by the simulation method. The other key limitation is that simulations need to be executed for a certain amount of time.

A number of different approaches have been developed to analyse non-functional properties of BPMN models. In particular there has been a focus on determining timing properties of BPMN models, but little work on general quantitative properties.

Work by Ling and Schmidt in 2000 (Ling & Schmidt 2000) present a time interval extension of the workflow nets of van der Aalst (Aalst 1997) in terms of timed Petri-nets (Peterson 1981). Their extension introduces a notion of safety in time which is analogous to the notion of boundedness in Petri nets (Peterson 1981), using this notion they basically preserve the original soundness theorems of workflows and the liveness theorems of Petri nets in their timed workflow nets. However, their work only provides for placing bounds on the total execution time for a processes and do not allow for analysis of time intervals on a per state basic. Further, treatment of other quantitative properties associated with a business process are only dealt with to a limited degree and due to need to consider completion run times, and may not readily extendible to other quantitative properties of interest.

Work by Wong and Gibbons (Wong & Gibbons 2009) complements their previous work developing a Communicating Sequential Processes (CSP) (Hoare 1983) based semantics for BPMN. By employing an extension of CSP which accounts for processes *responsiveness*, and an analysis technique that addresses the of timing of processes in such a fashion that a formal automated analysis is still possible. This impressive work allows for extensive analysis of BPMN models, but still does not cover arbitrary quantitative properties or stochastic behaviour.

Analysis of BPMN models extended with stochastic properties has seen limited development with only two approaches identified of dealing with general models which exhibit both probabilistic and non-deterministic transitions. Prandi et al. (Prandi, Quaglia, & Zannone 2008) have identified Probabilistic Symbolic Model Checker (PRISM) (Kwiatkowska, Norman, & Parker 2011) as ideally suited to the analysis of stochastic PRISM business processes. This effort involves conversion of PRISM models into a model expressed in the Calculus for Orchestration of Web Services (COWS) (Pugliese & Tiezzi 2012), which in turn is converted into a model that can be analysed using PRISM (Kwiatkowska, Norman, & Parker

2011). This approach adds unnecessary complexity in that it is possible to convert the notation of BPMN directly into the PRISM modelling language, and then allow PRISM to impose a semantic interpretation without the additional semantic restrictions of going via COWS. Further, the translations PRISM to COWS and in particular from COWS to PRISM is loosely defined and, in the form described by the authors, not amenable to algorithmic translation. This approach, however, does allow the use of rewards. Consequently, the PRISM model checker is potentially able to perform analysis of both quantitative and stochastic properties of a business process. However, details of how such properties will be included in the original BPMN models is not described.

1.3 *Core BPMN*

We will begin by constructing a formalized restricted subset of BPMN for the purpose of illustrating the application of model checking methods to business process optimisation. This subset seeks to be simple enough to allow for relatively straightforward analysis while still having sufficient expressivity to capture a wide range of workflows. Often called the *core* subset of BPMN, it consists of the eight elements found to be most commonly used in a large survey of real-world BPMN usage (Muehlen & Recker 2008); indeed more than 70% of models surveyed consisted only of these elements. The graphical elements of core BPMN are shown in Figure 1 and described below.

The process of modelling a workflow in BPMN involves composing a number of BPMN elements into a Business Process Digram (BPD). The intention is that a business process diagram captures the complete workflow of a business process, with separate sub-components of a workflow organised into separate pools. A BPD is formally defined

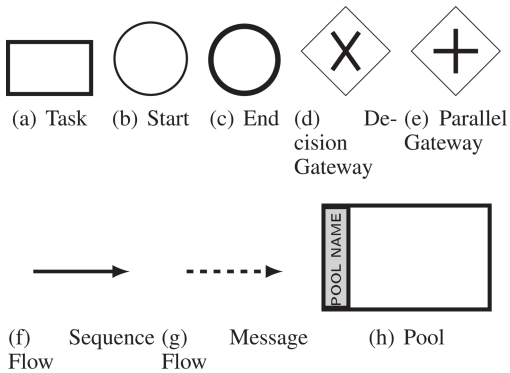


Figure 1. Core BPMN elements.

here as simple partitions of a process graph with synchronisation arcs as defined in definition 1, with the straightforward addition of a function to capture pools.

Definition 1 (Core BPD). A core BPD is an *extended process graph tuple* $BPD = (\mathbf{N}, \mathcal{F}, \mathbf{P}, \text{pool}, \mathbf{L}, \text{lab})$ *where* $\mathbf{N} \subseteq \mathbf{T} \cup \mathbf{E} \cup \mathbf{G}$*, is a set of nodes composed of the following disjoint sets:*

- *Tasks* $\mathbf{T}$*, are the basic actions performed as part of a business process.*
- *Events* $\mathbf{E} \subseteq \mathbf{E}^{\mathbf{S}} \cup \mathbf{E}^{\mathbf{E}}$*, where the disjoint sets* $\mathbf{E}^{\mathbf{S}}$ *and* $\mathbf{E}^{\mathbf{E}}$ *respectively represent start and end events.*
- *Gateways* $\mathbf{G} \subseteq \mathbf{G}^{\mathbf{D}} \cup \mathbf{G}^{\mathbf{F}} \cup \mathbf{G}^{\mathbf{M}}$*, where the disjoint sets* $\mathbf{G}^{\mathbf{D}}$, $\mathbf{G}^{\mathbf{F}}$ *and* $\mathbf{G}^{\mathbf{M}}$ *respectively represent exclusive decision gateways, parallel fork gateways, and parallel merge gateways.*

$\mathcal{F} \subseteq \mathcal{S} \cup \mathcal{M}$ *is a set of flow relations, where sequence flows* $\mathcal{S} \subseteq \mathbf{N} \times \mathbf{N}$ *relate nodes to each other and message passing* $\mathcal{M} \subseteq \mathbf{T} \times \mathbf{G}^{\mathbf{M}}$ *is a relation between tasks and parallel merge gateways.* $\mathbf{P} \subset \mathfrak{P}(\mathbf{N})$ *is a set of disjoint pools and pool* $: \mathbf{N} \to \mathbf{P}$ *maps nodes to a pool* $p \in \mathbf{P}$*.* $\mathbf{L}$ *is a set of unique labels and* $\text{lab} : \mathcal{F} \to \mathbf{L}$ *is a labelling function which assigns labels to flows.*

The definition of a BPD given in definition 1 models business processes by using elements of $\mathcal{F}$ to define a directed graph with nodes which are elements of $\mathbf{N}$. However, definition 1 allows for graphs which are unconnected, do not have start or end elements, and are free from various other properties which place them outside what is implied to be permitted in standard BPMN models. To ensure that a BPD describes a meaningful business process we have developed a set of structural semantics (well-formedness) rules (Herbert & Sharp 2012) which enforce restrictions on connecting elements, pool boundaries, and message passing.

When performing quantitative analysis of a graph based process language we choose structural semantic rules such that they impose the minimum semantic interpretation necessary to determine the control flow of a model. In the case of a BPMN BPD, it adds no more semantic interpretation than implied by the standard (Object Management Group 2011a). In the case of BPMN, when we have imposed restrictions they have been made only for simplicity and are discussed at length in previous work (Herbert & Sharp 2012).

It should be noted that by combining several Core BPMN elements most elements of the entire BPMN language can be simulated, although a few constructs pose more complex issues. Of particular note are inclusive gateways which pose a challenge as the specification of their semantics

include a non-trivial and non-local backwards search of the flow graph of the BPD. However, these can be addressed through the work of Christiansen, Carbone and Hildebrandt (Christiansen, Carbone, & Hildebrandt 2011) who present a method to translate this construct, in a large number of cases, into other BPMN processes with some restructuring of the overall BPD. In general, most elements of the full BPMN language can be incorporated by simply including a preprocessing step in the analysis of BPMN which translates non-core BPMN elements to core BPMN elements.

1.4 *Extending core BPMN*

We will extend our modelling formalism to better accommodate real-world processes which add further complexity, in that the processes may interact with elements outside the processes' control and whose behaviour is unknown. This motivates the need for probabilistic decision points in the modelling of business processes, because the outcomes of complex decisions within a process can appear random and/or not possible to predict. In such a stochastic system, characterizing properties such as the number of items that remain in a queue or the resources consumed per job done will require answers in terms of probabilities.

BPMN makes use of external conditions on decision gateways to select the outgoing flow from a decision point. These decisions are modelled by the set $\mathbf{L}$ and assigned to specific flows by the function *lab* introduced in definition 1. In practice, decision points in a business process will have outcomes which depend on some inherent property of the task or on outside factors. The idea is that at a decision point an active choice is made, and then that choice results in a number of different possible outcomes.

This behaviour, which is similar to a Markov Decision Process (MDP) (White 1993), where we wish to preserve the intention of actors in a process and still enable probabilistic behaviour, can be effectively captured by annotating the possible outcomes of specific decisions with pairs of labels and probabilities (l, p). We employ the following function to ensure meaningful assignment of these intention preserving probabilistic annotations.

Definition 2 (BPD Gateway Flow Probability Function). *Given a BPD, a decision gateway probability function is a partial function* $\mathcal{P} : \mathcal{S} \times \mathbf{L} \to [0,1]$ *which for a node* $g \in \mathbf{G}^{\mathbf{D}}$ *and label* $l \in \mathbf{L}$*, assigns probabilities to all outgoing sequence flows* (g, x)*, such that for a given* l*:*

$$\sum_{\forall x \in out(g)} \mathcal{P}((g,x),l) = 1$$

Definition 2 ensures that all decision gateways have an associated probability and that the sum of all probabilities for a given label l is 1.

Furthermore, many business processes make use of various limited resources such as stock levels, time, or available liquidity, and the accurate provisioning of these resources is the key to their safe and efficient execution. An essential activity in developing business processes that integrate well with their environments is accounting for these resources during their, frequently complex, execution. To enable quantitative analysis of business processes we add numerical data to our models by using the following function which associates positive real numbers with tasks in a BPD.

Definition 3 (BPD Task Reward Function). *For a BPD a reward function for a task* $t \in \mathbf{T}$ *is a partial function* $\mathcal{R} : \mathbf{T} \to \mathbb{R}_{\geq 0}$.

This function captures the notion that certain nodes have some reward or cost associated with the task. The term *reward* is somewhat misleading: there is no practical distinction between costs and rewards, and we can use these annotated values to keep track of whichever quantities may be of interest in a process. We may associate as many reward structures as we wish with a given BPD, so that a single task may have multiple different numerical properties which are incremented when the task is performed. The only restriction is that each reward structure is monotonic.

Further, within our implementation of these ideas: SBOAT, we allow some reward structures to be parametrised, allowing us to model limited resources involved in a process. In this case a reward has an associated upper and lower bound.

Note that the stochastic branching annotations and reward structures presented here are simple additions to the BPMN language, or other graph based process languages, and do not alter the implied semantics of the language.

2 QUANTITATIVE STOCHASTIC MODEL CHECKING

Current approaches to business process analysis are overwhelmingly manual and require time-consuming inspection by an expert. The focus is almost exclusively on qualitative properties and frequently quantitative properties are first examined only when the process has been implemented. Attempts to improve this have mostly focused on simulation, where sets of specific actions in a business process are explored in a stochastic fashion by performing simulation experiments to better understand the effects of running that process. A number of simulation approaches and corresponding tools,

such as (Tumay 1995), ARIS (Scheer & Nüttgens 2000), and FileNet (Netjes, Reijers, & van der Aalst 2000) have been developed. However these approaches have some fundamental differences from formal mathematical analysis.

The most prominent distinction between simulation-based verification and formal verification is that the former requires input vectors and the latter does not. The approach in simulation-based verification is first to generate input vectors, and then to derive reference outputs. The thinking process is reversed in the formal verification process. The user states what output behavior is desirable (without considering input stimuli), and then lets the formal checker prove or disprove it.

Although statistical simulation can be useful in some cases, only formal verification is complete, in the sense that it does not miss any point in the input space of a problem. Statistical simulation can explore some situations, but cannot observe all behaviors. Safety properties which guarantee that specific behavior will always, or, can never, occur need to be evaluated under all possible situations that simply cannot be achieved by the simulation method. The other key limitation is that simulations need to be executed for a certain amount of time whereas verification by model checking is typically unbounded, and can reason about the properties of infinite runs of a system.

Therefore, our approach makes use of formal verification in the form of model checking. The goal of this work is to make it possible to automatically transform a BPMN model of a production process into a form which can be formally analysed. This allows all possible execution paths through the production process to be efficiently examined. This is achieved by transforming the BPMN model into a MDP (White 1993) which is amenable to formal statespace analysis (i.e. mathematical analysis of the set of possible values the process can take during execution). These states represent possible configurations of the system being modelled with probabilistic state transitions being combined with non-deterministic choices between several discrete probability distributions over successor states. Model checking allows for the efficient exploration of the entirety of this space with a temporal logic employed to select sets of states of interest, and offers the possibility of verifying many properties of a system.

Performing model checking of Core BPMN is done by means of the state-of-the-art PRISM tool. This translation of BPMN models to a format that can be analysed by PRISM is detailed in (Herbert & Sharp 2012). The central issue in this translation is addressing parallelism. This is fundamentally accounted for by generating appropriately named PRISM *actions* that enforce synchronisation between modules. An illustration of this process for a simple pair of parallel fork and merge gateways and the resulting three guarded PRISM modules are shown in Figure 2. It should be noted that while this synchronisation between sub modules is performed by means of PRISM action labels, these are ultimately converted, due to the semantics imposed by PRISM, into additional system module variables which impose synchronisation be means of dedicated state variables.

The overall design of the analysis framework for analysing production processes via quantitative stochastic model checking is shown in Figure 4. The main idea is to convert formalized BPMN models into PRISM code and thereby perform Probabilistic Computational Tree Logic (PCTL) model checking of business processes. The only inputs required are the specification of a BPMN model annotated with probabilities and reward structures where required, and a PCTL query (highlighted in grey).

A key consequence of this approach to statespace generation is that in the semantics imposed by PRISM, concurrent elements of a business process do not execute synchronously, instead these transitions are instead arbitrarily interleaved in time (in the style of CSP (Hoare 1983) parallel composition). PRISM will generate all possible interleavings, as dictated by message passing, of separate BPDs and all possible interleavings within each BPD of all Core BPMN elements between parallel fork and merge gateways. An illustration of this interleaving behaviour for the concurrent part of the Core BPMN example process given in Figure 10 is shown in Figure 3.

Note how the possible paths from the *[fork]* gateway to the *[merge]* gateway cover all possible allowed interleavings of assessing and then scanning a patient, and examining the patient's medical

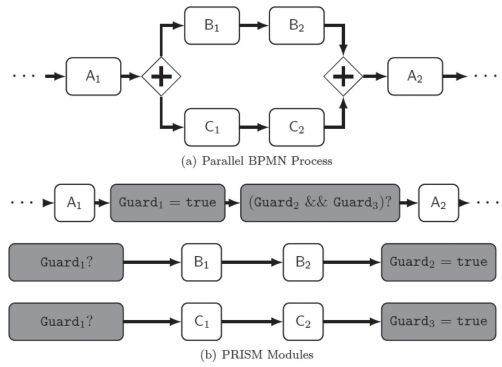


Figure 2. The BPMN to PRISM approach to handling parallelism in a Core BPMN model. Tasks B_1, B_2, C_1, C_2 will be executed after A_1 in all possible interleavings and then followed by the execution of $thsfA_2$.

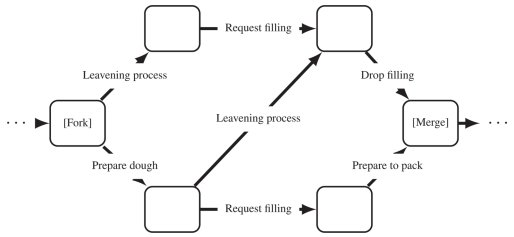


Figure 3. Illustration of interleaving semantics imposed by the PRISM model checker (extract of the statespace of the parallel processes of from Fig.10).

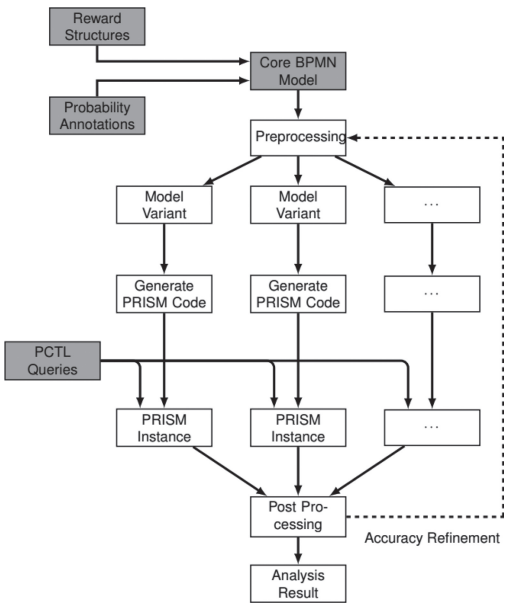


Figure 4. The overall approach taken to automated business process analysis.

record. This maximal interleaving ensures that all possible execution paths are explored, but does not capture so called "true concurrency". This semantic distinction is expressed by Baeten (Baeten 1993) by means of the *the total order assumption* which requires, for the assumption to hold that "all execution sequences of observable actions or events are totally ordered by precedence". This assumption is shown by Baeten (Baier & Katoen 2008) to be well suited to cases when an execution sequence is totally ordered by time and a totally ordered set, such as the non-negative real numbers is employed to model the time domain. Furthermore, when business processes are managed by BPM software, this multitasking, or multiprocessing, is enabled by a software or hardware scheduler. In this type of scheduling the actual execution semantics of a business process will have the total order assumption imposed upon their execution. This assumption ensures all execution sequences that will be possible in practice are present in a model generated by PRISM. Therefore verification of a system under the total order assumption closely matches its actual real world behaviour and verification of systems under the total order assumption provides a strong guarantee of their safety properties.

However, it is this interleaving behaviour which leads to the requirement that, when evaluating performance properties in the form of probability and reward queries, only upper or lower bounds on the expected values can be determined. Note that in a system where there is no non-determinism and only probabilistic behaviour, no interleaving behaviour is present and the bounds will converge, as this case, in essence, reduces to Discrete Time Markov Chain (DTMC) model checking (Baier & Katoen 2008).

This approach is implemented in our SBOAT tool as shown in Section 3.

2.1 *Stochastic model checking*

The central idea of this approach is to be able to perform stochastic model checking of BPMN models. We will employ the property specification language PCTL (Kwiatkowska, Norman, & Parker 2011) based on classical continuous stochastic logic (Hansson & Jonsson 1994) extended to probabilistic quantification of described properties, to define properties of interest. This logic allows us to reason about properties relating to: timing, occurrence and ordering of events, reward values, transient and steady-state probabilities, and best- and worst-case scenarios. An implementation of the PCTL logic is employed by the PRISM model checker in its property specification language and has the following basic elements.

First developed by David Parker as part of his PhD thesis (Parker 2003), the PRISM tool has seen extensive development and has grown to be a very capable model checker. PRISM is an open-source software tool which accepts probabilistic models written in a textual PRISM modeling language based on *Reactive Modules* (Alur & Henzinger 1999), a state-based language using guarded commands. Where properties for their analysis can be specified using the PRISM specification language, which implements the probabilistic temporal logics, PCTL, LTL, and PCTL*. PRISM includes multiple model checking engines, several of which are based on symbolic implementations (using binary decision diagrams and their extensions). These can enable the probabilistic verification of models of up to 10^{10} states (Kwiatkowska, Norman, & Parker 2011);

however, the tool achieves optimal performance on models in the range of 10^4 to 10^8 states.

The key constructs in the PRISM property specification language, as it applies to Markov decision processes, are the *P* and *R* operators. The *P* operator refers to the probability of an event occurring, more precisely, the probability that the observed execution of the model satisfies a given specification. The *R* operator is used to express properties that relate to rewards (more precisely, the expected value of a random variable, associated with particular reward structure) and since a model will often be decorated with multiple reward structures, we augment the *R* operator with a label. For example, to determine the mean time to exhaust the supply of cake filler we would specify the following property:

$$R_{time} =_? [F^{[0,\infty]} filler_empty] \quad (1)$$

In this property (eq. (1)) we employ the time-bounded operator F^I, where $I \in [t_1, t_2] \in \mathbb{R}^2$, to describe if a subsequent boolean variable becomes true, it remains true. Other operators allowed include, the operator U^I which allow for specification of execution paths where one boolean variable holds until another is true, and G^I, which can be seen as the dual of F^I: expresses the fact that a condition remains, rather than becomes, true. Note that these operators can be combined in arithmetic expressions, allowing more complex measures to be expressed.

2.2 *Quantitative properties*

For quantitative analysis of business processes we add numerical data to our models by using a reward function reward function which associates positive real numbers with tasks in a BPD.

Definition 4. (BPD Task Reward Function). *For a BPD a reward function for a task* $t \in \mathbf{T}$ *is a partial function* $\mathcal{R} : \mathbf{T} \to \mathbb{R}_{\geq 0}$.

$\mathcal{R}$ captures the notion that certain nodes have some reward or cost associated with the task. In practice there is no practical distinction between costs and rewards, and we use these annotated values to keep track of whichever quantities may be of interest in a business process, such as execution time or power usage. We may associate as many reward structures as we wish with a given BPD, so that a single task may have multiple different numerical properties which are incremented when the task is performed.

Note that the sequence flow probabilities, message flow probabilities, and reward structures presented here are simple additions to the BPMN language and do not alter its implied semantics.

3 SBOAT

SBOAT is a *Stochastic BPMN Optimisation and Analysis Tool*, which allows a user to model, and annotate with rewards and stochastic branching, a business processes as a BPMN BPD. Analysis is specified using a PRISM style PCTL query and depending on the nature of the query one or number of results are calculated. At the core of SBOAT is the PRISM model checker (Kwiatkowska, Norman, & Parker 2011) which performs analysis of individual models generated by the SBOAT. An overview of the design of SBOAT is shown in Figure 5.

Designing a BPMN model and adding annotations to a model is done in the modeller, shown in Figure 6. Within SBOAT we employ an *adjacency list* (Cormen, Leiserson, Rivest, & Stein 2009) data

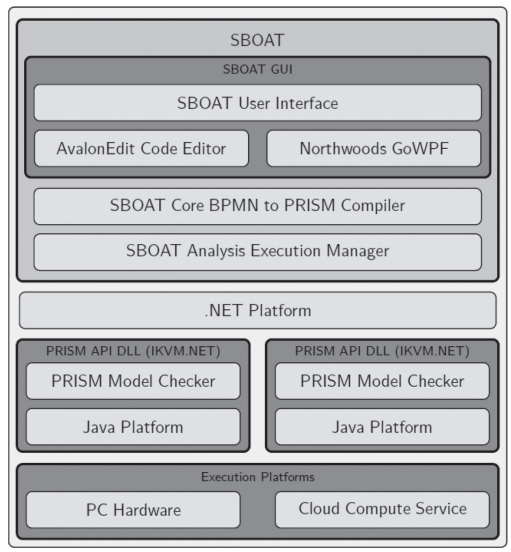


Figure 5. Overall design of SBOAT.

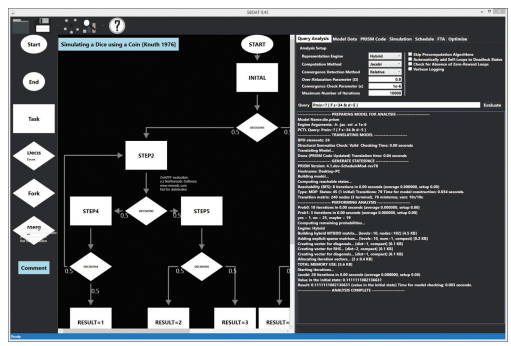


Figure 6. SBOAT 2.0 User Interface.

structure to store the modelled BPD as a directed graph.

This implementation approach allows nodes and edges to be of any data type, where edges implement a simple interface that defines connections to nodes. This flexibility also supports almost any type of reward annotation to be stored in nodes or edges. Further, the data structure is mutable and cloneable making it possible to build a suitable data structure for a wide range of possible graph based process languages. Internally, the data structure keeps a dictionary from nodes to a unordered list of edge elements.

The data structure used is serializable allowing for generation of XML files to store models. In the case of BPMN models, we emit files that comply with the XML based BPMN file format (Object Management Group 2011a), using the annotation features inherent in the BPMN file format to store rewards and stochastic branching probabilities. When importing data files we parse the BPMN XML and at that stage checks for the structural semantic rules of the model are made as new nodes and edges are added.

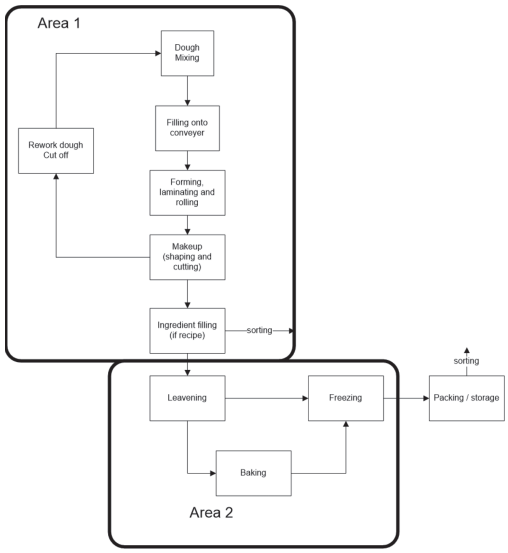


Figure 7. The production process at Baked Goods A/S.

4 CASE STUDY

Baked Goods A/S has two production lines. Line 1 develops cakes and pastries and line 2 develops baked goods like sausage rolls and pizzas. The company has an approximate overall waste of 20% for all products during the whole production cycle. The waste is calculated at different places on the production line, but currently it is only possible to get the overall waste percentage of a product. The production process is shown in Figure 7. The dough is prepared, then the product, for example a cake, is prepared and made, then baked or frozen, followed by packaging and then shipment. Dough leftover during production is reused in the preparation of new dough. Quality checks take place during and after production as well as after freezing where defective products are discarded.

Depending on the line and product, the packaging is either automatic or manual and either controlled for number of pieces and weight or just number of pieces.

The processing steps are as follows;

1. Dough mixing. The ingredients for the dough are mixed in vats with a screw-hook mixer. Water and flour are delivered automatically through transport tubes, all other ingredients are manually added including ice.
2. Lamination. If specified the dough is laminated, meaning folded in on itself and rolled out. This takes place continually. Dough is supplied into a dispensing system. The dough is split into two sheets of continues length, and if specified, a layer of fat is supplied in between these layers. The lamination step can be skipped by using the second dispensing machine situated further up the production line.
3. Make-up and filling. Make-up refers to cutting the shapes out from the dough carpet. The product can also be filled with creams etc.
4. Leavening. This is done to induce a faster rising of the product in order to achieve the wanted volume of the product. This is done by raising the temperature and having a high humidity. This will promote the growth of yeast producing gas and the humidity will counteract surface drying allow for the dough to expand without generating stress cracks etc.
5. Baking. A baking step can be used after leavening.
6. Freezing. Some products are frozen instead of baked and then baked at the customer site.
7. Packing. Products are packed in bags, sealed and packaged for shipping to the customer.

5 ANALYSIS OF CASE EXAMPLE

To illustrate an application of this method we will consider a specific example of a simple production process inspired from the baked goods case study involving bread production. To employ the method, one begins by building a BPD model of an existing production process. Figure 8 is an example of such a process which is annotated with rewards

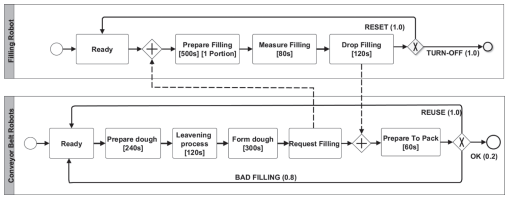


Figure 8. BPD model of a baking workflow process before optimization.

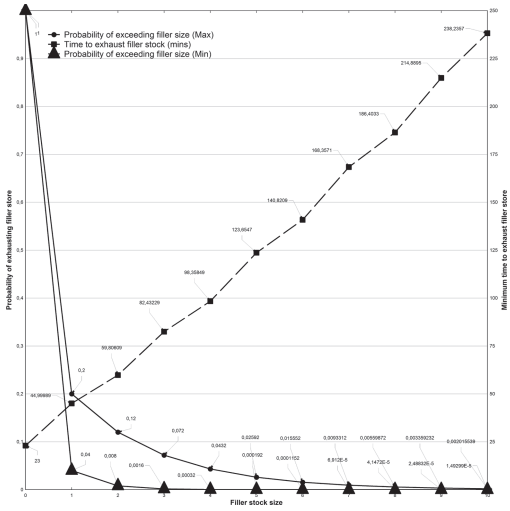


Figure 9. Quantitative safety analysis of the filling process for filler store sizes in the range 0–10.

and information about its stochastic behaviour. This naively-designed production process consists of two processes, Conveyor Belt modelling the actions of the machines on a conveyor belt, and Filling Robot which models the actions of robot which fills the dough with cream, or similar fillings, when needed.

In Figure 9 an analysis of the effect of allocating various amounts of resources to a business process is presented. This provides an assessment of both the probability bounds that a given resource level will lead to resource exhaustion, but also analysis of the non-functional property of the expected amount of time taken to reach such states. This type of provisioning analysis is frequently part of regulatory requirements for the introduction of new technologies (e.g. in the medical field (International Organization for Standardization 2003)) and the ability to perform this in an exact and automated fashion has been of considerable value to the project's industrial partner.

For the production process described in Figure 8 it would be desirable to see an improvement in the time taken for a conveyor belt machine to complete baking a cake. This is in other words the optimisation goal. Further, it would also be desirable that the rate of filling consumption and the consequent probability, given a specific filling stock size, of running out of the filling is kept as low as possible. This is the second optimisation goal.

In addition to the optimisation goals, a number of functional requirements exist for this process (formally expressed using the temporal logic PCTL in SBOAT). These requirements describe the sequences the steps the process have to be in:

1. The baking of the dough should take place before the leaving process of the dough.
2. All dough making, leaving, cut and filling, must take place before a cake is packed.
3. The conveyor belt machine cannot pack the cake before it has received filling.
4. The Filling Robot must ensure that a filling has been prepared and measured before it is sent to the conveyor belt.
5. When the conveyor belt determines that a bad dose of filling has been received it must immediately request a new dose.

Note that the final functional requirement (item 5) is not currently satisfied by the initial *BPD* shown in Figure 8.

Figure 10 illustrates one possible outcome of applying our optimisation methods to the BPD shown in Figure 8. Specifically, this is the outcome of 28 generational improvements of population size 500 of the process. Note that the new functional requirement (item 5) is now satisfied. In the case of this example the rates for sequencing and parallelising are set so that the Mutate function ensures that considerably more re-sequencing modifications are performed than parallelisation modifications.

In this run of our optimisation method we have identified two opportunities to parallelize actions. Within the Filling Robot process, the filling can be prepared and measured at the same time. In the conveyor belt process, it is possible to prepare

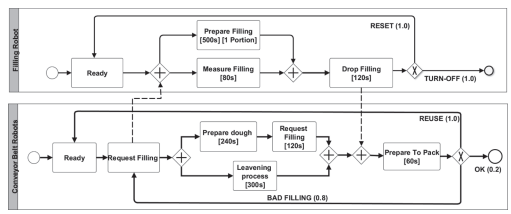


Figure 10. BPD model of a baking system after 28 generations of optimisations with a population size of 500.

dough and cut it while the dough simultaneously leaves. In both cases this saves time, as when performing actions in parallel only the path with the slowest behaviour is counted towards the parallel sections contribution to the reward value.

We have also determined that, in this simplified example, the conveyor belt process always orders filling to finish the cakes but the conveyor belt machines must wait while the *Filling Robot* performs its operations and then returns the filling. As the filling will inevitably be needed, and only the packing of the cake needs to be done after the dough has been made, it is within the functional requirements for the process, and results in a considerable time saving to order the filling immediately before even preparing the dough. This ensures that there will be no delay imposed on the *Conveyor Belt* process by the actions of the *Filling Robot* process. This simplified optimisation example does not violate the functional requirements and results in a significant reduction of the time taken for the execution of the production process.

Existing languages for the modelling of business processes such as BPMN or UML activity diagrams lack a formalised semantic basis (Börger 2012, Recker, Indulska, Rosemann, & Green 2005) which would enable formal analysis and subsequent automated scheduling. Further, these languages do not allow for modelling stochastic behaviour or provide mechanisms to effectively track the consumption of resources during execution. These aspects are therefore the key strengths of this optimisation method as no other method, to our knowledge, has all these features. Further, it should be noted that our method by employing the PRISM tool calculates exact values. However, this need for precision also means that a disadvantage of our approach is that it requires detailed knowledge of the workflow processes being optimised. Another disadvantage of our method is that to use the optimisation schedule in practice great computing power is needed which can be both expensive and time-consuming. However, our method allows for automatic optimal scheduling with mathematical precision and within specific parameters which can help organisations limit waste of, for example, energy or material as well as optimise production with regard to parameters such as time, human resources and cost.

6 SBOAT PERFORMANCE

In line with PCTL model checking theory, the model checking problem is polynomial in the size of the system statespace S. Furthermore, the translation of BPDs to PRISM models while subject to polynomial growth, constitutes only a small fraction of the time taken to perform model checking. Testing of the SBOAT tool, where the largest model explored has a million BPD elements and exhibits on average 1.5 two-way message exchange between BPD pools and features at most three parallel regions within each pool. This level of parallelism seem to reflects a scaled up version of the typical business processes encountered by the industrial partner.

As is common for evolutionary algorithms the time taken to perform each optimisation search is highly unpredictable, the focus in the design of SBOAT is on doing several optimisation searches in parallel, limited by the complexity of each individual model checking run. As the individual searches are completed, their results are compared, and if no significant improvement is being discovered, the pathologically slow searches are terminated. A plot of the average time taken to perform analysis at each generation along with the associated average statespace size is shown in Figure 11.

It is clear from Figure 11 that the analysis times are highly unpredictable, and as subsequent generations are constructed the variance of the model checking time increases. The linear growth in the upper bound of the model checking time taken for each variant implies a linear growth in the computational resources required to perform this analysis. For example, production of the plot in Figure 11 required the use of 512 CPU cores on the Microsoft Azure cloud platform. In addition, the analysis was set up so that when 80% of the cause checking a given population had fallen idle, generation of that population was terminated.

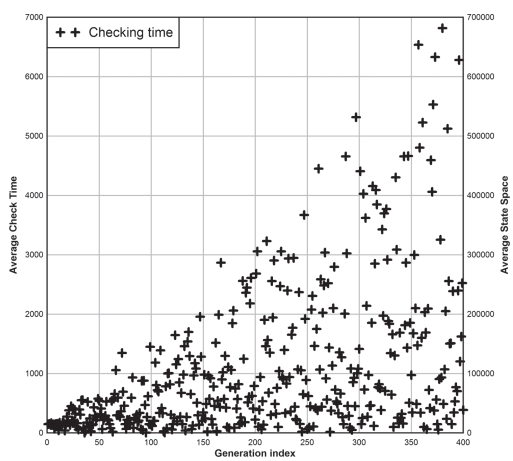


Figure 11. Optimisation analysis performance for a standard BPD with 1000 elements and a population size of 512 per generation. This plot is produced over combined analysis runs where $r_{resequence} \in [0.25, 0.65]$ and values of $r_{parallelize} \in [0.1, 0.2]$.

The focus of efforts to obtain more reliable performance from the optimisation approach is to employ *parallelisation* of individual model checking runs. In particular, the number of evolutionary generations produced and the population size of each generation dictate the average run time. Tuning these values to closely match the available computational resources in terms of parallel processing units (e.g. CPU cores) available provides significant speed up if all processing units can be kept busy. Experimentally extending child generation runs such that they terminate when a threshold fraction of parallel processing units become idle leads to overall reductions in run time at the expense of greater variance in convergence time. This approach leads to generally better results, both in terms of convergence and degree of improvement, than the naive alternative where, as fitness checking of each individual variant in a generation are completed, results are compared, and if significant improvement is not discovered, the pathologically slow searches are terminated. This seems to be due to the fact that while obviously incorrect models can quickly be determined to be incorrect, an individual long model checking run is a sign that no property violation has yet been found and may likely be a good candidate process for the next generation.

In practical use once an optimisation run has been completed, in the SBOAT tool, the final optimal BPD is rendered and displayed to the user.

7 CONCLUSIONS

In this paper we have presented an approach to analyse, enhance the safety of and optimise production processes using the software tool SBOAT. This tool presents an automated approach to restructuring of processes and allows practitioners to create processes which are safer and more efficient, based on the input they give to the tool. For a business practitioner, this input involves defining a model of a business process in the Core BPMN language, annotating the model with the resource consumption of each task, and choosing goals for the optimised derivative of the original process. The practical utility of this approach is demonstrated by means of a case study. The case showed that the framework could be used to reduce the risk of exhausting resources during production, and the impact in quantitative terms, of reaching these critical states (e.g. when a production stop occurs).

The key strength of this approach is the mathematical foundation for designing, analysing and improving production processes in a single unified framework. The SBOAT tool produces processes which are safer and more efficient given an initial process, quantitative properties and a goal for the final process. This is a fully automated approach, where the main constraint is the computational resources available to determine possible future configurations.

Further research will focus on refining the analysis framework and the software tool, SBOAT. Specific focus areas are the refinement of the evolutionary algorithm and extending SBOAT to include other graph-based languages.

REFERENCES

Aalst, W. (1997). Verification of workflow nets. In P. Azèma and G. Balbo (Eds.), *Application and Theory of Petri Nets 1997*, Volume 1248 of *Lecture Notes in Computer Science*, pp. 407–426. Springer Berlin Heidelberg.

Alur, R. & T.A. Henzinger (1999). Reactive modules. *Formal Methods in System Design 15*(1), 7–48.

Baeten, J. (1993). The total order assumption. In S. Purushothaman and A. Zwarico (Eds.), *Proceedings of the First North American Process Algebra Workshop, Stony Brook, New York, USA, 28 August 1992*, Workshops in Computing, pp. 231–240. Springer London.

Baier, C. & J.-P. Katoen (2008). *Principles of Model Checking*. Cambridge MA, USA: The MIT Press.

Börger, E. (2012, July). Approaches to modeling business processes: A critical analysis of BPMN, workflow patterns and YAWL. *Software and Systems Modeling (SoSyM) 11*(3), 305–318.

Christiansen, D.R., M. Carbone, & T. Hildebrandt (2011). Formal semantics and implementation of BPMN 2.0 inclusive gateways. In M. Bravetti and T. Bultan (Eds.), *Proceedings of the 7th international conference on Web services and formal methods*, Volume 6551 of *Lecture Notes in Computer Science*, Berlin, Heidelberg, pp. 146–160. Springer-Verlag.

Cormen, T.H., C.E. Leiserson, R.L. Rivest, & C. Stein (2009). *Introduction to Algorithms, Third Edition* (3rd ed.). The MIT Press.

Gallaher, M.P. & B.M. Kropp (2002, May). The economic impacts of inadequate infrastructure for software testing. Planning Report 7007.011, NIST, Gaithersburg MD, USA.

Gilbreth, F.B. & L.M. Gilbreth (1921). *Process Charts—First Steps in Finding the One Best Way*. New York, NY: American Society of Mechanical Engineers (ASME).

Hansson, H. & B. Jonsson (1994). A logic for reasoning about time and reliability. *Formal Aspects of Computing 6*(5), 512–535.

Herbert, L. & R. Sharp (2012, July). Quantitative analysis of probabilistic BPMN workflows. In *ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (IDETC/CIE2012)*, ASME Conference Proceedings, pp. 509–518.

Hoare, C.A.R. (1983). Communicating sequential processes. *Communications of the ACM 26*(1), 100–106.

International Organization for Standardization (2003). Medical devices: Quality management systems—requirements for regulatory purposes. ISO 13485.

Kwiatkowska, M., G. Norman, & D. Parker (2011). PRISM 4.0: Verification of probabilistic real-time systems. In G. Gopalakrishnan and S. Qadeer (Eds.), *Proceedings of the 23rd International Conference on Computer Aided Verification (CAV'11)*, Volume 6806 of *Lecture Notes in Computer Science*, London, UK, pp. 585–591. Springer-Verlag.

Ling, S. & H. Schmidt (2000). Time petri nets for workflow modelling and analysis. In *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, Volume 4, pp. 3039–3044 vol.4.

Muehlen, M.Z. & J. Recker (2008). How much language is enough? theoretical and practical use of the business process modeling notation. In *Proceedings of the 20th international conference on Advanced Information Systems Engineering*, Conference on Advanced Information Systems Engineering 2008, Berlin, Heidelberg, pp. 465–479. Springer-Verlag.

Netjes, M., H.A. Reijers, & W.M. van der Aalst (2000). Supporting the BPM lifecycle with FileNet. In T. Latour and M. Petit (Eds.), *EMMSAD Workshop at the 18th International Conference on Advanced Information Systems Engineering (CAiSE'06)*, pp. 497–508.

Object Management Group (2011a, January). Business Process Model and Notation (BPMN) 2.0. Standards Document formal/2011-01-03, Object Management Group, Needham MA, USA.

Object Management Group (2011b, August). OMG Unified Modeling Language (OMG-UML), infrastructure. Standards Document formal/2011-08-05, Object Management Group, Needham MA, USA.

Organization for the Advancement of Structured Information Standards (OASIS) (2007, April). Web Services Business Process Execution Language (WS-BPEL) version 2.0. Standards Document WSBPEL-v2.0-OS, Organization for the Advancement of Structured Information Standards (OASIS).

Ouyang, C., M. Dumas, & A. H.M.T. Hofstede (2007). Pattern-based translation of BPMN process models to BPEL web services. *International Journal of Web Services Research 5*(1), 42–62.

Ouyang, C., M. Dumas, A.H.M. ter Hofstede, & W.M.P. van der Aalst (2006). From BPMN process models to BPEL web services. In *Proceedings of IEEE International Conference on Web Services*, Washington, DC, USA, pp. 285–292. IEEE Computer Society.

Parker, D.A. (2003). *Implementation of symbolic model checking for probabilistic systems*. Ph. D. thesis, University of Birmingham, Birmingham, United Kingdom.

Peterson, J.L. (1981). *Petri Net Theory and the Modeling of Systems*. Upper Saddle River, NJ, USA: Prentice Hall PTR.

Prandi, D., P. Quaglia, & N. Zannone (2008). Formal analysis of BPMN via a translation into COWS. In *Proc. of the 10th international conf. on Coordination models and languages*, COORDINATION 2008, Berlin, Heidelberg, pp. 249–263. Springer-Verlag.

Pugliese, R. & F. Tiezzi (2012). A calculus for orchestration of web services. *Journal of Applied Logic 10*(1), 2–31.

Recker, J., M. Indulska, M. Rosemann, & P. Green (2005). Do process modelling techniques get better? a comparative ontological analysis of BPmn. In B. Campbell, J. Underwood, and D. Bunker (Eds.), *Proceedings 16th Australasian Conference on Information Systems*, Sydney, Australia. Australasian Chapter of the Association for Information Systems.

Ross, J.W., P. Weill, & D.C. Robertson (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Cambridge, MA: Harvard Business School Press.

Scheer, A.-W. & M. Nüttgens (2000). ARIS architecture and reference models for business process management. In W.M.P. van der Aalst, J. Desel, and A. Oberweis (Eds.), *Business Process Management, Models, Techniques, and Empirical Studies*, Volume 1806 of *Lecture Notes in Computer Science*, pp. 376–389. Springer.

Tumay, K. (1995). Business process simulation. In *Proceedings of the 27th conference on Winter simulation*, WSC '95, Washington, DC, USA, pp. 55–60. IEEE Computer Society.

Vergidis, K., A. Tiwari, & B. Majeed (2008, January). Business process analysis and optimization: Beyond reengineering. *IEEE Transactions on Systems, Man, and Cybernetics, Part C 38*(1), 69–82.

White, D.J. (1993). *Markov decision processes*. New Jersey, USA: John Wiley & Sons.

White, W.J., A.C. O'Connor, & B.R. Rowe (2004, May). Economic impact of inadequate infrastructure for supply chain integration. Planning Report 04-2, NIST, Gaithersburg MD, USA.

Wong, P.Y.H. & J. Gibbons (2009). A relative timed semantics for BPMN. *Electronic Notes in Theoretical Computer Science 229*(2), 59–75. Proceedings of the 7th International Workshop on the Foundations of Coordination Languages and Software Architectures (FOCLASA 2008).

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Research on information system and its impact on distribution process of supply chain

E. Pawlak
Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

ABSTRACT: Present economic development, growing competition on the logistic services' market as well as the fast pace of life and work of people lead to numerous problems emerging at all stages of the distribution system. This paper presents a new approach to the problem of organization and maintenance of distribution processes in state of reliability in the context of the accompanying information system. Considerations were carried out on the basis of real logistics system consisting of 13 points, dealing with all logistics services. Detailed study involved national groupage service and the quality and quantity of concluded contract of carriage in terms of an offer made to the client. Moreover focus was put on the analysis of types of defects, reasons of their occurrence and their consequences in the system. Results of the research will be used to develop procedures for conduct of damaged shipments in the sense of the information.

1 INTRODUCTION

Nowadays, when determining the level of logistics service the majority of attention is focused on price and quality of service. The subject and the range of research were determined based on own experiences and observation during the several years of work in logistics companies and after studying many publications from the logistics field.

The subject for observation and reflection are the actions—operating processes occurring inside the elements of the logistics system which are in the logistics and distributions companies. To the research adopted the concept of system in which it is treated as the internally correlated arrangement of the elements, which have a specific structure of the actions, a collection of methods of operation and rules of the organization, which fulfill a specific function and which are isolated from the environment for a specific purpose (Nowakowski 2011). As well to the research was adopted the main standard for company's services according to Mr. Christopher's definition—the main standard of service, what should be pursued in the company, is one hundred percent compliance with customer expectations.

The above assumptions and maintenance the system of capable of reliability is a goal to be achieved in the operation of objects and processes in the logistics system. In the literature can find many definitions of reliability referring to the technical objects and to carrying out operations and processes.

Adequate to the tests carried out, is the definition of according to which system reliability it is the ability of the system to undisturbed continuing implementation of tasks in support of the processes within the supply, transportation, maintenance and operation of infrastructure (Nowakowski 2011).

Equally important to the conducted research is the definition formulated in 1994 by L. Johansson, according to which maintenance the system of capable of reliability requires that all participants in the supply chain are adequately informed.

Should remember that points of contact and the information flow between different cells of supply chain are critical elements for the final results of operation in supply chain management (Rutkowski 2004).

Although issues regarding to the distribution network are treated in the literature very broadly was discovered the absence of full studies and research on the information system and its significant role in the network. Another reason for interest in the subject was to determine the absence of a comprehensive, dedicated tools to assess the quality and quantity of information in the system, despite the many existing and functioning market solutions.

2 RESEARCH AND ANALYSIS

The studies included actual distribution systems of logistics operator 3 PL which is involved in the logistics services, warehousing and distribution of goods nationwide. The study proved to be laborious

and time-consuming, because the test object consisted of 13 elements—local branches—with different degrees of automation, abundance of staff, object class, technical equipment and sequence of use and the validity in the structure of the whole logistics system. It has been observed that in each of the surveyed local branches which are obliged to maintain the designated level of reliability, are serviced from a dozen to several dozen commercial customers who have different requirements for the level of quality limit, efficiency, productivity and service efficiency and even in some cases they have the different, dedicated price lists.

In each object point of the distribution network there are different processes based on one of the computer systems. It has been observed that the service inside the terminal looks different at different logistic points due to the level of technological development of the object, i.e. the type and number of discharge gates, object class, the means of internal transport, the agreed method of aggregation data, the number of personnel needed to handle the stream of cargo both to the processes of loading and handling as well as to realise administrative and customer services. Also were observed different staff work schedules which are determined depending on the number of supported orders. These problems have not been undertaken because dimensioning and shaping logistics facilities were not be the purpose of research.

Detailed study covered included handling of groupage services and the quality/reliability of the national product in logistics network relative to an comercial service offer for the client. The study took into account only domestic groupage network system so only the parcels or consignments whose size do not exceed the permissible total weight of 4500 kg and the total number of cargo to 8 pallet (pallet space is defined as an field about the basis 1.2×0.8 m).

To the tested distribution network was developed diagram of a cargo flow (Fig. 1), which shows the fixed connections between successive points of the network, which are called the linehaul connections, and the two-stage linehaul connections, i.e. cargo flow lines with a double transhipment. Number of linehaul connections is the result of the economic viability specified for each linehaul, which is determined on the basis of fulfillment of vehicles, the transport distance, numbers of operations on the cargo, destination, cargo volume sended by external customers and their location.

Each of the points of the network—terminal—has its own local distribution area, territorially limited to a designated zone around its location. Distribution in this zone corresponds to a closed set of postal codes assigned to the network. Zones for network points are separable.

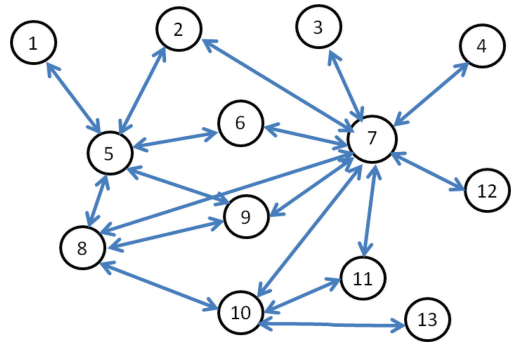


Figure 1. Diagram of a cargo flow for studied distribution network.

The customers are the sources of the flow of cargo. For the logistics terminal were defined sources dependent of the client location and kind of client loads:

- External—load derived from "its" customers located geographically close to the location of the point of logistics network.
- Internal—generated by the other points' customers to distribute in the local area.
- Storage i.e. customer of storage/load storage—loads from one's own area of high storage to distribute.

How to handle shipments and transmission of information depends on the type of customer and contractual requirements. The study included external and internal customers.

Tested, observed and compared the internal processes at each point of the logistic network, keeping in mind that a properly designed internal processes are affecting for reduction of time of cargo handling, the use of a smaller number of technical and human resources and, consequently, for reduce the costs of the whole logistic system and thus for increase the profitability of point-objects. From the made observations the conclusion was drawn, that the internal organisation of each points of logistic network should be constantly monitored and depending on the changing needs, it should be improved to minimize the losses of orders and congestions of internal movements. Also should remember about impact the reliability of individual points on the reliability of the entire logistics system.

Based on many hours of interviews and observations at the time of the collection of information on the operation and organization of the company, the study of literature developed a number of models, with particular emphasis on modeling information system. Starting the modular modeling of

the logistic system, which include the information system, was taken into account that it has an hierarchical structure. In the beginning the system was shown as a black box—Figure 2.

Delving into the layers can reach the information units constituting the information/messages which are transmitted in the system regardless of the media. The following presents only three selected representations of the developed few-layers model of the information process accompanying the distribution processes in the logistic and transport company. This process is part of the enterprise information system. Because all aspects of the business profile of organization did not lay in the area of interest in research, was applied simplification—have been omitted penetrating steps between the general model of an information system of the studied company (Fig. 2), the information system model of the tested logistic object (Fig. 3) and model of an information subsystem of the service of groupage distributions (Fig. 4).

It was considered that the model shown in Figure 4 can be regarded as a universal model of information process accompanying the implementation of groupage transport service in terms of the transaction, because they do not take account of the specific organizational structure of the company and only her functionality. When determining of the model's modules were taken into account only the consecutive points/stages/units as stages chain of transfer of informations. They were described only by slogans. It was considered that the customer for a company which provides logistic and transport services LCL is the sender (client) of consignment/load. He is the one who

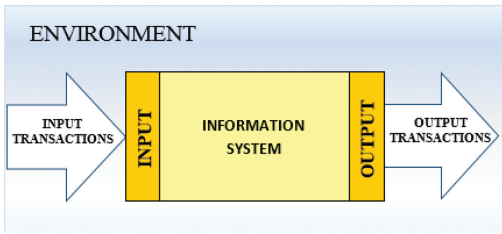


Figure 2. The general model of an information system of the studied company.

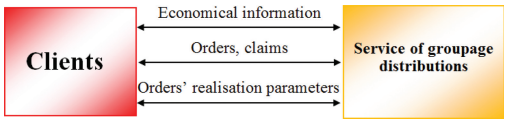


Figure 3. Model of information system of the tested logistic object.

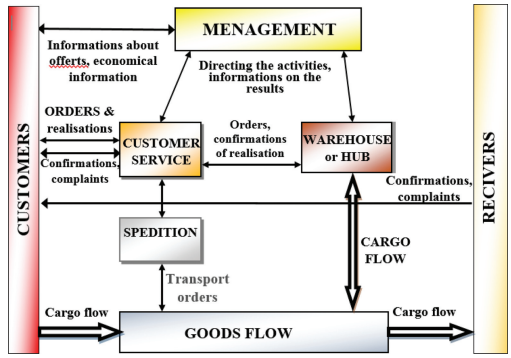


Figure 4. The structure of the object "Service of groupage distribution".

sets the needed conditions of logistic service and with whom is carried out the final financial settlement. For the tested subsystem of information the customer (sender) is as the initiating unit which initiates sending information and a whole process. For a presented model were developed graphically models of its modular components. After the development of the modular model of the system to the desired level of detail it was possible to start next step of analysis.

During the 6—months studies collected detailed data on the customer service for 980 clients in the form of an extensive database. Hundreds of thousands of data were collected for supported consignments and related with them processes and customers, inter alia were collected data on 143 978 consignments. After research the data were subjected to treatment. Work was begun from ordering of data, their selection and appropriate aggregation, and then were prepared the systematized results needed for further analysis in the form of an extensive database. Table presented below is an example of obtained results carried out at this stage of work. The fragment of database (Table 1) contains aggregated and sorted data on the number and type of errors observed in the selected time period—e.g. during 1 month.

Upon completion of this phase of work were started analyzing the examined objects and processes focusing on information system and his proper functioning, the used tools and the system's operators (the people). An additional effect the 6-month's studies of the distribution network was to design and develop a set of reports for qualitative research and quantitative distribution system. Were classified the most common errors in implemented services with their assessment of the cost—Table 2.

Based on the results of research on a sample of 24,913 orders in one month classified and specified

Table 1. Number and type of errors during 1 month.

	Wrong classification of pallets	No dock. transport and/or WZ	Incomplete information from the customer	Incorrect shipment dimension	Inadequacies of the system	Errors during emergency procedures	Unrealized service	Responsibility of distribution	Others responsibility	Shipments
OD1	23	32	47	64	178	13	70	28	42	3372
OD2	11	28	10	43	62	1	51	37	14	1224
OD3	8	11	8	21	24	0	12	7	5	513
OD4	49	41	47	85	278	37	74	17	57	1084
OD5	39	32	67	81	211	31	140	53	87	3293
OD6	2	5	6	3	8	1	4	4	0	993
OD7	41	59	47	77	239	19	146	75	71	5605
OD8	23	32	31	64	65	2	39	35	4	822
OD9	16	17	15	21	38	2	7	7	0	586
OD10	73	65	41	49	115	12	93	87	6	817
OD11	51	42	51	51	254	17	68	52	16	3461
OD12	12	4	41	17	78	7	9	6	3	1493
OD13	28	7	21	64	81	0	26	11	15	1650

the actual error participation in the flow of information in the consecutive paragraphs of network OD1-OD13 what shown on the graphs (Figs. 5–6).

For the analysis of errors in the system and evaluate the system reliability were used the event trees, which are the graphical cause-and-effect relationships models occurring during the solving problems and are built from the initiating events. Trees represent all the possible sequences of events that are initiating events consequence and allow to specify the probability of an adverse event.

In the researches were used them both for qualitative analysis to understand the situation which affected reliability problem, and for quantitative analysis to determine the probability of sequences of events. It is noted and accepted as an assumption for research, that although the observed processes and their service in each of the objects may vary, criteria relevant to the reliability of the information system are the same. From the analysis of the research presented in Figures 5–6 shows that the biggest distribution network problems are the incorrect data in the system generated by both external customers (data input to the operator system via the internet) and employees of the operator (direct manual data input to the system via computer workstation).

Conducted qualitative analysis of the information system allowed for define the cause-and-effect relationship of the system, identify the forcing factors and excess and deficiency of functional information that can lead to transition the system into a state of temporary or total inadequacy of the system.

On the basis of observations and studies were shown that compliance with procedures, regulations and technical specifications by a single element of the system does not ensure safety process as a whole. Permit on the occurrence of an adverse event in the flow of information accompanying to the groupage system, can lead to economic and structural losses.

During the research of the information system of the test object were developed and analyzed event tree of accompanying the flow of information during the execution of the contract for the transport of cargo groupage service. Figure 7 shows the idea (tree) of the system. Then were developed some of its components, i.e., tree branches, which in the figure are in the form of complex event symbols. For the study assumed 100% reliability of customer service module, forwardings module, warehouse and transportation services module, which means that they not generate their own's errors, which affect the reliability of the whole system. The probability of errors appearing on their outputs is only as result from processing incorrect data input put into the individual modules. In the analysis the basic events were data from the offers and price lists.

Table 2. Costs of errors occurred.

Classification of errors associated with the direct transfer of information:	Implications for the logistics chain	Cost of errors occurred
Lack information transferred between branches	Perfunctory information in the system	Decrease KPI/freight cost/ contractual penalty
Wrong information given—bad tracking number, wrong time of monitory note, supplying incorrect data	Incorrect execution of the service	Decrease KPI/freight cost/ contractual penalty
Missing or incorrect information transmitted from the driver	Incorrect execution of the services giving rise to the complaint	Decrease KPI/freight cost/ contractual penalty
Lack information on the fate of the consignment (omission consignment in the verification process of cargo flow)	Failure to perform the services	Decrease KPI/freight cost/ contractual penalty
Lack confirmation of delivery consignment in the system (loading terminals, recipient)	Re-verification of information	5 PLN/event
No information about the problems in distribution—damage, theft, loss of shipment delays	Re-verification of data and recovery of documents confirming the execution of the service	Decrease KPI/freight cost/ contractual penalty/costs of complaint proceeding
Transmission of incorrect dimensions of the shipment by all subsequent chain links	Re-labeling and specify appropriate dimensions, enter correct data into the system	Re planning and transport of the consignment

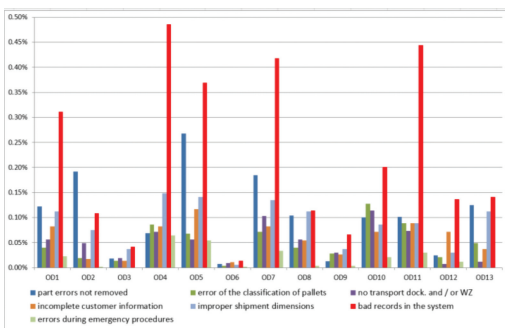


Figure 5. The number of the classified errors broken down on the points of the distribution network.

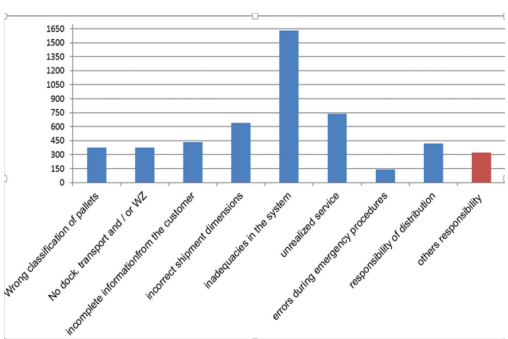


Figure 6. The monthly number of classified errors in the tested groupage network.

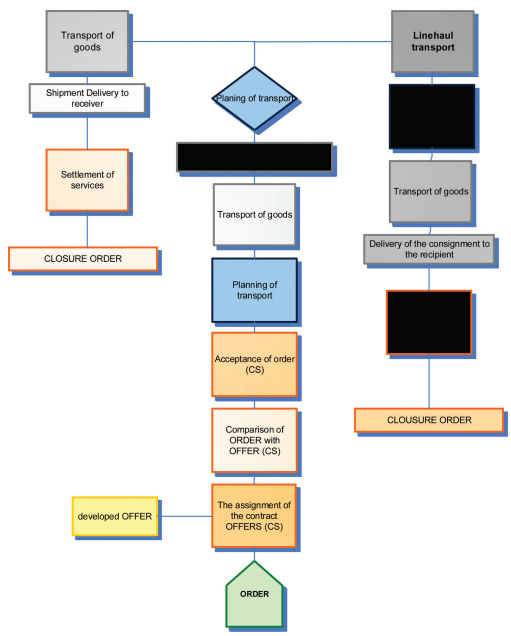


Figure 7. Event tree of information flow accompanying to the handling of the order of groupage service.

The task of a good sales representative is to prepare the satisfactory offer for the customer. But not only. The offer must be done on time and must guarantee a high quality of service, but also make a profit to the company. Disorders in achiev-

ing the above purposes are treated as a system failure. Each Offer should be carefully calculated and refined in detail. The ideal would be automatical create individual offers and service pricing.

Pricing dedicated for the Customer should include: the prices for transport services in accordance with the assumptions and broken down into areas of distribution (unit prices on 100 kg/m^3/ palete), the prices for additional services, price for redelivery of the Customer's fault, the cost of shipment canceled before issuing a driver, fuel surcharge and Viatoll. For the system study, it was assumed that the price list is optimal, and the proposed prices include all costs and founded profit. In the future the process of developing price list should optimize to create it in electronic/system version so that will be possible its processing in TMS (Transportation Menagement System) and CRM (Customer Relationship Manage-ment). Every time must be check the compatibility of each order received from the Customer to his the specific offer/contract. Lack of verification may result in the financial losses of a logistics operator and result in reduction in quality and thereby lead to the unreliability of the system.

Example of the process of verification the information in the contract with the information from OFFER shows Figure 8. It is process comparing information about the correct type of transported goods. All subtrees illustrating the processes dedicated comparing the other informations in the Contract with the corresponding informations from the Offer looks like the event tree on Figure 8.

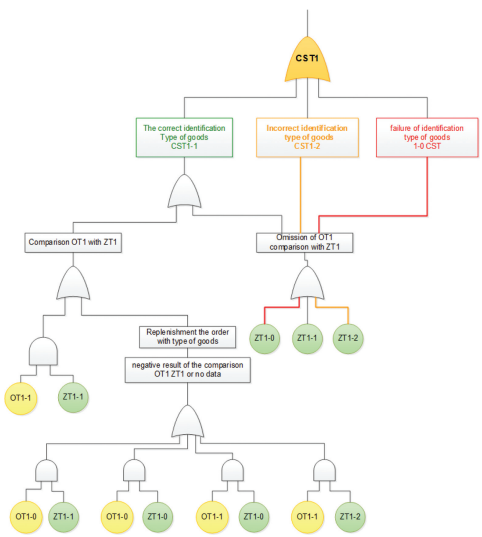


Figure 8. Process of comparing information about the correct type of goods (comparing ZT1 z OT1).

The operational staff of transport departments of (freight forwarders and dispatchers) is interested in:

- freight route—attributed to the location of pick up the shipment and where is to be further forwarded, other the next point of transshipment, or for distribution,
- Physical size of the freight—size and weight of the cargo in order to choose means of transportation and planning its fulfillment

Only on the basis of the above information may be chosen the means of transport, to plan his route, loading and transport to the recipient. The more detailed the data it is the higher the quality of service and lower costs associated with its implementation. Outline of the processing information for the freight forwarding is shown in Figure 9. The explanation to the symbols shown in Table 3.

After made the analysis of qualitative information system and studies the actual parcel distribution system made it possible to carry out quantitative analysis to determine the probability of adverse events resulting in a decrease in quality of service. Only on this basis can be shown that the accurate and timely flow of basic information (the offer and contract) has a significant impact on the maintenance of the system in the state of reliability.

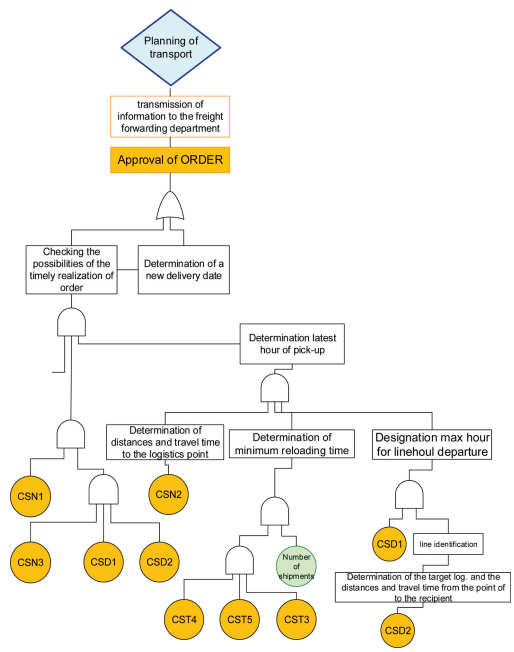


Figure 9. Tree of the processing information for the freight forwarding.

Table 3. The symbols—the information necessary for further processing.

Output	Information on the output
CST1	Type of good
CST2	Temperature conditions
CST3	Type of pallet
CST4	Height of the load unit
CST5	Weight of the load unit
CSN1	Time of order
CSN2	Place of pick-up
CSN3	Date and time of pick-up load
CSD1	Date and time of delivery loads
CSD2	Place of delivery

The analyzes carried out were the next step in the study of the role and importance of information flow in distribution groupage transport service networks. Through its research and analysis has become possible to carry out and to identification the initiating factors and to diagnostic the shortage and the excess of informational-functional in the information system. They could cause the element of logistics system could pass in a state of temporary or total disablement from the point of view of the tasks and logistics processes and organizational problems measured in terms of the customer expectations levels. The work has begun on the next stage, which will be to develop methods of assessment information system and its computer's implementation to the knowledge base of the expert system.

After final completion of the work will be possible to identify tools that streamline and improve the flow of information.

3 RESUME

The research and analysis made it possible to draw the general conclusion, that the reliability of the distribution system could be achieved through the elimination or significant reduction of errors in the information system. The qualitative studies demonstrated directly proportional information system status impact on the status of distribution groupage system.

Therefore it was concluded that the reduction of errors in the functioning distribution systems can be achieved by reducing the occurrence of errors in the information system. In order to improve the reliability of the system should be determined categories of the most common errors in it, their causes and the areas in which occurs and carry out an analysis qualitative and quantitative, to diagnose the causes and effects of errors in the information system.

Define them, and then to monitor and react to current changes have a significant impact on the reliability and quality of groupage transport services. In fact the well done analysis of errors in information system make it much easier to identify needs and areas for intervention, reorganization and formalization. In a word, such an analysis is a tool for management, significantly affects the growth of service quality, and consequently on the achieved economic results of the company and customer satisfaction, i.e. affects the economic situation of the company and its market position.

REFERENCES

Christopher M. 2000. Logistics and Supply Chain Management. Strategies for reducing costs and improving service levels. II edition, Warsaw, PCDL.

Ciesielski M.2006. Instruments of logistics management. Warsaw, PWE.

Gołembska E., Szymczyk M.1997. Computerization of logistics enterprises. Warsaw, PWN.

Gumiński R, Lubikowski K., Pawlak E. 2013, Influence of detects of selected elements of the distribution system on realiability of logistics processes Scientific Papers of the Institute of vehicles, 4 (95)/2013.

Jacyna M. 2009. Modeling and evaluation of transport systems, Warsaw, Publishing House of Warsaw University of Technology.

Kaźmierczak P. 2009. Errors in barcodes—significant impediments to the efficient operation of the supply chain, Packaging No. 11/2009,Sigma-Not.

Nowakowski T. 2011. Reliability of logistics systems, Wroclaw University of Technology Publishing House.

Nowakowski T., Werbińka S. 2009. On problems of multicomponent system maintenance modelling. International Journal of Automation and Computing, vol. 6, nr 4, pp. 364–378.

Nowakowski T. 2004. Problems of reliability of logistics systems„ Engineering machinery, vol.9, issue 1, Wrocław, Publishing House of the Wrocław University of Technology.

Radkowski S. 2005. Basics of safe technology, Warsaw, Publishing House of the Warsaw University of Technology.

Rutkowski K. 2004. Supply Chain Management—an attempt to clarify the term and definition of trade logistics. Materials Management and Logistics, 12/2004.

Siergiejczyk M. 2008. The possibilities of using virtual private networks in the management of transport companies, Theses of Transport (64), Warsaw, Publishing House of the Warsaw University of Technology.

Szopa T. 2009. Reliability and safety, Warsaw Publishing House of the Warsaw University of Technology.

This page intentionally left blank

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Availability and reliability of resources in an agile manufacturing systems

A. Stachowiak
Poznan University of Technology, Poznań, Poland

ABSTRACT: Agility is strategy that allows to cope successfully with dynamics and complexity of contemporary market and to respond to global customers' needs and requirements efficiently and economically. It is based on the idea that a company should respond to customers' needs providing them with products fitting their specific requirements. One of the most important and difficult decisions connected with agile strategy is definition of resources necessary to run various processes and if necessary develop products from the very beginning. After the resources are defined it is necessary to provide their availability and reliability. The aim of the paper is to identify strategy for technical resources management.

Agile approach is discussed in literature, and importance of human factor is stressed, while technical aspects are presented usually in a general way. The research starts with development of methodology for identification of structure of technical resources and their status (own/shared).

Reliability and availability (the scope of the conference) of resources seems to be crucial for ability to run customer-driven processes efficiently.

The expert system is to be designed for resources definition, and based on that reliability-providing strategy is to be suggested.

1 INTRODUCTION

Companies nowadays are facing numerous problems emerging from globalization, advance in technology and communication techniques and more and more sophisticated requirements of customers. These phenomena however are not only sources of risk but also of competitive advantage. Businesses capable of turning dynamics and complexity of contemporary markets into opportunities are potential winners.

Agility is strategy that allows companies to cope successfully with dynamics and complexity of contemporary market and to respond to global customers' needs and requirements efficiently and economically. It is based on the idea that a company should respond to customers' needs providing them with products fitting their specific requirements. One of the most important and difficult decisions connected with agile strategy is definition of resources necessary to run various processes and if necessary develop products from the very beginning. The resources definition is complex and demanding process as resources to be considered are of various character i.e. technical resources, human resources, knowledge, experience, know-how, environment etc. The hereby paper is to present an approach to resources definition to be used for agile manufacturing systems based on pull logic and enabling manufacturing on demand. Such definition of goals and constraints makes the decision model developed useful for companies running unique processes, providing unique or customized products and responding to specific requirements of customers to gain competitive advantage. Resources definition will be followed with capacity analysis and discussion on required level of capacity and costs it generates. Hence, the model is supported with maintenance strategy based on contemporary approach to the field. The tool applied for the final solution is an expert system as AI support seems to be crucial for complex and unique/individual project—author believes that agile manufacturing meets the criteria.

The structure of the paper is the following: the first part includes brief presentation of terms and approaches applied in the model, namely agile manufacturing systems, resources definition, reliability and availability aspects and expert systems brief presentation. The second part is presentation of the model developed with its main assumptions, while the third presents discussion on results obtained, concluding it and introducing further research perspectives.

2 RESEARCH FRAMEWORK

The model to be developed is based on agility paradigm (2.1. *Agile manufacturing*). To achieve

agility, the most important is to manage resources well, and all categories of resources necessary for processes performance should be considered and properly defined (2.2. *Agile resources definition*). To benefit from resources composition, high level of availability and reliability is expected, provided by application of adequate maintenance strategy (2.3. *Availability and reliability*), and finally decisions concerning resources and capacity identification, as well as maintenance profile definition, require support, benefiting from contemporary tools and techniques (*2.4. Expert systems*). The research framework presented briefly shows theoretical assumptions for the model developed.

2.1 *Agile manufacturing*

In their report on 21st century manufacturing enterprise strategy introduced in 1991 at Leigh university (Gunasekaran *et al.* 2002, Emigh 1999) the authors suggest that various production resources, including people, funds, technology and facilities should be integrated and managed as a whole; thus optimizing the utilization of resources and taking full advantage of advanced manufacturing technology and computers. As a result agile manufacture based on dynamic alliance is coming into being so that enterprises can remain competitive in a constantly changing business environment and is becoming a main competitive paradigm in the international market. It is defined as the ability to thrive in an environment of continuous and unpredictable change and profit from rapidly changing, global markets for customized customer-driven products and services.

Since its introduction agility, which has basically two meanings: flexibility and reconfigurability, has become a very important characteristics of a modern manufacturing enterprise. Generally, flexibility aspect refers to ability to make adjustments according to customers' needs, while reconfigurabiliy is the ability to meet changing demands (Li 2009).

Agile manufacturing through flexibility and reconfigurability emphasizes high customization of production, and is viewed as a breakthrough of traditional mass production. An agile corporation is adaptable, and capable of rapid reconfiguration to satisfy quickly changing market demands. Agile manufacturing crosses company borders. Core competencies of organizations can be pooled to satisfy various customer demands and reduce the time to market. One way to establish an agile manufacturing system is to employ agile manufacturing cells as building blocks to take advantage of cellular manufacturing's quick response and ability to accommodate changes in product mix. Cellular manufacturing can produce medium-volume/medium-variety part types more economically than other types of manufacturing systems and surveys affirm that many benefits have been gained from CM implementation including shorter manufacturing lead time and customer response time. This makes CM a logical choice for firms whose strategy is time-based competitive manufacturing.

Each agile manufacturing cell in the agile manufacturing system is capable of manufacturing a part family, and is connected via the internet with other agile cells from different enterprises to seek temporary market opportunities and accomplish manufacturing tasks cooperatively. Manufacturing can take place across organizational and geographic boundaries to exploit distributed resources from different partners in dynamic teams that can be formed quickly in response to rapidly changing market demands. Internet technology is a key to enable distributed agile cells to cooperate with each other by extending traditional information systems and eliminating barriers to integration (Yu *et al.* 2004).

The most distinctive characteristics of agile manufacturing systems include (Devadasan *et al.* 2005, Towill 2002, Golsby 2006)

- human resources characteristics, i.e.:
  - work assigned to multi-skilled, multi-functional and self-committed employees (achieved thanks to continuous, life-long learning,
  - involved employees, giving ideas and knowledge to be utilized in processes, fully empowered,
- management system characteristics, i.e.:
  - flattened, team-managed organization and structure,
  - devolution of authority based on integration and autonomy, learning approach to organization and management,
  - open organization based on partnership with suppliers,
  - responsive and dynamic profile,
  - based on simplified and shortened information flows,
  - providing customer delight,
- technical resources characteristics, i.e.:
  - application of flexible manufacturing systems, with possibility of automation application,
  - enabling flexible and easily collapsible set-ups, resulting in quick response to changes,
  - increasing productivity,
- manufacturing process characteristics, i.e.:
  - dominated by main assembly, following external manufacturing and procurement,
  - based on just-in-time purchase and short delivery cycles,
  - efficient, continuously improving,
  - economical.

There are numerous differences between traditional and agile manufacturing systems. Analysis

of requirements and expectations towards agile systems leads to the conclusion that they can be met only with predefined set of resources at required level of capacity (Stachowiak 2013).

2.2 *Agile resources and capacity*

Resources definition is quite simple—they enable performance, which makes the term broad. Resources to be taken into consideration at this stage of research are: machines and tools, space they need, people, their skill and knowledge.

Traditionally, machines to be used by a company are determined by processes the company is to perform. Analysis of technology applied for products manufacturing (operations, machines, performance and set-up times) allows to define a list of machines needed and their number. As people operate machines, their number is determined by number of machines and work organization (shifts etc).

However, the most important characteristic of a contemporary company is lack of precise data concerning products and technologies. Nowadays demands are difficult to define and that is why it is difficult or even impossible to define resources using traditional procedures. The new approach to resources definition is necessary. The basic assumption of the new approach is that resources are not dependent on demands when modeling a company (Stachowiak 2013). They constitute agile manufacturing system, however their definition is based mostly on strategic assumptions taken when founding a company (Fig. 1).

Agile resources definition is the process in which the most important aspect is definition of corporate strategy including rough identification of scope and range of business activity. Human resources definition should cover all the capabilities potentially necessary to perform company's processes, while technical resources should be defined in a way providing synergy between human and technical elements of the system.

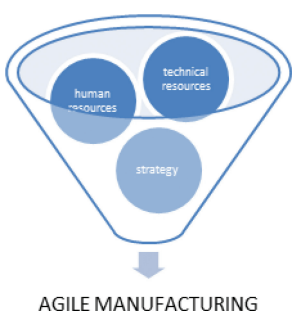


Figure 1. Agile resources definition.
Source: own work.

In a contemporary/agile manufacturing systems products and technologies definition is the first stage of manufacturing process as according to agile manufacturing definition the most important is meeting customers' demands, which results in treating customers as the first and the most important party in manufacturing process. Such cooperation is one of the main assumptions of agility and its consequence is that customers are no longer outside the company—they are integral part of it. They create product with the company and therefore the demands are impossible to forecast—they emerge too late. The beginning of manufacturing process is moved back—from making an order by a customer to stage of understanding the need of the customer. And that is why the demands cannot be the basis to define company's resources. The very first stage of resources definition should be considering ability to perform various processes in order to meet customers' requirements. Thus the kinds of machines should be chosen so that they performed as many processes as possible. The solution then is using either universal machines or as many special/of specific use as budget allows. Either idea is good as the most important resource are not machines but people and their skills.

Defining resources for contemporary company is mostly defining capabilities crucial for company's performance.

Capacity is the size of resources, hence it is traditionally referred only to tangible aspects of resources. As mentioned above it is impossible to define demand in terms of quantity and quality, which results in difficulties with definition of size and type if resources. The approach which can be applied here is definition of capacity based on strategic assumptions and constraints.

Capacity is the sum of human and technical resources:

$$C = \sum_{i=1}^{n} R_{hi} * c_{hi} + \sum_{i=1}^{m} R_{ti} * f_{ti} \quad (1)$$

where:

C	capacity
$i = 1 .. n$	number of employees
Rhi	human resources (employee i)
chi	capabilities of human resources (employee i)
$j = 1 .. m$	number of machines
Rtj	technical resources (machine i)
ftj	functions of technical resources (machine j)

while:

$$\sum_{i=1}^{n} k_{hi} * R_{hi} + \sum_{i=1}^{m} k_{ti} * R_{ti} \leq R_f \quad (2)$$

where:

Rf	financial resources of a company

khi cost of human resources (employee i)
ktj cost of technical resources (machine i)

Setting the capacity at the predefined level requires precise definition of available financial resources as this is the only constraint set. The cost of financial and human resources is defined basing on acquirement cost, maintenance cost, disposal cost and all the aspects applicable (the formula is general).

The formula presented refers capacity to economic and social aspects as capabilities of human resources and costs are considered (Stachowiak 2013).

2.3 *Reliability and availability of resources*

Reliability and availability of resources depends on implementation of proper maintenance strategy.

Availability of the resources depends primarily, on their selection (choosing resources respondent to company's goal and scope) and number, but also on their condition—hence they need to be well maintained so that they were available whenever needed. In agile manufacturing conditions it is especially important as manufacturing jobs are difficult to forecast and plan because of demands volatility and customer-orientation.

Reliability of resources mostly depends on their technical condition resulting in great importance of maintenance operations providing high level of reliability.

According to Narayan (2012), maintenance concerns the combination of all technical, administrative, and managerial actions during the life cycle of an item, intended to retain it in, or restore it to, a state in which it can perform the required function. The conclusion from the presented definition is the following: maintenance is not only technical tasks, such as disassembly and replacement of spare parts, lubrication, and repair. In practice, maintenance has a much wider spectrum involving numerous additional tasks (Jasiulewicz 2013).

The maintenance process is dynamic, as it has strong connotations to manufacturing process, and together with manufacturing process it has been changing over the years. Throughout the years several approaches to enhance the maintenance management have been developed and applied to a wide variety of organizations and systems, (Loska 2012).

The period up to around the 1950s (the end of WWII) was referred to as the "first generation" in maintenance. The feature characteristic for that period was taking up repairs or replacing machines and technical devices only after breakdown happened (so called reactive maintenance). The next generation of maintenance was initiated with the industrialization process. An increased number of machines and devices in companies, and their value, caused an increased interest for managers in lengthening exploitation periods of technical objects. Plans and schedules of preventive actions (e.g., inspections, services, general repairs) were being developed for each company. This generation is now referred to as preventive maintenance. From the beginning of the 1970s, new options for maintenance realization appeared with the development of diagnostic tools and new approaches to corporate management. Particularly, global striving for inventory management based on the Just In Time paradigm, the continuous improvement idea according to Total Quality Management philosophy, and waste elimination according to the Lean Manufacturing approach resulted in changing the approach to the role of maintenance in achieving corporate goals. The term "waste" was crucial for process performance in companies. Including a lean category to maintenance operations resulted in development of the Lean Total Productive Maintenance or Lean Maintenance approach described in literature (McCarthy & Rich 2004, Smith & Hawkins 2004). A combination of the classic approach of Total Productive Maintenance with Lean Manufacturing, as described by Nakajima (1988), enables achievement of predefined results (e.g., higher availability and reliability of equipment, repeatability of production) with a lower requirement for resources (spare parts, tools, energy, human labor) (Jasiulewicz 2013).

One of the latest approaches in maintenance is RCM. Moubray (1997) defines RCM as "a process used to determine what must be done to ensure that any physical asset continues to do what its users want it to do in its present operating context", characterizing RCM as a process to establish the safe minimum levels of maintenance, hence, the objective of maintenance should be to keep the equipment doing whatever its users want it to do, rather than to prevent failures for the sake of preventing failures (Jasiulewicz 2013). This makes the methodology crucial for providing reliability and availability of resources.

RCM methodology (Moubray, 1997) has three major goals:

- to increase safety and reliability of systems by focusing on the most significant functions (RCM is concerned mainly with what we want the equipment to do, not what it actually does);
- to prevent or to mitigate the consequences of failures, not to prevent the failures themselves (the consequences of a failure disagree depending on where and how items are installed and operated);
- to decrease maintenance costs by escaping or removing maintenance actions that are not strictly necessary.

Hence, determining the operating context and what the user wants the equipment to do is the starting point for the RCM process, which is applied by asking and answering the following seven questions (Moubray, 1997):

- What are the functions and associated performance standards of the machine in its present operating context?
- In what way does it fail to fulfil its functions?
- What causes each functional failure?
- What happens when each failure occurs?
- In what way does each failure matter in respect of the environment, human safety, losses, and expenses?
- What can be done to predict or prevent each failure?
- What should be done if a suitable proactive task cannot be found?

These main maintenance policies, rather than being applied independently, are integrated to take advantage of their respective strengths in order to maximize facility and equipment reliability while minimizing life-cycle costs (Jasiulewicz 2013).

2.4 *Expert systems*

There are numerous definitions of artificial intelligence, some more precise and others less. Some of the definitions are focused at psychological approach, while the others suggest that machines perform tasks more efficiently than humans or they are not able to mimic human behavior in an exact way (Rich *et al.* (1991), (Russel *et al.* 1995). In the following paper, the definition by Z. Bubnicki is used. According to this definition, artificial intelligence is a field of computer science, which deals with algorithmization and formalization of processes of thinking and concluding, as well as these of learning, perception, recognition etc. (Bubnicki 1993). As human intelligence is a capability, which allows to process information, solve problems, adjust to new tasks and situations, as well as understand, compare and contrast facts, learn and remember, develop thesis, theories and conclusions, analyze and think creatively (Rutkowski 2006) authors believe, that the definition mentioned above is the one presenting the idea in the best way possible.

The basic methods of artificial intelligence are: expert systems, genetic algorithms (Coley 1991), (Goldberg *et al*. 2003), (Man 1999), neural networks (Kosinski *et al.* (2007)), fuzzy sets (Yen (1998)). Expert Systems (ES) are a discipline of artificial intelligence, which gained numerous practical applications as the first on from the above list (Zielinski 1991). However, practically, hybrid systems are often used, as they benefit from combination of two or more types of systems. What is an expert system then? It is an "intelligent" computer program, which uses knowledge and concluding procedures to solve problems requiring human (expert) experience earned by long-lasting activity in a predefined field (Rutkowski 1991). Hence, the starting point for developing expert system is analysis of the problem to be solved. Undoubtedly, role of an expert (person who knows the field well enough to take efficient actions) at the stage of general design cannot be overestimated.

Expert systems work is based on realizing three basic, independent though cooperating modes i.e. knowledge base, concluding machine (concluding mechanism) and user's interface (Bubnicki 1993). However its structure may vary. It mostly depends on its application (Knosala 2007). Generally, expert system works thanks to implementing expert's knowledge to the knowledge base, defining concluding mechanism based on information available and designing user's interface to enable communication (Rutkowski 1991). Knowledge base of an expert system includes facts and rules and while facts information which is accepted and can be used by an expert, rules are logic phrases, which lead to new facts definition and enable solving problems defined.

Application of ES leads to numerous benefits for an enterprise (Pawłyszyn *et al.* 2010), (Pendersen *et al.* 1997). which makes them really popular managerial tool (Chwiałkowska *et al.* 1991) as they provide companies with much cheaper expertise comparing to "real" experts; they work much faster than experts, which results in cost and labor savings; they improve quality of expertise thanks to consequent concluding and smaller number of made mistakes; they provide higher flexibility of production and customer service and reduce time of work, which is expensive; they usually react faster than experts, especially when the problem solving requires operating with large quantities of data; they enable solving complex problems, too difficult for an individual or requiring knowledge larger than that of one man.

Expert systems are used in almost every area of human activity (Chwiałkowska *et al.* 1991), performing lots of activities supporting human activities. However, each area requires different, individual and often unique expert system, which should be constructed by analysis and gathering data in the predefined field, choice and application of proper concluding methods (concluding machine) and, in the end stage, designing an interface to enable communication between users and computers. More detailed description of stages of expert system construction can be found in (Hayes-Roth *et al.* 1993).

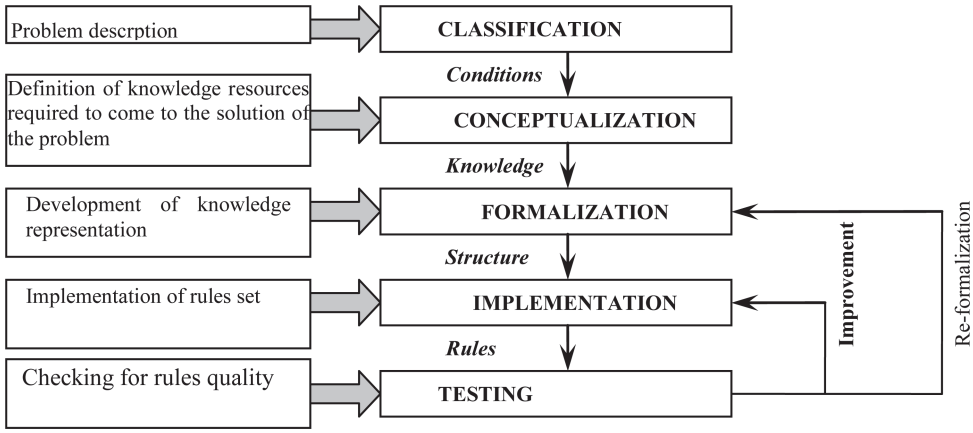


Figure 2. Stages of an expert system development process.
Source: (Knosala *et al*. 2002).

Construction of expert systems usually begins with definition of the problem to be solved, the range the problem should considered in and the way it should be solved (requirements, which should be met when searching for solutions of the problem, assessment of alternative solutions etc.). Construction of expert system is usually performed in the process including the staged presented in the figure below (Fig. 2).

More detailed description of stages of expert system construction can be found in (Hayes-Roth *et al*. 1983; Zieliński, 1999; Knosala *et al*. 2002).

Practically, there are many expert systems, and the most well-known and often used are: Dendral, Prospector, Mycin, XCON and many others (Shim, *et al*. 1999; Chromiec, Strzemieczna, 1994; Hayes-Roth *et al*. 1983), and the basic language used to record and perform logic operations is the one used in Prolog (Bubnicki, 1993; Bratko, 2001; Puppe, 1993).

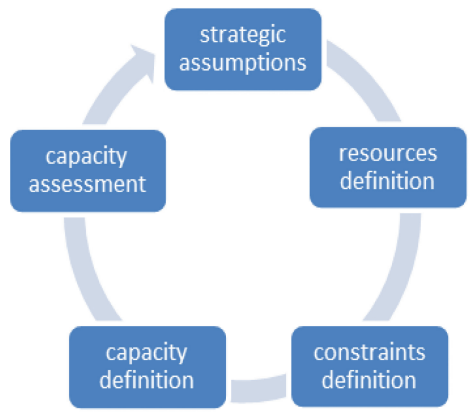


Figure 3. Sustainable approach to agile capacity planning.
Source: own work.

3 MODEL FRAMEWORK

Providing availability and reliability of resources in agile manufacturing system is a multi-stage procedure. It starts at strategic level of management providing identification of the general business rationale, identifying types of resources to be applied. The next step is identification of constraints and definition of capacity—decisions made at tactic level and followed by capacity assessment and providing with suitable maintenance actions.

Combination of resources definition, capacity definition and availability assessment results in the following model of approach to capacity planning in agile manufacturing systems, as presented in the following scheme (Fig. 3).

The model is organized as a cycle and is meant to mimic the idea of continuous improvement cycle, leading to self-learning and self-improving agile organization.

The first stage and initiation of the cycle is an idea to start a business and definition of preliminary strategic assumptions including branch, range and scope of processes to be realized.

The second stage is resources definition based on processes within the branch considered. Some flexibility is advised in this stage to provide agility at the highest rate possible.

The third stage is constraints definition and financial resources seem to be the most often

considered at this stage, however some legal, geographical or cultural aspects are in some circumstances under consideration as well.

The fourth stage needs data input from the previous ones (strategy, resources and constraints) and results in definition of company's physical structure.

The fifth stage is assessment of the structure developed in terms of predefined criteria and their optimization to reach predefined availability and reliability. The conclusion and results are used to redefine strategic assumptions and strive for excellence.

The model requires making numerous decisions, based on knowledge of the market, its trends, technologies, processes, products. The decisions are to be taken on repetitive basis, as in agile manufacturing systems customers' demand change. To cope with their complexity and high requirements concerning knowledge and experience, expert system was developed, providing reasonability of decisions and accuracy of actions. The structure of the system is the following:

Problem is described as definition of optimal composition of resources provided at required level of availability and reliability (capacity definition) for a given product or a potential customer.

Necessary knowledge resources include market data, description of techniques and technologies available, machines performing known operations and their parameters and maintenance profiles.

Knowledge is represented in databases linked and related with rules sets based on pre-identified relations and interdependencies. The stage requires thorough knowledge of the branch and processes.

The research is focused on one branch and the present stage comprises of identification and verification of rules for capacity and availability definition. Quality of decisions is to assessed with Delphi methodology during the next stage of the research, after carrying simulation experiments.

4 CONCLUSION

In contemporary/agile company products and processes definition is the first stage of manufacturing process, as according to agile manufacturing definition, the most important is meeting customers demand, which results in treating customers as an important stakeholder of manufacturing process. Such cooperation is one of the main assumptions of agility and its consequence is that they become a part of a company.

The very first stage of resources definition should be considering ability to perform various processes in order to meet customer requirements. Thus, the kinds of machines should be chosen so that they perform as many processes as possible. The solution then is using either universal machines, or as many specific as budget allows. Providing their ability and reliability then seems to be the key issue, together with careful appointing people and their skills to meet requirements of process.

The decisions made within the area are complex and based on numerous determinants, what is more they generate high risk, as their consequences are investments and changes in process organization. Hence quality of decisions is crucial, what makes AI support specially important and useful.

The research introduced in the paper is a part of general research conducted by the author and comprising various aspects of resources management in agile environment.

REFERENCES

Bratko I., (2001), "Prolog. Programming for Artificial Intelligence", 3rd ed., Addison-Wesley, Harlow.

Bubnicki Z., (1993), „Podstawy informatycznych systemów zarządzania", Wydawnictwo Politechniki Wrocławskiej, Wrocław.

Cholewa W., Pedrycz W., (1987), „Systemy doradcze", Wydawnictwo Politechniki Śląskiej, Gliwice.

Chromiec J., Strzemieczna E., (1994), "Sztuczna inteligencja. Metody konstrukcji i analizy systemów eksperckich", Akademicka Oficyna Wydawnicza PLJ, Warszawa.

Chwiałkowska E., (1991), "Sztuczna inteligencja w systemach eksperckich", Zakład Nauczania Informatyki "MIKOM", Warszawa.

Coley D.A., (1999), "An introduction to genetic algorithms for scientists and engineers", World Scientific, Singapore, New Jersey.

Devadasan S.R., Goshteeswaran S., Gokulachandran J., "Design for quality in agile manufacturing environment through modified orthogonal array-based experimentation", Journal of Manufacturing Technology Management, 2005, Vol. 16 Iss: 6, pp. 576–597.

Emigh J.: *Agile Manufacturing*, Computerworld, 8/30/99 vol. 33, issue 35, p.56.

Goldberg D.E., Grygiel K. [tł.], (2003), "Algorytmy genetyczne i ich zastosowania", Wydawnictwo Naukowo-Techniczne, Warszawa.

Goldsby, T.J., Griffis, S.E., Roath, A.S., Modeling Lean, Agile, And Leagile Supply Chain Strategies, Journal Of Business Logistics. Vol. 27(1), 57–80.

Gunasekaran A., Yusuf, Y.Y. (2002) *Agile manufacturing: a taxonomy of strategic & technological imperatives*, International Journal of Production Research, vol. 40, no. 6, pp. 1357–1385.

Hayes-Roth F., Waterman D.A., Lenat D.B., (1983), "Building Expert Systems", Addison-Wesley, London.

Jasiulewicz-Kaczmarek M., (2013), Sustainability: Orientation in Maintenance Management—Theoretical Background, In: Golinska P. et al. (eds.): Eco-Production and Logistics. Emerging Trends and Business Practices, Springer—Verlag Berlin Heidelber, pp. 117–134.

Kisielnicki J., Sroka H., (2005), "Systemy informacyjne biznesu", Wydawnictwo Placet, Warszawa.
Knosala R. i Zespół, (2007), „Komputerowe wspomaganie zarządzania przedsiębiorstwem. Nowe metody i systemy", PWE, Warszawa.
Knosala R. i zespół, (2002), "Zastosowanie metod sztucznej inteligencji w inżynierii produkcji", Wydawnictwo Naukowo-Techniczne, Warszawa.
Kosiński R., (2007), „Sztuczne sieci neuronowe: dynamika nieliniowa i chaos", Wydawnictwo Naukowo-Techniczne, Warszawa.
Li, C., Agile Supply Chain: competing in volatile market, Management Science and Engineering, Vol 3. No 2, 2009 pp 61–64.
Loska A. (2012). Remarks about modelling of maintenance processes with the use of scenario techniques. Eksploatacja i Niezawodnosc—Maintenance and Reliability 2012; 14(2): 5–11.
Man K.F., Tang K.S., Kwong S., (1999), "Genetic algorithms: concepts and designs", Springer, London.
Moubray, J. 1997 Reliability Centred Maintenance. 2nd ed. Butterworth-Heinemann. Oxford.
Mulawka J.J., (1996), „Systemy ekspertowe", Wydawnictwo Naukowo-Techniczne, Warszawa.
Pańkowska M., (2001), "Zarządzanie zasobami informatycznymi", Wydawnictwo Difin, Warszawa.
Pawłyszyn I., Maćkowiak N., Stachowiak A., Jańczak T., "Elements of artificial intelligence applied in warehousing" w Fertsch M., Grzybowska K [red.], (2010), "Logistics in the enterprises—selected aspects", Publishing House of Poznan University of Technology, Poznań.
Pedersen K., (1989), "Expert Systems Programming. Practical Techniques for Rule-Based Systems", John Wiley, New York.
Puppe F., (1993), "Systematic introduction to expert systems: knowledge representations and problem—sloving methods", Springer—Verlag, Berlin.
Rich E., Knight K., (1991), "Artificial Intelligence", McGraw-Hill, New York.
Russel S.J., Norvig P., (1995), "Artificial intelligence: a modern approach", Prentice Hall International Editions, Upper Saddle River, NJ.
Rutkowski L., (2006), „Metody i techniki sztucznej inteligencji", PWN, Warszawa.
Rutkowski L., (2009), „Metody i techniki sztucznej inteligencji", Wyd. II zmienione, PWN, Warszawa.
Shim J.K., Siegel J.G., Chi R., (1999), "Technologia informacyjna", Dom Wydawniczy ABC, Warszawa.
Towill, D. and Christopher, M., (2002), The supply chain strategy Conundrum: To be lean Or Agile or To be Lean And Agile?, International Journal of Logistics: Research and Application 5(3), 299–309.
Yen J., Langari R., (1998), "Fuzzy Logic: intelligence, control, and information", Prentice Hall, Upper Saddle River, New Jersey.
Yu, J., Krishnan K.K., A conceptual framework for agent-based agile manufacturing cells, Info systems J (2004) 14, 93–109.
Zieliński J.S. [red.], (1999), „Inteligentne systemy w zarządzaniu. Teoria i praktyka", PWE, Warszawa.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Initial FMEA analysis of the container transport chain

M. Zając & J. Świeboda
Wroclaw University of Technology, Poland

ABSTRACT: Intermodal transport is more and more popular mode of transport. There is stable increase of intermodal operation. Today the biggest container port operate more than 34 M TEUs. The complexity of the issues often results in a very selective analysis of the elements of supply chains in the context of the processes of logistics, as well as machine components, systems of traffic, so the issues related to technology. The purpose of this article is to present preliminary estimates of the causes and effects of risks occurring in the international intermodal transport, as well as evaluation of possibilities to avoid potential risks.

1 INTRODUCTION

Intermodal transport, in brief, is the freight transport using more than one means of transport at integrated loading unit (container or swap-body semi-trailer). The most important advantage of this type of transportation is overcoming high distances in respect of customs service. Intermodal transport is very complex way of cargo transportation, the cargo handling operations and components, important in the transport of hazardous materials. Table 1 shows the biggest ports in the world in 2012 and 2013, the order was determined by the amount of transhipped containers million TEUs.

From Table 1 it can be seen that the largest port is Shanghai, which reloaded in 2012, 32.5 million TEUs in the next year increased the amount of nearly million TEU. The next place is the port of Singapore, which reloads by 1 million TEU less than container port in Shanghai. Port, which is in third place reloads already 10 million TEU less than the port, which is the first in the ranking. Port of Ningbo, is on site 6, but among the top 10 ports, he had the biggest increase in container handling in 2013. Compared to 2012, it is up 7.1%. For the last places were the ports of Dubai and Tianjin. In 2013, largest ports transhipped total 204.1 million TEUs, an increase of 2.9% a year earlier. Intermodal freight market is dominated by China, because there are many major ports, only 3 other ports in Singapore, Busan and Dubai are located in other countries. The biggest container port in Europe is Rotterdam, which in turn in 2012 and 2013. reloaded nearly 12 million TEU. The next position is the Port of Hamburg, which reloaded around 9 million TEUs in 2013. was up 5% increase compared to 2012. Port of Piraeus, is in 8th place, but among the top ten ports in Europe, he recorded an increase in container handling by 15.3%. Ports dominant in Europe are in the Netherlands, Germany and Italy. In 2013, ports transhipped 56.31 million TEU in total, compared to ports in the world (204.1 million TEU), it is almost 160 million TEU less.

So much interest in intermodal transport requires a response in the area of technological logistics cargo handling. On operations in intermodal transport is known to many studies. These relate to issues of effectiveness or efficiency of the chain container. These publications taking risk issues (Vališ & Zajac, 2013 and Kierzkowski A. & M. Zajac 2012a).

Table 1. The largest ports in 2012 and 2013 (in million TEUs).

No.	Port	Country	2012	2013	2013/2012
1	Shanghai	China	32.5	33.6	3.30%
2	Singapur	Singapur	31.7	32.6	3.00%
3	Shenzhen	China	22.9	23.3	1.50%
4	Hong Kong	China	23.1	22.3	–3.60%
5	Busan	South Korea	17	17.6	3.30%
6	Ningbo	China	16.2	17.3	7.70%
7	Qingado	China	14.5	15.5	7.00%
8	Guangzhou	China	14.7	15.3	3.80%
9	Dubai	UAE	13.3	13.6	2.30%
10	Tianjin	China	12.3	13	5.70%
			198.3	204.1	2.90%

The complexity of the issues often results in a very selective analysis of the elements of supply chains in the context of the processes of logistics, as well as machine components, systems of traffic, so the issues related to technology (Nowakowski & Werbinska-Wojciechowska, 2012). Issues related to the readiness of the lifts were included in the several publications (Vališ & Zak & Humility 2014). Methods applied to issues of intermodal transport are included, among others, is the (Kierzkowski 2010 and Kierzkowski & Zajac 2012B and Vališ & Koucký & Žák 2012).

The purpose of this article is to present preliminary estimates of the causes and effects of risks occurring in the international intermodal transport, as well as evaluation of possibilities to avoid potential risks. Structure of the article is as follows: the next section presents logistical operations occurring in the international supply chain. Than the article includes a discussion on the choice of a suitable risk analysis process. Sequentially presented in the table descriptions associated with the FMEA analysis. The last part is a summary and set out the next stages of work.

2 LOGISTICS OPERATION IN INTERMODAL CHAIN

As previously shown, most cargo handling is implemented in a relationship with China, which have up to 3 ports included in the top 10 largest ports. In Figure 1 can be read, that in 2009 the main focus was Asia—Europe, which carried the 11 493 million TEUs, while in the direction of Europe—Asia transported was 5 458 million TEUs. Another relationship is Europe—North America, then Europe—India and the Middle East, and the least used was the direction of Europe—Central and South America. In the tab. 8 are summarized in the order of all logistics processes in the edible Intermodal transport in relation Asia—Europe.

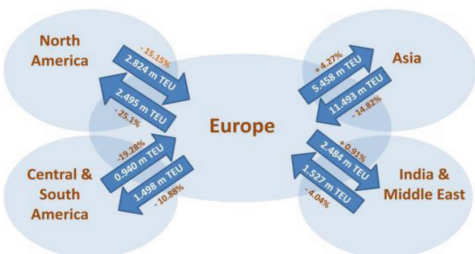


Figure 1. Container traffic at major European relations in 2009.

Figure 2 indicates the processes and operations carried out during the transport container from China to Europe in relation manufacturer—cargo reciver. Identification of the process will hereafter demonstrate risk during this process.

To be able to conduct a hazard analysis for intermodal transport should characterize all processes. It is advisable to know what operations, the operations are performed exactly in the process. In the following section describes the processes that are contained in Table 2.

I. Process 1, 22, 23, 27, 29—loading the container,
II. Process 2, 25, 32—road transport to the port or client,
III. Process 3, 12, 26—goods acceptance (customs service, freight forwarding),
IV. Process 4, 31, 33—unloading the container unit,
V. Process 5, 17, 21, 28—decision about place in a yard,
VI. Process 6, 19, 30—container warehousing in the port or container terminal,
VII. Process 7, 18—internal translocation (download container, transfer to another place, put aside by RTG crane),
VIII. Process 8, 15, 16, 20—translocation before loading,
IX. Process 9, 10, 13, 14—taking load by STS crane,
X. Process 11—ship transport,
XI. Process 24—rail transport.

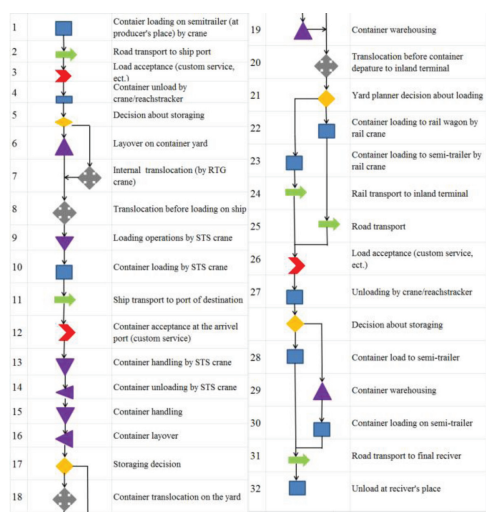


Figure 2. Logistics processes in intermodal transport.

Table 2. Identification of risks, its causes and effects.

Group no.	Process	Risk	Results	Causes
I	Loading the container	– incorrect loading	Impact in: human (penelty), other container (load fail), mean of transport (damage of mean of transport and/or load inside the container), block of containers on yard (damage of container and/or load);	– incorrect manipulation, – lack of experience
			– container falls (damage of container)	– lack of experience – crane overloading
			– breaking roap	– lack of experience – crane overloading – lack of maintenance
II	Road transport to the port or client	– cargo will be not deliver,	– load damage	– road accident
			– penalty of driver or another traffic member	– lack of experience, – lack of skills, – lack of maintenance, – ect.
			– cargo damage	– twist—lock not locked – road accident
			– truck damage	– road accident, – truck/semitrailer overload
III	Goods acceptance (customs service, freight forwarding)	– acceptance of damaged container	– damaged container can't leave the terminal	– incorrect interchange procedures
		– acceptance of container with forbidden goods	– process delay (check goods inside the container)	– intentional activity, – unintentional activity,
		– incorrect documentation service	– lack of documentation	– lack of experience – breaking the low
		– acceptance of incorrect container	– lose of money caused by storaging and sending to proper place	– lack of experience – human fatigue
IV	Unloading the container unit	– incorrect container unload	Impact in: human (penelty), other container (load fail), mean of transport (damage of mean of transport and/or load inside the container), block of containers on yard (damage of container and/or load);	– incorrect cargo manipulation – incorrect driver on the yard – lack of experience – human fatigue
			– container's fall (container and/or cargo damage)	– acceptance of overloaded container

(*Continued*)

Table 2. (*Continued*)

Group no.	Process	Risk	Results	Causes
V	Decision about layover	– container will be not delivered	– human wrong decision	– freight operator mistake – lack of experience
VI	Container warehousing in the port or container terminal	– incorrect container layover	– incorrect warehousing place	– wrong decision about layover place – lack of yard planner experience
			– damage of container by crane	– human factors
			– container fall	– Bad weather conditions
VII	Internal translocation	– damage of container and cargo inside	RTG Vehicle – container falls – broken rope – impact to: vehicle damage human (penelty) container on yard (container and cargo damage)	– lack of experience, – lack of skills, – lack of maintenance, – ect.
VIII	Container translocation before loading	– damage of container	Stradlle carrier Reachstracker – container falls – container impact to: human (penelty) container (cagro damage) mean of transport (mean of transport damage) damage of other containers	– lifting to heavy cargo – incorrect drive on yard
		– incorrect place on yard	– container missing on yard	
IX	Operating by container by STS crane	– cargo damage – deck damage – incorrect handling point	– container or/and cargo damage – ship damage – container missing	– transport system fail
X	Ship transport	– cargo not delivered – cargo loose – ship sinking	– lose of another commision – ship sinking	– storm – incorrect cargo/container bucking
XI	Rail transport	– container damage – train damage	– cargo damage – breaking wagon composition	– incorrect wagon service

3 THE RISK ANALYSIS IN INTERMODAL TRANSPORT

In the case of intermodal transport will be used FMEA process. Its main objective is consistent and systematic process to identify potential hazards and then eliminate or minimize the risks involved. The analysis was performed in order:

1. statement of purpose,
2. identification of defects and their consequences,
3. the importance of risk (R),
4. likelihood of risk (P),
5. detection of defects (W).

The purpose of the analysis is a valuable designation danger and risk of potential effects. Using mapped processes in Figure 2, in the next part of any operation can be described, setting a potential threat, effects and causes.

In the (Swieboda 2014) contains the exact values of the individual parameters, which were determined based on RPN. Table 3 presents the RPN values at each process steps.

Table 3. RPN values in intermodal chain.

No. process	R	P	W	R × P × W
I	10	1	4	40
	6	7	2	84
	7	3	2	42
	8	7	4	224
	8	3	6	144
	9	2	4	72
II	7	6	8	336
	10	7	10	700
	7	1	2	14
	8	7	10	560
III	2	2	6	24
	1	6	2	12
	6	1	2	12
	8	1	2	16
IV	10	1	4	40
	6	7	2	84
	7	3	2	42
	8	7	4	224
	7	3	2	42
V	6	4	2	48
VI	3	6	4	72
	7	7	6	294
	7	6	6	252
VII	8	3	2	48
	8	2	4	64
	7	3	2	42
	10	1	4	40
	8	7	2	112
VIII	8	3	6	144
	10	1	4	40
	6	7	2	84
	7	3	2	42
	8	7	4	224
	1	8	4	32
IX	9	2	4	72
	10	1	2	20
	1	6	4	24
X	7	3	2	42
	10	1	10	100
XI	8	2	4	64
	8	3	10	240

4 CONCLUSIONS

From Table 4 it can be seen that the highest result obtained is the RPN = 700 (group II), and the lowest score is RPN = 12 (group III). In this process group achieved the greatest results RPN. The highest score of 700 is the death of the driver or other participants in the road. This is a situation in which there is a collision of vehicles, vehicle collision with an obstacle, etc. Obvesly, the effect is disastrous, but it can't be forget that the fault does not always have to be on the side of the driver who drives the load; it may be the fault of another road user. The next value is the destruction of the vehicle 560, it may be at the aforementioned. Both of these findings are of high value due to the detection impossible, events on the road are random. The most smaller the RPN is the loss of cargo. It is possible that the driver did not protect the container during loading by a twist locks. It does not happen often, because the occupation operator can recall the driver while driving or notice a minimum loss of control of the vehicle, and then improve your mistake.

REFERENCES

Kierzkowski, A. (2010). Reliability models of transportation system of low cost airlines. In: *Reliability, Risk and Safety: Back to the Future* PP. 1325–1329.

Kierzkowski A.& Zajac M. (2012a). *Analysis of the reliability discrepancy in container transshipment.* 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012 1 PP. 826–831.

Kierzkowski, A.& Zajac, M. (2012b). *Uncertainty assessment in semi Markov methods for Weibull functions distributions.* Advances in Safety, Reliability and Risk Management—Proceedings of the European Safety and Reliability Conference, ESREL 2011 PP. 1161–1166.

Nowakowski T.& Werbinska-Wojciechowska S. (2012*). Zagadnienie utrzymania środków transportu–system wsparcia decyzyjnego*. Prace Naukowe Politechniki Warszawskiej. Transport, 2012, 37–54.

Swieboda J. (2014): Risk analysis on intermodal chain. Master thesis, Wroclaw University of Technology.

Vališ D.& Koucký, M.& Žák, L. (2012), *On approaches for non-direct determination of system deterioration*. In: Maintenance and Reliability, vol. 14, no. 1, p. 33–41.

Vališ D.& Zajac M.(2013). *Vulnerability of container terminal infrastructure.* In: Niezawodność infrastruktur krytycznych. Preceedings of XLI Winter School of Reliability.

Vališ D.& Zak L.& Pokora O. (2014). *Engine residual technical life estimation based on tribo data*. Maintenance and Reliability 16(2): 203–210.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Eds)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

On prudent activities in a complex system

I. Årstad
Petroleum Safety Authorities, Norway
University of Stavanger, Norway

T. Aven
University of Stavanger, Norway

ABSTRACT: In this paper we review the concept of "prudent activities" in the context of safety regulations for the Norwegian petroleum activities, the main aim being to assess whether the concept is adequate to reflect ambitious safety objectives in a complex environment. The work is carried out by discussing the suitability and relevancy of the concept in the light of theories and empirical studies addressing the challenges of complexity in the prevention of major accidents, as well as by assessing how initiatives taken by regulatory authorities and the oil and gas industry in recent years address the need to cope with complexity in practice. The paper concludes that, suitably interpreted, the concept of "prudent activities" is adequate for this purpose—what is required is an acknowledgement of some key principles of risk management to confront complexity and uncertainties.

1 INTRODUCTION

In this paper we study the concept of prudence, which is a fundamental concept in the Norwegian petroleum legislation, as it defines the paramount objective of safety related endeavours both for the companies and for the authorities. We are particularly concerned by what prudence entails in complex systems and explore whether the concept is adequate to reflect ambitious safety objectives in a complex environment. We limit the question to what may be relevant for the prevention of *major accidents* and discuss the subject from a safety management point of view, not a legal perspective.

The assessment is deemed necessary, because the concept of prudence has materially remained unchanged for a long time, while the industry has changed and our understanding as to how safety is created and eroded has evolved. As complexity increases, the occurrence and recurrence of major accidents are increasingly linked to how we fail to address complexity in practice. In this context, increasing pressure on current safety regulations to get simpler and clearer, actualizes also the question of what is prudent to simplify.

Thus there is a need to revisit the concept of prudence, and the purpose of the present paper is to provide insights into this concept and its practical use, by linking it to relevant theories and empirical studies, as well as to initiatives taken by regulatory authorities and the oil and gas industry in recent years, e.g. after the Deepwater Horizon accident. *Complexity* is the key issue in these theories, studies and initiatives.

The paper is organized as follows. Firstly in Section 2 we review the basic characteristics of complex systems as well as the necessary perspective to address those in practice. On this basis, we present in Section 3 our assessment of the adequacy of the concept of prudence to convey ambitious safety objectives in complex systems. Then in Section 4 we discuss how some initiatives taken lately by the industry and the authorities reflect the particular needs of complex systems and prudence in practice. Finally, the last section provides our conclusions about how complexity is reflected in the concept of prudence, and some recommendations on how to enhance prudence in complex systems.

2 COMPLEX SYSTEMS

We begin by clarifying the theoretical basis of our assessments. In the present paper, we use the term *major accident* to address acute events with severe consequences and we view major accidents as non-linear phenomena that emerge in a complex system. This view is at the basis of systemic accident models and resilience engineering (Hollnagel et al. 2012), the concepts of system accidents as outlined by Perrow (2011), the drift into failure studied by Dekker (2012) and of the black swans and antifragility concepts analysed by Taleb (2010, 2012).

Systemic approaches refer to *systems*, in the sense summarized by Ackoff (1999): "A system

is a set of two or more elements that satisfies the following three conditions.

- The behavior of each element has an effect on the behavior of the whole.
- The behavior of the elements and their effects on the whole are interdependent.
- However subgroups of the elements are formed, each has an effect on the behavior of the whole and none has an independent effect on it.

The essential properties of a system taken as a whole derive from the interactions of its parts, not their actions taken separately."

The concept of system is generic and can be applied to a technical system (e.g. a BOP), a management system (e.g. a maintenance management system), an organisational entity (a company's drilling department), a company, a group of interrelated companies (e.g. an operating company and contractors involved in the drilling of a well), a national industry etc. In this article, we focus on complex systems, as systemic approaches focus on the importance of understanding complexity to better grasp what contributes to the emergence of major accidents and what may explain their recurrence, and to prevent them more efficiently. Thus, we assess the concept of prudence in relation to the characteristics of a complex system, as described by, i.a., Dekker (2012) and summarized by Snowden & Boone (2007):

- "It involves large numbers of interacting elements.
- The interactions are nonlinear, and minor change can produce disproportionately major consequences.
- The system is dynamic, the whole is greater than the sum of its parts, and solutions can't be imposed; rather, they arise from the circumstances. This is frequently referred to as emergence.
- The system has a history, and the past is integrated with the present; the elements evolve with one another and with the environment; and evolution is irreversible.
- Though a complex system may, in retrospect, appear to be ordered and predictable, hindsight does not lead to foresight because the external conditions and systems constantly change.
- In a complex system the agents and the system constrain one another, especially over time. This means that we cannot forecast or predict what will happen."

Thus, complex systems are open systems, not exhaustively describable and understandable. They are characterized by a multitude of interdependent factors, both within the system itself and between the system and its environment, both punctually and over time. Interactions are non-linear, creating unfamiliar relations between input and output or between an event and its consequences. Minor changes can produce disproportionately major consequences. The outcomes of interactions are not certain and straightforward, as there are positive and negative feed-back-effects reinforcing or suppressing various influences, and many cause-and-effect relationships are unclear.

We focus also on the adequacy of the concept of prudence in the light of the challenges of managing complex systems. A decision that improves the safety in one part of the system may create a safety problem in another part of the system. A decision that is rational and effective at one time might be irrational and destructive at another time. A non-compliance that may be of no consequence 100 times may suddenly be determinant for the emergence of an accident. For complex systems, the outcomes of decisions may not be visible or immediately foreseeable, and measures might create problems while intending to achieve the opposite. This ambiguity is pointed out by, for example, Dekker (2012), when he addresses the dangers of protective structures, by Hollnagel et al. (2012) addressing the increasing complexity induced by measures deemed necessary in the wake of major accidents, and by Taleb (2010, 2012), addressing the dangers of treatment in excess of benefits—fixing past failures is not necessarily positive for future success, and past success is not sufficient information about how to achieve future success.

Complexity causes large uncertainties. And seeing risk as a function of uncertainty (Aven 2013), complex systems represent a higher risk than simpler systems. Complexity is in itself a risk factor, and the ambiguity of complex systems infers that routes to failure are also routes to success. Thus, both major accidents and system safety are emergent phenomena in complex systems (Dekker 2012 p. 158).

Our assessments refer both to complex and simpler systems. The complexity of systems is often explained in comparison to simple and complicated systems (Snowden & Boone 2007), or just in comparison to a complicated system (i.a. Page & Miller 2007). In essence, simpler systems are characterized by their tractability, linear interactions, less volatility, less ambiguity, less uncertainty; thus, they are more predictable and manageable.

Systemic approaches argue that we cannot define and solve all safety issues as though they belonged to a simple or complicated domain, as though complexity could be "simplified away" without consequences. But, systems are not either complex or not, they are both, and the systemic approach forces us to consistently differentiate between the characteristics of the *whole* system and

the characteristics of the *parts*. Complex systems may have simple or complicated parts, but, as a whole, they have the characteristics of complex systems: they are intractable and their interactions and outcomes are emergent, adaptive, volatile and ambiguous. Complex systems are closer to living organisms than to machines. Thus, while we may be able to define, understand predict, plan, design, manage or control simple and complicated parts of the whole, we cannot do the same with the whole. While we may be able to reconstruct what has happened in a simple or complicated part of the whole after an accident, we cannot do the same with the whole. Hindsight may give some foresight for a simple or complicated part of the whole, but not for the whole. Oversight may be achievable for a simple or complicated part of the whole, but not for the whole. Thus, safety for the whole (system safety) cannot be achieved solely by managing safety for the parts taken separately. It requires something more and different. It requires a system thinking approach that forces us to relate to the messiness of "reality", not obliterate or eliminate it. It allows instead for *both* zooming in on simple or complicated sub-systems, addressing important details, and for zooming out on the bigger picture, addressing the context and interdependencies of sub-systems.

3 THE CONCEPT OF PRUDENCE

To address the adequacy of the concept of prudence, we have reviewed the Norwegian petroleum legislation and underlying documents (Draft resolutions and bills) from the perspective of what systemic approaches deem relevant to prevent major accidents. We have assessed whether it conveys a systemic approach and an acknowledgement of complexity, both in the conducting of petroleum activities and in what it takes to achieve prudence. This article being centered on the prevention of major accidents, we have focused on the term of prudence applied to *safety*, defined (Framework regulations 2013 Section 2) as a broad term, centred on prevention—of more or less severe harm, in the shorter or longer term, whoever or whatever may be harmed (people, the environment, assets, production or transport of hydrocarbons).

Demonstrating prudence is the most fundamental regulatory requirement imposed upon the companies when conducting petroleum activities in Norway. The term 'prudence' is used to translate the Norwegian term "forsvarlig", which reflects high ambitions, an internalized sense of responsibility, and also the ability to defend the pertinence of choices and outcomes. All three aspects are found at the core of the concept of prudence in the reviewed legislation and they are seen as particularly well suited to the needs of complex systems.

The concept of prudence is seen to support the view that the system to be managed by the companies is a complex system, and that prudence is the emergent outcome of many interdependent processes and variables. The Petroleum Act (1996) views prudence as the resultant of managing successfully interdependent considerations, such as i.a. good resource management, high safety standards safeguard of the environment, compliance, coexistence with other activities (shipping, fishing, aviation, etc.) or subsea facilities (pipelines, cables, etc.). The Framework regulations (2013) under the Act recognize explicitly the dynamic interaction of offshore and onshore processes and view prudence as dependent on the management of interdependent matters such as safety, health, working environment, pollution control, production and transport regularity. They recognize the need to assess the overall load of individual factors and to not take for granted that what may be good enough locally, individually, punctually or one-dimensionally, may not be good enough when you take into account interdependencies, consider a bigger picture, or a longer time perspective etc. Thus, they recognize the ambiguity inherent in complex systems, where interdependencies can as likely create synergies as conflicting objectives, and where the pursuit of success demands trade-offs which can be at the source of failure. They recognize the volatility of complex systems, as prudence is defined as a moving target, which demands both to be maintained and further developed, in tact with technological and other developments in society. Thus, they acknowledge that prudence for the whole system cannot be limited to prudence for the parts.

Requiring prudence entails to be able to demonstrate or justify that prudence is achieved systematically and deliberately, not by chance, and that what is achieved is in accordance with all applicable regulatory requirements (also the required prudence). Thus, both prudence and compliance are defined as the essential objectives of the necessary management processes. Requiring prudence in addition to compliance expresses the expectation of an internalized sense of responsibility. It recognizes that compliance may not always be sufficient to achieve prudence, and that compliance, in some instances, may even come into conflict with prudence. For example, if new knowledge shows that a previously accepted standard solution is dangerous, the concept of prudence infers that an adequate response must follow, without waiting for the legislation to be updated. Thus, knowingly using a dangerous solution is not compatible with demonstrating prudence. Furthermore, limiting safety issues to legal issues is known to be the driver of a negative

tick-the-box-approach, diverting attention and resources away from what is the desired safety performance, personal responsibilities, continuous vigilance, the need to improve current performance or adapt to changing conditions. Thus, requiring prudence in addition to compliance reinforces the high ambitions attached to the concept of prudence: aiming at doing the right thing is the preferred driver, thus going further than just aiming at doing things right.

The legislation is viewed to convey that prudence and compliance must be contextualized to express high enough safety ambitions in a complex system. Activities in Norwegian petroleum activities are spread over a huge territory with very different geological and environmental conditions, and display a technological and operational diversity reflecting over 40 years of activity and a dynamic internationalized industry. Attempting to specify in regulations all adequate solutions for all possible contexts would not be realistic, nor compatible with the volatility and non-linearity of complex systems. Simplifying complexity away by requiring the same detailed solutions for all activities (if it were possible) would not be prudent either, as such solutions would be prudent to some, but irrelevant, inadequate, ineffective or insufficient for others. Thus, the Norwegian regulations posit that safety solutions must be contextualized and that the same high ambitions must apply for all. Instead of requiring the same specific solutions for all, they require the same safety *functions* for all, regardless of how challenging the context might be. Thus, doing things right, in the sense of being in compliance with the requirement of prudence, implies essentially taking the responsibility to *recognize* what is the right thing to do and *do* the right thing, at all times, thus adapting to changes when necessary.

Overall prudence is seen to rely on efforts in many different areas, and on the integration and contextualization of a wide spectrum of different management processes. Thus, prudence for the whole system cannot be limited to prudence for the parts. We see for example that the Petroleum Act (1996) presents prudence as the central condition for a company's "license to operate". As such, it is also a central objective of a company's corporate management system and corporate risk management system. And as activities are deemed prudent if they are prudent also from a safety point of view, safety management (Framework regulation 2013) is an integral part of a company's corporate management. Safety management has two main objectives: to ensure prudence and compliance with requirements pertaining to safety. In the current regulatory context, a risk management system is required as a means to contextualize important safety management processes and ensure that safety solutions are adapted to the actual needs in each particular case. Barrier management (Management regulations) is furthermore an integral part of the risk management system, as it is an important means to ensure that technical and operational safety measures on the installations take account of accidental scenarios, which are deemed relevant. Prudence requires the contribution of many more management processes, which are important for system safety, e.g. maintenance management, knowledge management, strategic management, change management, etc. Most of those processes are interdependent and linked in a non-linear fashion. It entails that each management process constitutes an important but insufficient contribution towards prudence. For example, barrier management is important but not sufficient to manage the risks that need to be addressed; risk management as here defined is important but not sufficient to manage safety, i.e. achieve prudence and compliance with regulatory safety requirements; and prudence from a safety point of view is important but not sufficient to demonstrate prudence in the sense of the Petroleum Act. Figure 1 illustrates the system boundaries that a company must consider in order to conduct prudent activities in accordance with the current safety legislation. It illustrates also how different management processes contribute to achieving prudence in the sense of high safety standards and compliance with safety regulations (darker areas), and how those are integrated in corporate governance and management systems aiming at ensuring overall prudence as outlined in the Petroleum Act.

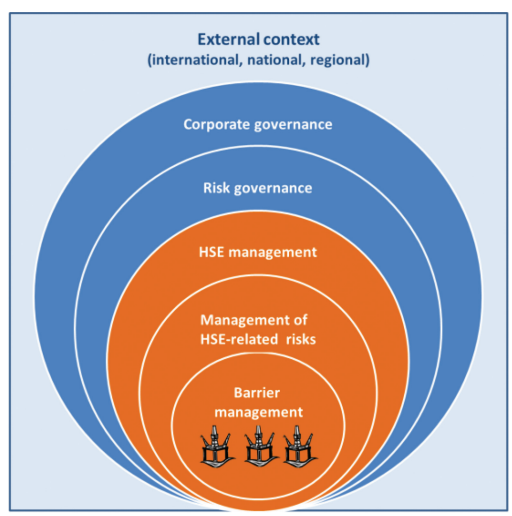


Figure 1. Integration of some management systems—company perspective.

Regulating prudence in a complex system is demanding. We see that the reviewed legislation appears to be in tact with newer management standards, as it bears the marks of their increasing acknowledgement of complexity over time. The legislation itself appears to be a complex system, as it cannot be reduced to a set of independent paragraphs. For example, compliance with one detailed requirement taken individually cannot compromise compliance with a higher standing requirement and the safety of the whole. Detailed paragraphs must be contextualized and understood in conjunction with several central requirements, which apply without being repeated over and over again. The legislation is also the result of processes with the active participation of parties in the industry and many other influences. Thus, the legislation itself functions as a complex system opened both to the environment it regulates and to a wider environment.

Operating in this complex domain is considered demanding. In addition to an ambitious regulatory regime, there is a severe selection process to ensure that license shares or operatorships are granted to companies that are competent and responsible, i.e. with a sustainable risk appetite, compatible with prudent behaviour. Enabling diversity is also viewed as necessary for coping with complexity. To this end, the legislation supports the legitimacy of different stakeholders (licensees, operator, management, workers' representatives, trade unions, any individual in the system) and demands their involvement in safety matters. This is meant to activate different objectives, interests and competences, accommodate for inputs and controls with different perspectives, and stimulate contradictions of assumptions. Thus, the complexity of conducting prudent petroleum activities appears tangibly and consistently acknowledged in the infrastructure put in place to achieve the high safety ambitions it is deemed necessary to convey.

4 PRUDENCE IN PRACTICE

We have seen that the concept of prudence and its regulatory context supports the view that complex systems fail in complex ways, and that prudence depends on all parties acknowledging that complexity. We have also sought to assess whether it is necessary to give more attention to complexity *in practice,* as there are recurrent warnings as to our systematically defining and solving safety issues as though they all belonged to a simpler domain, i.e. as though obliterating complexity was a valid option to cope with complexity. To that end, we have reviewed some of the main initiatives taken, both by the authorities and the industry, after the Deepwater Horizon accident (i.a. OGP 2011, OLF 2012, PSA-N 2011abc, Report to the Ministry of Labour and Social Affairs 2013, Reports to the Ministry of Oil and Energy 2010, 2012, White papers nr. 8, 10, 28), some reports and recommendations following six major accidents (Buncefield 2007, 2008ab, Deepwater Horizon 2011, HSC 2000, 2001, HSE 2000, Montara 2010, 2013, NOU, 2008. 8, The BP U.S. Refineries Independent Safety Review Panel 2007), as well as current practice with regard to risk management. We have looked for what Dekker (2012) refers to as "the language of complexity", i.e. how we demonstrate a system perspective in practice, by what we express through our words and silences, our actions and passivity.

We have seen that investigation reports after major accidents confirm that not taking complexity into account is a relevant system safety issue, as they point at systemic issues, including interdependencies between processes across objectives, functions, organizations, etc., both punctually and over time. Nevertheless, improvements put forward in the wake of those accidents do not often reflect a language of complexity. The focus is mostly on technology, the people and processes at the sharp end of the business, and on more requirements, more controls, more documentation, and more detailed analyses. This stands in contrast to the warnings of systemic models, arguing that limiting ourselves to more "safety by constraints" increases complexity and sustains some important conditions for the emergence of major accidents. Thus, there seems to be a systemic flaw in what we learn in practice: we limit lessons from major accidents to what belongs to the simple and complicated domains, and justify the relevancy and virtue of improvements independently from the complex domain in which they will function.

We have seen that there are still many examples of "undercommunication" of interdependencies between processes and objectives, as though safety issues themselves were in practice a closed system in the simple or complicated domain. Most of the communication concerning system safety is in practice limited to matters concerning the sharp end of the business, i.e. the installations. Thus, in safety matters, everybody may be looking mostly in the same direction, at the installation, and at the same information, about the installation. Thus, there might be a substantial blind spot, where people involved in processes concerning e.g. cost-efficiency, strategy, resource allocation, re-organizing, etc. may not have a sense of ownership of the risks they introduce by their own decisions. There is also recurrent communication about safety regulations being a threat to the expansion and profitability of the industry, as though compliance were a luxury without a bearing on expansion and profitability, as though prudence concerned a closed system independent of

the business itself. Communication about the contribution of such statements on system safety is less common. There are also recurrent demands that regulatory improvement of safety should undergo a formal cost-benefit-analysis, as though there were enough prudence for a while. It is not nearly as common to witness communication about the need for buffering uncertainty to achieve prudence in ever-changing complex/open systems. There is little communication too about how to address externalities, or the benefit of a "dynamic nonevent" (Weick & Sutcliffe 2011) in economic terms, or the benefit of a safety paragraph in isolation from its regulatory or operational context. Demands to reduce the risk of major accidents through "simple" solutions, such as more detailed regulations and more responsibilities transferred to the authorities are much preferred in practice than communication about the dangers of binding more of the authorities' few resources on standardized control activities, or how innovative approaches can improve system resilience through more risk ownership, contextualization, differentiation and diversity.

The "language of complexity" in some risk management practice is not clear either. It is not uncommon to see risk management limited to a compliance-driven exercise, consisting of standardized discrete processes, centred on analytical tools, focusing mostly on one sub-system (the installation), which is assumed to be a closed system, i.e. without safety-significant interdependencies with other parts of the system, or other systems, neither punctually nor over time. Vulnerabilities are limited to one type of consequence (harm to people), all interactions are assumed to be linear, and hindsight is assumed to give sufficient foresight. The resulting probabilistic measures of risk are assumed to embody all significant uncertainties about the context, the design, maintenance and operation of barriers, the competence, discipline and rationality of people, relevant constraints, dilemmas, pressures, paradoxes, etc. Emphasis is put on measuring risk and comparing this measure to an acceptance criterion, not on understanding what contributes to risk and needs attention, and the limits of such understanding. Such processes will often merely confirm the rarity of major accidents, limit the motivation to invest in system safety and comfort complacency in the system.

Not talking the "language of complexity" is apparent in compliance-driven approaches, based on the use of few regulatory requirements, isolated from their context. Limiting risk management to measuring risk and comparing this measure to an acceptance criterion at particular points in time, as mentioned above, is an example. Such an approach makes it possible to justify for example to normalize the evacuation of an installation each time the weather conditions imply that the annual probability of losing a main safety function exceeds 10-4. Over time this could justify building installations that are unsafe under certain weather conditions, and planning to evacuate workers regularly could become a design criterion. This approach would justify the acceptability of the collapse of an installation, as long as it was unmanned, as it is not repeated in each paragraph that the integrity of an installation is required both for the sake of people, the environment, assets and production. Thus, seeking to reduce regulatory compliance to compliance with a few paragraphs separate from the rest of the legislation comes in conflict with the concept of prudence, both punctually and over time.

Not acknowledging complexity in practice is also apparent in the resistance to change existing practices, for example the practice of quantifying accidental risk in a 25-year perspective and in areas as huge as the Barents Sea (1400000 km^2), which inevitably generates the information that the probability of encountering a major accident is low, the consequences potentially huge, and the uncertainties unlimited. Focus on risk quantification diverts all attention away from system safety, and risk measures are instead misused to either justify (irrespective of uncertainty) that there is nothing to worry about, or that the level of uncertainty commands extreme worry, regardless of existing knowledge (White papers nr. 8, 10, Hauge K.H. et al. 2013). Such mechanisms resonate with the safety eroding forces described i.a. by Dekker (2012) in his concept of drift into failure, and by the National Commission on the BP Deepwater Horizon Oil Spill (Deepwater 2011), addressing the dominance of the systemic conflict between environmental and industrial considerations, probabilistic expressions of accidental risk being instrumental as a leverage by both sides in that conflict. This may also be an illustration of the relevancy of Perrows' (2011) focus on the political nature of risk assessment. Thus, we view the shortcomings of the "language of complexity" in themselves as an expression of the complexity of the system.

5 CONCLUSIONS

In this article, we have reviewed the concept of prudence, which is central in the Norwegian petroleum legislation. We have chosen to approach the concept of prudence through the lens of systemic accident models, which link the occurrence of major accidents to complexity and their recurrence to our shortcomings with respect to coping with complexity in practice. We have seen that coping with complexity requires a systems thinking approach in addition to the current analytical approach.

We have shown that demonstrating prudence is the condition for a company's "license to operate" in Norwegian petroleum activities, and that it reflects high ambitions with respect to safety standards, both punctually and over time. Prudence also implies compliance with regulatory requirements, which, in this particular context, means that actual challenges are recognized, safety measures adapted to those challenges, and required safety functions are fulfilled. As the safety legislation itself is a complex system, compliance with the requirement of prudence for the whole system cannot be limited to compliance with each requirement taken separately. Thus, requiring prudence in addition to compliance recognizes the dangers of compliance-driven approaches and detailed requirements. It expresses the expectation of an internalized sense of responsibility, where aiming at doing the right thing is the paramount objective of regulatory compliance, thus going further than just aiming at doing things right. We have seen that both the concept of prudence and its regulatory context are adapted to the challenges inherent to the complexity of the petroleum activities and to the view that safety management belongs to the complex domain. The concept of prudence reflects a consistent acknowledgement of complexity, both of petroleum activities, of the system necessary to manage safety, and of regulating and supervising system safety. There is also compatibility with systemic accident models and systemic approaches to safety management. Thus, both prudence and system accidents are viewed as properties that emerge from a web of adaptive interactions within a company and between a company and its continuously changing environment and the developments of technology, knowledge and society.

Even though the complexity of conducting prudent petroleum activities is recognized through the design of the regulatory infrastructure, we have pointed at the challenge to align the regulatory intentions with prudent practice. We have argued for the relevancy of paying attention to warnings as to our propensity to define and solve safety issues as though they all belonged to a simpler domain, i.e. as though obliterating complexity was a valid option to cope with complexity.

We support the view that systems thinking can support a "language of complexity", which can improve our coping with complexity, thus enhancing prudence in practice. It may contribute to more precise articulation of the choices we make with respect to the boundaries of the sub-systems we consider, and the safety-relevant environment of these sub-systems. This may improve current practices, by enabling greater precision as to the risks we do (and do not) consider, understanding that the risk of a major accident is not tractable, and that what we can address is a more tractable part of a bigger picture, e.g. the risk for personnel on installation X, given an event A, our uncertainty covering i.a. the reasons behind such an event, the reasons why barriers may fail and other types of consequences. Thus it may contribute to a better use of current analytical tools, adapted to zoom in on barriers at the sharp end of the business, and develop other tools to zoom out on what may contribute to the emergence of accidents which render barriers necessary. It may increase our awareness of the limits of our understanding and conclusions, and enable us to better buffer or reduce uncertainties linked to our decisions. It may also expose other risks than those usually in focus and mobilize a wider range of relevant risk owners. It may reveal the safety-relevancy of information which is available today but not currently labelled as safety-relevant. It may foster better attention to our own contribution to risk, while current practice is often centred on others' contribution. It may contribute to more purpose-driven risk management, thus more focus on *recognizing* risk and on the need to generate adequate understanding to practise wisdom (Ackoff 1989), as the concept of prudence commands.

The language of complexity is also useful in that it helps consider current shortcomings concerning our recognition of complexity as a normal expression of the system's complexity itself, i.e. something which will always be there to a certain extent, because it is rooted in many mechanisms which cannot be "fixed". It is something to acknowledge, buffer and adapt to. In exposing the normal "messiness" of "reality", the systemic approach contributes to understanding the forces in action in the system, the fact that actual performance often differs from normative performance, and that it contributes both to the resilience of the system and to the fragility of the dynamic equilibrium that prudence represents. The language of complexity helps us to "get real", reduce naïve illusions about simple solutions, reduce our vain indignations about the messiness of "reality", increase our humility as to what we can know, understand and fix, and how much harm we may do, either unintentionally or by being willing to do good, whatever function we have in the system. Thus, the language of complexity contributes to justifying the high ambitions outlined in the current safety legislation, and the necessity of competent and responsible actors in the whole system, to sustain prudent activities.

ACKNOWLEDGEMENTS

The work has been partly funded by the Petromaks program of the Research Council of Norway.

REFERENCES

Ackoff, R.L. 1989. From data to wisdom, *Journal of Applied Systems Analysis*. 16: 3–9.

Ackoff, R.L. 1999. *Ackoff's Best: His Classic Writings on Management*. Kindle Edition.

Aven, T. 2013. Practical implications of the new risk perspectives, *Reliability Engineering and System Safety*, 115:136–145.

Buncefield, 2007. *Recommendations on the design and operation of fuel storage sites*. Buncefield Major Incident Investigation Board.

Buncefield, 2008a. *The Buncefield Incident 11 December 2005—The final report of the Major Incident Investigation Board—Volume 1*. Buncefield Major Incident Investigation Board. ISBN 978 0 7176 6270 8.

Buncefield, 2008b. *The Buncefield Incident 11 December 2005—The final report of the Major Incident Investigation Board—Volume 2a*. Buncefield Major Incident Investigation Board. ISBN 978 0 7176 6318 7.

Deepwater Horizon, 2011. *Deep Water—The Gulf Oil Disaster and the Future of Offshore Drilling– Report to the President*. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. ISBN: 978-0-16-087371-3.

Dekker, S. 2012. *Drift into Failure*. Ashgate Publishing. Kindle Edition.

Facilities regulations, 2013. *Regulations relating to design and outfitting of facilities, etc. in the petroleum activities*. http://www.ptil.no/facilities/category400.html.

Framework regulations, 2013. *Regulations relating to health, safety and the environment in the petroleum activities and at certain onshore facilities*. http://www.ptil.no/framework-hse/category403.html#_Toc357595226.

Hauge, K.H. & Blanchard, A., Andersen, G., Boland, R., Grøsvik, B.E., Howell, D., Meier, S., Olsen, E. & Vikebø, F. 2013. Inadequate risk assessments—A study on worst-case scenarios related to petroleum exploitation in the Lofoten area. *Marine Policy* http://dx.doi.org/10.1016/j.marpol.2013.07.008i.

HSC, 2000. *The Ladbroke Grove Rail Inquiry, Part 1 Report*. Health and Safety Commission. ISBN 0 7176 2056 5.

HSC, 2001. *The Ladbroke Grove Rail Inquiry, Part 2 Report*. Health and Safety Commission ISBN 0 7176 2107 3.

HSE, 2000. *The Train Collision at Ladbroke Grove 5 October 1999. A report of the HSE investigation*. Health and Safety Executive. ISBN 0 7176 1918 4.

Hollnagel, E., Woods, D.D. & Leveson, N. 2012. *Resilience Engineering*. Ashgate Publishing. Kindle Edition.

Management regulations, 2013. Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities. http://www.ptil.no/management/category401.html.

Montara, 2010. *Report of the Montara Commission of Inquiry*. Montara Commission of Inquiry 2010. ISBN: 978-0-9808190-1-4.

Montara, 2013. *Draft Government Response to the Report of the Montara Commission of Inquiry*. ISBN 978-1-921812-13-2.

NOU, 2008. 8: *The Loss of the "Bourbon Dolphin" on 12 April 2007*.

OGP, 2011. *Process Safety—Recommended Practice on Key Performance Indicators*, Report no. 456.

OLF 2012. *Deepwater Horizon—Lessons Learned and Follow-up*. Report from the Norwegian Oil Industry Association.

Page, S.E. & Miller, J.H. 2007. *Complex Adaptive Systems: An Introduction to Computational Models of Social Life (Princeton Studies in Complexity)* Princeton University Press– A. Kindle Edition.

Perrow, C. 2011. *Normal Accidents: Living with High Risk Technologies*. Princeton University Press. Kindle Edition.

Petroleum Act, 1996. *Act 29, November 1996. No. 72 relating to petroleum activities* http://www.npd.no/en/Regulations/Acts/Petroleum-activities-act/.

PSA-N, 2011a. *Memorandum—Industry Action Based on the PSA's Follow-up of the Deepwater Horizon Accident*. Petroleum Safety Authority Norway.

PSA-N, 2011b. *Deepwater Horizon-ulykken- vurdering og anbefalinger for norsk petroleumsvirksomhet June 2011*. Petroleum Safety Authority Norway.

PSA-N, 2011c. *The Deepwater Horizon Accident—Assessments and Recommendations for the Norwegian Petroleum Industry—Summary*. Petroleum Safety Authority Norway.

Report to the Ministry of Labour and Social Affairs, 2013. Regulatory supervision and HSE-legislation in Norwegian petroleum activities. (In Norwegian *Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet,* Rapport avgitt av ekspertgruppe til Arbeidsdepartementet 27.8.2013 ifølge mandat av 31.10.2012).

Report to the Ministry of Oil and Energy, 2010. Increased recovery on the Norwegian Continental Shelf. (In Norwegian *Økt utvinning på norsk kontinentalsokkel)*.

Report to the Ministry of Oil and Energy, 2012. Increased drilling and well activities on the Norwegian Continental Shelf. (In Norwegian *Økt bore- og brønnaktivitet på norsk sokkel*).

Snowden, D.J. & Boone, M.E. 2007. A leader's framework for decision making, *Harvard Business Review*, http://hbr.org/2007/11/a-leaders-framework-for-decision-making/ar/1.

Taleb, N.N. 2010. *The Black Swan: Second Edition: The Impact of the Highly Improbable Fragility*. Random House Publishing Group. Kindle Edition.

Taleb, N.N. 2012. *Antifragile*: *Things that Gain from Disorder*. Penguin Books Ltd. Kindle Edition.

The BP U.S. Refineries Independent Safety Review Panel—January 2007.

Weick, K.E. & Sutcliffe, K.M. 2011. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Wiley. Kindle Edition.

White paper nr. 8, 2005–2006. *Integrated Management of the Marine Environment of the Barents Sea and the Sea Areas off the Lofoten Islands*. Report No. 8 to the Storting, 2005–2006.

White paper nr.10, 2010–2011. *First update of the Integrated Management Plan for the Marine Environment of the Barents Sea-Lofoten Area* Report to the Storting (white paper), 2010–2011.

White paper nr. 28, 2010–2011. *An industry for the future—Norway's petroleum activities*. Report to the Storting (white paper) Meld. St. 28, 2010–2011.

Safety and Reliability: Methodology and Applications – Nowakowski et al. (Ed.)
© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02681-0

Parallel computing for system availability and applications

R. Briš & S. Domesová
Technical University of Ostrava, Czech Republic

ABSTRACT: Rapid development of computer technology recently requires adequate novelties of source codes and appropriate software. New parallel computing technology based on HPC (High Performance Computing) for availability calculation will be demonstrated in this paper. The technology is particularly effective in context with simulation methods, but analytical methods are taken into account as well. Basic algorithms for availability calculations must be improved to achieve better computation efficiency. Parallel processing is executed by two ways, firstly by the use of the MATLAB function parfor and secondly by the use of the CUDA technology. The computation efficiency is compared and demonstrated on selected examples from practice.

1 INTRODUCTION

System is a set of components that work together and form a functional unit. Real systems include technical machines, production lines, computer networks and other devices. In practice, it is often required to model reliability characteristics of such systems. Using models of system availability, system operators are able to assess operational costs, determine how many people are needed to maintain the system, estimate expected yields, etc.

In applications related to availability modelling an important sub-problem is often encountered: The logical structure of the system and availability of each component at a given time $t \in \mathbb{R}$ are known and with this knowledge availability of the whole system at the time $t \in \mathbb{R}$ should be determined, i.e. the probability that the system is operational at the time should be calculated (in some cases the time evolution of the probability is required). This problem was solved in the past by many different algorithms that can be roughly divided into analytical and simulation ones. The simulation approach is employed when analytical techniques have failed to provide a satisfactory mathematical model or defy solution of the problem in closed form or the solution becomes unwieldy. The principle behind the simulation approach is relatively simple and easy to apply. However the common simulation techniques are slow and take a lot of time to provide accurate results. Nevertheless, this technique is the only practical method of carrying out reliability or risk studies, particularly when system is maintained and arbitrary failure and repair distributions are used or some special repair or maintenance strategy is prescribed.

The Monte Carlo (MC) method allows complex systems to be modeled without the need to make unrealistic simplifying assumptions, as is inevitably done when using analytical methods. With the increasing availability of fast computers, MC methods become more and more powerful and feasible (Briš, R. 2008). As they have the potential of obtaining solutions of models which are very close to reality, they can yield relevant and useful results. In the past twenty years, applications of MC simulation methods on a variety of system engineering problems have indicated that such techniques can provide significant improvements in the realistic assessment of reliability and availability of complex systems. Recent reliability analyses of complex systems based on the MC method bring very efficient estimators (Zdráhala, A. & Briš, R. 2011). Finding of an appropriate estimator must be necessarily connected with a variance-reduction technique. There exist efficient techniques that provide significant reduction in variance, when they are correctly applied (Rubinstein, R.Y. & Kroese, D.P. 2008). The application of these techniques gives other potential for optimization of the simulation algorithms solving complex practical reliability problems.

Another problem connected with the application of the MC method is slow convergence. To mitigate this issue, several techniques have been developed such as those based on the importance sampling and other classical methods (Fishman, G.S. 1996). Another possibility to improve the convergence is provided by the so-called conditioning methods which directly modify the modeling or the simulation procedure, as for example in the Petri net approach (Perez, D. et al. 1996, Signoret, J.P., et al. 2013). In spite of

all these advanced techniques, in most practical cases whenever reliability characteristics must be determined exactly and efficiently, the analyst faces computing problems, i.e. slow convergence and large simulation time. That is because systems are more and more complex and demands on reliability are continually growing. For example, NEC producer (Mochizuki, Y. et al. 2006) has offered system components for use in supercomputers in order to support the need for an extremely high performance. The improving reliability will be an essential feature of the products of the next generation.

The above mentioned computing problems are solvable by applying parallel processing of computing algorithms. This new computing technology is possible to put into practice just on assumption that an adequate computing infrastructure exists, which can be used for the HPC (High Performance Computing) calculations. In Technical University of Ostrava such a new supercomputing center is recently built. This paper demonstrates basic approach to the parallel computing for system reliability characteristics. Both analytical and simulation method is discussed in context of computer efficiency.

2 SYSTEM AND ITS REPRESENTATION USING ADJACENCY MATRIX

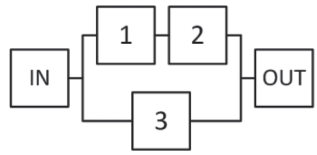
Consider a system consisting of n components, $n \in \mathbb{N}$. At a given time $t \in \mathbb{R}$ each component is in one of two disjoint states, operational or failed. To the i-th component a state indicator b_i belongs. If the component is operational, $b_i = 1$, otherwise $b_i = 0$. The vector $\mathbf{B} = (b_1, b_2, \ldots b_n)$ is called the state vector of the system. The set of all possible state vectors is called the state space of the system and denoted by V. Since just components with two possible states are considered, the state space has 2^n elements (Dubi, A. 2000).

The system state is determined by the states of its components. The function $S(\mathbf{B}): V \rightarrow \{0,1\}$ defined as:

$$S(\boldsymbol{B}) = \begin{cases} 1 & \ldots \ \textit{system is operational}, \\ 0 & \ldots \ \textit{system is failed}, \end{cases}$$

is called the system function.

The logical structure of systems is often represented using block diagrams. A block diagram is a directed graph with two special vertices (in Figure 1 marked IN and OUT), the remaining vertices symbolize components of the system. A directed edge connecting two vertices indicates that there is a direct path between corresponding system elements in indicated direction. Let's say



	IN	1	2	3	OUT
IN	0	1	0	1	0
1	0	0	1	0	0
2	0	0	0	0	1
3	0	0	0	0	1
OUT	0	0	0	0	0

Figure 1. Block diagram and corresponding adjacency matrix.

that the system is operational if there exists a path between the IN element and the OUT element passing only through functional components. For the system function:

$$S(\boldsymbol{B}) = \begin{cases} 1 & \ldots \ \textit{system is operational}, \\ 0 & \ldots \ \textit{otherwise} \end{cases}$$

holds.

For implementation purposes, it's suitable to represent the block diagram equivalently using the adjacency matrix M of size of $(n+2) \times (n+2)$. The first row and column of the matrix is used for the IN element, the last row and column for the OUT element. The remaining rows and columns represent the components of the system. If a directed edge between elements i and j exists, $(M_{ij}) = 1$, otherwise $(M)_{ij} = 0$.

3 METHODS OF AVAILABILITY QUANTIFICATION

As mentioned above, the following task is solved in this paper:

"A system with n independent components and an appropriate system function $S(\mathbf{B})$ is given. Further availabilities of all components are known. There is necessary to quantify the availability of the system."

The state space of the given system includes 2^n state vectors. By substituing each state vector into the system function, the state space can be divided into two disjoint subsets $V_0 = \{\mathbf{B} \in V | S(\mathbf{B}) = 0\}$, $V_1 = V \setminus V_0$. Let's denote the availability of the i-th component by p_i. Further denote:

$$\beta_i = \begin{cases} p_i & \text{if} \ \ b_i = 1, \\ 1 - p_i & \text{if} \ \ b_i = 0. \end{cases}$$

Therefore the probability $P(\mathbf{B})$, that the system is in state defined by a specific state vector $\mathbf{B} = (b_1, b_2, \ldots, b_n)$ can be calculated as:

$$P(\mathbf{B}) = \prod_{i=1}^{n} \beta_i.$$

At this point both solving methods can be presented, the analytical and the simulation one.

3.1 *Analytical method*

Availability A is the probability that the system is operational at the considered time, i.e. that it is in a state belonging to V_1. This probability can be calculated as the sum of probabilities $P(\mathbf{B}_j)$, that the system is in state $\mathbf{B}_j \in V_1$. Therefore the availability A can be expressed as:

$$A = P\left(S(\mathbf{B}) = 1\right) = \sum_{j=1, \mathbf{B}_j \in V_1}^{2^n} P(\mathbf{B}_j)$$
$$= \sum_{j=1, \mathbf{B}_j \in V_1}^{2^n} \prod_{i=1}^{n} \beta_i^j.$$

Using this formula, the algorithm for the analytical computation of system availability can be easily constructed. Notice that each state vector of the system is evaluated, so it can be expected that the computation time increases exponentially with respect to the number of components.

3.2 *Simulation method*

One of the ways to avoid evaluating the state of the system for each state vector is to solve the problem using the Monte Carlo method. The problem is simulated using appropriate random variable X. Here the following random variable is chosen:

$$X = \begin{cases} 1 \ldots S(\mathbf{B}_j) = 1, \\ 0 \ldots S(\mathbf{B}_j) = 0. \end{cases}$$

It should be verified that the mean value of X equals the availability A. For the mean value:

$$E(X) = \sum_{j=1}^{2^n} X_j \cdot P(\mathbf{B}_j) = \sum_{j=1, \mathbf{B}_j \in V_1}^{2^n} P(\mathbf{B}_j) = A$$

holds, i.e. the random variable X is selected properly.

The experiment consists of generating a random state vector and determining the value of X_j. The vectors are generated according to following rule: The probability that a specific state vector $\mathbf{B}_j$ is generated equals the probability $P(\mathbf{B}_j)$. After N repetitions of this experiment a random sample X_1, X_2, … X_N is obtained. The sample mean $\overline{X}$ of this random sample estimates the mean value of the variable X and therefore the availability A.

3.3 *System state evaluation*

The operation $S(\mathbf{B})$ is an important part of both approaches. It is an algorithm which for a system given by an adjacency matrix and for a given state vector **B,** determines the state of the system, i.e. if the system is operational. The algorithm consists of two primary steps:

- removal of failed components
- deciding if the system is operational

and is defined as follows:

1. Remove rows and columns that belong to failed components from the adjacency matrix.
2. Create three empty sets ACTUAL, AVAILABLE and VISITED. Move system elements that are directly connected to the IN element to the AVAILABLE set.
3. Move elements from AVAILABLE to ACTUAL. Move elements that are directly connected to some of the elements in ACTUAL and that are not in VISITED to AVAILABLE.
4. If AVAILABLE contains the OUT element, terminate the algorithm, system is through.
5. If AVAILABLE is empty, terminate the algorithm, system is not through.
6. Move elements from ACTUAL to VISITED. Continue with step 3).

Considering the estimation of the computation time, notice that steps 3 to 6 are executed at most m times, where m is the number of operational components of the system, $m \leq n$. This means the state of the system is calculated in n iterations at most.

4 PARALLELIZATION

Both the analytical and the simulation algorithm described in the previous section were implemented in the MATLAB language, at first as a sequential application and then both algorithms were parallelized. The principal of the parallelization consists in dividing the task into multiple simultaneous threads, each of them executing a different part of the calculation. The aim is to optimize the algorithms and to reduce the computing time.

The Monte Carlo method is suitable for parallelization, because the experiments are independent and may be realized in different threads. Assume that $M \cdot r$ experiments should be executed in r threads. This means that in the k-th thread M random state vectors are generated and for each of

them the system state is evaluated. The output of the thread is the total number of generated vectors for which the system was operational, denote by S_k. The estimated availability can be easily obtained from the intermediate results as:

$$\bar{X} = \frac{1}{M \cdot r} \sum_{k=1}^{h} S_k .$$

Similarly in case of the analytical algorithm, the state space can be divided into several parts and the state vectors evaluated in different threads.

4.1 *The parfor loop*

MATLAB programming tool allows a simple parallelization of loops with fixed number of recurrences using the "parfor" keyword. In case of the Monte Carlo method, the loop over all the sample size is parallelized and in case of the analytical algorithm it is the loop over the state space. Number of threads in which the calculation is executed equals at most the number of used processor cores.

4.2 *The CUDA technology*

These algorithms can be efficiently parallelized using CUDA (Compute Unified Device Architecture). This technology allows to use the NVIDIA graphics cards for parallel computing. The threads are organized in blocks and the blocks are organized in a grid (CUDA C Programming Guide 2013). In case of the graphics card used in this simulation there can be at most 1024 threads per block and 65535 × 65535 blocks per grid. Furthermore the maximum amount of available memory cannot be exceeded.

In each thread the so called "CUDA kernel" is executed. This special function is written in a file with the ".cu" extension, syntax is similar to the C++ language. There is a possibility to work with these files directly from the MATLAB environment. But first it is needed to create a ".ptx" file (Parallel Thread Execution) using external compiler (NVIDIA CUDA Compiler). From these two files the kernel object can be created in MATLAB.

MATLAB also allows an allocation of arrays on the graphics card, these arrays are used as input and output variables of the kernels. For the realization of experiments, here random state vectors generation, an array of length $n \cdot N$ of random numbers from $U(0,1)$ is pre-allocated on the graphics card (n is number of components, N is number of experiments). To generate the i-th state vector n numbers from this array are used (beginning with the position $i \cdot n$ when indexing from 0).

4.3 *Bitwise operation*

A further optimization of both algorithms can be achieved using bitwise operations. Their proper use results in a reduction of computing time as well as in lower memory requirements, which is especially important when using the CUDA technology.

The state indicator of a component is always zero or unity. To save the state indicator it is thus adequate to use one bit. In this context, simulation variables of data type "unsigned int" are used having the length of 32 bits. The binary code of such variable consists of 32 digits (0/1), each of them represent the state of one component.

In this simulation the bitwise operations are used in the CUDA kernel code. Their use in the pure MATLAB implementation is not suitable, because the bitwise operations are extremely time-consuming.

5 TESTING

For testing purposes the following well-scalable problem is used:

"A system of n component with a serial structure is given. Availability of each component equals 0.999. There is necessary to quantify the availability of the system."

The system with serial structure is represented by the adjacency matrix in Figure 2.

The problem was solved for various values of n using both the analytical and the simulation method. All of the implementations were tested under equal conditions on two processors Intel Sandy Bridge E5-2665, 8 cores each. The CUDA parallelization was tested on the graphics card NVIDIA GT 555M. The results of tests are shown in following tables and graphs.

The analytical algorithm was tested on small systems with 24 components at most. The following Tables 1–3 show that the analytical method is unsuitable for large systems, because (as expected) the computing time increases approximately exponentially with respect to n. However, for small systems, its use is appropriate since exact results are obtained.

The following parallel scalability graph in Figure 3 shows the computation time decreas-

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & & & & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Figure 2. Adjacency matrix for testing system.

Table 1. Sequential analytical algorithm test.

n	2	4	8	10	12	16	20	24
Time [s]	0.0013	0.0014	0.021	0.083	0.33	5.3	87.4	1411

Table 2. Analytical algorithm using parfor (time [s]).

n	2	4	8	10	12	16	20	24
2 threads	0.031	0.029	0.038	0.068	0.19	2.73	43.7	698.8
4 threads	0.072	0.037	0.042	0.058	0.12	1.52	24.0	388.5
8 threads	0.047	0.053	0.055	0.061	0.09	0.84	12.9	208.0
16 threads	0.094	0.095	0.100	0.089	0.11	0.55	7.54	122.1

Table 3. Analytical algorithm using CUDA and bitwise operations.

n	2	4	8	10	12	16	20	24
Time [s]	0.038	0.038	0.038	0.037	0.037	0.039	0.062	0.45

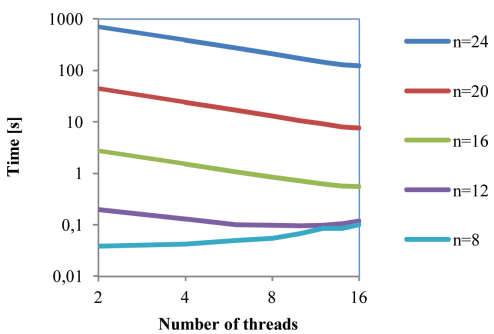


Figure 3. Simulation algorithm using parfor: scalability graph.

ing when the number of threads grows from 2 to 16 threads (note the logarithmic scale of both axes).

In case of the simulation algorithm besides the computation time also the estimated availability $\overline{X}$ and PRSD (percentage relative standard deviation) were recorded, what is demonstrated in Tables 4–6. Random samples of size 10^5 were used. Number of system component was significantly increased as well, to $n = 200$.

Also in case of the Monte Carlo method it has been shown that the computation can be significantly reduced by the use of parallel computing. This fact is illustrated in the following scalability graph in Figure 4, for several sizes of the system. The scale of both axes is logarithmic.

6 INDUSTRIAL EXAMPLE

In this section an example of a concrete engineering problem is presented, for its solution the aforementioned methods are used. The task is to simulate the availability of a fire detector system with independent components, basic motivation see in Rausand & Hoyland (2004). The block diagram is shown in Figure 5, according to it, the corresponding adjacency matrix can be constructed.

Assume that the system is in its useful life period, i.e. the failure rate and the repair rate of each component are constant. Therefore the availability $p_i(t)$ of the i-th component is given by Dubi (2000):

$$p_i(t) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} e^{-(\lambda_i + \mu_i)t}, \tag{1}$$

where λ_i is the failure rate and μ_i the repair rate of the i-th component, exactly specified in Table 7.

Assume that in time $t_0 = 0[h]$ all of components are operational. The availability of the system is simulated in time, thus an appropriate time discretization should be chosen. Here for example the constant step of 6 hours is chosen. At this point the simulation of the availability course in time can be computed. For each time step, availability of each component is first calculated using formula (1), then the availability of the whole system is calculated using one of the methods presented in sections 3–4. It is convenient to plot the results for each time step into a graph, see Figure 6.

Table 4. Sequential simulation algorithm, sample size 10^5.

n	10	20	40	80	120	160	200
A	0.9900	0.9802	0.9608	0.9231	0.8869	0.8521	0.8186
X	0.9903	0.9802	0.9613	0.9221	0.8862	0.8518	0.8201
PRSD	3.2036	2.2279	1.5761	1.0881	0.8823	0.7582	0.6752
Time [s]	12.26	19.14	34.25	66.89	100.65	135.85	173.35

Table 5. Simulation algorithm using parfor (time [s]).

n	10	20	40	80	120	160	200
2 threads	6.17	10.59	17.62	33.86	51.29	69.54	89.07
4 threads	3.22	5.53	9.01	17.41	26.36	35.71	45.63
8 threads	1.67	3.01	4.64	8.88	13.45	18.27	23.02
16 threads	0.97	1.56	2.54	4.81	6.86	9.36	11.86

Table 6. Simulation algorithm using CUDA and bitwise operations.

n	10	20	40	80	120	160	200
Time [s]	0.2336	0.027	0.0655	0.1803	0.358	0.5784	0.8684

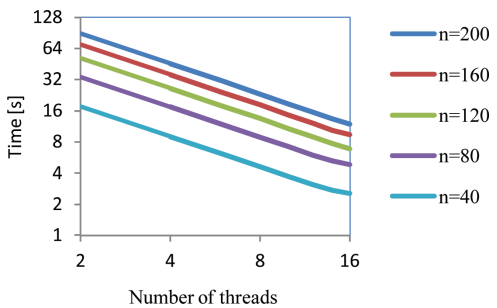


Figure 4. Simulation algorithm using parfor: scalability graph.

Table 7. Failure and repair rates.

i	Description	λ_i [h^{-1}]	μ_i [h^{-1}]
1	DC current source	$3 \cdot 10^{-5}$	0.018
2, …, 7	Smoke detector	$8.7 \cdot 10^{-4}$	0.025
8	Voting unit	$1.1 \cdot 10^{-4}$	0.02
9	Manual switch	$2 \cdot 10^{-5}$	0.01
10, …, 15	Fuse plug	$1.3 \cdot 10^{-3}$	0.03
16	Pressure switch	$2.5 \cdot 10^{-4}$	0.11
17	Start relay	$4.3 \cdot 10^{-4}$	0.11

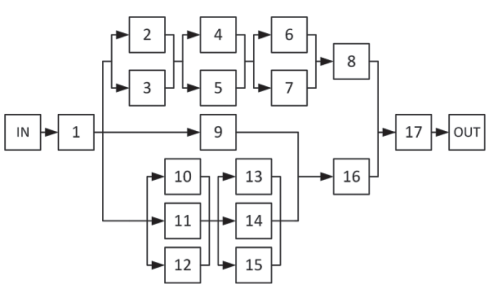


Figure 5. Block diagram of a fire detection system.

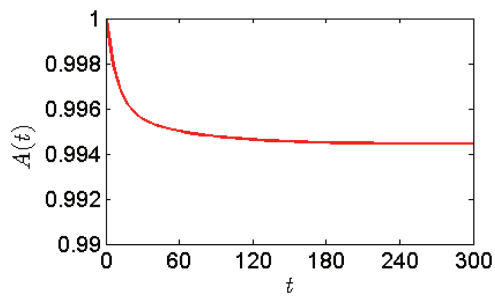


Figure 6. Dependence of the availability on the time: analytical method.

Table 8. Computation time comparison.

Algorithm type	Method	Time [s]
Sequential	Analytical	543.09
Parfor in 16 threads		47.68
CUDA		1.965
Sequential	Monte Carlo	435.21
Parfor in 16 threads	(sample size 10^5)	34.27
CUDA		1.034

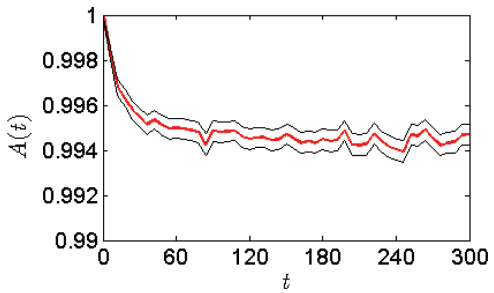


Figure 7. Dependence of the availability on the time; Monte Carlo method.

The following Table 8 compares the computation time needed to calculate the availability in 50 time steps (plotted in the graphs in Figures 6–7) by different types of the algorithm.

7 CONCLUSIONS

This paper was aimed at two specific algorithms (one analytical and one simulation) which can be used in applications related to availability modelling of systems represented by the adjacency matrix. The following two ways of implementation of these algorithms into parallel processing were introduced:

– parallelization using the MATLAB parfor loop,
– parallelization using the CUDA technology together with the use of the bitwise operations.

Using these two parallelization techniques, the computation efficiency of both algorithms was successfully enhanced. More significant reduction of the computing time was achieved using the second technique. For instance the practical example presented in Section 6 was computed over a computing time which is 275 times shorter than the computing time used for the original sequential implementation.

The parallel scalability was illustrated on the first of the techniques (the parfor loop). The scalability graphs in Figures 3–4 confirm that the use of parallel computing is always more efficient than the traditional approach using the sequential implementation.

On testing example we showed that the simulation methodology is particularly convenient when the number of system component increases. For instance if the number of system component approaches to $n = 200$, this method gives acceptable results, whereas using the analytical method is impossible.

ACKNOWLEDGEMENT

This paper has been prepared in the framework of the IT4Innovations Centre of Excellence project, reg. no. CZ.1.05/1.1.00/02.0070 supported by Operational Programme 'Research and Development for Innovations' funded by Structural Funds of the European Union and the Government of Czech Republic.

REFERENCES

Briš, R., 2008. Parallel simulation algorithm for maintenance optimization based on directed Acyclic Graph. *Reliability Engineering & System Safety,* 93(6): 874–884.

CUDA C Programming Guide [online], 2013. PG-02829-001_v5.5, July 2013. Available at <http://docs.nvidia.com/cuda/pdf/CUDA_C_Programming_Guide.pdf>.

Dubi, A., 2000. *Monte Carlo Applications in Systems Engineering*. New York: John Wiley & Sons, Ltd.

Fishman, G.S., 1996. Monte Carlo, Concepts, Algorithms, and Applications. New York: Springer Series in Operation Research, Peter Glynn.

Mochizuki, Y., Hayashi, Y., Oda, N., Takeuchi, K., & Takeda, K., 2006. Technology for High Reliability System LSIs. *NEC, Technical Journal* 1(3).

Perez, D., Garnier, R., Chevalier, M. & Signoret, J.P., 1996. A comprehensive method to speed up generalised stochastic Petri net Monte Carlo simulation for non-Markovian systems. In *Proceedings of ESREL'96-PSAM III, vol. 3, pg 1941–1946, June 1996, Crete, Greece.*

Rausand, M. & Hoyland, A., 2004. *System Reliability Theory*. 2nd edition. Hoboken, New Jersey: John Wiley & Sons, Inc.

Rubinstein, R.Y. & Kroese, D.P., 2008. *Simulation and the Monte Carlo Method.* New York: John Wiley & Sons, Ltd.

Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S., & Thomas, P., 2013. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. *Reliability Engineering & System Safety,* 113: 61–75.

Zdráhala, A. & Briš, R., 2011. Generalized test-cases for dynamic reliability: A Monte Carlo approach. In Radek Matoušek (ed.), *MENDEL 2011–17th International Conference on Soft Computing; Proc. intern. conf. 326–333, Brno, 2011*. Brno: University of Technology, Faculty of Mechanical Engineering, 1st edition.

This page intentionally left blank

This page intentionally left blank

Within the last fifty years the performance requirements for technical objects and systems were supplemented with: customer expectations (quality), abilities to prevent the loss of the object properties in operation time (reliability and maintainability), protection against the effects of undesirable events (safety and security) and the ability to restore performance (resilience). The need to adapt the operation of complex systems in such an uncertain and volatile environment has caused the necessity to formulate new and well established achievements associated with modeling, testing and evaluation of these properties. The concept of a complex system applies not only to the technical ones but also the infrastructure of major importance for social life such as transportation and logistics systems, buildings, power systems, water distribution systems or health services.

Safety and Reliability: Methodology and Applications contains the proceedings of the 24th European Safety and Reliability Conference (ESREL 2014, Wroclaw, Poland, 14-18 September 2014), and discusses theories and methods and their applications in the areas of risk, safety and reliability. The book will be of interest to researchers and practitioners, academics and engineers working in academic, industrial and governmental sectors.

ISBN 978-1-138-02681-0

9 781138 026810

an **informa** business

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
Schipholweg 107C
2316 XC Leiden, NL
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK