

Florian Brauner

Securing Public Transportation Systems

An Integrated Decision Analysis Framework for the Prevention of Terrorist Attacks as Example



Springer Vieweg

Securing Public Transportation Systems

Florian Brauner

Securing Public Transportation Systems

An Integrated Decision Analysis
Framework for the Prevention
of Terrorist Attacks as Example

Florian Brauner
Wuppertal, Germany

Dissertation submitted to the 'School of Mechanical Engineering and Safety Engineering' of the University of Wuppertal in 2015. Title: "Assessment of the Effects of Security Measures - An Integrated Decision Analysis Framework for the Implementation of Security Measures using Terrorist Threats in Rail-bound Public Transportation Systems as Examples". The empirical research was funded by the German Federal Ministry of Research and Education (grant no. 13N12305).

ISBN 978-3-658-15305-2 ISBN 978-3-658-15306-9 (eBook)
DOI 10.1007/978-3-658-15306-9

Library of Congress Control Number: 2016948251

Springer Vieweg

© Springer Fachmedien Wiesbaden 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer Vieweg imprint is published by Springer Nature
The registered company is Springer Fachmedien Wiesbaden GmbH

Preface

In the field of civil security research, many research efforts come down to technological security measures and how these measures improve security (e.g., in critical infrastructure). Information about natural disasters, hazards, and threats such as terrorism are communicated around the world in seconds due to media or social media. Although security standards are very high in Germany, the feeling of insecurity in society has never been so high. Different stakeholders (e.g., politicians, authorities, providers) have the challenge of maintaining public awareness without increasing insecurity in society. The implementation of increasing numbers and types of security measures provides more security and moves attitudes toward a positive perception of security, but the objective and subjective effects of security can be opposed. The assumptions that highly effective security measures are always accepted and raise customers' perception of security are not necessarily true in all cases. Often, the restrictions and interference caused by measures (e.g., loss of privacy, personal rights, freedom, or integrity) lead to dissatisfaction and negative attitudes.

These interferences are difficult to deal with in social-technological systems and challenging for decision-makers to handle but must be considered as part of integrated risk management. Therefore, new approaches are needed to introduce social-scientific aspects into risk management systems and decision support.

This book aims to enhance risk management systems with the subjective effects of security measures using rail-bound public transportation system as an example. It is an interdisciplinary research, combining engineering, social science, and economics to develop a contribution for end-users (public transportation providers).

Dr.-Ing. Florian Brauner

Cologne, May 1st, 2016

Content

1	Introduction.....	1
1.1	Objective of the Study	2
1.2	Procedure of the Study.....	4
2	Security Measures and Their Perception in Critical Infrastructure Context.....	5
2.1	Security and Its Research Players.....	5
2.2	The Vulnerability of Public Transportation.....	7
2.3	Effects of Security Measures: Risk Management Systems.....	11
2.4	Security as Part of Customers' Confidence and Satisfaction.....	14
2.5	Security Perception.....	16
2.6	Non-/Acceptance of Security Measures.....	18
2.7	Summary of the Literature.....	22
3	Research Concepts	25
3.1	Research Assumptions and Hypotheses.....	25
3.2	Conceptual Frame of Security Perception and Security Measure Acceptance.....	26
3.3	End-User Requirements.....	30
3.4	Limitations.....	31
4	Acceptance of Security Measures	33
4.1	Concept of the Survey	34
4.1.1	Development of Methodology for Data Acquisition and Analysis.....	36
4.1.2	Structure of Survey and Execution.....	37

4.2 Step 1: Database of Security Measures.....	39
4.3 Step 2: Translation Process of Security Measures into Interference Criteria.....	40
4.3.1 Consequence Categories as Part of Customer Perception	41
4.3.2 Translation into Interference Criteria	41
4.4 Step 3: Survey—Data Analysis	44
4.4.1 Online Survey Results	45
4.4.1.1 Analysis of Respondents’ Security Perceptions— Online Survey.....	46
4.4.1.2 Acceptance of Interference Criteria Caused by Security Measures	52
4.4.1.3 Ranking of Acceptance of Negative Impact Caused by Security Measures	58
4.4.2 Field Survey Results.....	61
4.4.2.1 Analysis of Respondents’ Security Perception— Field Survey.....	63
4.4.2.2 Acceptance of Interference Criteria Caused by Security Measures	73
4.4.2.3 Ranking of Acceptance of Negative Impact Caused by Security Measures	79
4.4.3 Comparison of Online Survey versus Field Survey.....	83
4.4.4 Further Expert Interviews and Panel Discussion.....	91
4.4.4.1 Expert Validation of Soft Interference Criteria— Travel and Preparation Time	91
4.4.4.2 Customer Panel Discussion of Soft Interference Criterion—Information	95
4.4.5 Interference Ranking and Discussion of Survey Results.....	99
4.5 Step 4: Acceptance Matrix of Security Measures Re-translation Process.....	103
4.6 Summary and Results of the Acceptance Analysis.....	112

5 Application—Integration of the Data into Risk Management Systems.....	115
5.1 Multi Criteria Decision Analysis in Risk Management.....	116
5.1.1 Criterion 1: Technical/Objective Effectiveness of Preventive Security Measures	121
5.1.2 Criterion 2: Costs of Security Measures.....	124
5.1.3 Criterion 3: Acceptance of Security Measures	127
5.2 Example Scenario for Application.....	128
5.3 Data Aggregation for Decision Criteria.....	129
5.4 Decision Making Process and Sensitivity Analysis.....	142
5.5 Summary and Results of the MCDA for End-users' Risk Management	145
6 Synthesis.....	151
6.1 Discussion of the Methodology	152
6.1.1 Verification of Results.....	152
6.1.2 Pros and Cons of an Acceptance Indicator Based on Interference Criteria.....	157
6.2 Comparison to Other Social/Technical Studies	158
6.3 Reflections on Theory/Future Research Needs.....	163
7 Conclusion	167
References.....	171
Annex A—List of Security Measures in Public Transportation System....	181
Annex B—Questionnaires of Survey.....	193
Annex C—Process Modeling—Results Expert Workshop.....	203
Annex D—Data Sheet and Report MCDA Software	209

List of Figures

Figure 1:	Closed system (airport on the upper side) and open system (KVB on the lower side) (Source: KVB 2015, adapted by author)	8
Figure 2:	Transit security measures, their purpose and applicability under different threat levels (Source: Carnegie et al. 2010:9 according to Staes et al. 2006)	11
Figure 3:	Effects of security measures according to RiKoV modified by author (Source: author according to Brauner et al. 2013a) ...	13
Figure 4:	Transit agencies' assessment of security needs (Source: Carnegie et al. 2010:11 according to American Public Transit Association 2004)	15
Figure 5:	Transit security measures and passengers' potential awareness (Source: Carnegie et al. 2010:8).....	19
Figure 6:	Achieving the appropriate balance (Source: Dunmore 2010, adapted by author).....	20
Figure 7:	Flow chart of research procedure (Source: author).....	28
Figure 8:	Structure of Chapter 4 'Acceptance of Security Measures' (Source: author)	34
Figure 9:	Indicators for security and safety in public transportation platforms-a case study (Source: Winzer et al. 2009).....	35
Figure 10:	Triangulation of methodologies for data acquisition (Source: author according to Brauner et al. 2013d)	37
Figure 11:	Executed survey in the study acceptance analysis (Source: author)	38
Figure 12:	Categories of security measures (Source: author, according to Burkhard et al. 2008, Brauner et al. 2013a)	39
Figure 13:	Consequence categories of interference criteria (Source: author and KVB 2014)	41

Figure 14:	List of consequence categories and interference criteria (Source: author)	42
Figure 15:	Example of connections among security measures and IC (Source: author)	43
Figure 16:	Gender and age distribution of online survey respondents (Source: author)	45
Figure 17:	Pareto chart of respondents' sense of security in public transportation systems (Source: author).....	47
Figure 18:	Gaussian curve and bar diagram of the sample (Source: author)	48
Figure 19:	Results of online survey for personal rights IC (n=1,339) (Source: author)	53
Figure 20:	Results of online survey for integrity IC (n=1,339) (Source: author).....	54
Figure 21:	Results of online survey for anonymity IC (n=1,339) (Source: author)	55
Figure 22:	Results of online survey for comfort/fare increases IC (n=1,339) (Source: author).....	56
Figure 23:	Results of online survey for comfort/security fee IC (n=1,339) (Source: author)	57
Figure 24:	Results online survey IC comfort (n=1,339) (Source: author)...	57
Figure 25:	Results of online survey for flexibility IC (n=1,339) (Source: author)	58
Figure 26:	Ranking of IC acceptance according to the online survey (Source: author)	60
Figure 27:	Ranking of consequence categories of the online survey (Source: author)	61
Figure 28:	Location and distribution of field survey in the KVB plan (Source: KVB 2015, adapted by the author).....	62
Figure 29:	Distribution of the gender and age of respondents to the field survey (Source: author).....	63
Figure 30:	Pareto chart—sense of security in the public transportation system (Source: author)	64

Figure 31:	Gaussian curve and bar diagram of sample (Source: author).....	65
Figure 32:	Distribution of the different questionnaires (Source: author).....	74
Figure 33:	Results of field survey for personal rights IC (Source: author)..	75
Figure 34:	Results of field survey for integrity IC (Source: author).....	76
Figure 35:	Results of field survey for anonymity IC (Source: author).....	76
Figure 36:	Results for field survey of comfort/fare increases IC (Source: author)	77
Figure 37:	Results of field survey for comfort/security fee IC (Source: author)	78
Figure 38:	Results of field survey for comfort IC (Source: author).....	78
Figure 39:	Results of field survey for flexibility IC (Source: author)	79
Figure 40:	Ranking of IC acceptance in field survey (Source: author)	81
Figure 41:	Ranking of consequence categories of the field survey (Source: author)	82
Figure 42:	Graph diagram—comparison of sense of security (Source: author)	84
Figure 43:	Comparison of the acceptance results in the online and field surveys (Source: author)	85
Figure 44:	Comparison of the acceptance of personal rights IC in the online and field surveys (Source: author)	86
Figure 45:	Comparison of the acceptance of flexibility IC results in the online and field surveys (Source: author)	87
Figure 46:	Comparison of the acceptance of the integrity IC in the online and field surveys (Source: author)	88
Figure 47:	Comparison of the acceptance of the comfort IC in the online and field surveys (Source: author)	89
Figure 48:	Comparison of the acceptance of the anonymity IC in the online and field surveys (Source: author)	90
Figure 49:	Expert estimation of travel time interference caused by different security measures (Source: author).....	92
Figure 50:	Expert estimation of preparation time interference caused by different security measures (Source: author).....	93

Figure 51:	Kiviat-diagram of combined results of non-acceptance of the interference criteria (online and field surveys) (Source: author)	102
Figure 52:	Model for decision-making—Effects of Security Measures (Source: author)	119
Figure 53:	Attribute tree of measurable attributes in gradient boxes, criteria, and overall measurable goal in white boxes. Dependence of attributes on the alternatives (represented as diamonds) is shown by dashed lines. (Source: Comes et al. 2011)	120
Figure 54:	Estimation of security measure performance (Source: Brauner et al. 2014f, adapted by author)	122
Figure 55:	Plan of fictive subway station (Source: author, Brauner et al. 2014d)	128
Figure 56:	Process steps of attack mode according generic process model (Source: Brauner et al. 2014d)	130
Figure 57:	Model of subway station (Source: author)	131
Figure 58:	Positions of cameras for video surveillance (Source: Brauner et al. 2014d)	132
Figure 59:	Positions of intelligent video surveillance (Source: Brauner et al. 2014d)	132
Figure 60:	Positions of police officers with K9 (Source: Brauner et al. 2014d)	133
Figure 61:	Position of access control (left) and detectors (right) (Source: Brauner et al. 2014d)	134
Figure 62:	Bar chart of the criterion technical/objective effectiveness of preventive security measures (Source: author, KIT software 2014)	136
Figure 63:	Bar chart of the criterion costs of security measures (Source: author, KIT software 2014)	138
Figure 64:	Bar chart of the criterion non-acceptance of security measures (Source: author, KIT software 2014)	139
Figure 65:	Bar chart of interference criteria for six example security measures (Source: author, KIT software 2014)	141

Figure 66:	Stacked bar chart of MCDA of all three criteria (Source: author, software KIT 2014)	143
Figure 67:	Results of sensitivity analysis for objective effectiveness (Source: author, software KIT 2014)	144
Figure 68:	Results of sensitivity analysis for costs of security measures (Source: author, software KIT 2014)	145
Figure 69:	Critical infrastructure resilience (CIR) study (Source: Brauner 2015).....	165

*(The Figure 1 & Figure 28 are pictures under copyright, authorized by
i+d Verkehrsplanungs- und Design GmbH, Leverkusen)*

List of Tables

Table 1:	Explanation approaches of risk acceptance (Source: Renn 1980, adapted by author).....	21
Table 2:	Research steps in the study (Source: author)	29
Table 3:	Development of indicators (Source: author)	32
Table 4:	List of selected security measures (Source: author)	40
Table 5:	Questions of online survey (Source: author).....	44
Table 6:	Online survey cross-analysis—perceived security and gender of respondents (Source: author)	50
Table 7:	Online survey cross-analysis for sense of security and age of respondents (Source: author).....	52
Table 8:	Field survey cross-analysis—sense of security and gender of interviewed passengers (Source: author).....	67
Table 9:	Field survey cross-analysis—sense of security and age of respondents (Source: author).....	69
Table 10:	Field survey cross-analysis—sense of security and location of interviews (Source: author).....	71
Table 11:	Field survey cross-analysis—sense of security and time of interviews (Source: author).....	73
Table 12:	Weighting coefficients for travel time IC (Source: author).....	94
Table 13:	Weighting coefficients for preparation time (Source: author) ...	94
Table 14:	Participants of the panel discussions (Source: KVB and Groskopf 2014, adapted by author).....	96
Table 15:	Acceptance results of the votes before and after providing information about the security measures (Source: KVB and Groskopf 2014, adapted by author).....	97
Table 16:	Ranking of IC acceptance (Source: author)	100

Table 17: Acceptance Matrix (Source: author) 104

Table 18: Example overview of costs of security measures
(Source: Pickl et al. 2009, adapted by author) 125

Table 19: Criterion 1—Estimation of the preventive effectiveness of
SeMe (Source: author, according to Brauner et al. 2014d) 135

Table 20: Criterion 2—Costs for SeMe in one subway station
(Source: author, according to Pickl et al. 2009)..... 137

Table 21: Pros and cons of MCDA for decision-makers
(Source: author) 147

Table 22: Requirements of indicators (Source: UN/ISDR 2008 adapted
by author)..... 153

Table 23: List of pros and cons of a combined (non-) acceptance
indicator for security measures (Source: Birkmann 2013;
Fekete 2010; Saisana and Tarantola 2002, adapted by author) 157

Table 24: Comparison of qualitative results and quantitative results
from the BMRB acceptance study (Source: Turley and Stone
2006, author) 160

Table 25: Comparison of body scanner acceptance in open and closed
(public) transportation systems (Source: Mitchener-Nissen et
al. 2011, author) 162

List of Acronyms

Asymp.	Asymptotical
AVL	Automatic vehicle location
BBC	British Broadcasting Corporation
BMBF	Bundesministerium für Bildung und Forschung (engl. Federal Ministry of Education and Research)
BMI	Bundesministerium des Innern (engl. Federal Ministry of Interior)
BVG	Berliner Verkehrsgesellschaft AöR
CAD	computer-aided dispatch or computer-assisted dispatch
CCTV	Closed Circuit Television
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIR	Critical Infrastructure Resilience
CNN	Cable News Network
COM	European Commission Communication
CUAS	Cologne University of Applied Sciences
df.	Degree of Freedom
DIN	Deutsches Institut für Normung e.V
ESRIF	European Security Research & Innovation Forum
et al.	latin: et alii, et aliae, et alia in engl.: “and others”
FEMA	Federal Emergency Management Agency
FTA	Federal Transit Administration
HAMLeT	Hazardous Material Localisation and Person Tracking
IC	Interference Criteria
I-cam	Intelligent Camera Systems
IEC/ISO	International Electrotechnical Commission/International Organization for Standardization
IPCS	International Programme on Chemical Safety
IRGC	International Risk Governance Council
K9 or K-9	Police dog (sniffer dog)
KIT	Karlsruher Institute of Technology
KRITIS	Kritische Infrastrukturen (eng. Critical Infrastructure)

KVB	Kölner Verkehrs-Betriebe AG
LCC	Life Cycle Costs
MADM	Multi Attribute Decision Making
MCDA	Multi Criteria Decision Analysis
MODM	Multi-Objective Decision Making
n or N	Numbers
NEAT	Network for the Economic Analysis of Terrorism
OECD	Organisation for Economic Co-Operation and Development
ÖPNV	Öffentlicher Personennahverkehr (engl. Public Transportation)
PhD	Doctor of Philosophy
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RiKoV	Risks and Costs of Terrorist Threats to Rail-bound Public Transportation Systems
SeMe	Security Measures
SI	Security Indicator
Sig.	Significance
SinoVe	Sicherheit in offenen Verkehrssystemen/Eisenbahn (engl. Security in Open Traffic Systems)
SuSiTeam	Subjektive Sicherheit im ÖPNV (engl. Subjective Security in Public Transportation Systems)
TCO	Total Costs of Ownership
TNT	Trinitrotoluene, $C_6H_2(NO_2)_3CH_3$ or 2-Methyl-1,3,5-trinitrobenzene
U.S. GAO	United States Government Accountability Office
UITP	International Association of Public Transport
UN	United Nation
UN/ISDR	United Nations Office for Disaster Risk Reduction
VDI	Verband Deutscher Ingenieure (eng. Association of German Engineers)
VDV AG Security	Verband Deutscher Verkehrsunternehmen e.V. (engl. Association of German Transport Companies, Workgroup Security)

Glossary

Critical Infrastructure: “Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital [to the United States] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” (Department of Homeland Security 2013).

Insecurity: Insecurity is a feeling of a person who “[...] perceives the world as a threatening jungle and most human beings as dangerous and selfish [...]” (Maslow 1942:35).

Interference Criteria: “Interference criteria describe the effect of security measures upon customers while they use the public transportation system. The assessment of the acceptance of these interference criteria allows referring to an accepted selection of security measures” (author).

Prevention: “Activities to provide outright avoidance of the adverse impact of hazards and means to minimise related environmental, technological and biological disasters” (UN Living with Risk Report 2004:17).

Risk: “The probability of harmful consequences, or expected losses (death, injuries, property, livelihoods, economic activity disrupted or environment damaged) resulting from the interactions between natural or human-induced hazards and vulnerable conditions” (UN Living with Risk Report 2004:36).

Risk analysis: “A process for controlling situations where an organism, system or (sub) population could be exposed to a hazard. The risk analysis process consists of three components: risk assessment, risk management and risk communication” (IRGC 2005:150 according to IPCS 2001).

Risk assessment: “A process intended to calculate or estimate the risk to a given target organism, system or (sub) population, including the identification of attendant uncertainties, following exposure to a particular agent, taking into account the inherent characteristics of the agent of concern as well as the characteristics of the specific target system. The risk assessment process includes four

steps: hazard identification, hazard characterisation (related term: dose-response assessment), exposure assessment and risk characterisation” (IRGC 2005:143).

Risk management: “The identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks. An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future” (Business Dictionary 2012).

Security: “Freedom from risk or danger; safety. 2. Freedom from doubt, anxiety, or fear; confidence. 3. Something that gives or assures safety” (American Heritage Dictionary of the English Language 2000).

Differentiation of security and safety: “Security addresses problems caused intentionally. This differs from safety which addresses problems caused accidentally” (UITP 2010:1).

Terrorism: “Any activity that (1) involves an act that is (a) dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws [of the United States or] of any State [or other subdivision of the United States]; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping” (DHS, NIPP 2006:105).

Uncertainty: “Uncertainty is a multi-faceted characterization about data or predictions made from data that may include several concepts including error, accuracy, validity, quality, noise and confidence and reliability” (Dungan 2002:1).

1 Introduction

“It is important to realise that decision-making regarding risks is very complex and that not only technical aspects but also political, psychological and social processes all play an important role. In this complex decision-making process a clear identification of the risks and of the effects of risk reduction measures is very useful”
(Jonkman et al. 2003:2).

Providers of critical infrastructure face the problems of achieving the appropriate balance of securing the infrastructure against threats and problems, on one hand, and conveying a feeling of security to customers on the other hand. Providers often neglect the multidimensional impacts—positive as well as negative—of implementations of security measures (SeMe). For example, the implementation of security measures not accepted by customers or security measures that restrict privacy may lead to dissatisfaction and, in the worst case, to a loss of customers. Currently, risk comparisons do not sufficiently cover justification of acceptability of a technology (Renn 1994).

Looking closely at terrorism in public transportation systems, the questions of how the risk of terrorism or security can be measured and how decision-makers can balance perceptions of objective security and subjective security to find an adequate level of security are raised.

This leads to several dilemmas on different levels:

1. Authorities: Daase and Kessler characterized terrorism as a construct of too many ‘known unknowns’ (Daase and Kessler 2007). As a result, policy actions and administrative leaders of authorities is a balancing act of dealing with terrorism. On one hand, they must warn and provide information about the risks of terrorism to the public without scaring and threatening. On the other hand, they must mediate an image of being capable of acting and having control over a situation. Maintaining this expectation without overestimation in context of limited insight of possible attacks is a dilemma authorities face (Schneckener 2013).
2. Providers: Public transportation providers face a dilemma on the customer level. Terrorism is a ‘not-yet-event activating actions’ (Beck 1986). This

means operators must secure their systems on an acceptable level to achieve the appropriate balance between security level and restriction of customers' privacy and personal rights. Otherwise, they experience a lack of customers' satisfaction that could lead to a loss of customers.

This book provides answers to the dilemma of providers and the question of how public transportation provider can assess the effects of security measures considering technical/objective effectiveness, economic effects, and subjective effects (acceptance of customers) of the security measures.

1.1 Objective of the Study

Currently, there is no satisfying assessment of the perception of security measures for a holistic evaluation of measures in risk management systems (Spencer 2013). Consequently, security measures are considered only in terms of their effect on reducing risks, and even this may be difficult in context of threats such as terrorism. Public perception is often a neglected aspect of these types of traditional risk assessments. An overview of the extent and effects of public perception with a focus on risk management is clearly missing but desirable. This is why the Commission of the European Communities expects and encourages all stakeholders of security research to consider “the understanding of human factors, social and ethical values including public perception relating to threats and security measures as well as the acquisition of the necessary skills to deal with such matters” (COM 2004:6).

In fact, many cities in the world measure their attractiveness by quality of life. Human security as part of this regional or municipal indicator is not currently considered because this aspect is missing approaches (Da Palma 2012). The value of perceived human security is highly desirable, especially for evaluation of the societal effects of security measures and the satisfaction of societal needs.

One of the main research questions of this book seeks to identify the individual parameters that influence public perception of security measures toward aversion and consider whether these parameters can be integrated into a composite indicator.

1st Research Question: How can customers' acceptance of security measures in a public transportation system be measured? How can a composite indicator (subjective effect) for each security measure be derived?

In this research, rail-bound public transportation systems are used as an example for two reasons: Firstly, a large number of passengers (customers) use this critical infrastructure every day, for this reason customer satisfaction including a security perception is very important. The large number of passengers facilitates the data acquisition to estimate the public perception. Secondly, contrary to other critical infrastructure, the system is an openly accessible, wide-branched system that is highly vulnerable for anthropogenic hazards/threats such as terrorism. Each security measures implemented by providers mainly have direct consequences on the customers.

The public transportation providers' point of view is in focus of the second part of this research. The implementation of security measures is challenging considering different structural requirements and decision parameters. In particular, rare events such as terrorist threats are difficult to prepare for and defend against because a lack of data provides inaccurate information about the probabilities of such events and the high, expected damages. Normative risk assessment approaches fail assessing terrorist attacks. A standard procedure for assessing terrorist attacks in risk management systems as well as decision making for security measure implementation considering different effects of security measures are missing and desirable, too. This leads to the second research question.

2nd Research Question: What are appropriate decision criteria for the implementation of security measures in a public transportation system to prevent terrorist attacks? How can a decision process be structured to find the most appropriate security measure based on the criteria in a holistic risk management system?

In this book, objective effectiveness of security measures, economic costs of security measures, and socio-technical acceptance of security measures are aggregated into risk management using the example of terror threats in public transportation. In the domain of public transportation, the Association of German Transport Companies (VDV) claims that analysis of customers' security perception has an important role in the holistic security concept (Burkhard et al. 2008). In addition to the objective of a safe and secure transit operation, the perceptions of security and customers' acceptance have considerable influence on the performance of a public transportation system.

1.2 Procedure of the Study

After an introduction in chapter one, the second chapter provides a review of the literature on security measures and their perception in public transportation systems to examine the question of why terrorism is a major issue in public transportation systems and determine the challenges to protect such systems. The existing literature is reviewed to examine the effects of security measures and how they can be assessed in risk management systems.

The third chapter introduces the research framework and methodology used to capture the required data. The author explains his approach of the triangulation method to reach the research objective and explains the assumptions and limitations made.

The fourth chapter describes data acquisition and the assessment of the collected data. In this book, the author discusses two customer questionnaires (online and in the field) and several experts interviews and includes the results of a tabletop exercise with security experts in public transportation systems.

The fifth chapter explains the integration of the results of the acceptance analysis into a decision analysis process. The chapter explains a decision-tool for risk management, including the objective and subjective effects of security measures. Following the wishes of some public transportation providers, the author includes the costs of security measures as a decision criterion as well. To demonstrate the decision process, an example scenario is used to apply the results of the acceptance analysis.

The sixth chapter critically discusses the results of this study concerning validity, including the synthesis of different entities into a decision tool with strengths and limitations that should be considered by decision-makers (end-users). Furthermore, possible research opportunities for ongoing research are identified.

The present research was embedded in a joint research project by RiKoV titled “Risks and Costs of Terrorist Threats in Public Transportation” (Pickl et al. 2011). In this project, the author developed a methodology to determine vulnerability of public transportation systems based on different scenarios. This includes a methodology to determine the objective (preventive) effectiveness of security measures (see Section 5.1.1). The results provide an example use case and risk management system that will serve as a platform for the integration of this study.

2 Security Measures and Their Perception in Critical Infrastructure Context

Since the 9/11 terrorist attacks, public and political awareness of security has been a major concern. Providers of critical infrastructure have worked to fortify potential targets and protect critical gates, even in the area of public transportation. Attacks in Madrid (2004) and London (2005) emphasized this development and showed that there is still a certain level of vulnerability in public transportation systems.

According to Carnegie et al. (2010), the evolution of public safety and security concerns in the public transit industry over the last three decades can be traced in the literature. In fact, there is a thematic cut: while the literature during the 1980s and 1990s on transit security focused almost entirely on protecting transit passengers, personnel, and facilities from ordinary criminal activities, the primary focus has shifted to terrorism and similar threats since 2001. Many guidelines have been published by (governmental) organizations e.g., the U.S. Federal Transit Administration, the Association of German Transport Companies (Burkhard et al. 2008), and the German Federal Ministry of the Interior (Bundesministerium des Innern 2005). Academic publications are limited because of the scarcity of available information on security initiatives (Carnegie et al. 2010).

This section presents a review of the literature on the impact of terrorist attacks on public transportation systems as well as the challenge of preventing harmful attacks and the possibilities available to secure this critical infrastructure. Furthermore, it discusses the perception of security on customer levels and how effects of security measures are investigated in different disciplines.

2.1 Security and Its Research Players

Security can be defined as the product of human action and behavior—something that has to be produced and ensured. In general discussions about national security or internal security, all efforts come down to security measures (Nagenborg 2011). The main intention of these measures is to protect people, objects, and the

environment from intentionally produced harm. Such discussions focus on the attackers, their reasons, the vulnerability of the company or critical structure, and potential damages that might occur because of an attack. In this context, decision-makers use countermeasures and preventive security measures to improve the level of security, but this is just one aspect of the effects of security measures. Decision-makers using risk management systems often neglect the subjective effects of hazards and countermeasures. The subjective side of security deals with human perception. Decision-makers often neglect this aspect when attempting to improve the security situation in their company because it is abstract and difficult to measure. Many scientists of different disciplines have discussed how people perceive security in daily life, the way threats work and how they affect individuals and societies, how individual security measures work, and what level of security is appropriate and not liberticidal (as George Orwell illustrated in his book “1984”). The importance of security perception is obvious. A satisfactory perception of security is a basic human need (Cömertpay et al. 2007) although the influencing mechanisms are almost incomprehensible. The balance between technical security solutions and perceived security by end-users often are mismatched because of different influencing factors (Köhn and Bornewasser 2012). This can cause inappropriate costs for decision-makers as well as a loss of customers.

Currently, security research programs such as the German Civil Security Research Programme of the Federal Ministry of Education and Research (BMBF) convey societal effects of research, specifically the increasing permeation of technology in society (2012). In particular, the effect of new technology on society is part of this research. New threats such as terrorism, natural disasters, pandemics, and increasing vulnerability of critical infrastructure require a high level of prevention and/or interoperability of actors connected with technology solutions. To obtain sustained comprehension, there must be a dialogue between all stakeholders such as the government, economy representatives, and community members to achieve a high level of security (BMBF 2013b). This *high-level security solution* shall protect the democratic values of society. Often, security measures by themselves cannot provide a high level of security (e.g., full-body scanners at airport security gates). *Acceptance* by society and its implications thus becomes an important aspect. The development of new security concepts requires a multi-dimensional approach, including different disciplines such as *engineering, natural sciences, and social sciences*.

One possible solution is the multi-directional approach taken by the BMBF. According to this approach, there are two directions—horizontal and vertical. The horizontal direction comprises engineering and natural sciences that are fused together with humanities and social sciences by dialogue. As a result, technical solutions are discussed from the point of view of social questions and social ef-

fects. The vertical direction consists of the economy, stakeholders, and users (e.g., operating companies or providers, critical infrastructure, and public authorities). This group discusses the impact of technical solutions on the behavior of the public and personal rights. Both directions convey the social aspect and the impact of research on the society as part of security improvement.

2.2 The Vulnerability of Public Transportation

*“Public transport systems are even safer than air travel, yet the feeling of insecurity is often greater”
(Dunmore 2010:10).*

Today, critical infrastructure can be defined as “[...] assets, systems, and networks, whether physical or virtual, so vital [...] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” (Department of Homeland Security 2013).

Public transportation faces different security problems and threats. Since 9/11, threats have included arson, explosives, weapons of mass destruction, sabotage, network failure, cyber-attacks, disruption of power, use of a transit vehicle as a weapon or weapon delivery mechanism, and hostage-taking. Staes et al. (2006) examined terrorist attacks against transit and concluded that 32% occurred on busses, 26% occurred on subways and trains, 12% occurred in train stations, and 7% occurred in bus terminals (Carnegie et al. 2010). Public transportation is an ideal target for terrorist threats because numerous customers use it, many stations have open access, and its use is impersonal. While air travel is a closed system with defined security controls at the input and output stream, public transportation is an open system based on the mobility of a maximum number of passengers. An impersonalized ticket allows criminals to enter a complex network with many possibilities to hide and perform harmful actions (Rhode 2012). Providers have an overview of neither the total number of customers nor their names or their exact localization. These specific factors complicate a standardization of a certain security level.

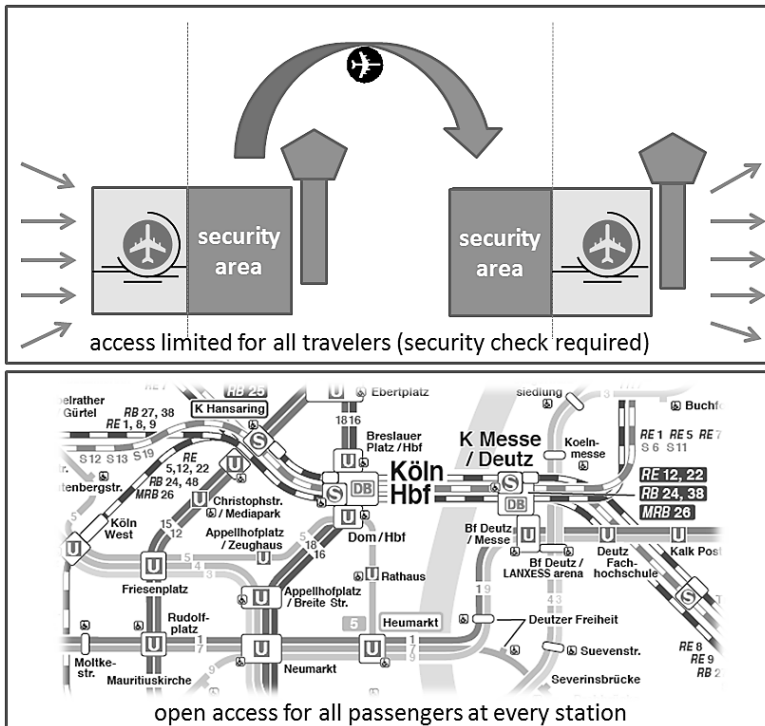


Figure 1: Closed system (airport on the upper side) and open system (KVB on the lower side) (Source: KVB 2015, adapted by author)

A second effect of this open system is the identification of passengers with the system itself. Normally, passengers use public transportation as a system with no control of public space, which causes a certain impersonality and lack of confidence (Dunmore 2010). In air travel, a pilot or a cabin steward is always in charge of taking care of passengers. They are specially trained to stay cool and calm and professionally handle difficult situations to ensure a secure feeling among the passengers. Thus, the value of identification and personification is much higher in air travel. Contrary to this, an impersonal system such as public transportation is much more prone to criminal intent than a closed and controlled system. Graffiti, vandalism, ticket fraud, sexual harassment, or other criminal intentions are problems of public transportation. For example, the cost of graffiti removal on Deutsche Bahn trains and BVG in Berlin amounted to 15.4 million Euros in 2008 (Berliner Morgenpost 2009).

The character of these critical infrastructure and the open system make it a lucrative target for terrorists. The word *terrorism* comes from the Latin origin *terror* and means *fear/scare*. It is an anthropogenic hazard with a high subjective threat component for citizens. An important consideration in the analysis of terrorist attacks is that this phenomenon follows no statistical patterns like natural disasters. “Most estimates of the probability of an event are based on some understanding of their past frequency. Simple applications of this frequency theory of probability can fail spectacularly when the possible event has occurred only rarely or never at all” (Falkenrath 2000:28). Initiated by human beings, it is an action of a decision process, including rational factors, subjective factors, and even reactions to, for example, policy decisions (Spencer 2013).

The following section chronologically discusses some major terrorist attacks on public transportation systems. These may show vulnerability when taking into account the intentional demolition, safety problems caused accidentally are not considered.

- Tokyo (Japan): On March 20, 1995, five members of the Aum-Shinrikyo sect released toxic gas in the subway/metro of Tokyo to avert a planned police raid on the sect’s headquarters. During rush-hour traffic on Monday morning around 08:00 am, the five members of Aum-Shinrikyo each carried two plastic bags filled with liquid sarin and released it in different trains by punching the bags with the tip of an umbrella and then leaving the train. The liquid sarin vaporized and spread into the environment. As a result, 12 passengers died and 5,500 passengers were injured.
- Madrid (Spain): During rush hour (7-8 am) on March 11, 2004, 10 bombs exploded in four trains of the Madrid public transportation system. All four trains were travelling on the same route from Alcala de Henares to the Atocha station. The explosions occurred around 7:30 am as the trains were nearing Atocha station. A total of 191 people died and more than 1,800 passengers were wounded. Later, three additional bombs, which had not detonated, were found in the destroyed trains.
- London (United Kingdom): On July 7, 2005 at 08:50 and 09:47 am, four explosions occurred in central London. Three bombs exploded in underground trains around Liverpool Street and Edgware Road and between King’s Cross and Russell Square. The last explosion took place an hour later in a double-decker bus in Tavistock Square. As a result, 56 people (including four suicide bombers) died and more than 700 were injured.
- Cologne (Germany): On July 31, 2006, two bombs, each composed of an 11-liter butane gas tank and a 4.5-liter tank of fuel, were hidden in suitcases and carried into two different trains of the Deutsche Bahn at the main station. The bombs had a timed detonator for 2:30 pm; fortunately, the bombs malfunctioned and did not explode. The suitcases were later found by staff

and brought to the lost-and-found office, where they were recognized and securely kept by the police. Using the Closed Circuit Television system (CCTV) of the Cologne main station, the police were able to identify the two assailants and arrested them in Kiel and Tripoli three weeks later.

- Mumbai (India): Several attacks have occurred in the city of Mumbai. In 2003, a bomb exploded in a train next to the Mulund station, killing 10 people and injuring 25. On July 11, 2006, a severe attack with seven bombs killed 209 people and injured over 700 in Bombay. On November 26, 2008, a fatal attack occurred at ten different locations in the city, including the train station at Chhatrapati Shivaji terminus. The group of attackers used explosive devices and guns and took hostages. In this attack, 164 people were killed and over 200 injured (CNN 2013).
- Volgograd (Russia): On December 29 and 30, 2013, two separate suicide attackers killed overall 34 people (including themselves) in two bomb attacks. The first attack took place in the entrance hall of Volgograd station next to a metal detector. The bomb with an equivalent to 10 kilograms of TNT killed 18 people and injured 44 people in the hall. One day later, a second bomb exploded in a trolleybus in Dzerzhinsky district, killing 16 people and injuring 41.
- Thalys-Train (France/Belgium): On August 21, 2015, an Islamic attacker tried to execute a terror attack in a high-speed Thalys-Train travelling from Amsterdam to Paris. Next to Brussels, the attacker pulled two hand weapons and started to shot. Several passengers overpowered the attacker, so that only two passengers were injured.
- Brussels (Belgium): On March 22, 2016, two suicide bombers have blown up in the departure hall at Brussels Airport. Shortly afterwards committed another attacker a suicide attack in the Maelbeek metro station. The attacks killed a total of 32 people.

Discussion about countermeasures that are effective against specific threats (response) focuses mainly on the reduction of probability of harm (prevention) and cost-effectiveness. The Federal Transit Administration (FTA) of the U.S. Department of Transportation recommended in a guideline called the “Public Transportation System Security and Emergency Preparedness Planning Guide” that all public transportation providers undertake a threat and vulnerability assessment based on a series of scenarios. According to the threat level, countermeasures can be specifically chosen.

2.3 Effects of Security Measures: Risk Management Systems

Carnegie et al. (2010) mentioned different ways to classify transit security measures, and the literature provides different classifications of security measures such as *prevention*, *response/mitigation*, and *monitoring* or *deterrence*, *and detection*, *mitigation*, and *response* (FTA 2003). They can also be classified according to threats against *components* of public transportation (e.g., stations, tunnels, vehicles, and railways). Staes et al. (2006) classified security measures in public transportation in accordance with *threat level* and *purpose* (see Figure 2).

Threat Level	Measures	Purpose
Minimum	- Simple physical barriers - Simple locks	Impede unauthorized external activity
Low	- Basic local alarm system - Simple security lighting - Basic security physical barriers - High security locks	Impede and detect unauthorized external activity
Medium	- Advanced remote alarm system - High security physical barriers - Watchmen - Basic communication	Impede, detect and assess unauthorized external activity
High	- CCTV - Perimeter alarm system - Highly trained armed guards - Access controls - High security lighting - Local law enforcement coordination - Formal contingency plans	Impede, detect and assess unauthorized external and internal activity
Maximum	- Sophisticated alarm system - Onsite armed response force	Impede, detect, assess and neutralize unauthorized external and internal activity

Figure 2: Transit security measures, their purpose and applicability under different threat levels (Source: Carnegie et al. 2010:9 according to Staes et al. 2006)

Depending on system boundaries, security can be measured with objective indicators. For example, statistics on crime, burglary, theft, and vandalism can show certain developments. Measurement of conditions before and after implementation of a security measure allows drawing conclusions about their effects. Several studies are available in the literature.

For example, Welsh et al. (2010) analyzed five studies on the effectiveness of using security guards for formal surveillance. In the first three studies, statistics of car theft in parking lots was used to measure before, during, and after security guard patrols. The studies of Laycock and Austin (1992) and Barclay et al. (1996) indicated numbers of thefts decreased when using security guards, and that the effect can be strengthened by also establishing a media campaign (Bar-

clay et al. 1996) or using additional security measures such as fences (Laycock and Austin 1992). Hesselings's study (1995) also observed a decrease of thefts but observed the same phenomenon in a control area without security guards. In the other two studies on "urban citizen patrols" in 1986 and 1989, the results were quite different. Kenney (1986) compared the crime statistics of 14 monitored subway stations with 14 unmonitored subway stations in New York. He measured a lower rate (2.7%) of criminal acts in monitored stations. Pennell et al. (1986, 1989) compared two urban districts over 30 months and found a burglary decrease of 25% in district A with patrols compared to 15% decrease in the control district B without patrols. In case of violent crime, they also captured decreases of 42% and 22%, but the control district experienced the larger reduction without urban citizen patrols. A later check showed that police officers were patrolling the control district. The results cannot be proven as correct (Welsh et al. 2010). These examples illustrate the difficulties of measuring the effects of security measures in the form of reliable statistical data. This makes it even difficult to transfer the results into risk management systems.

In the case of terrorism, probabilistic statistics are not available. Terror acts are rare events that cannot be statistically captured in reliable probability statements about certain scenarios and target objects. Therefore, research projects such as RiKoV, which measure the risks and costs of terrorist threats in public transportation, attempt to provide new approaches for holistic risk assessment, including analysis of the effects of security measures influencing the risk of terrorist acts (Lechleuthner et al. 2012).

The RiKoV project uses an adapted risk definition following Wilson et al. (2007) that consists of the three parts:

1. The threat (ability and motivation of terrorists)
2. The vulnerability of the system (based on the scenario and structural conditions)
3. The consequences of the attack (in terms of deaths, incidents, material damages, and short and long-term economic losses) (Wilson et al. 2007; Brauner et al. 2013b).

In this context, the different effects of security measures can be considered with a risk management formula. Figure 3 displays the modes of security measures effects. The preventive effect of security measures that attempt to prevent a specific threat is considered as part of the vulnerability. The author defines vulnerability as the strength or weakness of a potentially targeted asset and the protective systems for a specific threat (Brauner et al. 2014b, 2014e). In addition a second definition by Risk Analysis and Management for Critical Asset Protection

(RAMCAP) was used that describes a protective system as all existing capabilities and countermeasures at the asset or facility and their effectiveness (RAMCAP 2006). This includes analysis of preventive security measures, which Kersten and Klett (2008) called “*security measure type 2*”. The other effect (i.e., reducing the consequences of certain events), is called “*security measure type 1*”.

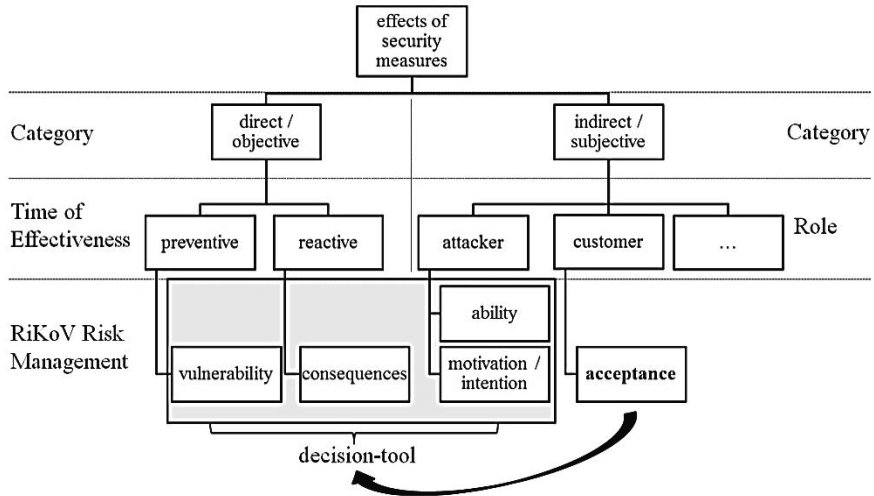


Figure 3: Effects of security measures according to RiKoV modified by author (Source: author according to Brauner et al. 2013a)

The management process does not consider the aspect of customer acceptance although this effect is already an essential part of the implementation decision. Kersten and Klett (2008) described in their book “IT-Security Manager” seven categories that should be considered in the validation process of security measures in IT systems. The categories can also be transferred to other sectors such as critical infrastructure (e.g., public transportation). The first step is testing suitability, which determines whether the security measure is appropriate, meaning it reduces the consequences (type 1) and/or prevents the threat (type 2). In this step, there is no discussion or assessment of the sufficiency of the security measure, but this is part of the second step, which is called an effectiveness check. The security measures should be sufficient according to the type in order to have an effect on the threat or consequence. The third step, which is interaction, assesses security measures regarding their effects on each other. Thus, security measures that influence other measures negatively can be identified. The practicability is the focus of the fourth step. In this step, the different security measures are ranked by their usability and possibility of error. Complex process-

es are more vulnerable, so the less complex a security measure in its context, the higher the practicability. Next, proof of acceptance is measured. The fifth step examines security measures regarding physical interference, unreasonable burden, and social discrimination from the users' point of view. The main part of this step is the assessment of perceived interference by the user rather than the assessment of actual physically interference. The last two steps determine economic efficiency and adequateness. Adequateness is more or less a corrective step that provides the possibility for a final evaluation of the security measure according to the protection demand. The adequateness analysis should avoid under- and overstatements (Kersten and Klett 2008).

According to Kersten and Klett 2008, acceptance analysis is an inherent part of a security measure implementation plan. It is often neglected, the author assumes this is caused by a lack of *easy-to-apply methodologies* as well as the difficulty of data acquisition, therefore this has to be considered in this study (marked in Figure 3).

2.4 Security as Part of Customers' Confidence and Satisfaction

Public transportation depends on customers' confidence and satisfaction. Customer satisfaction generally refers to maintaining customers' convenience and comfort. A lack of confidence leads to the feeling of insecurity and avoidance of public transit, which, in turn, leads to a negative impact on the economy. One approach to win customers' confidence is providing efficient customer services, increasing staff, security controls, and police patrols, or installing technical solutions such as camera systems. All these security measures act as deterrent factors and can prevent crime or harmful actions. However, from another point of view, a high amount of security measures—particularly the presence of police and security personnel—might arouse suspicion and the feeling of insecurity among passengers. In his 2010 article, "*Achieving the Right Balance*", Dunmore analyzed different arguments and claims for a number of measures. In his opinion, motivated, well-trained, and balanced customer service is the key to appropriate customer security perception.

The American Public Transit Association conducted a survey that included 120 public transit agencies to analyze the implementation of security measures post-9/11 (Carnegie et al. 2010). They determined the following: 88% of the agencies had adopted new or expanded existing security measures after 9/11, and 74% had already increased their security level before 9/11. In addition, the survey included an assessment of security needs as shown in Figure 4.

Needs and funding priorities	Very Important	Important
<i>Operating Funding</i>		
Funding Current Transit Agency/Local Law Enforcement Security Personnel	60.8%	17.5%
Funding Additional Transit Agency/Local Law Enforcement Security Personnel	52.9%	27.5%
Funding for Over-Time/Extra Personnel During Heightened Alert Levels	50.5%	29.7%
Creation of New Security Units, e.g., K-9 Teams	14.4%	24.4%
Training for Security Personnel	48.7%	38.1%
Security Training for Other Personnel	45.7%	39.7%
Security Planning Activities	42.6%	44.3%
Joint Transit/Law Enforcement Training	45.7%	36.2%
Customer Outreach	31.0%	40.5%
Access to Security Intelligence Information	34.5%	36.3%
Ongoing Technical Support for Security Plan Development	45.1%	40.7%
<i>Capital Funding</i>		
Automated Vehicle Locator Systems	67.9%	18.8%
Radio Communications Systems	85.7%	10.7%
Passenger-Operator Intercoms	21.6%	43.1%
Security Cameras On-Board Vehicles	72.6%	20.4%
Security Cameras in Stations	75.0%	16.3%
Public Address Systems On-Board Vehicles	42.2%	36.7%
Public Address Systems in Stations	42.4%	38.4%
Security Fencing Around Facilities	54.4%	32.5%
Chemical/Biological/Radiological Detection Devices	19.8%	34.0%
Intrusion Detection Devices	42.1%	33.3%
Controlled Access to Facilities and Secure Areas	71.1%	23.7%

Figure 4: Transit agencies' assessment of security needs (Source: Carnegie et al. 2010:11 according to American Public Transit Association 2004)

Convinced of the idea of a total quality management (continuous improvement process) and security needs, providers still face financial problems in implementing security measures. In Germany, many providers are municipal organizations. This leads to a rearrangement of the customers' role: On one side are passenger demands on the transit provider and on the other side is the municipality's demands on the transit provider. Taxes often supplement financing so that the books balance. In times of increasing costs and tight transit budgets, many transit providers have been forced to focus on the primary objective of maintaining system infrastructure in a state of good repair or managing growing ridership, neglecting security measures (Belyová and Schulze-Bramey 2009).

In 2002, the U.S. Government Accountability Office (GAO) listed insufficient funding as the most significant challenge to secure transit. The objective tricolon of effectiveness, efficiency, and customer satisfaction are linked and

thus decisions regarding implementation of security measures often require trade-offs between these three security-related objectives (Guerrero 2002, Carnegie et al. 2010).

2.5 Security Perception

The security allows two perspectives an *objective/structural* and a *subjective/perception* dimension. Both dimensions *objective* and *subjective security* can have diametrically opposed positions (Meng and Vollbracht 2014; Köhn and Bornewasser 2012). The assumption that a highly effective security measure is always accepted and raises customers' perception of security is false. Furthermore, the statement that the more security measures are implemented, the higher the security perception, is incorrect; there is no positive correlation (Wurtzbacher 2003).

The German research project "Subjektive Sicherheit im ÖPV Test und Evaluation Ausgewählter Maßnahmen" (SuSiTeam) defined *subjective security as a feeling of being secure*. Subjective insecurity is a continuum of feelings and situation assessment that is disturbed or even enhanced by a perceived threat of becoming a potential victim (Hempel et al. 2011).

The absence of fear or a feeling of safety is a basic need according to Maslow (1943), which is why security can be defined as a product or service, that has to be ensured like drinking water otherwise perception and emotions will become an additional threat. In Germany, in the last decade, the character of the dimensions has changed and merged. For example, the determination of threats is becoming more and more difficult due to their abstract character: Is a possibility or the feasibility of a terrorist attack a concrete threat?

However, the occurrence of a specific threat influences human security rather than the daily environment. Da Palma et al. (2012) described *human security as a construct of a different kind such as economic security, health security, and regional or local security*. According to their investigation, the regional or local community level affects citizens' quality of life and security. Regional developments (e.g., increasing urbanization, poverty, and increasing urban crime such as theft, burglary, and vandalism) and acts of physical or psychological injury (e.g., murder, infanticide, assault, rape, sexual abuse, and acts of intimidation and terror) influence the perception of security (Da Palma et al. 2012).

In case of terrorism, the behavior of the individual influences the group behavior. In microsociology sciences, this effect is called the *group with a common destiny* that handles situations in a *collective reflex* at an emotional level. As

a result, a lack of rational processing of information leads to possible uncontrolled behavior patterns (Schulze-Bramey 2012). These situations are difficult to handle, therefore, an understanding of influencing parameters helps to improve preventive action. Subjective security of customers is influenced by different parameters. Wagner and Lehnigk (2010) published already known parameters in public transportation systems such as individual parameters (e.g. gender, age, demography, state of health), proximity parameters (e.g. state of repair, dilapidation, security measures, amount of costumers), and other parameters (e.g. image, state of security, time of the day).

Köhn and Bornewasser (2012) examined parameters of security perception. They determined that, among all *unknown factors*, individual knowledge about the current security situation, individual attitude, and individual experience of protection/mitigation handling influence security perceptions.

Carnegie et al. (2010) examined a study of the Federal Transit Administration in 2001 that assessed the security perception of 25 transit agencies in the United States with 2,593 customer interviews and 634 vehicle operator interviews. He said the following:

- “The overall perception of security was generally very high among customers. More than 45% of customers perceived their transit systems to be very secure and another 30% perceived their systems to be secure. [...]
- Consumer perception of security was lower for multi-modal systems and systems with more than 250 buses compared to smaller systems.
- Among security measures, security cameras and police patrols made customers feel the most secure (about 33% for each), followed by lighting (about 12%), intercom (about 9%) and other measures (about 13%).
- Customers felt most threatened by teenagers who they worried may harm them in some way. The crimes they worried about most were robbery and assault.
- Female passengers’ perception of security was markedly lower than male passengers.
- Operators’ perception of both in-vehicle and at-station security was distinctly lower than customers.
- About 35% of operators had observed security breaches, while only about 12% of customers observed such events.” (Carnegie et al. 2010:12, according to FTA 2001).

In comparison, a 2011 analysis of the R+V Insurance that examined the German fear of terrorism in relation to the number of terror events that occurred, revealed that the average *level of terror fear* has been about 47.5% since 9/11 (prior it was 27.7%) (R+V Insurance 2011). Concerning societal risk aversion to extreme

events, Slovic et al. noted that the population seems to accept societal impact more easily from many small accidents than from accidents that are more serious but less frequent (Slovic et al. 1984).

2.6 Non-/Acceptance of Security Measures

The literature contains several definitions of acceptance. Most deal with the product/service and customer relationship and are similar to: “Acceptance is defined as gaining agreement from the customer that the deliverables produced [...] meet the criteria defined by the customer” (Westland 2006:84). The origin of the word *acceptance* comes from the Latin word *accipere*, which means to receive and honor e.g. a recommendation. Webster’s Dictionary defines acceptance as: “an agreeing either expressly or by conduct to the act or offer of another so that a contract is concluded and the parties become legally bound” (Webster 2014). In public transportation, this is the “transport agreement”. The fact that acceptance is not bounded to a specific request between different people is important for the understanding of the concept. More often, acceptance is implicit by a certain act that can be misunderstood by incorrect assumptions or misinterpretation of reactions.

In the discussion of acceptance, the visibility of measures to customers plays a major role. Measures are divided into *covert* and *overt* measures. While physical barriers, security personnel, and television cameras are visible to customers, other measures such as emergency plans, remote sensors or detectors, and employee training are not visible (see Figure 5).

Transit Security Measure	Visibility to Passengers
Facility-specific Measures	
Physical barriers	High
Locking systems/Access control	Low
Public address systems and signage	Medium
Sweeps/inspections	High
Alteration of operations	Low
Local alarm system	Low
Perimeter alarm systems	Low
Advanced or sophisticated remote alarm system	Low
Simple or high security lighting	High
Watchmen	High
Highly trained armed guards	Very High
K-9 units	Very High
Remote sensors or detectors	Low
CCTV	Medium
Vehicle-specific Measures	
Panic button for operators	Low
Two-way radio	Medium
CAD/AVL technologies	Low
Onboard video camera	Medium
Onboard security personnel	Very High
Onboard sworn police	Very High
Protective structure for operator	Low
Specially trained operator	Low
Other Measures	
Designated "Shelter in place" locations	Low
Decontamination site	Low
Mitigation equipment	Medium
Fire suppression equipment	Medium
Employee awareness program	Low
Employee screening	Low
Basic communication	Low
Intelligence/Information sharing	Low
Formal contingency plans	Low
Evacuation and assembly lockdown	Low
Drills	High

Figure 5: Transit security measures and passengers' potential awareness
(Source: Carnegie et al. 2010:8)

Public transportation providers often implement security measures and expect consensus from customers. While acceptance is difficult to measure, non-acceptance can be measured more easily by assessing customers' increasing replies in *feedback/complaint management*, *social media*, or, in the worst case, *decreased ridership*. As a result, (non-) acceptance is a social phenomenon, which can be described as a basic action feature and structure feature of the interpersonal life together (Lucke 1995), which fluctuates depending on the object, sub-

ject, and context. In the field of risk acceptance, Renn defined acceptance as a result of a decision process influenced by the subjective weighted consequences and probabilities (Renn 1980).

The construct of acceptance itself is very complex. Achieving the appropriate balance between positive, objective benefits and negative interference of customers (Dunmore 2010) is a major challenge.

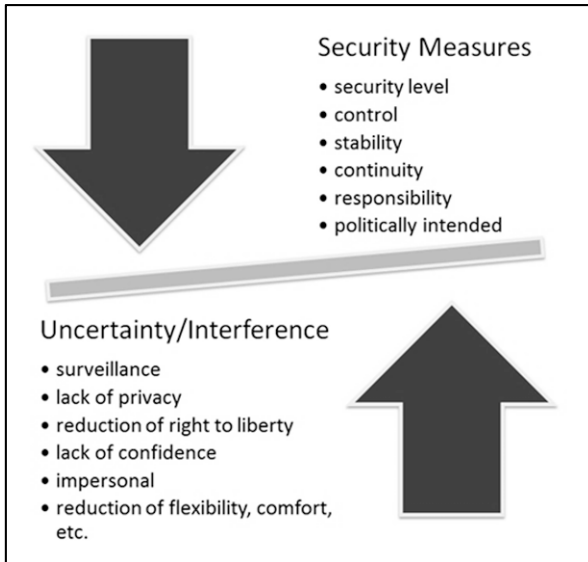


Figure 6: Achieving the appropriate balance (Source: Dunmore 2010, adapted by author)

Different approaches of different scientific fields can be applied to some degree to the topic of technology, security, and risk acceptance. The assignment is often not clear, but Renn (1980) worked out a summary of the different theories of technology and risk acceptance in general in context of nuclear energy (for details see Table 1).

Table 1: Explanation approaches of risk acceptance (Source: Renn 1980, adapted by author)

Area of Science	Theory	Brief Description	Authors
Economy	Theory of marginal utility	Estimation of marginal cost-benefits; comparison of individuals, groups, and society	Felix, Renn
	Economic theory of policy	Requirement maximization through resource mobilization and political Influence	Downs, Frey, Titz
Risk theory	Normative risk assessment	Best approach to estimate cost-benefits; risk minimization and alternative choices	Rowe, Lowrance, Kates, Fischhoff, Sagan
	Normative decision-theory	Process optimization to help decision-makers to a 'fast' rational decision	Coombs, Orkent, Raiffa
	Descriptive decision theory	Determination of the determinants of the actual decision-making process	Janis/Mann, Pollatsek, Tversky, Vlek, Stallen, Coombs
	Revealed preference analysis	Historical risks as indicators for the assessment of future risks	Starr, Cohen
	Referred or expressed preference analysis	Empirical determination of risk elements through questionnaires	Fischhoff, Slovic, Lichtenstein
Psychology	Psychoanalysis	Transfer of psychoanalytic terms and concepts	Schild, v. Erichsen, Wünschmann, Tubiana
	Psychology reduction theory	Transfer of psychological mechanism of perception	Pahner, Pelicier
Social psychology	Risk perception	Perception effects in risk estimation (attributive biases)	Maynard, Tversky, Fischhoff, Slovic, Vlek, Kogn, Bierbrauer, Frantzen, Schmid-Jörg
	Risk socialization	Interpretative patterns for risk assessment	Gutmann, (Battelle), Cohen/Hansel
	Attitude concept	Attitude of subject cause acceptance	Otway, Niehaus, Davis, (v. Buiren), Fishbein
	Communication concept	Controversy is part of misdirected or distorted communication	Goerke, (Eisenbart, Crebsbach)
Sociology	Economic sociology	Results of scientific economy processes	Notwotny, Tschiedel, Prüß, Hülsmann
	Empirical conception	(Dis-)functional discussion of value orientation	Lübbe, Schoeck, Douglin, Tognacci, Melber, Turley & Stone, Gerhold
	System-analytical concept	Exchange of system and policy periphery	Schneckener, Daase
	Conflict theory concept	Discussion of interest conflicts and participation	Scharioth, Paschen, Andritzky
	Normative democracy	Discussion toward more democracy	Schumacher, Moßmann, Daase, Engert, Junk

This list is a brief overview of different approaches, and there is a great deal of social research work missing. However, it provides an impression of how many different points of views exist regarding determining acceptance in the context of technology and risk. Regardless of which approach is chosen, all the theories have their strengths and limitations (e.g., relying on assumptions) and are more or less comprehensive and accurate.

An approach that is easy to handle and applicable for decision-makers, is highly desirable but missing due to the complexity of this topic. Therefore, research institutes in different science disciplines and commercial organizations often execute acceptance studies on behalf of providers.

2.7 Summary of the Literature

The literature review shows the complexity of this research area. Different players are involved such as research (different disciplines), policies, authorities, industry, and society. A dialogue between all stakeholders is highly desirable and has to be supported (COM 2004).

Especially, critical infrastructure are vulnerable; their “[...] incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” (Department of Homeland Security 2013) and have to be protected. Especially public transportation systems are highly vulnerable due to their open access and service to the public. Their operators have the dilemma to secure their systems on an acceptable level considering limited budgets, policy demands, and customer satisfaction.

Having a closer look on terrorism, an additional component is added to an already vulnerable system. Terrorism is an anthropogenic threat with low probability but high consequences. Normative risk approaches fail in assessing terror threats because the discrepancy can hardly be evaluated. New holistic risk management approaches are necessary to assess terrorist risks considering provider’s needs (Pickl et al. 2011).

Security measure shall improve the security of public transportation system in context of terrorism. Various security measures in different categories are available, but their effectiveness on preventing terrorist attacks cannot be proven by statistics. Therefore, their objective effectiveness is mainly assessed by statistically data of crime act reduction, vandalism, etc.

Statistical data of crime act reduction (cp. Laycock and Austin 1992, Welsh et al. 2010, Barclay et al. 1996, Hesseling 1995, Kenney 1986, Pennell et al. 1986, 1989) cannot be transferred to terrorist events. Furthermore, in the field of sub-

jective (technology) acceptance of security measures, the variety of research possibilities and theories from different scientific disciplines leads to confusion and discouragement on the provider level. Recommendations (such as Commission communication COM 2004 or Burkhard et al. 2008) exist but in a very general manner and provide no definite framework. Although security measures have a positive effect, their operation causes more or less hindrances and restrictions for the customer. “Achieving the Right Balance” (Dunmore 2010) between objective security and customer satisfaction is a challenging task for public transportation provider. Hence, public acceptance of security measures is an important part of customer satisfaction and therefore of total quality management of the provider (Degenhart and Fiedrich 2004).

An explicit structural framework is missing, especially one that is capable of capturing the consequences of security measures at the customer level to compare them with the benefit expected by the provider. So how can the objective and subjective effects be measured and included in a risk management system? To answer this question and other arising questions, objectives are defined and a conceptual framework developed in Chapter 3.

3 Research Concepts

“That sense of contributing to a community is never more rewarding than when you discover something that you believe can improve your readers’ lives by changing what and how they think”
(Booth et al. 2003:8).

The assessment of security measures against terrorist threats according to their objective and subjective effects and the development of a structural decision-support framework require a research concept that provides an interface of the procedure, the used methodologies, and how the results are applied in a decision-support system.

In Section 3.1, some working hypotheses and limiting conditions are set to conduct the study. A conceptual framework with a research procedure is developed, based on hypotheses as explained in Section 3.2. This represents the study procedure and the methodological steps executed. One objective is the application of decision criteria in a supporting decision tool to find the most suitable security measure taking into account end-user requirements and needs. Therefore, the author compiled the requirements of public transportation providers (end-user) to choose an appropriate decision-support system, which is described in Section 3.3. Lastly, the limitations of the research concept are considered in the discussion of the results and the already known limitations are presented in Section 3.4.

3.1 Research Assumptions and Hypotheses

The following assumptions are set to address terrorist threats:

Firstly, public transportation systems are especially vulnerable because any interruption of operations hurts daily life and affects many customers. In this study, risk management measures, especially security measures, that have a preventive effect on terrorist attacks are considered. Kersten and Klett (2008) called them “*security measure type 2*”. Security measures that mitigate the effects of

terrorism or reduce possible consequences (*security measure type 1*) are not considered in this study.

Secondly, terrorism itself is manifold. An overall effectiveness of security measures in every possible scenario in a complex system such as public transportation is unrealistic. Therefore, a scenario-based approach is chosen to prove the objective effectiveness of security measures within the given scenario. The values of effectiveness might change with the scenario.

Thirdly, threats such as terrorist attacks lead to mistrust in the security and safety of the system and to a loss of customers and other related consequences (e.g., increase of individual traffic). Hence, security measures accepted by the customer have to be implemented to overcome any feeling of mistrust of the system. The interference and restrictions caused by security measures are identified and researched to measure the effects of security measures on customers in public transportation systems. Every implemented security measure in public transportation systems causes more or fewer hindrances and restrictions for the customer. *Every security measure can be characterized by the consequences affecting the customer (hypothesis).*

The author has set the goal of contriving an indicator for security measure acceptance that can be easily transferred to already implemented security measures (retrospective analysis) as well as proposed measures (prospective analysis). Decision-makers can use this composite indicator representing the subjective effects at the customer level to determine the extent to which security measures are accepted or not. The acceptance of security measures depends on the level of restrictions and interference caused by it to the customer. *The determination of the acceptance of interference as well as the influence of the security measure can be an indicator of the subjective effects of each security measure (hypothesis).*

3.2 Conceptual Frame of Security Perception and Security Measure Acceptance

To achieve the study objectives, a conceptual framework was needed to address the research questions in a structural manner. Shields and Rangarajan (2013) defined a conceptual framework as “[...] the way ideas are organized to achieve a research project’s purpose” (Shields and Rangarajan 2013:24). This framework contains the used data (input), the applied methodological steps (processing) and the results (output). In complex research procedures, where different study results are determined and re-processed in further research action, a flow chart

gives an overview of the research procedure. Figure 7 presents the flow chart of this study.

The study is divided into three phases: The first phase is called **Planning** and contains a description of the research objectives, requirements, literature review, and concept. The second phase, called **Execution**, includes data acquisition, processing, and a discussion on the results of three criteria. The three criteria were derived from an experts' requirement workshop and literature review (guidelines for public transportation providers). In the last phase, **Application**, the criteria results are applied in a structural decision-making process using multi-criteria decision analysis (MCDA) (see Figure 7).

The determination of the subjective, social-technical criterion, *acceptance*, was the most challenging part due to an absence of concepts regarding the capturing of data. The author focused on this criterion in this study; previous study results were available for the determination of the *technical/objective effectiveness* and *economic costs*.

Certain things have to be considered to estimate a social-technical indicator: According Simpson and Katirai (2006), indicators have been used to measure social processes but still amount to a simplification of complex systems. "General problems known for indicators and indices include subjectivity, bias, weighting, aggregation, normalization, and selection of indicators and data sources. The purpose of building indicators is to derive general approximations over a number of research units and to be able to make comparisons between these units" (Fekete 2010:20).

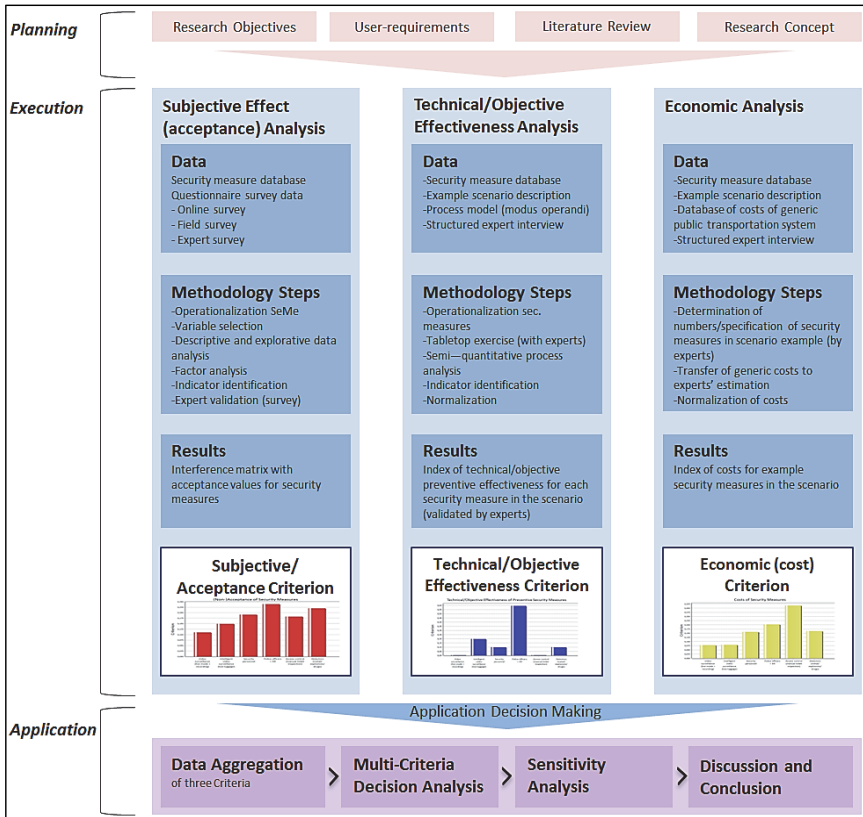


Figure 7: Flow chart of research procedure (Source: author)

The acceptance of security measures is such an indicator as well as an overall security perception. Both indicators include subjectivity, bias, normalization, and weighting problems as well as different data sources. In addition, a solid measurement of acceptance requires a broad understanding of the security measures not expected of customers. Such aspects as the availability of data, applicable methodologies, and the intended research objectives should be factored into the design of the indicator. A common understanding of how security measures affect customers is a key approach to solving the complexity of accepting measures in public transportation systems.

Following the framework, the author executed these steps:

Table 2: Research steps in the study (Source: author)

Identify and define the research goal (Sections 1.1 and 3).	
Subjective, social-technical criterion acceptance	Develop a concept of survey for data acquisition (Section 4.1).
	Collect and describe security measures in public transportation systems; establishing the security measure database (Section 4.2).
	Convert the developed security measures into operation plans; investigate potential direct and indirect effects of security measures on customers' acceptance (interference analysis) (Section 4.3).
	Collect data through customer surveys and identifying possible data gaps and, if indicated, conducting an error analysis. A survey of experts should be part of the validation process (Section 4.4).
	Re-translation process of interferences into security measures (Section 4.5).
Technical/ objective effectiveness criterion	Adapt semi-quantitative methodology for expert-interview according generic process model for data acquisition (Section 5.1.1).
	Adapt software demonstrator for analysis, prepare operation plans of security measures according security measure database (Section 5.1.1).
	Collect data in tabletop exercise (Section 5.3).
	Analyze results, create indicator of effectiveness (normalization) (Section 5.3).
Economic criterion costs	Determine numbers/specification of security measures in scenario example (tabletop exercise) (Section 5.1.2).
	Transfer of generic costs to experts' estimation and normalization (Section 5.3).
Decision analysis multi-criteria decision analysis	Define criteria and attributes (Section 5.1).
	Describe an example scenario for decision-making, defining modulus operandi, location, weapon, target of a fictitious terrorist attack (Section 5.2).
	Apply the criteria to the scenario, data acquisition (Section 5.3).
	Data aggregation in multi-criteria decision analysis software; execute example decision-making (weighting of importance) and stability analysis of weighting (sensitivity analysis) (Section 5.4).
	Summarize results and reflecting pros and cons of MCDA (Section 5.5).
Discussion of scope and limitations, validation of results, and conclusion (Sections 6 and 7).	

3.3 End-User Requirements

This interdisciplinary study is end-user orientated and ends with the development of an exemplary decision process for the implementation of security measures against terrorist threats in public transportation systems. Therefore, the author collected user requirements for the decision process and possible decision-support systems (tools). The author discussed the following requirements for a decision tool with security experts of railway public transportation providers and researchers in this field at the 10th World Congress of Railway Research¹.

Requirements for a decision tool for risk management of terrorist attacks:

1. Easy to use, applicable, uncomplicated (user-orientated)
2. Universally applicable to all security measures
3. Determination of the objective effects of security measures
4. Includes the possibility to display the costs of security measures
5. Assessment of subjective effects of security measures
6. Weighting by the end-user according to company preferences
7. Documentation of decision-making processes

The requirements were re-assessed at a tabletop exercise, which was executed in cooperation with the Kölner Verkehrs-Betriebe AG (KVB) including experts of KVB, Berliner Verkehrsgesellschaft AöR, and Münchener Verkehrsgesellschaft mbH in 2014.

Based on these requirements, the author developed the research concept including three decision criteria as well as different methodologies to provide and deliver the required data for the decision-making process. End-users wished for an easy-to-use software platform that allowed criterion weighting and sensitivity analysis to evaluate decision processes. The author used software executing multi-criteria decision analysis (MCDA) developed by the Karlsruhe Institute of Technology and an own security measure database. The database includes various security measures, implementation costs, preventive effectiveness, and their subjective effects on the customer. The MCDA and the knowledge database allowed the author to perform different decision-making processes treating social acceptance of security measures as an integrated part of risk management.

¹ 10th World Congress on Railway Research 2013, Nov. 25-28, 2013 in Sydney, Australia.

3.4 Limitations

The *acceptance* as socio-technical criterion is influenced by different parameters, e.g., a parameter is the current security perception in the immediate social proximity (Wurtzbacher 2003). The survey in the present research was conducted in the city of Cologne. The captured results do not represent the overall public acceptance of Germany or the world although the results provide information about general tendencies.

Additionally, no information about the terrorism context was provided to the customers due to the fact the acceptance of security measures rises with the individual perceived threat level (Krasmann et al. 2014). Assessment of customers' acceptance was based on the daily routine of travelers in Cologne in order to avoid bias. Furthermore, the acceptance security measures may follow habituation effects, which have to be proven. Customers can assess their perception of new security measures from a different point of view. Analysis should consider positive as well as negative trends.

The surveys were executed in cooperation with the Kölner Verkehrs-Betriebe AG, therefore the following limitations should be considered in the analysis and conclusions:

- Scoping is set up on the municipal level (the City of Cologne, Germany).
- Role: Statistical population is public transportation customers (in fact respondents of survey).
- Type of security measure effect: active (functions alone) and passive (needs further measures).
- Time period of security measure effect: preventive effect.
- Costs of security measures: all costs (life cycle costs).
- Subjective effects of security measures can be described in caused interferences.
- Objective effects of security measures: Effectiveness in reducing the vulnerability of a scenario event.
- The target audience is scientists and decision-makers who deal with intentional, anthropogenic risks in critical infrastructure.

- Limiting characteristics are the captured data in space and time:
 - The data are collected on the municipal level: generalization or transfer of results have to be proven carefully, especially regarding environmental factors of different public transportation systems. In addition, the data provides a temporal look at the current security/safety feelings of customers. Prospective events or development might influence data.
 - Analysis results of potential security measures related to safety/security objectives of public transportation are collected in a database (current state of the art) and future technologies can be added.
 - The survey investigates the acceptance of security measures in the context of security perception but it does not take into account other dimensions such as legitimacy, morality, and ethicality levels.

Table 3: Development of indicators (Source: author)

Goal	Measurement of customers' acceptance of security measures
Target group	Scientists and decision makers dealing with implementation of security measures
Focus	Social sphere of security perception
Component of analysis	Security perception, interference criteria
Elements	The customers of the Kölner Verkehrs-Betriebe AG
Context	Securing a public transportation system against terrorist threats
Research area and scale	City of Cologne, Germany
Point in time	Before the next terrorist act

4 Acceptance of Security Measures

“Once you can accept the universe as matter expanding into nothing that is something, wearing stripes with plaid comes easy”
Albert Einstein (1879-1955).

As described in Section 2.6, the literature provides different approaches to measuring risk acceptance, technology acceptance, or security perception. In the field of technology acceptance, Meng and Vollbracht (2014) claimed, most models are based on (a) input models, (b) input-output models, or (c) cycle models. All models use the end-user and the technology as the focus of their investigation. In the context of public transportation, the operator/provider represents the end-user. A transfer of the models to customers' acceptance is not possible. Furthermore, the models consider only technology and cannot be used to investigate other security measures such as personnel, organizational, and construction measures (Meng and Vollbracht 2014).

As a result, empirical approaches are used to focus on the customers' point of view. The following section explains the process of empirical data acquisition and assessment. In Section 4.1, the concept of the survey is introduced and then followed by a four-step program of execution developed by the author (see Figure 8).

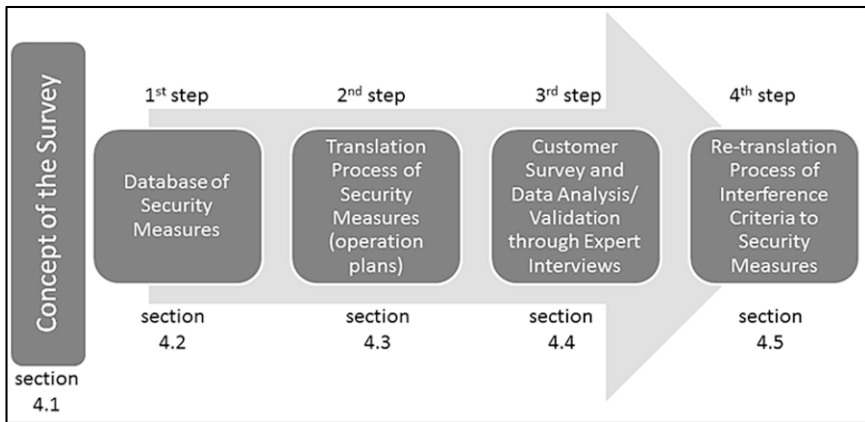


Figure 8: Structure of Chapter 4 ‘Acceptance of Security Measures’ (Source: author)

4.1 Concept of the Survey

Social factors are often difficult to understand, making it necessary to have a structural methodology to collect valid data. Even more challenging is the fact that subjective factors are latent and can be investigated mainly in specific situations. Hypothetical survey questions (like *would you accept this security measure, which prevents terrorist attacks?*) do not present accurate and valid results regarding acceptance, feelings, and perceptions because the situation and the specific perceptions cannot be reproduced (Schlüter et al. 2010), which is why some scientists use in situ surveys to obtain valid data. This is not possible in the context of terrorist attacks.

In addition, it is difficult to assume that the respondents comprehend the mechanisms of all security measures and assess them in the right context. Furthermore, human acceptance depends on security perception and is a construct influenced by specific cultural, locational, situational, and individual factors. Our individual perception uses background information from surrounding conditions as well as from socio-cultural and individual imprinting. These are influenced by many factors such as societal values, psychological profile, character traits, and instincts, which complicate any measurement (Wills-Herrera et al. 2012; Maslow 1943; Wagner and Lehnigk 2010).

Therefore, how can a subjective value such as acceptance be measured without bias? A solution was found in a study by Winzer et al. 2009. They were

searching for security indicators and presented their survey concept (see Figure 9), showing that while objective process quality and individual behavior are directly measurable, subjective process quality itself is only *indirectly* measurable. The acceptances of different security measures can be seen as a subjective process quality. As a result, indirect measurements are used based on *easily understandable statements about the acceptance of interference caused by security measures*. The concept includes different surveys and assessment framework that results in an innovative questionnaire. The empirical concept of using the interference criteria to draw conclusions about the acceptance of security measures is a new approach not previously used and is based on the research assumptions (Section 3.1).

In the following Section 4.1.1, the methodology is explained in detail as part of the survey concept, as well the innovative questionnaire, which contains the questions regarding acceptance of the interference of security measures (Section 4.1.2).

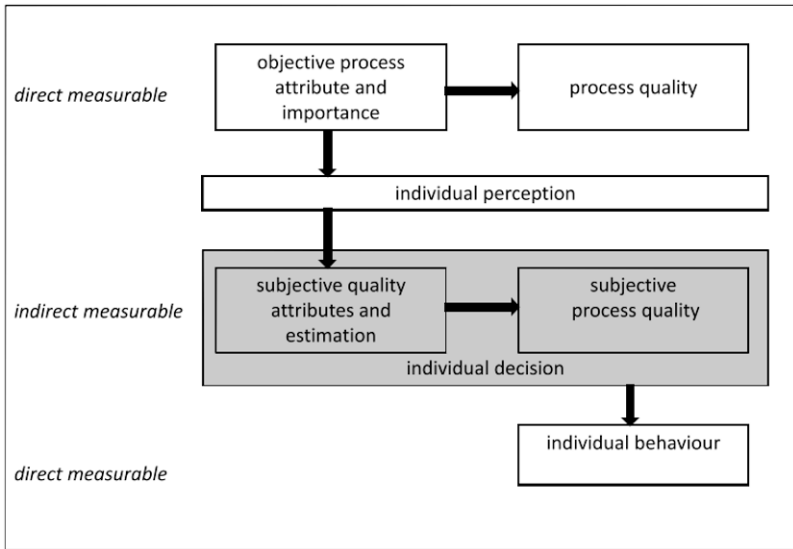


Figure 9: Indicators for security and safety in public transportation platforms-a case study (Source: Winzer et al. 2009)

4.1.1 *Development of Methodology for Data Acquisition and Analysis*

Because subjective values such as perception and acceptance are relatively abstract social constructs (Tversky and Kahneman 1974; Slovic 2000), the author used different empirical methods based on triangulation that included qualitative and quantitative methodologies to explore the public acceptance of security measures in accordance with security perception in public transportation systems (Denzin 1970).

First, a security measure database is required. The author and his team collected 81 different security measures, including descriptions of their objective effects on a public transportation system. This database originally combined a new vulnerability method and a scenario database to estimate the vulnerability of a system according to different scenarios (Brauner et al. 2014b, 2014e). The security measures were clustered into their mode of action and used in this study as the primary database (Brauner et al. 2013a).

The acceptance of security measures can be determined by surveying customers of public transportation systems. Because customers do not know all security measures in detail and the context of terrorism is strongly influenced by a subjective threat component, direct questioning could lead to incorrect acceptance results. To prevent this, a new approach was developed in this study.

Using the hypothesis *“Every security measure can be characterized by the consequences affecting the customer (hypothesis),”* security measures were denoted by the extent of their interference.

“Interference criteria describe the effect of security measures upon customers while they use the public transportation system. The assessment of the acceptance of these interference criteria allows referring to an accepted selection of security measures” (Brauner et al. 2013d: 6).

The levels of interference are criteria that can be easily dealt with according to their acceptance.

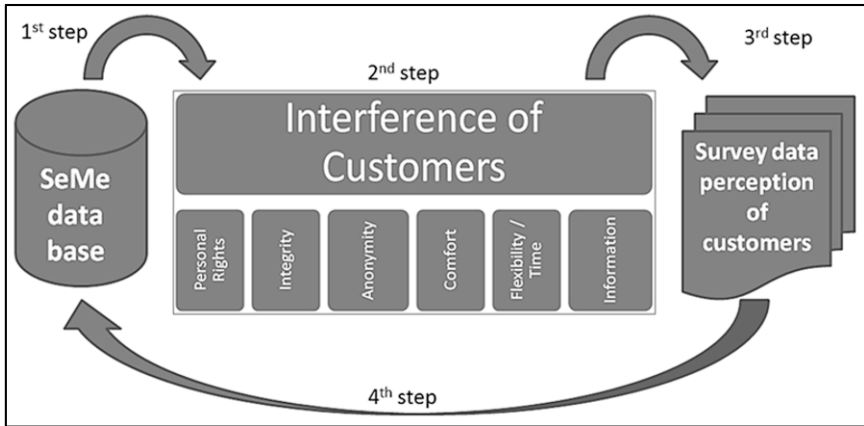


Figure 10: Triangulation of methodologies for data acquisition (Source: author according to Brauner et al. 2013d)

The approach is structured in a four-step *translation and re-translation process*. First, the security measure (SeMe) database was translated into interference criteria that influence customers individually when they use the public transportation system. The IC are clustered in the categories *personal rights*, *integrity*, *anonymity*, *comfort*, *flexibility/time*, and *information*. A detailed description of the IC is provided in Section 4.3. Second, the translation matrix can be used for online surveys as well face-to-face interviews (field interviews) of public transit customers to estimate the acceptance of each IC. In the third step of this methodology approach, a ranking of the IC is made on the basis of the results obtained from customer answers.

In the fourth and final step, the results are *re-translated* in a statement about the acceptance of each security measure. This process is supported by expert interviews. At the end, customers' acceptance of the different security measures are quantified allowing further application in risk management (explained in Section 4.6).

4.1.2 Structure of Survey and Execution

In cooperation with the Kölner Verkehrs-Betriebe AG (KVB), several possibilities of questioning customers were identified:

- *Field survey:* In a field survey, customers can be questioned about how their current perception of security is influenced by their surroundings. It also allows questions about the acceptance of interferences.
- *Online survey:* The KVB department of customer service has a database of registered customers who can be contacted for questioning. This allows easy, simultaneous access to many customers. Because customers complete a voluntary questionnaire at home and not while using a public transportation system, questions about their current security perceptions in the public transportation environment are answered from memory.
- *Panel discussions:* KVB suggested the use of panel discussions to validate results of surveys. This allows collection of qualitative feedback regarding the quantitative results of surveys.

Finally, all three options were adopted. This allowed a comparison of the results of the online survey with the results of the field survey as well validation through panel discussions.

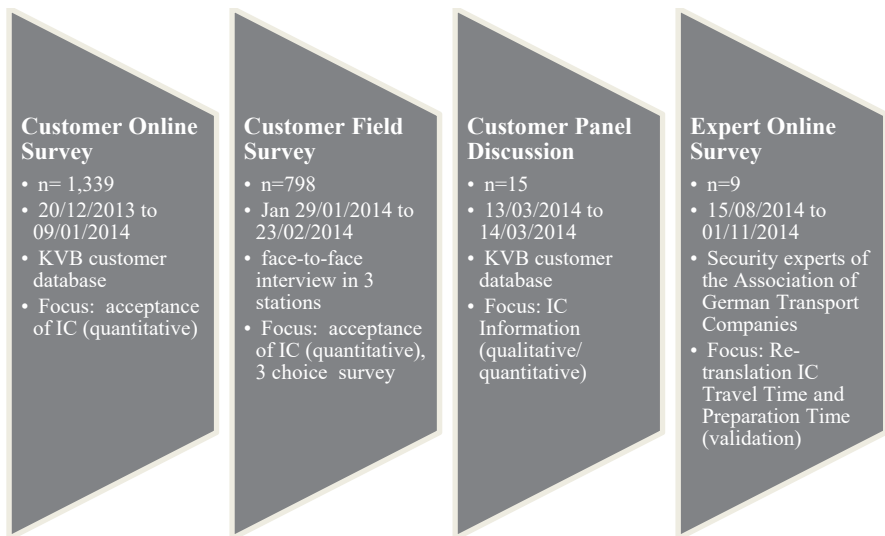


Figure 11: Executed survey in the study acceptance analysis (Source: author)

The development of the methodology, concept, and ideas was completed by the author while the execution of the surveys was supported by KVB, which assigned GROSCHOPF Rescue Engineering Consulting for the execution and documentation of the surveys. Later, a forth survey of security experts (Association of German Transport Companies) was done to validate some interference criteria.

4.2 Step 1: Database of Security Measures

In the joint RiKoV research project, Brauner et al. identified 81 security measures that are currently used or are prospectively usable in public transportation systems (Brauner et al. 2013a). Figure 12 clusters the security measures into the type of measure, their mechanism, and time of effect in the event of a terrorist attack. The data were collected through a comprehensive literature review.

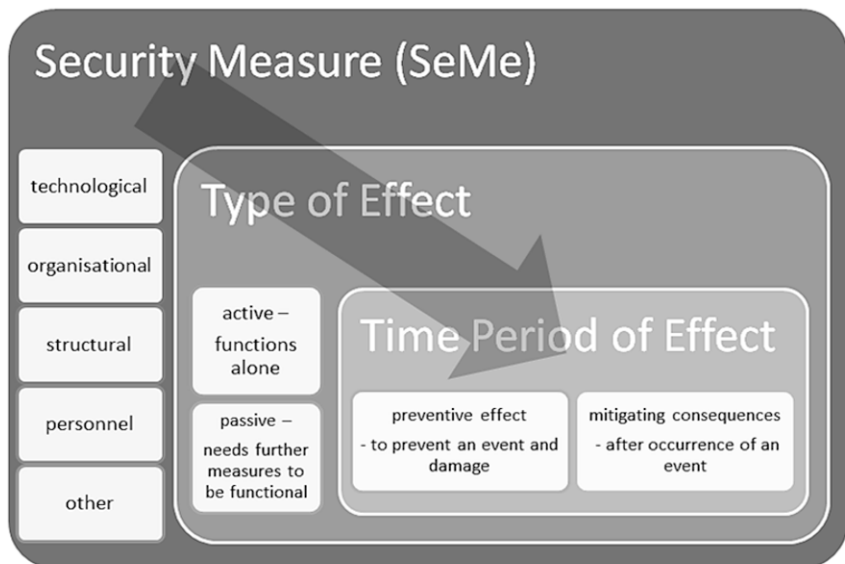


Figure 12: Categories of security measures (Source: author, according to Burkhard et al. 2008, Brauner et al. 2013a)

Several security measures such as those using personnel have different effects, including a preventive and mitigating effect on terrorism. There are also interde-

dependencies among the security measures increasing or diminishing their effects. A detailed description of all security measures is available in the Annex A—List of Security Measures in Public Transportation System.

Not all security measures are appropriate to prevent terrorist attacks (see Section 4.2) or influence customers’ perceptions (e.g., communication equipment of personnel or emergency plans). Accordingly, the author selected 29 security measures that have a substantiate effect in attack prevention according *security measure type 2* (Kersten and Klett 2008) (see Table 4).

The selected security measures were used for the acceptance analysis, and the operation plans of the security measures were extracted to identify the interference from the customers’ perspective.

Table 4: List of selected security measures (Source: author)

Video surveillance	Access controls (ac), Luggage controls (lc)	Detectors	Personnel
• live mode • videotaping • including light intensifier • IR thermography • face recognition • license plate recognition and recording • behavior recognition • detection of explosives or chemical and biological weapons (IR camera) • voice recording + analyzing	• ac: manual ticket inspection • ac: automatic ticket inspection • ac: with RFID/ credit-card or smartphone identification • ac: with biometric detection (face, fingerprint, iris recognition, etc.) • ac: with body scanner (terahertz radiation) • lc: manual luggage control • lc: automatic luggage control	• identifying aromas • increase in sweating • increase in body temperature • mobile detection of explosives • metal detectors • fluid detectors • sound recognition + hook-up • detection of CBRN (HamLet)	• security service • inspector/ ticket collector • police officers • plain clothes officers • patrol with dog

4.3 Step 2: Translation Process of Security Measures into Interference Criteria

This section describes the translation process of the security measures into interference criteria via estimating consequence categories (Section 4.3.1) in a first step and further into interference criteria (the smallest form of customers’ interference) (Section 4.3.2).

4.3.1 Consequence Categories as Part of Customer Perception

In consultation with the KVB, the author identified six categories that directly influence customers' acceptance of security measures (see Figure 13). These are called consequence categories; each security measure causes more or fewer consequences in these categories.

Personal Rights	In this category, all interference criteria are summarized that influence the physical privacy (e.g., intrusion of privacy by personnel of the operator or police).
Integrity	Acceptance of interference criteria that influence the integrity of customers (e.g., physically integrity during body control).
Anonymity	The capturing and saving of all kinds of customer data is part of this category.
Comfort	The constriction of the comfort (e.g., reduction of seating possibilities are concluded in this category).
Flexibility / Time	Interference criteria that reduce the flexibility of the customer are summarized here (e.g., luggage limitations, prolonging of travel time etc.).
Information	The knowledge and information of security measures are major part of the acceptance itself and summarized in this category.

Figure 13: Consequence categories of interference criteria (Source: author and KVB 2014)

The category *information* has a special role. Acceptance as well as security perceptions are both highly influenced by the information and knowledge about security measures. In reverse, especially misdirected information (e.g., media) lead to the feeling of insecurity and lack of acceptance, as the implementation of body scanners at German airports showed. The individual *state of information* cannot be captured for 81 security measures in a customer survey; the author, therefore, researched this part with a selection of different security measures in a panel discussion with 15 customers (see Section 4.4.4.2).

4.3.2 Translation into Interference Criteria

Interference criteria (IC) describe the specific influence of a security measure on customers. It is the *smallest form of interference* customers experience during their travel using public transportation systems. IC are also the basis of customers' reaction process and thus highly understandable. Processing these interferences and valuing them allows customers to make a rational decision of acceptance or non-acceptance of a security measure. The author and the KVB identified 26 IC shown in Figure 14 related to the consequence categories.

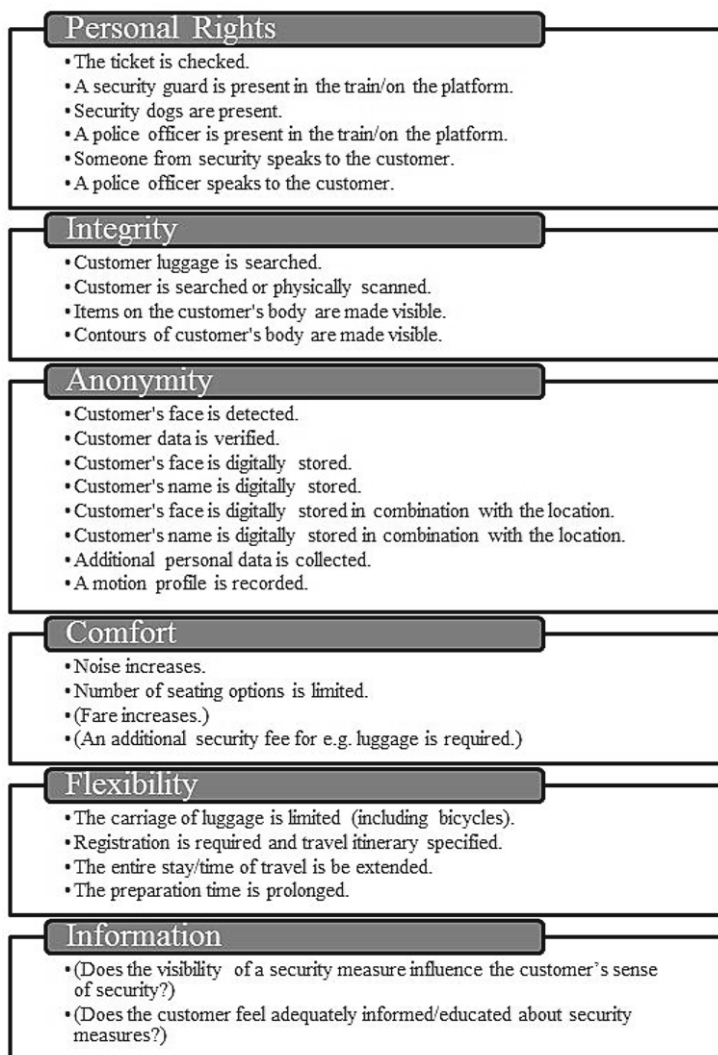


Figure 14: List of consequence categories and interference criteria (Source: author)

Almost every IC, except the *information* category, is a statement that can be answered by customers with an acceptance decision of “yes” or “no”. As security measures may require different IC at the same time and at different levels of intensity, the structure itself is fuzzy. While some of the IC are highly definable in

terms of appearance and can be easily answered by customers with clear statements of acceptance or refusal (yes or no), some are not concrete and cover a range of action (e.g., overall travel time or preparation time). For these unspecified IC, experts can assess the dimension of the security measures' effects using the MCDA (see Section 5.1).

According the security measure database, the multi-dimensional connections among measures are definable. Figure 15 is an example of seven security measures.

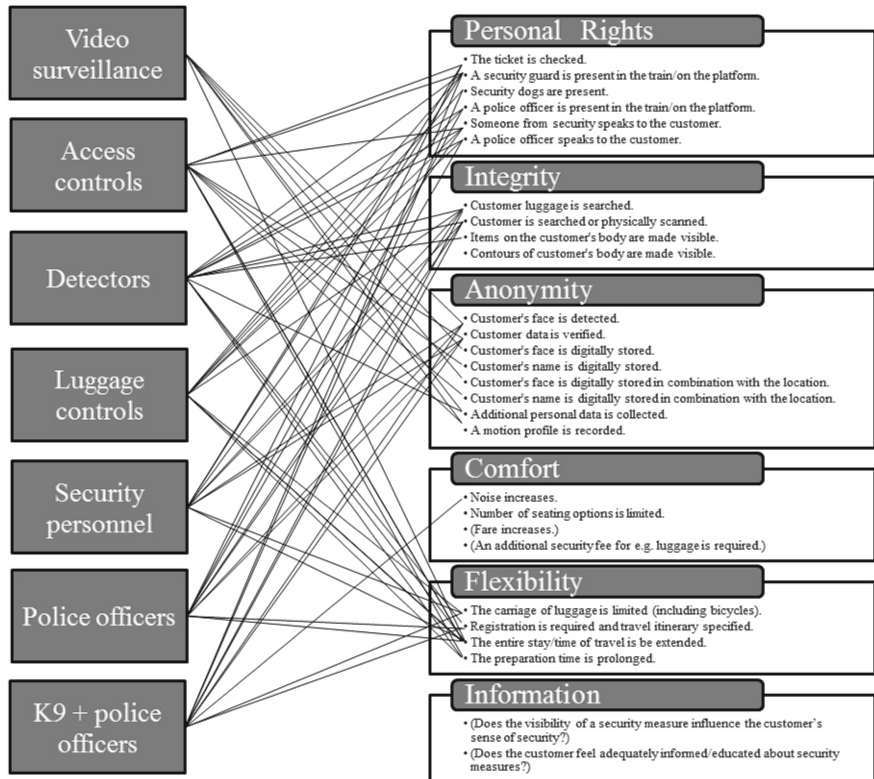


Figure 15: Example of connections among security measures and IC (Source: author)

4.4 Step 3: Survey—Data Analysis

KVB and the author commissioned the GROSkopf Rescue Engineering Consulting to acquire data (KVB and Groskopf 2014). Data acquisition took place from December 2013 to March 2014. Although the author did not participate in data collection, he designed, set up, and analyzed the data according to the research question. SPSS Statistics Version 22 was used for data analysis.

The online survey consisted of 54 questions, and the field survey of 56 questions. Therefore, the field survey used three choices (Surveys A, B, and C), with each having an equal share of acceptance questions. Both surveys included questions for further research of KVB and the author. A list of all the questions is available in Annex B—Questionnaires of Survey. The questions used in this study are listed in Table 5.

Table 5: Questions of online survey (Source: author)

Area	Topic	Question	Scale
Security Perception	State of current sense of security using public transportation (1 question)		Ordinal scale
Acceptance	Interference Criteria (acc. Section 4.3)	Personal rights (6 question)	“Yes/no” (dichotomous, nominal scale)
		Integrity (4 question)	
		Anonymity (8 question)	
		Comfort (2 question)	
		Flexibility (4 question)	
	Fare increase	In context of security measures (1 question)	Ordinal scale
	Additional security fee	e.g., for luggage (1 question)	Ordinal scale
Statistical data	Gender (1 question)		Nominal scale
	Age (1 question)		Cardinal scale, ordinal scale
Special Field Survey	Location (1 question)		Piusstr, Heumarkt, Appellhofplatz
	Time of survey (1 question)		Ordinal scale
	Choice of questionnaire		Nominal scale

The results of the survey are presented in the following sections. Firstly, the results of the online survey including an analysis of the security perception of the customers, the acceptances of the elements of interference and their ranking (see Section 4.4.1) are given. Secondly, the results of the face-to-face (field) survey is

presented, following the same analysis structure (see Section 4.4.2). Thirdly, the results are compared in the form of a validation in Section 4.4.3. The IC that deal with *time* and *information* issues were treated separately in an expert survey and customer panel discussion in Section 4.4.4.

4.4.1 Online Survey Results

The online survey was conducted from December 20, 2013 to January 9, 2014 using the KVB database of registered customers and an invitation on the homepage of the KVB website. In all, 1,339 respondents participated in the survey. Of this, 1,083 (80.9%) were registered customers and 256 (19.1%) participated using the homepage invitation link. The online group consisted of 41.7% female and 57.1% male respondents, and 1.2% of the respondents did not answer this question.

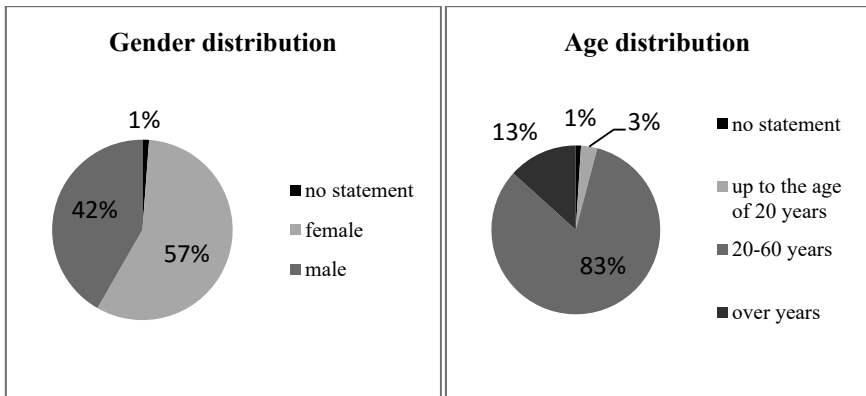


Figure 16: Gender and age distribution of online survey respondents (Source: author)

Although the survey was not age based (specific groupings), three major age groups were later established:

- Between 20 and 60 years old (82.6%)
- Over 60 years old (13.3%)
- Below 20 years old (3.1%)

The group clustering was based on the makeup of the major customer groups in the KVB passenger database. For respondents to the online survey, 82.6% were between the age of 20 and 60, 13.3% were over the age of 60, and 3.1% under 20. One percent of the respondents did not answer this question.

4.4.1.1 Analysis of Respondents' Security Perceptions—Online Survey

Descriptive Analysis:

The first question asked respondents about their current sense of security when using public transportation systems. Although it is a subjective question, respondents were asked to categorize their feelings into one of five categories from very bad to very good. The results showed a generally positive attitude toward the security of public transportation systems. Over 76% indicated they felt secure with answers in the acceptable or good categories. In addition, 10.2% indicated they felt very secure (a total of 86.2%). In the negative perception sector, 11.1% indicated they felt bad, and 2.0% indicated they felt very bad. Only 0.7% did not answer this question. The cumulative percentage graph in Figure 17 shows this result as a strong increase in the sector of satisfaction and a slight increase in the sector of dissatisfaction. In conclusion, more than three-quarters of the online survey respondents indicated they felt secure using public transportation in the Cologne area. This demonstrates respondents had a positive security image of the public transportation system. Hempel et al. (2011) found similar results in their SuSiTeam research project. Answering in the categories of “strongly agree” and “rather agree”, 34% and 54% of respondents (customers of the Berlin public transportation system) assessed their security perception positively (Hempel et al. 2011).

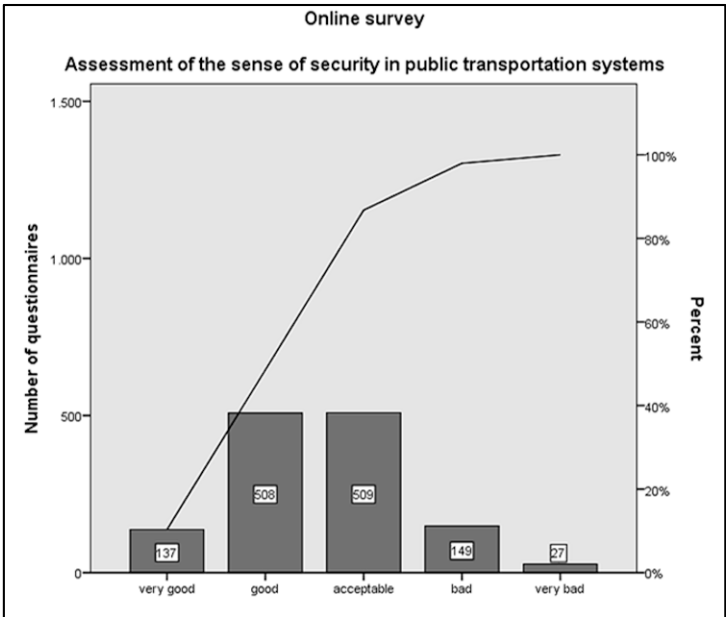
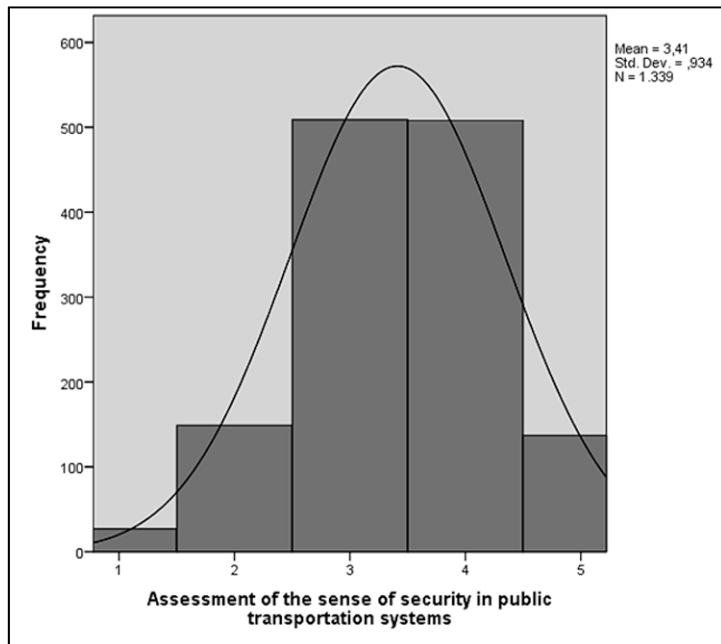


Figure 17: Pareto chart of respondents' sense of security in public transportation systems (Source: author)

A test of normality was used to determine if the above results can provide further information or be transferred to other areas. While the bar diagram in Figure 18 shows an similar tendency to the Gaussian curve that represents normal distribution, the Kolmogorov-Smirnov test as well as the Shapiro-Wilk test disproved any significance with a high degree of freedom (df). Thus, the results can be considered normalized; however, only a conservative analysis of skewness and kurtosis can prove this. An explorative analysis of skewness revealed a negative value of -0.497 with a standard error of 0.067. A skewness of zero would prove exact symmetrical behavior, but the negative value proves asymmetrical behavior toward the mean variable, in particular the measured values that scatter more on the left side. Figure 18 illustrates this behavior as the tail is longer on the left side of the graph. The correlation of skewness and standard error indicates that the measured mean variable is also skewed in the statistical population. Therefore, the empirical formula is that if the value of skewness (a non-negative value) is more than two times larger than its standard error, the mean variable is also skewed in the statistical population (Brosius 2014, Bühl 2014). In this case, the skewness is seven times larger than its standard error, which indicates the mean variable is also skewed in the statistical population. Analysis of the steepness of

the curve (kurtosis) provides a positive kurtosis value of 0.622 and a standard error of 0.134. This value demonstrates that the distribution of values is steeper than the normal distribution (Gaussian curve). The relation of kurtosis and standard error (standard error is 4.7 times smaller than the kurtosis value) indicates that similar results are expected in the statistical population.



Tests of Normality

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Assessment of the sense of security in public transportation systems	,217	1339	,000	,886	1339	,000

a. Lilliefors Significance Correction

Figure 18: Gaussian curve and bar diagram of the sample (Source: author)

Explorative Analysis:

A further investigation of female and male customers shows a small shift in feeling. Male respondents felt more secure with more answers in the very good category (11.5%) than female customers (8.4%). Male and female responses were

similar for the good category at 37.4% and 39.4%, respectively. Male and female responses in the acceptable category were 35.9% and 41.4%, and responses in the bad category were 13.0% and 9.0% for males and female, respectively. Male and female responses for the very bad category were similar at 2.2% and 1.8%, respectively. Male respondents had a tendency to assess the extremes higher than female respondents, who trended toward the middle (see Table 6). This effect combined with clustering reveals a higher positive feeling of security for female respondents (89.2%) than male respondents (84.8%). Clustering included the acceptable, good, and very good categories.

The expected count is a hypothetical value and displays the expected count for each value/cell if there is no statistical correlation between perceived security and gender. Comparison with the estimated counts can be used as a reference marker to obtain an impression of the correlation (Brosius 2014). In this case, especially in the bad and acceptable categories, there are large differences of counts and expected counts. In addition, another effect was extracted. In all categories except acceptable and good, the expected counts for females were higher than the collected counts (with the reverse effect for males). Correlation with such results is expected.

Pearson's chi-squared test reveals whether or not the result is applicable for the population. This statistical test of significance proves the hypothesis that there is no relation between the perceived security and gender for the population in general. Analyzing this data, the asymptotical significance is 0.028, which means this hypothesis is true with a probability of 2.8%. This means in reverse, in context of the population, that gender and perceived security in public transportation systems are correlated with a probability of 97.2% (see Table 6) according Pearson's chi-square test.

Table 6: Online survey cross-analysis—perceived security and gender of respondents (Source: author)**Crosstabulation: sense of security in public transportation systems * gender**

			Gender		total
			male	female	
Sense of security in public transportation systems	very bad	count	17	10	27
		expected count	15,6	11,4	27,0
		% within gender	2,2%	1,8%	2,0%
	bad	count	99	50	149
		expected count	86,1	62,9	149,0
		% within gender	13,0%	9,0%	11,3%
	acceptable	count	274	231	505
		expected count	291,7	213,3	505,0
		% within gender	35,9%	41,4%	38,2%
	good	count	285	220	505
		expected count	291,7	213,3	505,0
		% within gender	37,4%	39,4%	38,2%
	very good	count	88	47	135
		expected count	78,0	57,0	135,0
		% within gender	11,5%	8,4%	10,2%
total		count	763	558	1321
		expected count	763,0	558,0	1321,0
		% within gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10,857 ^a	4	,028
Likelihood Ratio	11,018	4	,026
Linear-by-Linear Association	,022	1	,882
N of Valid Cases	1321		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 11,40.

Table 7 shows the distribution of the age of respondents in relation to their feelings about security. Cross-analysis was applied to reveal potential correlation between age and perceived security in public transportation systems.

A first inspection exposed a highly unequal overall count in the three age groups. The reason for this imbalance lies in the structure of the customer clientele. Nevertheless, results based on the age group up to 20 years were interpreted carefully. Two trends were identifiable when comparing the different age groups. Initially, the relative values decreased from the good to very bad categories in all age groups. The second trend was in the categories themselves. In the outer very good and very bad categories, but also in the good category, the relative values decrease with increasing age of respondents. In the bad and acceptable categories, the opposite effect was observed. The expected counts underline these trends.

Clustering into positive (very good + good + acceptable) and negative (very bad + bad) feelings revealed a clear trend line. With increasing age, positive perception of security in public transportation systems decreases toward a more negative feeling. The same trend is also recognizable if the acceptable category is considered neutral and thus excluded.

However, the significance of the result for the population was undetermined. The Chi-square test resulted in an asymptotical significance of 0.002 for the null hypothesis, which indicated correlation with a probability of 99.8%. While four cells did not have the minimum of five expected counts (two nearly had the expected count), the result can be assumed correct.

Table 7: Online survey cross-analysis for sense of security and age of respondents (Source: author)

Crosstabulation: sense of security in public transportation systems * age of interviewed passengers						
			Age of interviewed passengers			total
			up to 20 years	20 to 60 years	over 60 years	
Sense of security in public transportation systems	very bad	count	1	24	2	27
		expected count	,8	22,6	3,6	27,0
		% within age of interviewed passengers	2,4%	2,2%	1,1%	2,0%
	bad	count	0	117	32	149
		expected count	4,6	124,4	19,9	149,0
		% within age of interviewed passengers	0,0%	10,6%	18,1%	11,3%
	acceptable	count	15	417	74	506
		expected count	15,7	422,6	67,7	506,0
		% within age of interviewed passengers	36,6%	37,7%	41,8%	38,2%
	good	count	16	430	59	505
		expected count	15,7	421,8	67,6	505,0
		% within age of interviewed passengers	39,0%	38,9%	33,3%	38,2%
	very good	count	9	117	10	136
		expected count	4,2	113,6	18,2	136,0
		% within age of interviewed passengers	22,0%	10,6%	5,6%	10,3%
total	count	41	1105	177	1323	
	expected count	41,0	1105,0	177,0	1323,0	
	% within age of interviewed passengers	100,0%	100,0%	100,0%	100,0%	

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	24,382 ^a	8	,002
Likelihood Ratio	27,411	8	,001
Linear-by-Linear Association	14,128	1	,000
N of Valid Cases	1323		

a. 4 cells (26,7%) have expected count less than 5. The minimum expected count is ,84.

4.4.1.2 Acceptance of Interference Criteria Caused by Security Measures

This section provides the results of the online survey regarding the acceptance of the IC. The IC, explained in Section 4.3.2, represent the different consequences of security measures at the customer level.

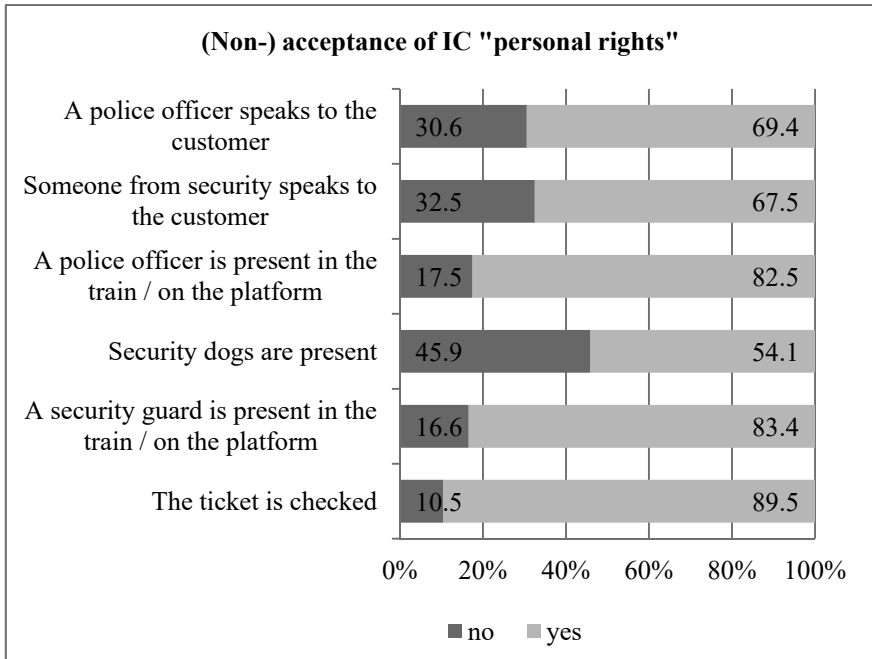


Figure 19: Results of online survey for personal rights IC (n=1,339)
(Source: author)

In the personal rights category, the respondents expressed high acceptance of situations where security measures affect them. A ticket check was accepted by 89.5% of respondents, followed by the presence of security guards in trains or on platforms with 83.4% positive answers and the presence of police officers with 82.5% (see Figure 19). The next IC in the ranking is “police officer speaks to the customer” with 69.4% positive respondents. The gap between the IC is due to the degree of interference that arises when personnel is merely present or actively interacts with customers with actions such as speaking with them. This is also the case for “security staff speaks to customer” with 67.5% positive acceptance. The last IC in this category is the presence of security dogs in trains or on platforms, which was accepted by approximately half of the online survey respondents (54.1%).

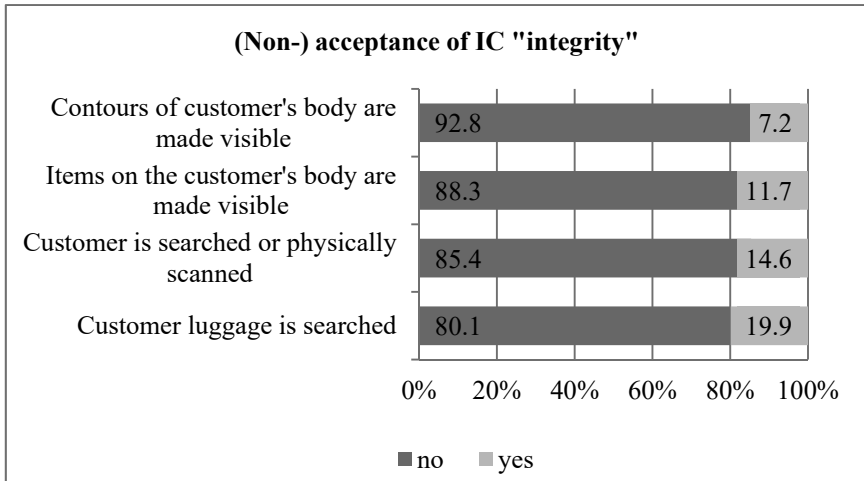


Figure 20: Results of online survey for integrity IC (n=1,339) (Source: author)

The IC in the integrity category were highly unaccepted. Among the four IC in this category, luggage control was the most accepted with 19.9% positive acceptance, followed by physical security checks that check customers for weapons and hazardous substances with 14.6%. The visualization of personal items or contours of customers' bodies using metal scanner or body scanner technology was even more unaccepted with 11.7% for body item checks and 7.2% for contour checks. A major reason for this customer reaction is the uncertainty about visualization data and further usage/storage issues.

In the anonymity category, the effect of uncertainty about data was examined in more detail. For seven IC, different personal data information is queried (see Figure 21). The collection of data and its storage were both highly unaccepted. In ranking, capturing customers' name was accepted by 20.0% of the respondents followed by capturing customers' faces with 11.1% acceptance. While capturing customers' faces was accepted by 20.0% of respondents, only half of this number accepted further storage of names in a database (10.1%). In the case of date and location storage, acceptance dropped further with 7.8% accepting storage of face and location data and 7.4% accepting storage of name and location data. Almost the same amount of respondents did not accept the digitally stored images of faces (7.2%). Other IC with low acceptance were the storage of additional customer data such as behavior (5.8%) or motion profiles (4.0%).

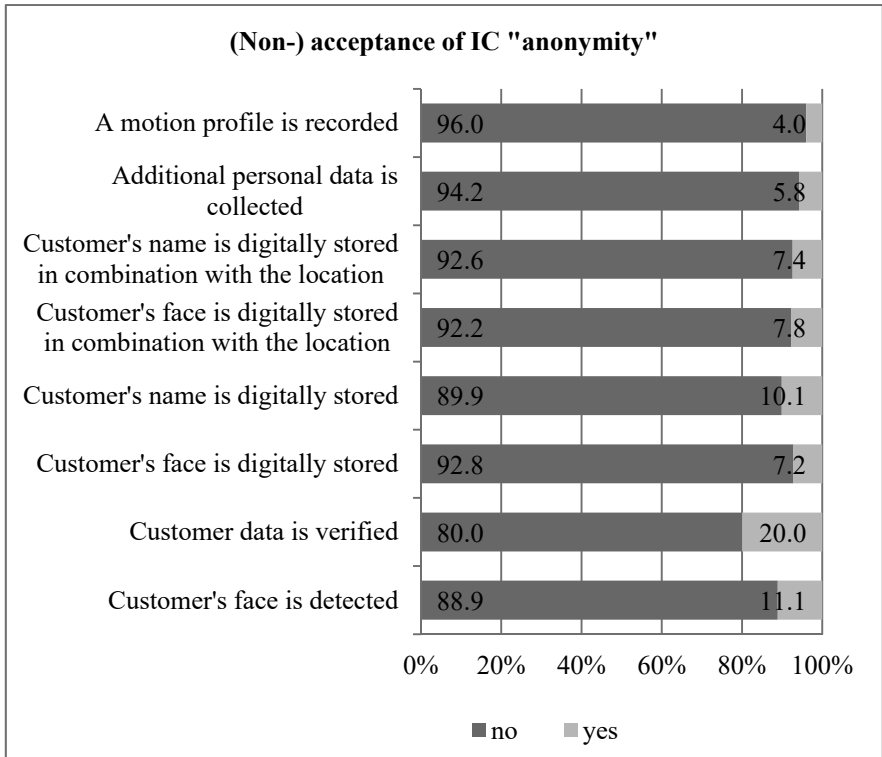


Figure 21: Results of online survey for anonymity IC (n=1,339) (Source: author)

The comfort category was divided into two sections: fare/fee and others. The split was due to the different kind of questions; while some questions could be answered with yes or no, questions about possible fare increases and security fees were weighted questions that depend on the amount of the fare increase. In the online questionnaire, the respondents were asked to what extent they would accept an increase in fares if its purpose was to improve the security situation in public transportation systems. Overall, 65.0% of the respondents indicated they would not accept any fare increase, and 26.7% indicated they would accept an increase of less than €0.50. Acceptance sharply declined in accordance to the price increase in fares. Only 6.3% would accept a fare increase between €0.50 and €1.50 and almost none (0.5%) would accept fare increases over €1.50 (see Figure 22).

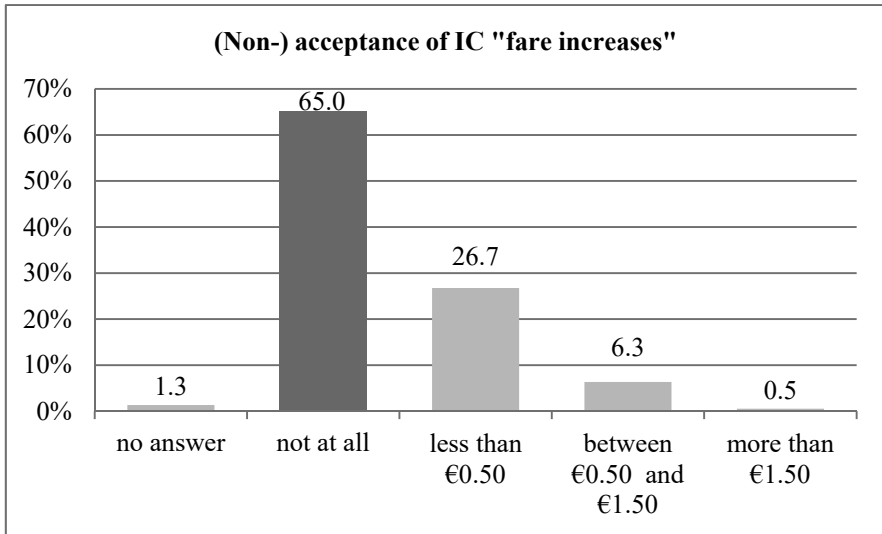


Figure 22: Results of online survey for comfort/fare increases IC (n=1,339)
(Source: author)

To gain a more abstract image, the survey also asked about the willingness of an unspecified security fee for, example, luggage allowance. The results were comparable to the fare increases IC. More than half of the respondents (63.6%) indicated they would not accept any security fee, and a further 19.3% would hardly accept one. In terms of positive acceptance, 11.7% of the respondents would accept a security fee and an additional 3.0% would highly accept it. Full acceptance of a security fee was indicated by 1.3% of the respondents (see Figure 23).

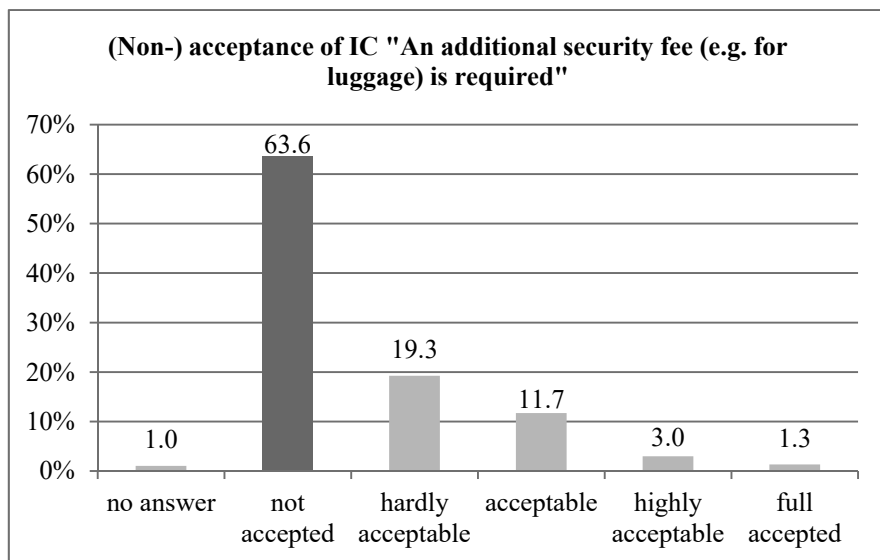


Figure 23: Results of online survey for comfort/security fee IC (n=1,339) (Source: author)

Security measures can cause interference in the field of comfort. The reduction of seating options was accepted by 23.5% of respondents and an increase in noise level was accepted by 19.7% (see Figure 24).

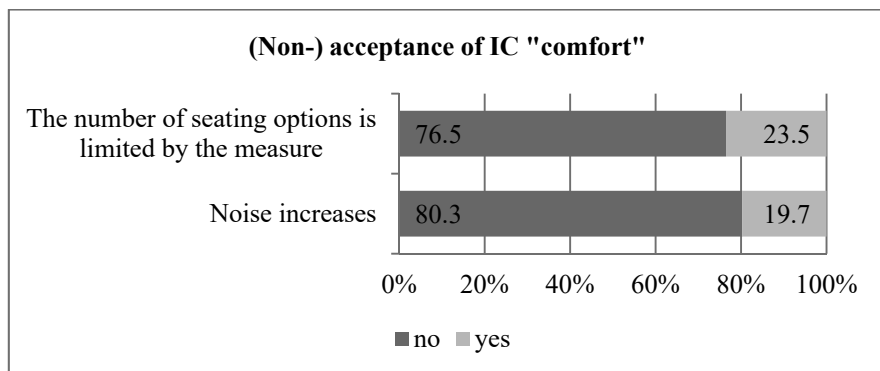


Figure 24: Results online survey IC comfort (n=1,339) (Source: author)

In the flexibility category, IC that affect the flexibility of customers before, during and after public transportation system use were combined. The IC with the highest acceptance in this category (22.0%) is the limitation of luggage such as

those commonly used for flight transport. In public transportation systems, this also includes bicycles. Next in the ranking are three IC affect customers' time. Interference of prolonged travel time was accepted by 15.3% of respondents, followed by prolonged preparation time with 10.6% acceptance. The last IC in the ranking is the registration and specification of a travel itinerary before beginning a trip. This IC was accepted by 8.8% of respondents (see Figure 25).

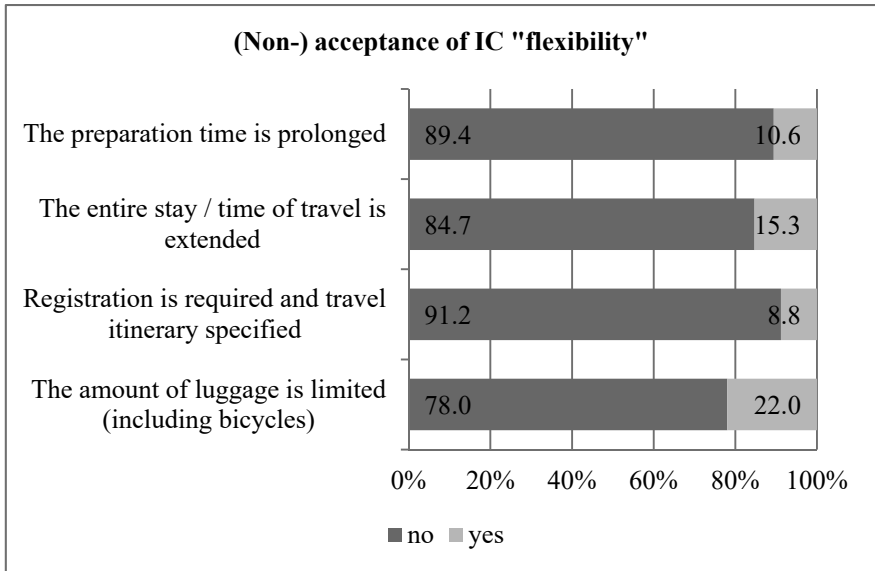


Figure 25: Results of online survey for flexibility IC (n=1,339) (Source: author)

4.4.1.3 Ranking of Acceptance of Negative Impact Caused by Security Measures

This section provides conclusions of the IC analysis and addresses the question how respondents perceive the different consequence categories in comparison to each other. The results provide attribute values for further application in a security measure decision-tool (discussed in Section 4.6).

Figure 26 displays a ranking of all IC in the order of highest to lowest acceptance. The list shows that already implemented interferences such as ticket control (89.5%) and the presence of personnel (security staff at 83.4% and police officers at 82.5%) were highly accepted. Even further disturbances in the form of

communication with personnel (police officers at 69.4% and security staff at 67.5%) were still highly accepted. In the case involving the presence of security dogs, the image changes; only half (54.1%) of the respondents accepted the presence of security dogs. This IC is the only IC in the middle sector of the acceptance scale.

The IC that tended toward the non-acceptance sector were divided into two groups. The first group includes mostly IC in the flexibility, comfort, and integrity categories, while the second group includes anonymity IC, specifically the use of personal data. The last group has high non-acceptance with values below 10% acceptance.

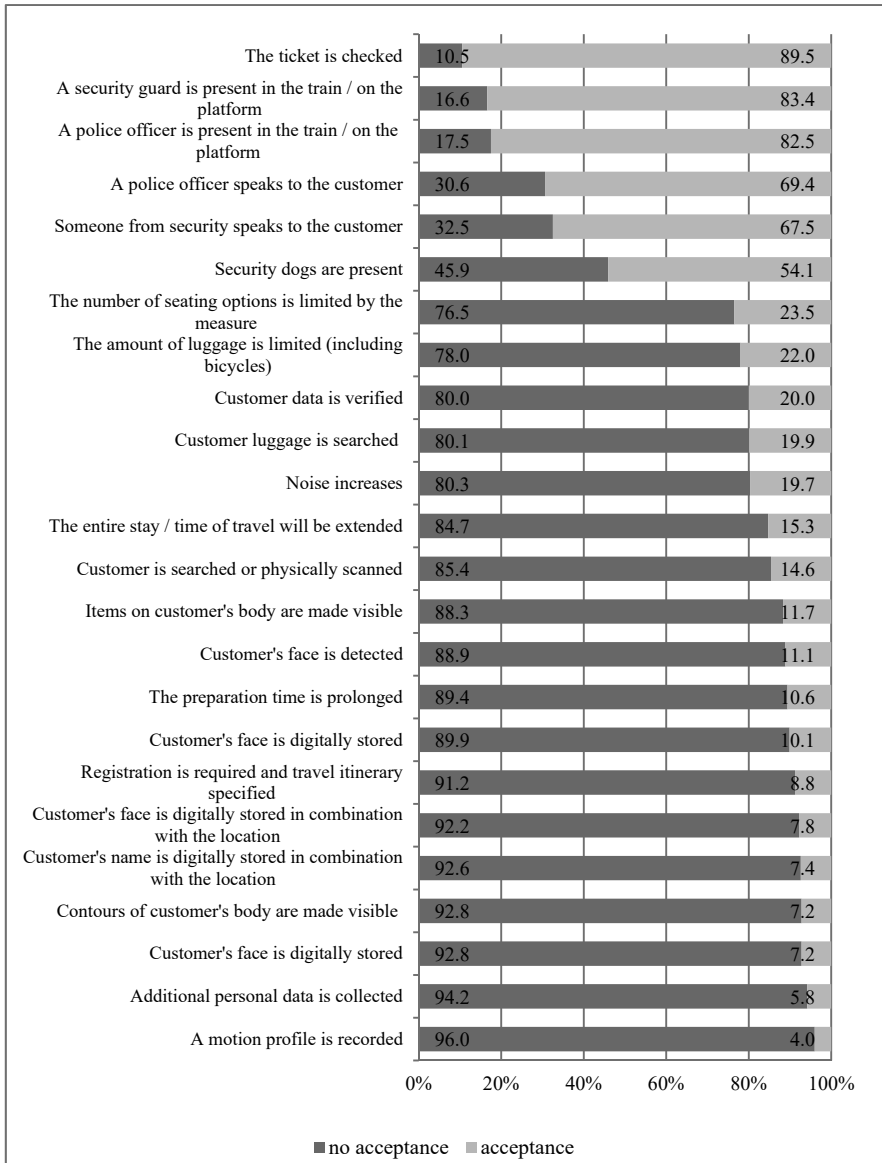


Figure 26: Ranking of IC acceptance according to the online survey (Source: author)

A comparison of the IC clustered into consequence categories provided further information about customers' acceptance assessment and which categories were more or less accepted. In Figure 27, the results show a positive ranking result of 74.4% (arithmetic value) for all IC in the personal rights category. The break in acceptance is also recognizable in the bar chart in Figure 26. The comfort category had a mean acceptance of 21.6%, followed by flexibility with 14.9% and integrity with 13.4%. The final consequence category in the acceptance ranking was anonymity with 9.2% mean acceptance.

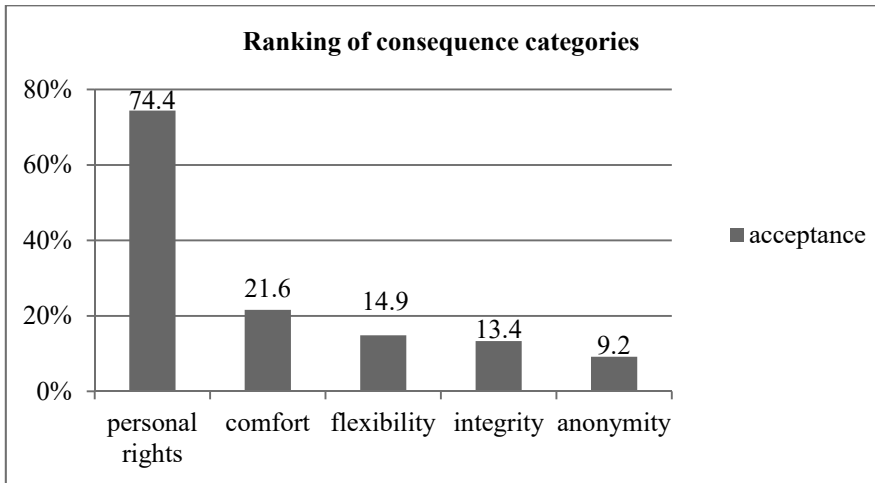


Figure 27: Ranking of consequence categories of the online survey (Source: author)

Accordingly, interferences caused by the security personnel measures were highly accepted, and almost all other interference was located in the non-acceptance sector. The re-translation of the IC back into security measures (see Section 4.4.4) shows that all security measures that have a high impact on *anonymity*, *integrity*, and *flexibility* were issues of customer acceptance.

4.4.2 Field Survey Results

A field survey was conducted from January 29, 2014 until February 23, 2014 in three different KVB stations. In the duration from February 10, 2014 until February 17, 2014, the author interrupted the data acquisition because a damaged overhead cable caused problems with train connectivity and additional waiting times for customers. To avoid any reflection of this situation in customer as-

assessment in the form of misdirected overall dissatisfaction, the author stopped the survey for a week.

The survey was conducted in two highly frequented stations in the inner city (Heumarkt and Appellhofplatz) and one smaller station outside of the inner circle of Cologne (Piusstraße) (see Figure 28).

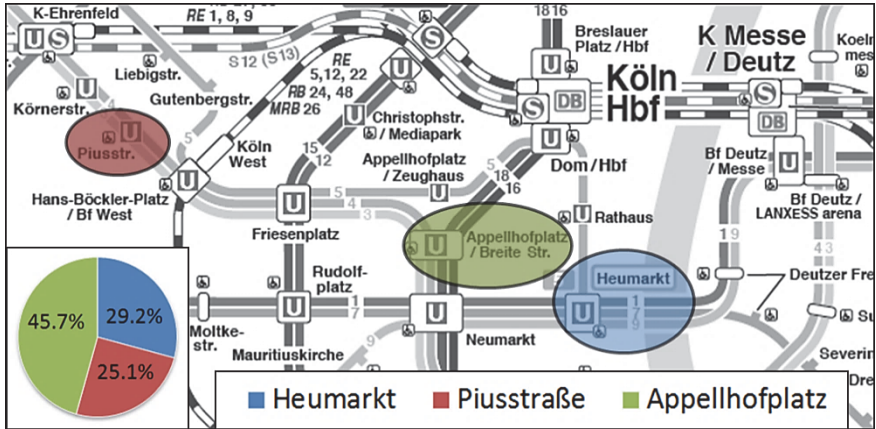


Figure 28: Location and distribution of field survey in the KVB plan (Source: KVB 2015, adapted by the author)

Overall, 798 customers participated in the field survey. The participants were face-to-face interviewed customers who had just used or were going to use the public transportation system. The questionnaires were collected in the stations as follows: 45.7% in Appellhofplatz, 29.2% in Heumarkt, and 25.1% of in Piusstraße (valid percent). Respondents of the field survey were 46.1% female and 50.9% male, and 3.0% did not answer this question.

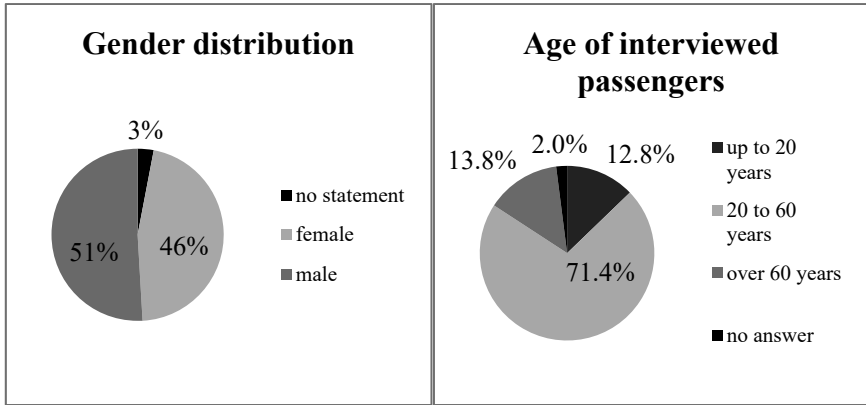


Figure 29: Distribution of the gender and age of respondents to the field survey (Source: author)

The author divided the respondents into three age groups as with the online survey. The majority of the respondents were between 20 and 60 years of age (71.4%) followed by over 60 (13.8%) and 20 and under (12.8%). A total of 2.0% of respondents did not want to specify their age.

4.4.2.1 Analysis of Respondents' Security Perception—Field Survey

The determination of security perception in the field survey required a close review according to parameters such as those mentioned in Section 2.5. The survey used an ordinal scale from very bad to very good. Ordinal scales are commonly used in satisfaction studies because the values represent a ranked order but do not denote solid values with defined spacing in between.

Descriptive Analysis:

The first step indicated that most respondents in the field survey indicated a good feeling toward security. A total of 795 customers responded to this question, and the Pareto chart in Figure 32 shows the distribution of the replies in numbers and percentages. In the positive sector, 11.4% felt security in the public transportation system was very good, followed by the majority of 49.2% who assessed security as good. One-third (31.3%) of the respondents evaluated security as acceptable. Smaller percentages of 6.7% and 1.4% expressed that security was bad or very bad, respectively (see Figure 30). As a result, over 90% of respondents accepted or positively assessed security in the KVB public transportation system.

The cumulative percentage graph in Figure 32 illustrates this, with a strong pitch in the satisfaction sector and a lower pitch in the dissatisfaction sector.

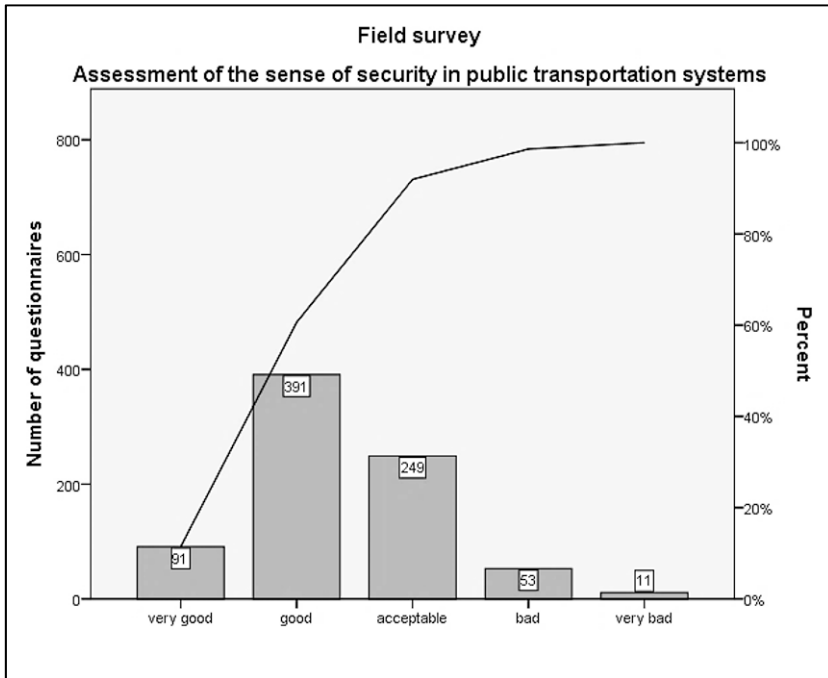
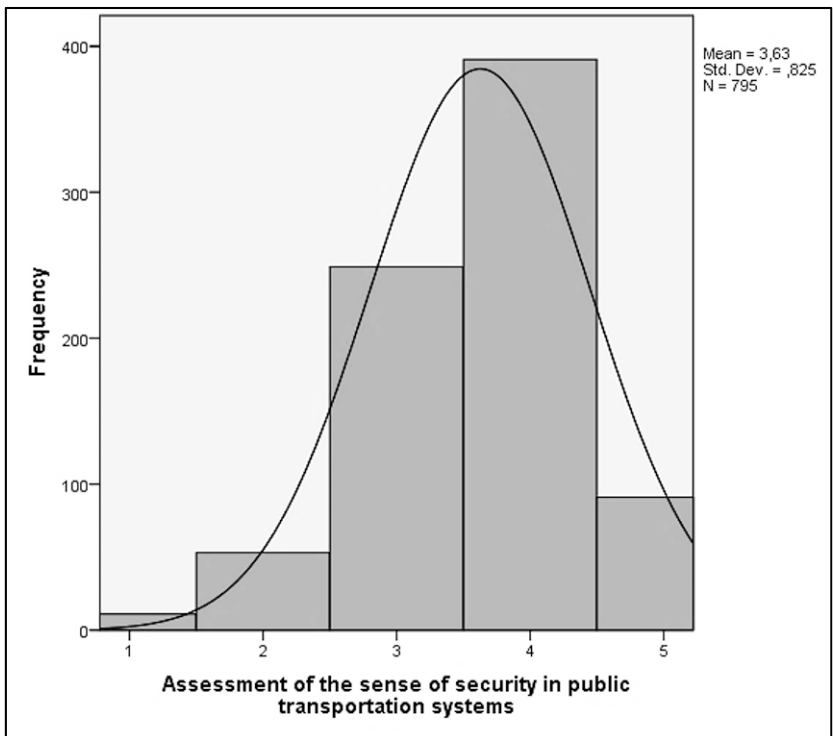


Figure 30: Pareto chart—sense of security in the public transportation system (Source: author)

In the second step, a test of normality was used to determine if the above results can provide further information or be transferred to other areas. While the bar diagram shows a similar tendency to the Gaussian curve, which represents normal distribution (see Figure 31), a Kolmogorov-Smirnov test as well as the Shapiro-Wilk test disproves any significance and show a high degree of freedom (df) based on the present sample. In the case—the result seems normalized—a conservative analysis of the skewness and kurtosis may give further information.



Tests of Normality						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Assessment of the sense of security in public transportation systems	.281	795	.000	.857	795	.000

a. Lilliefors Significance Correction

Figure 31: Gaussian curve and bar diagram of sample (Source: author)

The skewness is a negative variable of -0.523 with a standard error of 0.087. The negative variable illustrates asymmetrical behavior toward the mean variable, specifically the measured values that scatter more on the left side. This can also be seen in Figure 31 in the form of a longer tail. The correlation of skewness and standard error indicates that the measured mean variable is also skewed in the statistical population. In this case, it was six times larger than its standard error, so the mean variable is also skewed in the statistical population (Brosius 2014). Kurtosis investigates the steepness of the curve. The kurtosis value was positive

at 0.456 and a standard error of 0.173. This means the distribution of values is steeper than the normal distribution (Gaussian curve). The small standard error (2.6 times smaller than the kurtosis value) indicates that the same result can be expected in the statistical population.

Explorative Analysis:

Explorative analysis was conducted to extract further details about which parameters affect the perception of security. Firstly, the combination of security perception and gender as well the age of the interviewed passengers were inspected in a cross-table analysis.

The cross-analysis in Table 8 shows that females felt a slightly better sense of security than males. The additional expected value is a hypothetical value that expresses a reference for the hypothesis “there is no relation between sense of security and gender”. For example, if a total of 32.0% accept the perceived security in public transportation systems, then an additional 32.0% of the 406 male passengers should also accept it. The expected value was 130.1, and the determined value was higher with 141. Thus, the expected value was lower for females. A shift is recognizable in this case; there are two shifts toward males in the bad/acceptable category and two shifts toward females in the good/very good category. This underlines the finding that the interviewed female passengers have a slightly better sense of security when using public transportation systems. The applicability of this to the population can be proven by a statistical test of significance such as Pearson’s chi-square test. This test proves the hypothesis of no relation between the sense of security and gender of the passenger. Based on this data set, the asymptotical significance is 0.077, which means this hypothesis is true with a probability of 7.7%. The reverse states that there is a correlation between gender and sense of security in public transportation systems with a probability of 92.3% (see Table 8) according to Pearson’s chi-square test.

Table 8: Field survey cross-analysis—sense of security and gender of interviewed passengers (Source: author)**Crosstabulation: sense of security in public transportation systems * gender**

			Gender		total
			female	male	
Sense of security in public transportation systems	very bad	count	5	6	11
		expected count	5,2	5,8	11,0
		% within gender	1,4%	1,5%	1,4%
	bad	count	21	32	53
		expected count	25,1	27,9	53,0
		% within gender	5,8%	7,9%	6,9%
	acceptable	count	106	141	247
		expected count	116,9	130,1	247,0
		% within gender	29,0%	34,7%	32,0%
	good	count	182	192	374
		expected count	177,1	196,9	374,0
		% within gender	49,9%	47,3%	48,5%
	very good	count	51	35	86
		expected count	40,7	45,3	86,0
		% within gender	14,0%	8,6%	11,2%
total	count		365	406	771
	expected count		365,0	406,0	771,0
	% within gender		100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8,421 ^a	4	,077
Likelihood Ratio	8,447	4	,077
Linear-by-Linear Association	6,849	1	,009
N of Valid Cases	771		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 5,21.

Secondly, the relation between the age of the interviewed passengers and sense of security when using public transportation systems was analyzed in a cross-analysis. Table 9 shows the results of this cross-analysis. At first glance, the interviewed passengers over 60 years had a worse sense of security than the younger respondents did. In the very bad/bad and acceptable categories, passengers over 60 years were higher than average while in the positive good and very good categories, the relative values were lower than average. In the under 20

group, the values were lower in the acceptable category and higher in the very good category than average. A shift toward the positive extreme was observed. The 20 to 60 age group was nearly even with respect to average distribution of answers.

Pearson's chi-square test was used to determine whether or not the result is applicable for the population. The asymptotic significance was rounded to null (instead of the exact 8.199×10^{-5}). This result cannot be considered reliable because the expected counts in two cells are less than five. Concrete significance was not proven in this case.

Table 9: Field survey cross-analysis—sense of security and age of respondents (Source: author)

Crosstabulation: sense of security in public transportation system * age of interviewed passengers					
			Age of interviewed passengers		
			up to 20 years	20 to 60 years	over 60 years
Sense of security in public transportation systems	very bad	count	2	3	6
		expected count	1,4	8,0	1,5
		% within age of interviewed passengers	2,0%	0,5%	5,5%
	bad	count	7	33	13
		expected count	6,9	38,7	7,4
		% within age of interviewed passengers	6,9%	5,8%	11,9%
	acceptable	count	24	184	40
		expected count	32,2	181,1	34,7
		% within age of interviewed passengers	23,8%	32,3%	36,7%
	good	count	50	288	40
		expected count	49,0	276,1	52,9
		% within age of interviewed passengers	49,5%	50,6%	36,7%
	very good	count	18	61	10
		expected count	11,5	65,0	12,5
		% within age of interviewed passengers	17,8%	10,7%	9,2%
total	count	count	101	569	109
		expected count	101,0	569,0	109,0
		% within age of interviewed passengers	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	32,309 ^a	8	8,199E-005
Likelihood Ratio	26,984	8	,001
Linear-by-Linear Association	14,017	1	,000
N of Valid Cases	779		

a. 2 cells (13,3%) have expected count less than 5. The minimum expected count is 1,43.

One of the influencing parameters of subjective security (see Section 2.5) is the location and environment surrounding passengers. The field survey was conducted in three stations with different structural conditions.

The cross-analysis in Table 10 shows a similar distribution of counts for all stations. Passengers at Piusstraße station were less likely to indicate they felt good or very good than passengers at the other stations. The passengers had a slight tendency toward the acceptable category. The distribution of perception of security in Heumarkt station follows the total average values. The respondents at

Appellhofplatz station had the highest percentage of scores in the good category (52.8%) but also had the lowest score of all three stations in the acceptable category at 27.8%.

Pearson's chi-square test showed a significance of 64.7%, but this result should be carefully considered due to the presence of two cells with an expected count below five at a of freedom of eight. This means the results are not reliable. Overall, passengers at Piusstraße station felt less secure than passengers in the other stations, but this interpretation should be carefully considered due to the low number of counts.

Table 10: Field survey cross-analysis—sense of security and location of interviews (Source: author)

Crosstabulation: sense of security in public transportation systems ^ location						
			Location			total
			Heumarkt	Piusstraße	Appellhofplatz	
Sense of security in public transportation systems	very bad	count	3	2	6	11
		expected count	3,2	2,8	5,0	11,0
		% within location	1,3%	1,0%	1,7%	1,4%
	bad	count	15	14	23	52
		expected count	15,2	13,1	23,7	52,0
		% within location	6,6%	7,1%	6,5%	6,7%
	acceptable	count	77	71	99	247
		expected count	72,1	62,3	112,6	247,0
		% within location	33,8%	36,0%	27,8%	31,6%
	good	count	105	89	188	382
		expected count	111,5	96,4	174,1	382,0
		% within location	46,1%	45,2%	52,8%	48,9%
	very good	count	28	21	40	89
		expected count	26,0	22,4	40,6	89,0
		% within location	12,3%	10,7%	11,2%	11,4%
total	count	228	197	356	781	
	expected count	228,0	197,0	356,0	781,0	
	% within location	100,0%	100,0%	100,0%	100,0%	

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,999 ^a	8	,647
Likelihood Ratio	6,013	8	,646
Linear-by-Linear Association	,464	1	,496
N of Valid Cases	781		

a. 2 cells (13,3%) have expected count less than 5. The minimum expected count is 2,77.

For cross-analysis of the perception of security and the time of interview (see Table 11), the data were clustered to achieve more counts in the different categories. The data were clustered into three periods according to three different groups of passengers. The first user period includes all passengers who mainly ride during rush hour to travel to work or other daily activities (rush hour is Monday-Friday from 6-10 am and 3-6 pm). The second group covers all passengers who ride in the evening and night (Monday-Thursday from 8 pm-2 am and Friday-Saturday from midnight-4 am). This group includes midweek evenings and weekend nights. The third group consists of all passengers who travel in the afternoon on weekends (in contrast to midweek rush hour). The cross-tabulation

revealed a dependency of the time of interview and sense of security. Rush hour passengers followed the total average. More than 90% accepted or had a positive sense of security when travelling in the public transportation system. However, this changed in the evening. In comparison to rush-hour passengers, evening passengers had higher relative rates in the bad and very good categories. Although there were fewer counts, evening passengers had a tendency toward the higher extremes and fewer counts in the middle part of the perception scale (acceptable/good). Passengers in the weekend afternoon time period showed the opposite effect, with higher relative counts in the acceptable category (39.7% compared to the total average of 31.6%). These results are emphasized by the expected counts.

Overall, the interviewed passengers who use the public transportation system during the evening and night felt about 5% less secure (acceptable+good+very good = 87.7%) than the passengers interviewed during rush hour (92.8%) and weekend afternoons (92.0%). This result has a statistical significance level (from Pearson's chi-square test) of 0.095, which means this hypothesis is true with a probability of 90.5%. However, two cells had expected counts of less than five so the hypothesis of "time affects the sense of security in public transportation systems" should be considered with precaution.

Table 11: Field survey cross-analysis—sense of security and time of interviews (Source: author)**Crosstabulation: sense of security in public transportation systems * time of interview**

			Time of interview			total
			rush-hour (Mo-Fr 6-10 / 14-18)	evening (Mo- Thu 20-2 / Fr- Sa 0-4)	afternoon weekend (Sa + Su 14-18)	
Sense of security in public transportation systems	very bad	count	8	1	1	10
		expected count	6,5	1,5	2,0	10,0
		% within time of interview	1,6%	0,9%	0,7%	1,3%
	bad	count	27	11	11	49
		expected count	31,7	7,5	9,8	49,0
		% within time of interview	5,5%	9,5%	7,3%	6,5%
	acceptable	count	150	29	60	239
		expected count	154,6	36,7	47,7	239,0
		% within time of interview	30,7%	25,0%	39,7%	31,6%
	good	count	251	56	66	373
		expected count	241,3	57,2	74,5	373,0
		% within time of interview	51,3%	48,3%	43,7%	49,3%
	very good	count	53	19	13	85
		expected count	55,0	13,0	17,0	85,0
		% within time of interview	10,8%	16,4%	8,6%	11,2%
total	count		489	116	151	756
	expected count		489,0	116,0	151,0	756,0
	% within time of interview		100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13,510 ^a	8	,095
Likelihood Ratio	13,117	8	,108
Linear-by-Linear Association	,950	1	,330
N of Valid Cases	756		

a. 2 cells (13,3%) have expected count less than 5. The minimum expected count is 1,53.

4.4.2.2 Acceptance of Interference Criteria Caused by Security Measures

This section displays the results of the field survey regarding the acceptance of IC. Due to the huge number of IC and the resulting expected high dropout rate, the IC categories were split into three different questionnaires. In the field survey, the interviewers were instructed to constantly alternate among the three questionnaires. The distribution of the questionnaires was almost equal as Figure 32 shows.

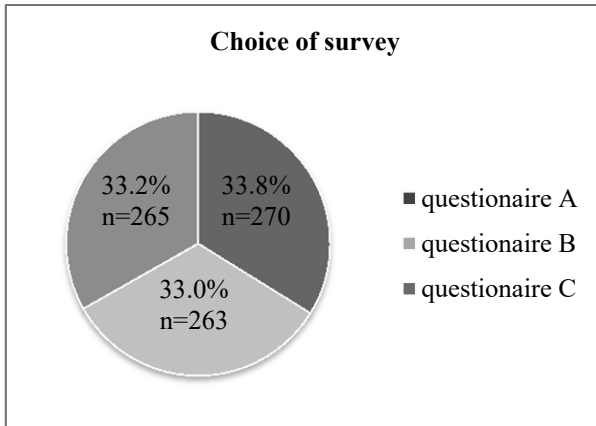


Figure 32: Distribution of the different questionnaires (Source: author)

In the personal rights category, about 265 respondents of the field survey highly accepted the presence of security guards (93.3%) and police officers (80.1%) in trains or on platforms. However, actual communication with security guards (77.2%) and police officers (68.8%) was less accepted. Ticket checks (which are standard procedure in public transportation systems) were highly accepted by 82.5% of the respondents. Communication with police officers and the presence of security dogs were also highly accepted (70.0% positive answers) (see Figure 33).

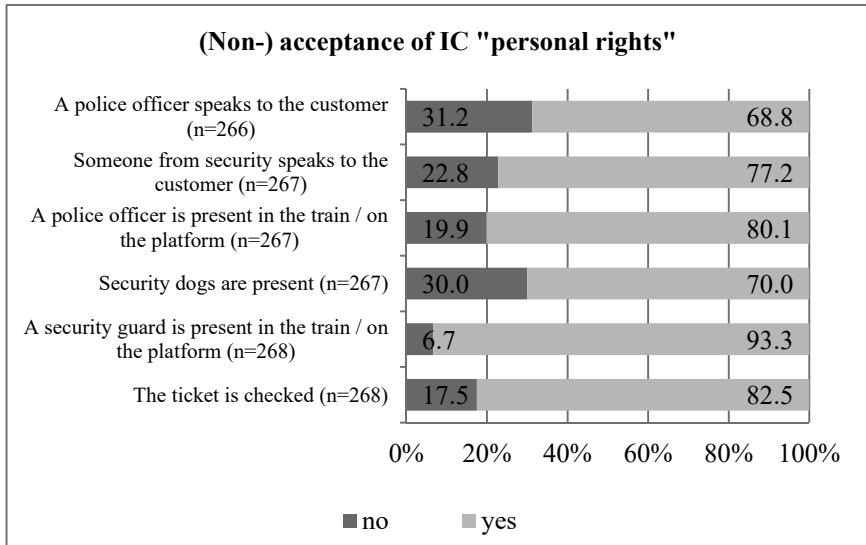


Figure 33: Results of field survey for personal rights IC (Source: author)

In contrast to the personal rights category, the IC of the integrity category were less accepted. Within this category, the respondents accepted luggage control with 40.5% positive answers, and checks of items on customers' body using detector technology were accepted with 39.7% positive answers. Physical body checks and the visualization of body contours were less accepted, and 32.7% of respondents to the field survey accepted contour visualization and 31.3% accepted physical body checks in public transportation systems (see Figure 34).

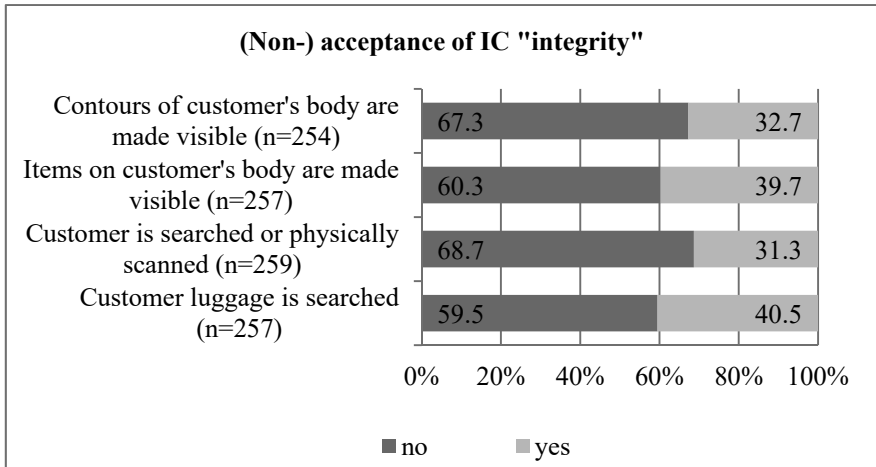


Figure 34: Results of field survey for integrity IC (Source: author)

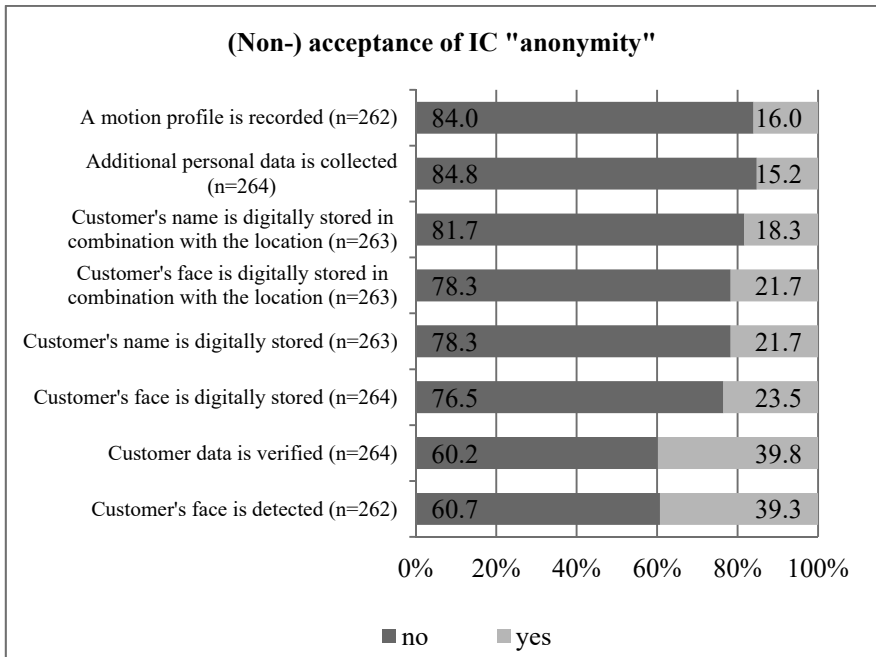


Figure 35: Results of field survey for anonymity IC (Source: author)

The customers of the Cologne public transportation system did not highly accept IC in the anonymity category. Within this category, the highest acceptance score was 39.8% for capturing customers' names and 39.3% for the digital capture of customers' faces. Only 23.5% accepted the digital storage of faces. This is similar to the digital storage of customers' names and faces in combination with location, which were both accepted by 21.7% of respondents. Even fewer customers accepted the storage of names in combination with location (18.3%) and the creation of motion profiles (16.0%). The last IC in the ranking of this category was the collection of additional personal data (15.2%).

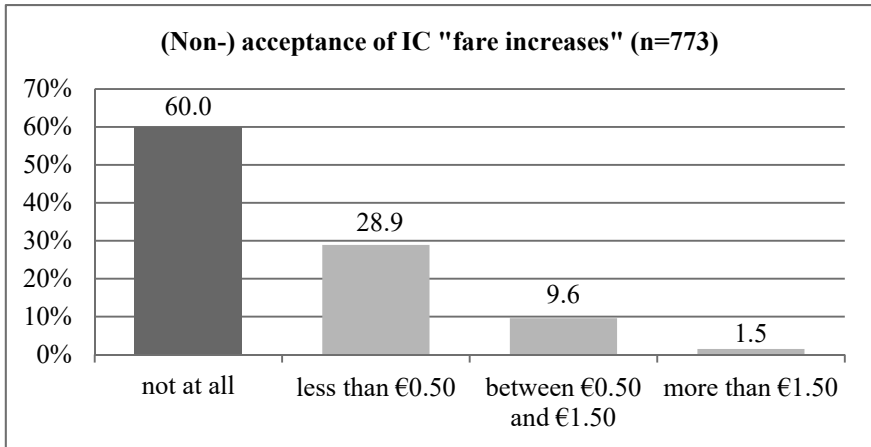


Figure 36: Results for field survey of comfort/fare increases IC (Source: author)

In the field survey, 773 customers were asked if they would accept a fare increase if security were also to increase as a consequence. More than half of the customers indicated they would not accept any increase in fares (60.0%). A third of the respondents would accept a fare increase if it was less than €0.50 (28.9%). Even fewer (9.6%) indicated they would accept a fare increase between €0.50 and €1.50 and only 1.5% indicated they would accept increases in fares of over €1.50 (see Figure 36).

Looking closely at the acceptance numbers for an additional security fee (e.g., for luggage carriage), the data show a similar decrease. Although the amount of the security fee was not specified, 61.2% of the 768 customers who answered the question would not accept an additional security fee, and only 22.0% would hardly accept one. In the field of acceptance, 13.3% would accept a security fee and 2.8% would highly accept a security fee. Less than 1% (0.8%) would fully accept a security fee (see Figure 37).

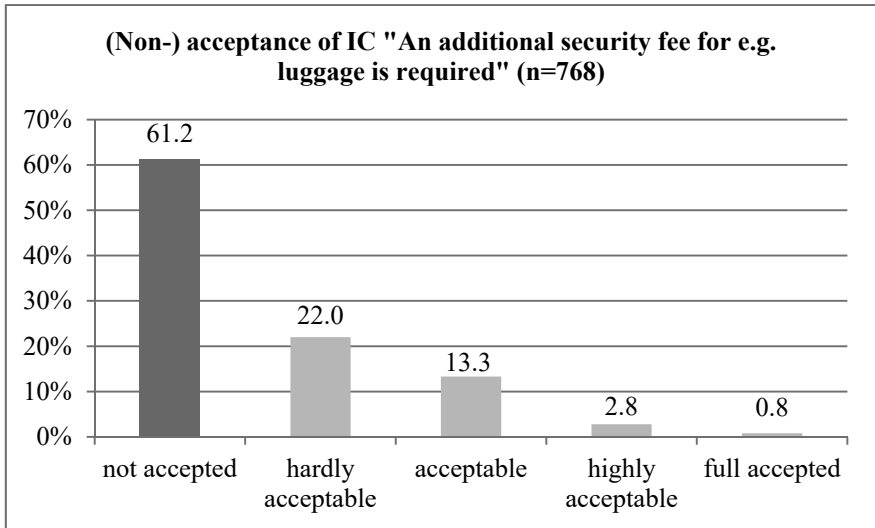


Figure 37: Results of field survey for comfort/security fee IC (Source: author)

In the comfort category, acceptance rates were similar for IC resulting in reduced seating and increased noise. The reduction of seating options caused by security measures was accepted by 41.4% of respondents, followed by 39.5% of the respondents who would accept an increase in noise (see Figure 38).

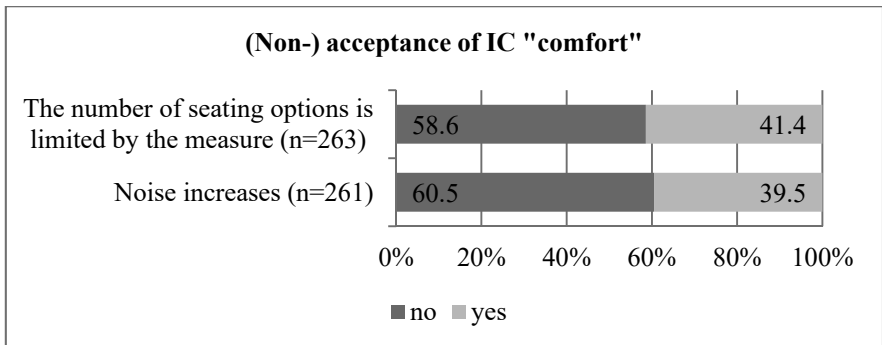


Figure 38: Results of field survey for comfort IC (Source: author)

Almost half of the respondents (47.7%) accepted prolonging the entire stay/time of travelling in the public transportation system in the flexibility category. Slightly fewer respondents (43.6%) accepted prolonged preparation time. Limi-

tations of luggage (e.g., for bicycles) was accepted by 34.3% of the customers questioned in the stations. The last IC item was registration required and specify travel itinerary, which was accepted by 19.4% of the respondents (see Figure 39).

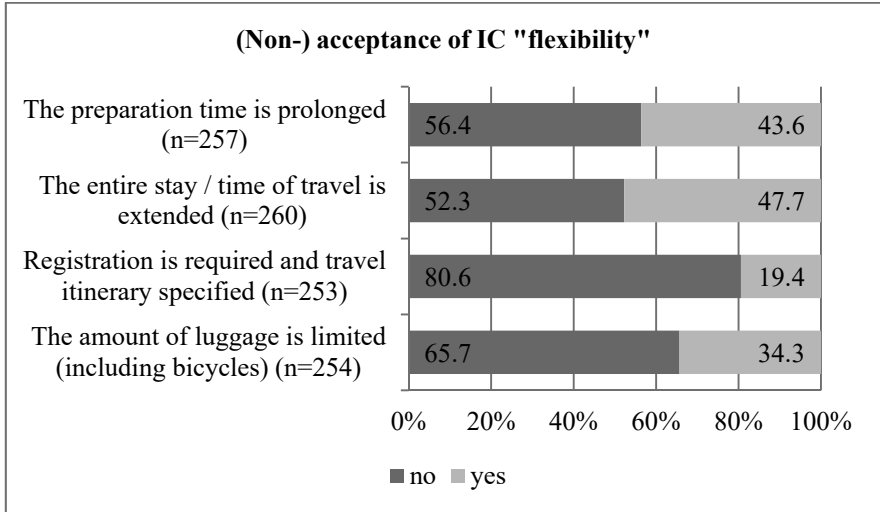


Figure 39: Results of field survey for flexibility IC (Source: author)

4.4.2.3 *Ranking of Acceptance of Negative Impact Caused by Security Measures*

This section concludes the analysis of IC included in the field survey in the form of a comparison among all of the IC. In a first step, all IC were ranked regardless of their consequence category. In the second step, the IC were combined according to their consequence category (Section 4.3.1) and compared.

Figure 40 shows the ranking of all IC and splits them into three sectors (i.e., high, middle, and non-acceptance). The high acceptance sector (~100–65%) contains all IC that include personnel presence or interaction as well as ticket checking. These IC were already implemented in the KVB system and thus, customers had adapted to them. Acceptance between the IC in this sector and those in the next was a step of almost 20%, which differentiates the two sectors.

Most of the IC are located in the middle sector of acceptance (30 to 65%). This sector is led by two IC of time—the extension of travel time (47.7%) and the prolonging of the travel preparation time (43.6%)—followed by comfort,

flexibility and integrity IC such as number of seating options (41.4%), luggage control (40.5%), physical scans of customers (31.3%).

The last sector containing IC with the lowest acceptance (30 to 0%) is not clearly definable. There is a small step recognizable between physically scanning customers (31.3%) and face recognition/storage (23.5%), but an interesting effect lies in the fact that the following IC belong to the anonymity category. An analysis of the consequence categories highlights this effect.

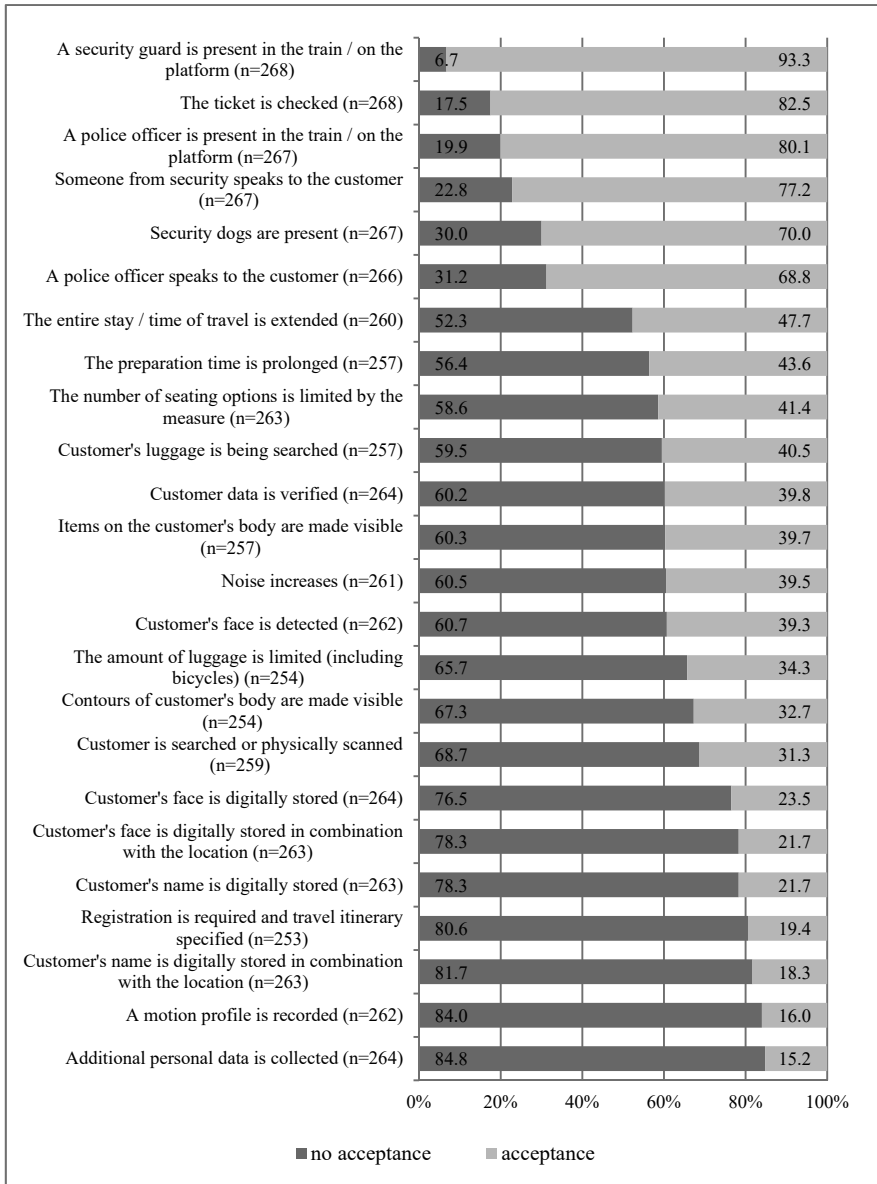


Figure 40: Ranking of IC acceptance in field survey (Source: author)

Figure 41 displays results of the consequence category rankings. The clustering reveals the same observation as mentioned above. The anonymity consequence category that considers all IC dealing with data acquisition and storage was the least accepted category. In contrast, the personal rights consequence category containing all IC with personnel interaction was the most accepted. No equal distribution of these IC was observed and showed peaks instead. The flexibility and integrity categories were on the same level in the ranking and were accepted by a third of the respondents. The comfort category was slightly more accepted at 40.5% on average.

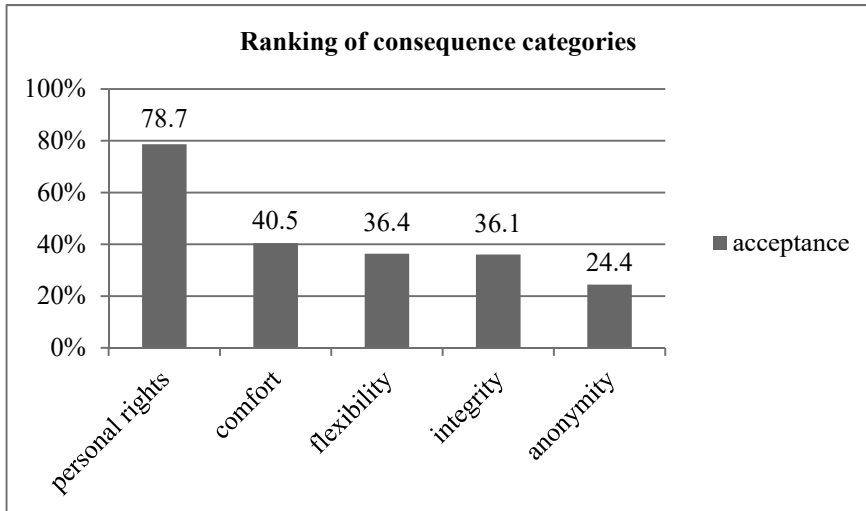


Figure 41: Ranking of consequence categories of the field survey (Source: author)

As a result, the high peaks of the personal rights and, contrarily, anonymity categories prove their concrete acceptance by respondents. IC that were already implemented in the public transportation system were more accepted than IC that were not common. The effect of adaptation plays a major role in the answers of the respondents to the field survey. Furthermore, interferences affecting comfort reduction found greater acceptance than restrictions on the flexibility and integrity of customers. The observation of customers and storage of data were not highly accepted, although the interferences physically affect customers much less than body checks.

The re-translation of the IC back into security measures (see Section 4.4.4) showed which measures had a high impact on the *personal rights*, *comfort*, *flexibility*, *integrity*, and *anonymity* categories.

4.4.3 *Comparison of Online Survey versus Field Survey*

The methodological framework includes two different data acquisition approaches to investigate the different foci of the customers. The perception of security is influenced by many different parameters and this includes the direct environment of the customers. While an online survey offers the possibility of reaching many customers at the same time and capturing data in a structured way, respondents answer questions out of the context of a public transportation system, which may result in assessment of security based on experience and imagination of the customers. Respondents to a field survey are more likely use their current location (in the public transportation system) when deciding on their answers and process their environment as part of their decision.

Direct comparison of sense of security of respondents (see Figure 42) revealed that respondents to the field survey felt slightly more secure than respondents to the online survey. Clustering the acceptable, good, and very good categories exposed a higher security feeling of five percentage points. The red line on the graph and the higher values on the negative left side underline this result. The blue line on the graph representing the field survey also has a peak in the good category with 11 percentage points more than the red online survey graph. This development potentially shows that the environment and direct experience of a travel in the KVB Cologne public transportation system affects customers in a positive manner. However, the strength of this statement cannot be proven in this context.

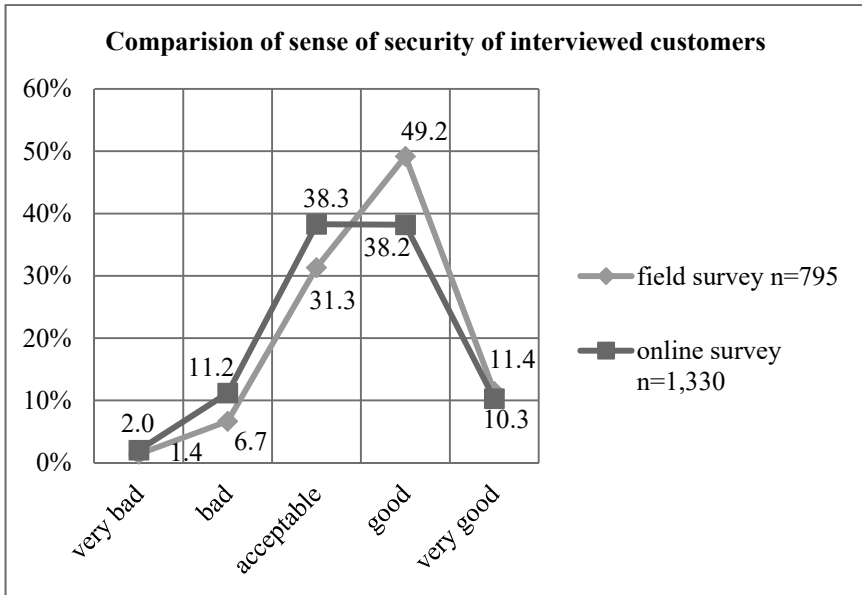


Figure 42: Graph diagram—comparison of sense of security (Source: author)

The different perception of security may also cause a different assessment of the IC either positively or negatively. This section discusses this effect.

The comparison in Figure 43 reveals a mismatch of the assessment of acceptance between online and field survey respondents. In general, customers responding at the train stations had higher acceptance in every consequence category than online respondents. In particular, field survey respondents had a more positive attitude toward interferences in the comfort, flexibility, and integrity categories. Even the usage and storage of personal data, which is in the anonymity category, was more accepted with fifteen points. A potential reason for this development is that customers who are in the process of travelling do not perceive as much interference based in their current experience as customers using their imagination in the context of a different setting.

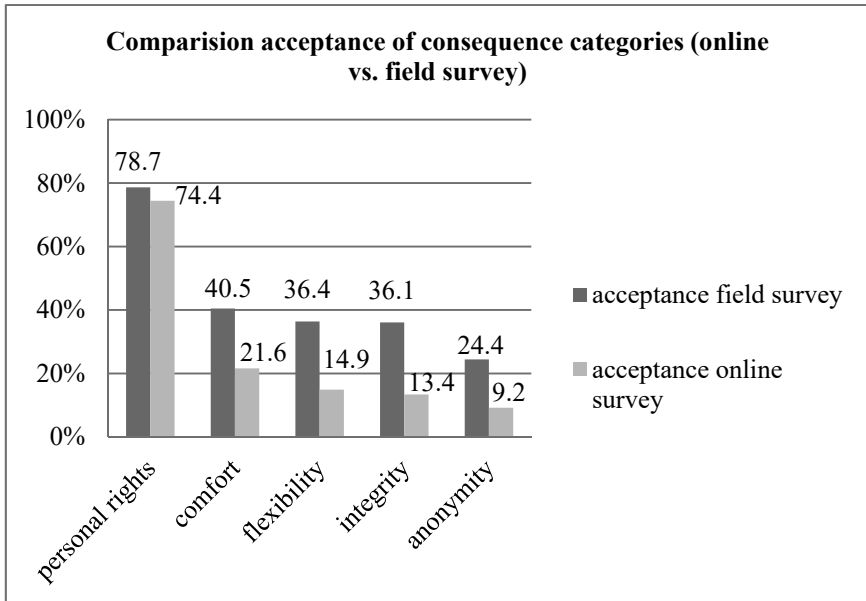


Figure 43: Comparison of the acceptance results in the online and field surveys (Source: author)

In the following, the results of IC acceptance of both surveys are compared:

Looking closely at the various IC in each category, Figure 44 reveals that security guards and security dogs were more accepted by respondents in the stations than the online respondents. In particular, security dogs were accepted by field survey respondents by an additional 16 percentage points. A similar development is recognizable in the presence of security guards and communication with security staff IC with additional 10 percentage points. The IC considering police officers (presence and interaction) was almost equally accepted in both surveys. An inverse effect of higher unacceptance was identified for the ticket check IC. Field survey respondents accepted this IC less than online respondents by seven percentage points, which was likely caused by direct experience of travel. Overall, all IC in this category had high acceptance in both surveys.

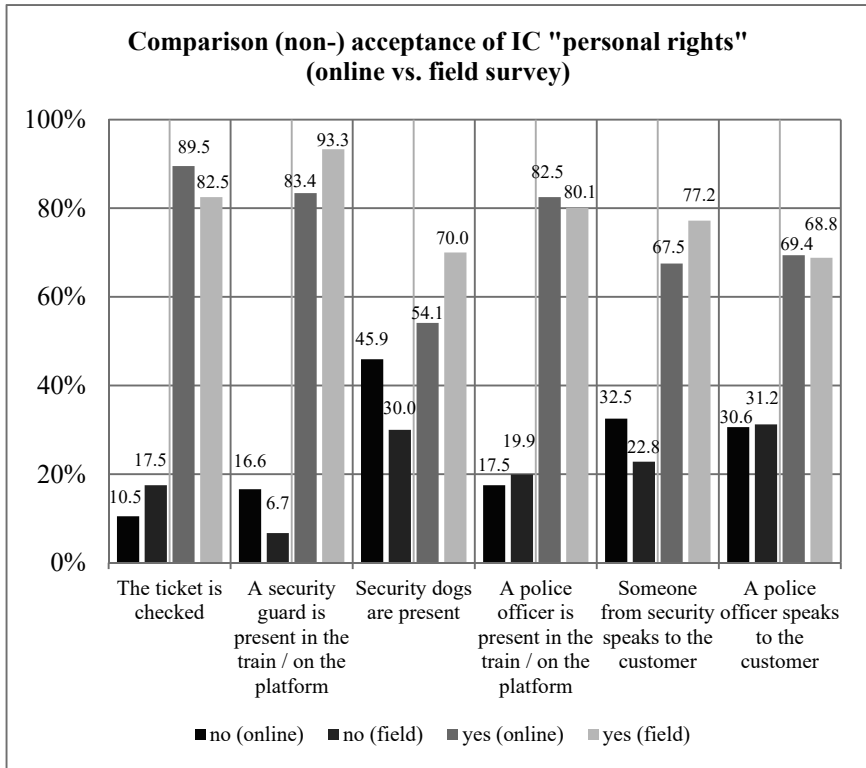


Figure 44: Comparison of the acceptance of personal rights IC in the online and field surveys (Source: author)

In the flexibility category, the observed shift toward the negative sector is recognizable in Figure 45 in the blue non-acceptance bars. Field survey respondents had greater acceptance of all IC than online respondents. In particular, the preparation time IC shows the greatest differentiation with 33 percentage points, followed by time of travel with 32 percentage points. Field survey respondents had a habituation effect to time and were affected by the travel they had undertaken or were going to undertake. The limited luggage and required registration IC also follow this trend with 12 and 9 percentage points difference. Overall, the perception of online respondents toward interference from IC was more conservative and more severe.

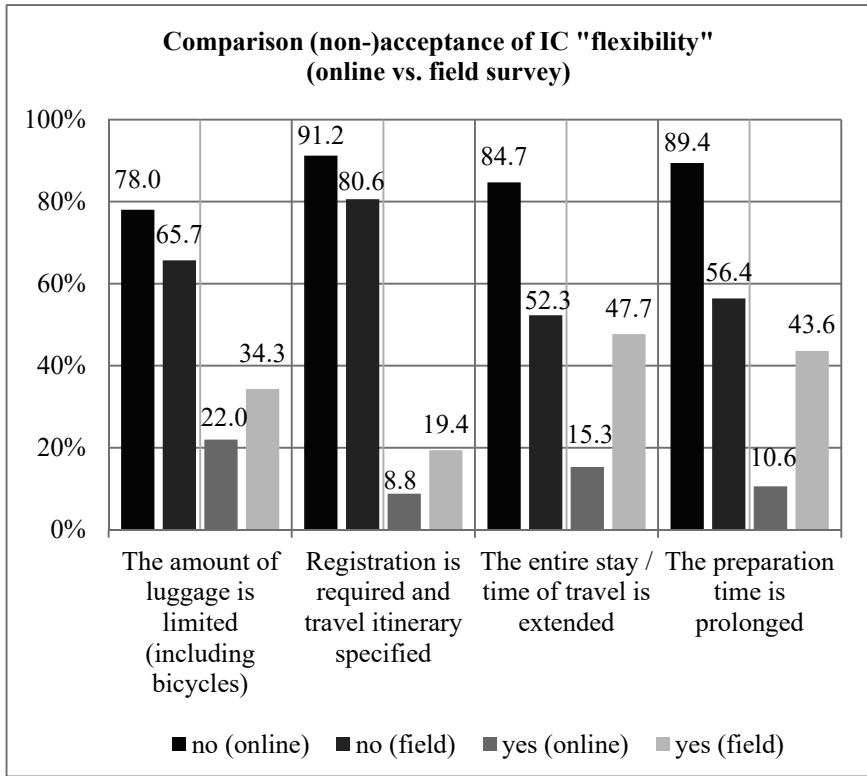


Figure 45: Comparison of the acceptance of flexibility IC results in the online and field surveys (Source: author)

In the integrity category, the same development is visible. Particularly, the visualization of items on customers' bodies and visualization of contours IC were highly different when comparing the surveys. Disregarding the high non-acceptance of these IC overall, field survey respondents accepted the visualization of items on customers' bodies by more than 28 percentage points and the visualization of contours by more than 25 percentage points than online survey respondents. In comparison to IC in the other consequence categories, the face detection IC in the anonymity category was the only one with a similar difference in acceptance in both surveys. Figure 46 also shows a shift between surveys for the luggage control and customer scan IC with 21 and 17 percentage points, respectively.

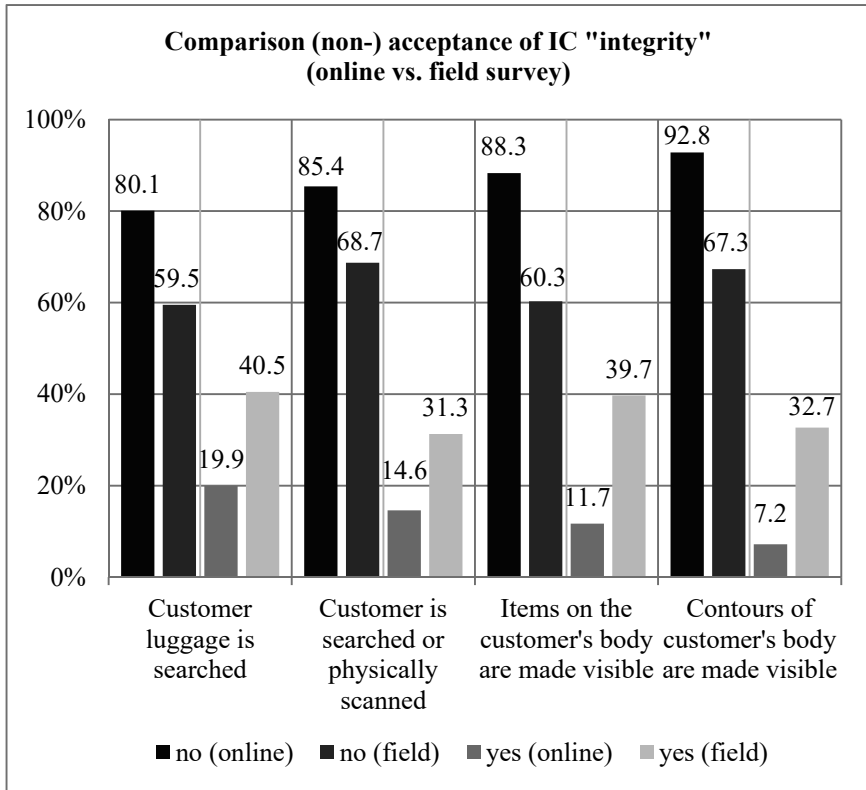


Figure 46: Comparison of the acceptance of the integrity IC in the online and field surveys (Source: author)

Comparison of the noise and seating options IC in the comfort category also displays the shift toward more positive acceptance by field survey respondents. Customers interviewed in stations accepted the noise IC by 20 percentage points more than online respondents. The seating options IC was accepted by more than 18 percentage points (see Figure 47).

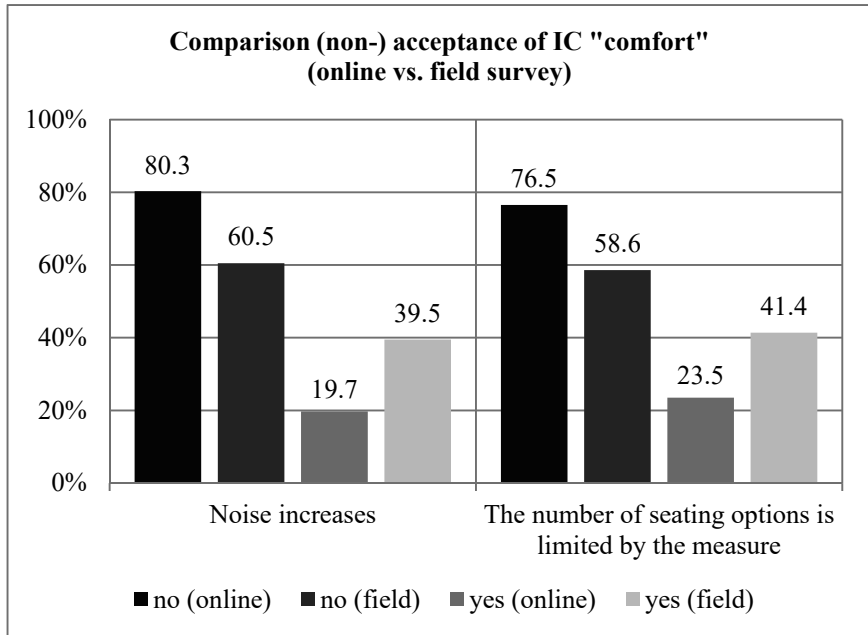


Figure 47: Comparison of the acceptance of the comfort IC in the online and field surveys (Source: author)

Comparison of online and field survey results for the anonymity category reveals equal effects (see Figure 48). As mentioned previously, the face detection IC was highly different with 28 percentage points, followed by name capture with 20 percentage points. The other IC fluctuate between 10 and 16 percentage points difference towards a more positive perception of the IC in the field survey.

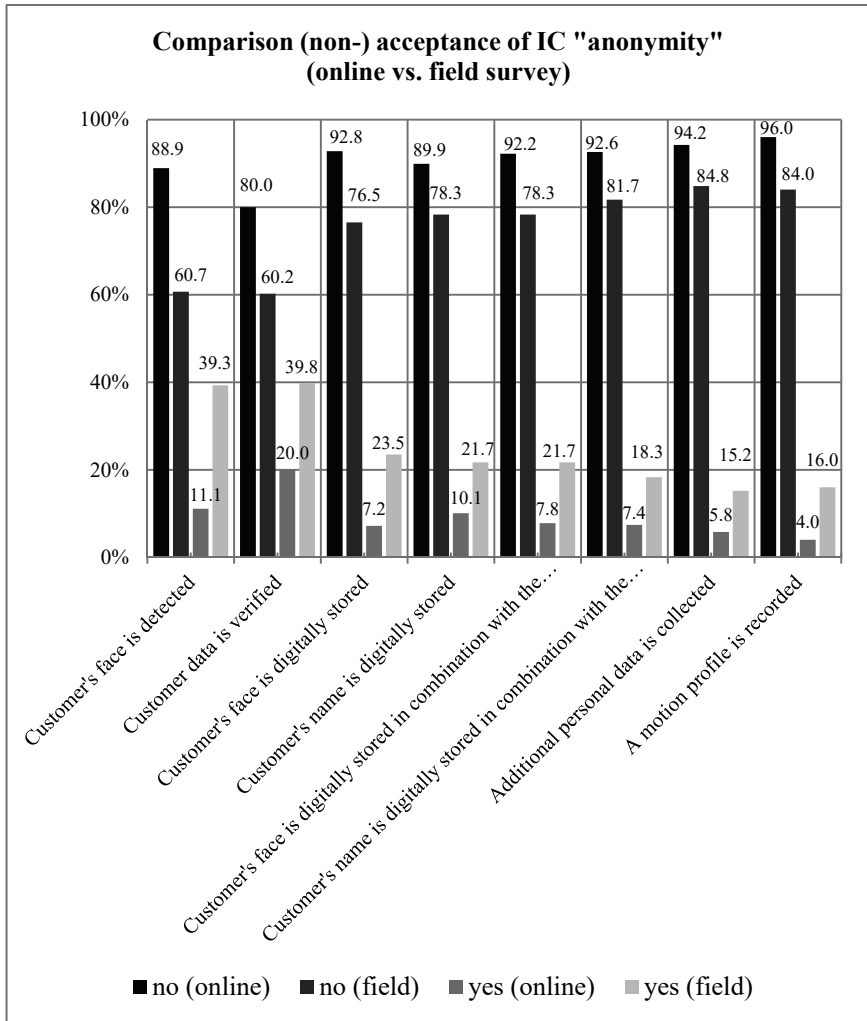


Figure 48: Comparison of the acceptance of the anonymity IC in the online and field surveys (Source: author)

Overall, it can be concluded that the passengers interviewed in stations assessed interference less negatively than online survey respondents did. The only exceptions were the ticket check and presence/interaction with police officers IC in the personal interactions category (see Figure 44), which were almost equally or more highly accepted by online respondents. Consequently, this affects the val-

ues of differences on the category level. The difference is smaller (about four percentage points) than the difference of other consequence categories (15 or more percentage points).

4.4.4 Further Expert Interviews and Panel Discussion

Most IC can be re-translated into security measures by a simple data transfer and by answering questions regarding their occurrence (yes/no relation). Other IC can be associated only minimally because the quantity of interference is important as well. An example for such interferences are time issues (travel and preparation time) or information issues. Analysis was performed to determine, which security measures increased travel or preparation time of customers the most as well as how much customers knew about the security measures, and how an increase in information would affect their acceptance.

Respondents answered these questions according to their own ideas about the extent of interference they would or would not accept, without any relation to specific security measures. These values are soft factors and often depend on customization effects (Kersten et al. 2013).

Further investigation of the IC is required to consider the present status. The author used expert interviews to estimate the influence of security measures on time IC because security experts are well informed about *increased time (travel time/preparation time)* caused by these measures. In addition, a customer panel discussion was conducted to estimate the effects of *information* on acceptance.

4.4.4.1 Expert Validation of Soft Interference Criteria—Travel and Preparation Time

From August to November 2014, nine security experts of the Association of German Transport Companies participated in structured online interviews to estimate the degree of interference of soft IC on customers regarding specific security measures.

Specification of Overall Travel Time:

Figure 49 shows the results of the experts' estimation for different security measures. Some results were unequivocal while some were ambivalent. The nine experts were certain that highly prolonged travel time for any kind of luggage control should be expected, regardless of automatic or manual inspection. The same tendency was identified for entry inspection (by body scanner) and ticket inspection but was much less distinctive. Automatic ticket inspection as well as

platform edge doors (PEDs) or any kind of automatically functional detectors have a lower influence on the overall travel time including waiting time.

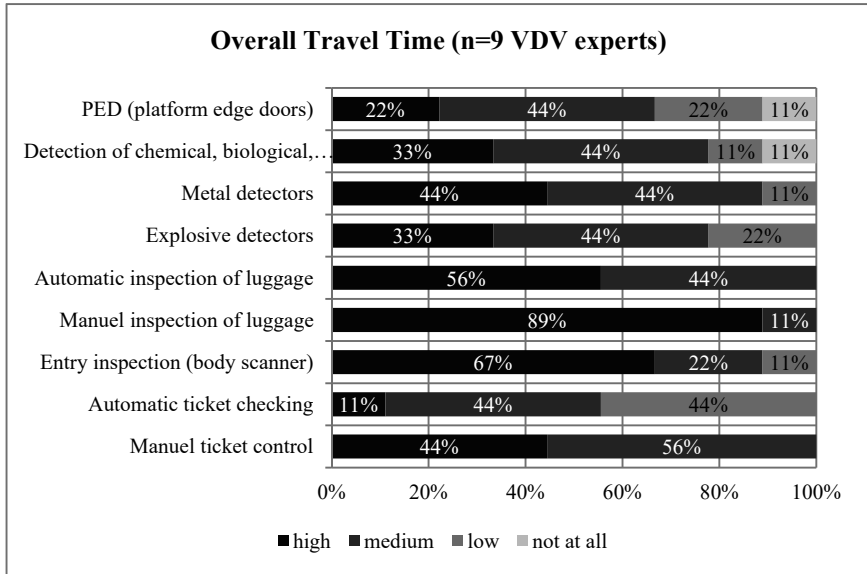


Figure 49: Expert estimation of travel time interference caused by different security measures (Source: author)

Specification of Preparation Time:

The author also asked experts about the influence of security measures on customers' preparation time before a journey. Figure 50 displays the results of the six potentially influencing measures. Almost half of the experts estimated high preparation time for all measures involving inspection or examination of luggage or customers with the exception of online registration of luggage, which was mostly estimated as having a medium effect on the preparation time.

Three of nine experts estimated the influence of mobile explosives detectors and online registration of route and passenger name on preparation time to be low. Four experts estimated the interference of both measures to be high.

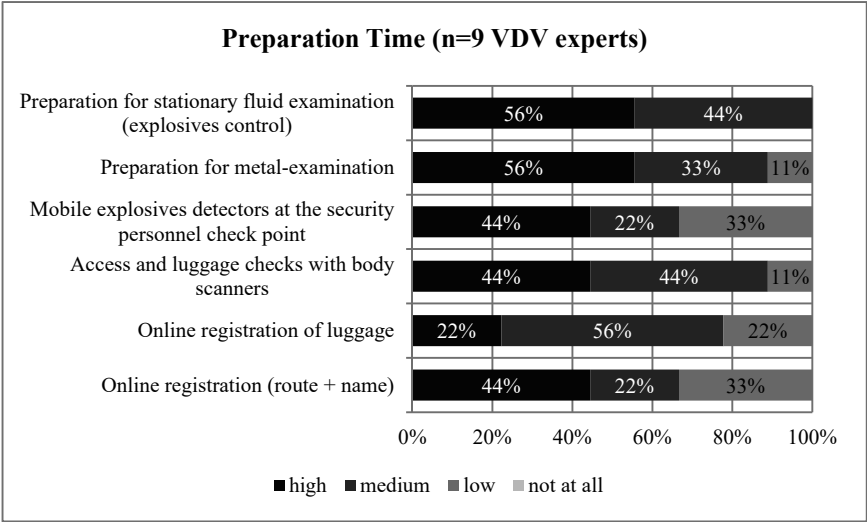


Figure 50: Expert estimation of preparation time interference caused by different security measures (Source: author)

The results of both questions were indefinite and showed ambivalence. It is difficult to estimate the effects of security measures in general without having a specific construction in mind. For the re-translation matrix, the ICs were weighted according to the answers and awarded points. Each answer in the high category was awarded with three points, each answer in the middle category two points, and so on down to the not-at-all category, which was awarded with zero points. To calculate the weighting coefficient, the following formula, which expresses the division of the total achieved points divided by the maximum achievable, was used.

$$w_{IC} = \frac{\sum_0^3 n_x}{w_{max}}$$

The weighting coefficients for the *travel time IC* are presented in Table 12, for the *preparation time IC*, Table 13 presents the results. The results are used in the re-translation matrix as pre-weighting of the soft IC related to time.

Table 12: Weighting coefficients for travel time IC (Source: author)

Expert Value Assessment/Overall Travel Time	n_x	high (3)	middle (2)	low (1)	not at all (0)	Total	Max.	Weighting coefficient w_{IC}
points		3	2	1	0			
Manual ticket control	9	12	10	0	x	22	27	0.81
Automatic ticket checking	9	3	8	4	x	15	27	0.56
Entry inspection (body scanner)	9	18	4	1	x	23	27	0.85
Manual inspection of luggage	9	24	2	0	x	26	27	0.96
Automatic inspection of luggage	9	15	8	0	x	23	27	0.85
Explosives detectors	9	9	8	2	x	19	27	0.70
Metal detectors	9	12	8	1	x	21	27	0.78
Detection of chemical, biological, radiological, or nuclear (CBRN) hazardous substances	9	9	8	1	0	18	27	0.67

Table 13: Weighting coefficients for preparation time (Source: author)

Expert Value Assessment/Preparation Time	n_x	high (3)	middle (2)	low (1)	not at all (0)	Total	Max.	Weighting coefficient w_{IC}
points		3	2	1	0			
Online registration (route + name)	9	12	4	3	x	19	27	0.70
Online registration of luggage	9	6	10	2	x	18	27	0.67
Access and luggage checks with body scanners	9	12	8	1	x	21	27	0.78
Mobile explosives detectors at security personnel check points	9	12	4	3	x	19	27	0.70
Preparation for metal detector examination	9	15	6	1	x	22	27	0.81
Preparation for stationary fluid examination	9	15	8	0	x	23	27	0.85

4.4.4.2 Customer Panel Discussion of Soft Interference Criterion— Information

The influence of information on acceptance is a major issue. It is natural to mistrust objects and procedures that are unknown and/or difficult to comprehend. To understand the influence of information on the acceptance of security measures, a methodology is needed to capture this effect in quantitative values. In this case, the author could not use expert interviews because actual customer knowledge and comprehension of security measures had to be considered.

However, asking customers in an online or field survey about their understanding of all security measures contained in the database was inconvenient. As a result, the author requested KVB to conduct three panel discussions with customers. Overall, 15 customers of the KVB (outlined in Table 14) accepted invitations.

Table 14: Participants of the panel discussions (Source: KVB and Groskopf 2014, adapted by author)

Group	Cus-tomer	Gender	Age	Security sensation	Use of public transit	Alternative transport possibility
A	1	female	20-60	acceptable	more than 8 times a week	no
	2	male	> 60	acceptable	more than 8 times a week	yes
	3	male	20-60	good	more than 8 times a week	no
	4	male	20-60	good	more than 8 times a week	yes
	5	male	> 60	acceptable	more than 8 times a week	no
	6	male	> 60	good	6–8 times a week	yes
	7	female	20-60	good	more than 8 times a week	yes
B	1	male	20-60	acceptable	1–2 times a week	yes
	2	female	20-60	acceptable	1–2 times a week	yes
	3	male	20-60	good	more than 8 times a week	no
C	1	male	20-60	good	more than 8 times a week	yes
	2	male	20-60	good	2–5 times a week	yes
	3	female	> 60	good	2–5 times a week	yes
	4	female	> 60	good	2–5 times a week	yes
	5	male	20-60	good	6–8 times a week	yes

After a short introduction and capture of basic data and questioning about their current sense of security, the participants were asked to assess their acceptance (ranging from “very bad” to “strongly” accepted) of different security measures listed on a poster. One vote was allowed for each measure. The moderator provided no information about the security measures before and during the voting. The chosen security measures consisted of already implemented measures in public transportation system, measures known in the sector of aviation, and future measures that have been communicated in the media.

After the voting, the different measures were explained in detail in a presentation to the participants and questions answered to help their understanding. In a second round of voting, participants were asked to vote again considering the new information and their own comprehension for the security measures. Table 15 displays the results of both votes (before and after additional information was provided).

Table 15: Acceptance results of the votes before and after providing information about the security measures (Source: KVB and Groskopf 2014, adapted by author)

Security Measure	strongly	good	acceptable	bad	very bad	no answer
	before/ after	before/ after	before/ after	before/ after	before/ after	before/ after
Video surveillance (live mode)	10/11	2/3	3/1	0/0	0/0	0/0
Face recognition (adv. video surveillance)	1/3	3/3	5/3	3/1	3/5	0/0
Access controls with automatic ticket inspection	10/9	2/0	1/2	1/2	1/2	0/0
Access controls with body scanner (terahertz radiation)	1/1	0/0	1/0	1/1	10/13	2/0
Manual luggage control	1/1	0/0	0/1	7/3	7/10	0/0
Detection of CBRN (HAMLet)	0/0	1/0	3/2	0/2	6/9	5/2
Security service	7/9	6/3	1/2	0/0	1/1	0/0
Police officers	7/7	3/3	3/4	0/1	1/0	1/0
Patrol with dog	5/7	4/6	2/0	2/0	0/2	2/0
Overall	42/48	21/18	19/15	14/10	29/42	10/2

The comparison of the two votes shows that some participants changed their mind about acceptance after receiving information about the security measures. Video surveillance in live mode, which is already implemented in the KVB

public transportation system, was a highly accepted measure. Two participants changed their mind in the second vote from ‘acceptable’ to ‘good’ and ‘strongly’ accepted. Additional face recognition is currently not installed in the KVB system, and for this measure, the majority of answers in the first round was in the middle section of acceptance in the first round. After the additional information was provided, the majority of answers fell into the extremes of ‘strongly’ and ‘very bad’.

Access control with ticket inspection and manual luggage control are known measures from other transportation systems and had a slight decrease in acceptance in the second vote. In contrast, security service and police officers showed an opposite effect toward positive acceptance. Interestingly, for the security measure ‘police officers’, one participant refused to vote in the first round and waited for further information to make up his/her mind.

New technological measures such as body scanners or contact-free detection systems (e.g., HAMLeT²), which work without pat down were highly unacceptable. Further information reinforced the non-acceptance. Even participants who gave no answer in the first round voted negatively in the second. Opinions about ‘patrols with dogs’ were widely varied. In the second round, the answers were located further at the extremes. Although two participants assessed their acceptance as very bad, the majority indicated positive acceptance.

This short analysis reveals no significant patterns that can be transferred to the acceptance database. Dealing with information about security measures is an important issue for public transportation providers and cannot be neglected. It is a challenge for the public relations department and an important factor because it influences the perception of measures and thus their acceptance as well. Owing to the complexity of this topic, this factor cannot be included as a decision-tool factor.

Additional Limitation: Customers’ comprehension influences the acceptance of security measures positively and negatively. The implementation of security measures have to be supported by communication strategies (public relations) to facilitate understanding and acceptance.

² Further information on the HAMLeT project is available at http://fb05.h-brs.de/Projekt_HAMLeT.html

4.4.5 *Interference Ranking and Discussion of Survey Results*

The comparison of both surveys (Section 4.4.3) revealed differences in their results. Although, the results of the field survey showed higher acceptance, an important fact needs to be considered: While the online survey is based on 1,339 respondents (all answered all IC questions), the field survey has only 798 respondents divided into three groups (A=270, B=263, and C=265).

This had to be considered in the aggregation process by a weighting according the number of respondents. Using SPSS the two data sets were fused together and a relative number derived based on the total count of respondents.

Table 16 is a summarized ranking based on results from both surveys and considers the absolute number of responses in the field and online surveys. Calculation of arithmetic means of the relative numbers did not sufficiently consider the differences in the surveys. Therefore, each absolute count of (non-) acceptance was part of this final ranking. The results are displayed in Figure 51 through a Kiviat-diagram, which is also known as spider chart. This spider chart is a helpful graphical method of displaying the IC and reveals the same observations mentioned in Sections 4.4.1 and 4.4.2.

Table 16: Ranking of IC acceptance (Source: author)

rank- ing	Interference Criteria (IC)	non-acceptance [%]	acceptance [%]
1	The ticket is checked	11.6	88.4
2	A security guard is present in the train/on the platform	14.9	85.1
3	A police officer is present in the train/on the platform	17.9	82.1
4	A police officer speaks to the customer	30.6	69.4
5	Someone from security speaks to the customer	30.9	69.1
6	Security dogs are present	43.3	56.7
7	The number of seating options is limited by the measure	73.6	26.4
8	The amount of luggage is limited (including bicycles)	76.1	23.9
9	Customer data is verified	76.7	23.3
10	Customer luggage is searched	76.8	23.2
11	Noise increases	77.1	22.9
12	The entire stay/time of travel is extended	79.4	20.6
13	Customer is searched or physically scanned	82.7	17.3
14	Items on the customer's body are made visible	83.8	16.2
15	The preparation time is prolonged	84.1	15.9
16	Customer's face is detected	84.3	15.7
17	Customer's name is digitally stored	88.0	12.0
18	Contours of customer's body are made visible	88.8	11.2
19	Registration is required and travel itinerary specified	89.5	10.5
20	Customer's face is digitally stored in combination with the location	89.9	10.1
21	Customer's face is digitally stored	90.1	9.9
22	Customer's name is digitally stored in combination with the location	90.8	9.2
23	Additional personal data is collected	92.7	7.3
24	A motion profile is recorded	94.1	5.9

In the *anonymity*, *flexibility*, *comfort*, and *integrity* consequence categories, ICs were less accepted and are illustrated with high peaks in red in the chart. IC in the *personal rights* consequence category were highly accepted, represented by blue peaks in the chart.

This Kiviat-diagram provides a very useful tool for public transportation provider for customer satisfaction and marketing approaches. The IC acceptance presents a subjective impression of the customers' preferences. Köhn and Bornewasser (2012) described it as a diametrically opposed position of *objective* and *subjective security*. It can be assumed that the high acceptance of personnel presence is a customer demand, although other security measure might have the same or better effectiveness. To prove this, the re-translation of IC acceptance into security measures has to occur.

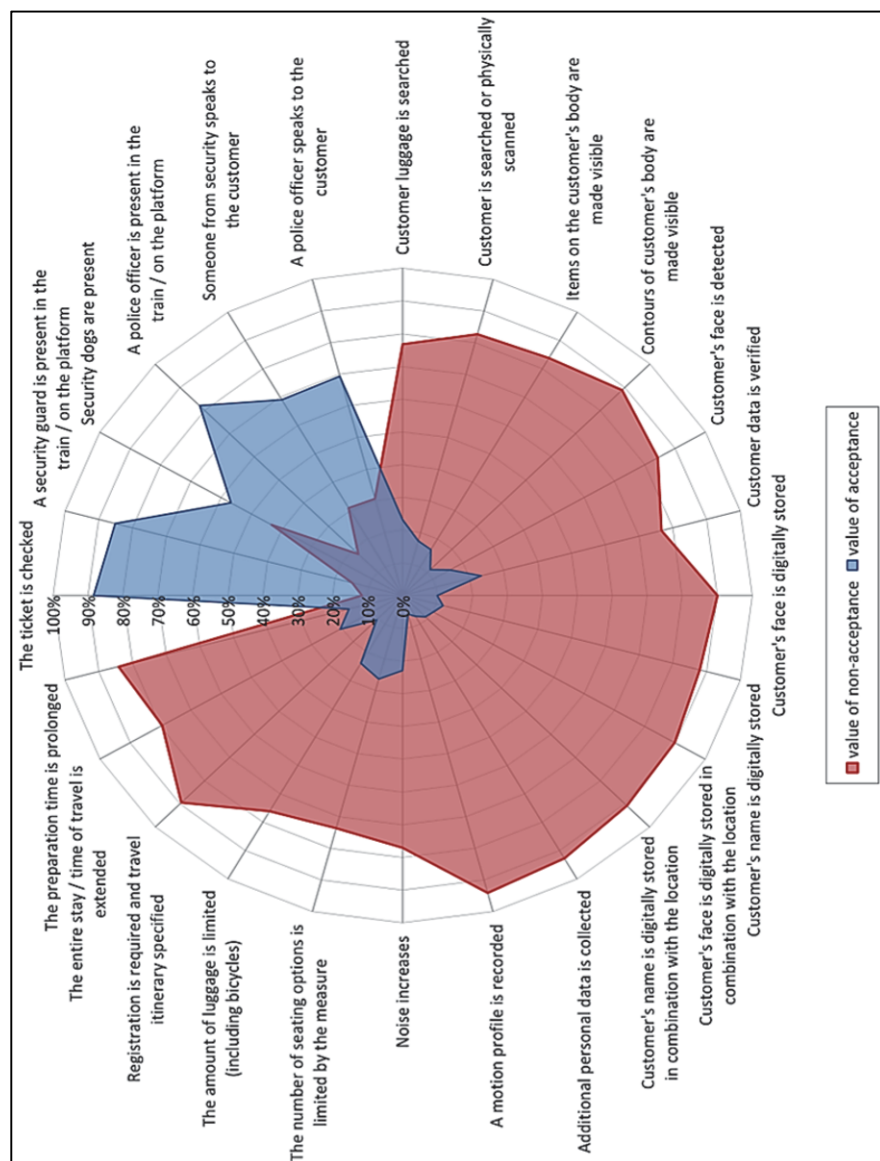


Figure 51: Kiviati-diagram of combined results of non-acceptance of the interference criteria (online and field surveys) (Source: author)

4.5 Step 4: Acceptance Matrix of Security Measures Re-translation Process

Two parts of the study were fused together in the fourth step: The author identified 81 security measures in public transportation systems in the VDV categories “technological, (con-) structural, personnel, organizational and other” measures, which were reduced to 29 security measures in the first step (Section 4.2).

The aggregated acceptance results of the survey were transferred back to the security measures according to their allocation estimated by the first translation process. The author chose a matrix as an appropriate form to display the re-translation. The re-translation process was accomplished by comparing the ICs with the security measures in a matrix (see Table 17). This requires a profound knowledge about the security measure to avoid bias. The allocation has to be executed by each public transportation provider individually, taking into account the conditions and knowledge of the security measures. To limit (subjective) assumptions to a minimum, the author suggests the inclusion of more experts in this process. The matrix in this case is an example created in cooperation with the help of experts’ discussions.

The matrix in Table 17 presents the non-acceptance scores of each IC in relation to the security measures. In the current selection of security measures, no measure affects the *seating options limitation IC*, resulting in a blank column. The other security measures have more or less different non-acceptance values of the ICs derived from the passenger questionnaire and expert interviews.

Security Measure		Access controls (ac), luggage control (lc)						
Personal rights	The ticket is checked	11.6	11.6					11.6
	A security guard is present in the train / on the platform	14.9		14.9	14.9	14.9	14.9	
	Security dogs are present					43.3		
	A police officer is present in the train / on the platform			17.9	17.9	17.9	17.9	
	Someone from security speaks to the customer	30.9		30.9	30.9	30.9	30.9	
	A police officer speaks to the customer			30.6	30.6	30.6	30.6	
Integrity	Customer luggage is searched					76.8	76.8	
	Customer is searched or physically scanned			82.7	82.7			
	Items on the customer's body are made visible				83.8			
	Contours of customer's body are made visible				88.8			
Anonymity	Customer's face is detected			84.3				
	Customer data is verified	76.7	76.7	76.7				76.7
	Customer's face is digitally stored			90.1				

	Customer's name is digitally stored		88.0	88.0				88.0
	Customer's face is digitally stored in combination with the location			89.9				
	Customer's name is digitally stored in combination with the location	90.8	90.8	90.8				90.8
	Additional personal data is collected		92.7	92.7	92.7		92.7	92.7
	A motion profile is recorded	94.1	94.1	94.1				94.1
Comfort	Noise increases							
	The number of seating options is limited by the measure							
Flexibility	The amount of luggage is limited (including bicycles)				76.1	76.1	76.1	
	Registration is required and travel itinerary specified	89.5	89.5	89.5	89.5	89.5	89.5	89.5
	The entire stay / time of travel is extended	64.3	44.5	44.5	67.5	76.2	67.5	44.5
	The preparation time is prolonged	58.9	56.3		65.6	56.3	56.3	

Security Measure		Detectors							
Personal rights	The ticket is checked								
	A security guard is present in the train / on the platform				14.9	14.9	14.9		14.9
	Security dogs are present	43.3							43.3
	A police officer is present in the train / on the platform				17.9	17.9	17.9		17.9
	Someone from security speaks to the customer				30.9	30.9	30.9	30.9	30.9
	A police officer speaks to the customer				30.6	30.6	30.6		30.6
Integrity	Customer luggage is searched				76.8	76.8	76.8		76.8
	Customer is searched or physically scanned	82.7	82.7	82.7	82.7	82.7			82.7
	Items on the customer's body are made visible				83.8	83.8			83.8
	Contours of customer's body are made visible								
Anonymity	Customer's face is detected								
	Customer data is verified								
	Customer's face is digitally stored								
	Customer's name is digitally stored								

	Customer's face is digitally stored in combination with the location								
	Customer's name is digitally stored in combination with the location								
	Additional personal data is collected	92.7	92.7					92.7	92.7
	A motion profile is recorded								
Comfort	Noise increases								
	The number of seating options is limited by the measure								
Flexibility	The amount of luggage is limited (including bicycles)	76.1			76.1	76.1	76.1		76.1
	Registration is required and travel itinerary specified								
	The entire stay / time of travel is extended	55.6	55.6	55.6	55.6	61.9	55.6		53.2
	The preparation time is prolonged				58.9	68.1	71.5		58.9

Security Measure		Personnel	security service	inspector / ticket collector	regular service	police officers	plain clothes officers	patrol with dog
Personal rights	The ticket is checked		11.6	11.6		11.6		
	A security guard is present in the train / on the platform		14.9					14.9
	Security dogs are present							43.3
	A police officer is present in the train / on the platform					17.9	17.9	
	Someone from security speaks to the customer		30.9					
	A police officer speaks to the customer					30.6	30.6	
Integrity	Customer luggage is searched		76.8					76.8
	Customer is searched or physically scanned		82.7			82.7	82.7	82.7
	Items on the customer's body are made visible							
	Contours of customer's body are made visible							
Anonymity	Customer's face is detected		84.3	84.3	84.3	84.3	84.3	84.3
	Customer data is verified		76.7	76.7		76.7	76.7	76.7
	Customer's face is digitally stored							
	Customer's name is digitally stored							

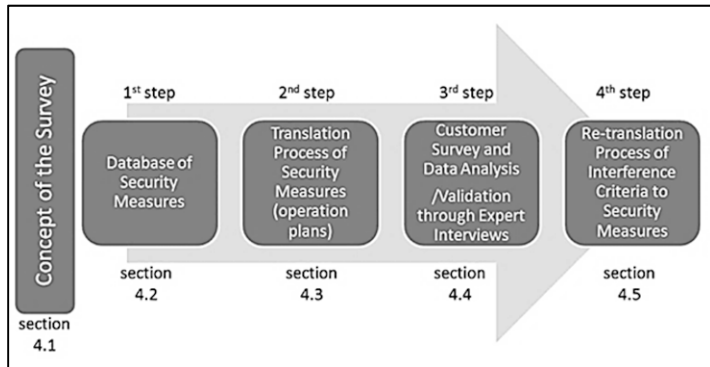
	Customer's face is digitally stored in combination with the location							
	Customer's name is digitally stored in combination with the location			90.8				
	Additional personal data is collected							
	A motion profile is recorded							
Comfort	Noise increases							77.1
	The number of seating options is limited by the measure							
Flexibility	The amount of luggage is limited (including bicycles)		76.1		76.1			
	Registration is required and travel itinerary specified		89.5	89.5		89.5	89.5	89.5
	The entire stay / time of travel is extended			79.4				79.4
	The preparation time is prolonged							

4.6 Summary and Results of the Acceptance Analysis

Winzer et al. (2009) showed that subjective process quality could only be measured indirectly. The *acceptances of different security measures* could be seen as subjective process quality. As a result, the following working hypothesis was introduced: *Every security measure can be characterized by the consequences affecting the customer.*

Considering that, the acceptance of security measures depends on the level of restrictions and interferences caused by the security measures for the customer, the acceptance of these interferences represent a measurable index for the acceptance of the security measure. In a four-step research plan, the acceptance of security measures was ascertained through indirect measurement of the acceptance of their related interferences.

In a first step, 29 security measures were identified that could help to prevent terrorist attacks. The data were derived of a database



consisting of 81 different security measures in public transportation systems. In cooperation with the KVB, seven consequence categories were identified including a category called *information*. The category *information* was treated separately, because a quantitatively approach was not feasible; therefore, panel discussions were held for qualitative statements. For the rest, the effects of the security measures on customers were looked at in cooperation with the KVB, and 26 different interference criteria established. These were prepared for an empirical investigation in the customer survey (second step).

From December 2013 until February 2014, an online and a field survey were performed questioning 2,137 customers (sum) of the KVB about their acceptance of interferences caused by security measures. The answers of online and field survey were compared for validation, revealing that customers responding at the train stations (field survey) had a slightly higher acceptance level in the all categories compared to online respondents.

To achieve a common acceptance index for each IC, the acceptance values were aggregated according to the absolute numbers of respondents. At this point, the aggregations of soft ICs of time issues were not clear. Security measures cause various lengths of delays; so, the relative values of the customers needed a weighting according to the strength of the interference. In an expert survey, nine security experts of the Association of German Transport Companies were questioned to help weighting this soft IC.

The influence of *information* on security measure acceptance was investigated in a panel discussion (n=15) that revealed a high effect of *information* on the overall acceptance of security measures and security perception. The influence can be positive or negative. Therefore, the implementation of security measures has to be supported by communication strategies (public relations) to facilitate understanding and acceptance. In the acceptance analysis, this cannot be represented in quantitative values.

At the end of the acceptance analysis, the security measure database was expanded by the *subjective effect of security measures* on customers in the form of interferences and their relative acceptance values collected by the respondents of customers of the Cologne public transportation systems. It represents a universal matrix for further decision analysis in risk management systems. This answers the first research question: *How can customers' acceptance of security measures in a public transportation system be measured?* It improves "the understanding of human factors, social and ethical values including public perception relating to [...] security measures [...]" (COM 2004:6) and is a contribution to the overall comprehension of security measures.

The acceptance of security measures based on interferences stands for the *subjective effects of security measures*. It is a decision criterion that has to be considered in a decision-support system of risk management, apart from other decision criteria such as *objective effectiveness* and *economic* thoughts. For this reason, an enhanced decision analysis is needed to assess the different criteria for a risk management goal (*second research question*).

5 Application—Integration of the Data into Risk Management Systems

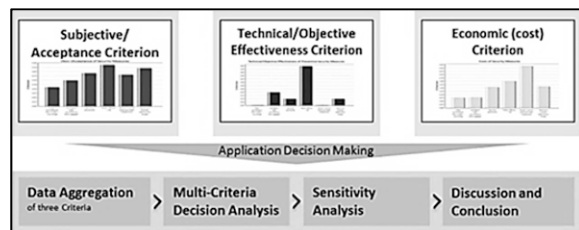
“Technical performance is not the only criterion for judging acceptability, so that additional, unfortunately contested social and economic criteria have to be included”

(Renn 1994:87).

Many risk management systems more or less adequately address the different risks faced by an organization. Regulations such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 31010 (2009) support decision-makers of critical infrastructure in identifying appropriate techniques according to their preferences. Critical infrastructure protection (CIP) elements such as public transportation systems face additional challenges (see Section 2.1). Research projects such as RiKoV develop new risk management approaches for public transportation systems, addressing CIP challenges, e.g. terrorist threats. The author introduces a new approach including three decision criteria in an assessment tool for the implementation of security measures, which considers social-technical, technical/objective and economic criteria in a holistic manner. Therefore, the results of the acceptance study are applied to a relevant scenario and processed in a decision tool, based on multi-criteria decision analysis (MCDA).

Therefore, the chapter starts with an introduction to multi-criteria decision analysis (Section 5.1) and the determination of decision criteria. In Section 5.2 an illustrative scenario of a

terrorist attack in a fictitious subway station is presented to accomplish a risk management process. Using this scenario, the author determines the data for three different decision criteria including the preventive efficiency of security



measures, the life cycle costs, and the results of the public acceptance analysis in Section 5.3. Finally, the criteria are implemented in the MCDA software for a decision weighting procedure and stability (sensitivity) analysis in Section 5.4. A final summary with all results of the MCDA and the pros and cons of this analysis are presented in Section 5.5.

5.1 Multi Criteria Decision Analysis in Risk Management

Multi-criteria decision analysis (MCDA) supports decision-makers in complex decision-making situations in finding feasible solutions taking into account multiple conflicting objectives. The objective of MCDA is to provide a framework for a systemic and transparent presentation of alternatives in a decision process. To do such an analysis, decisions must be free of uncertainties and/or ignorance, or else further methods have to be applied (Comes et al. 2011). To ensure this, the author needed well-described criteria that allow a systemic analysis of alternatives in a decision process considering the requirements of the end-users.

In the reference model RiKoV, risk (R_s) is a scenario-based product of terrorist threats (T) (consisting of the ability (A), motivation (M)), vulnerability (V), and consequences (C) of the occurrence of a terrorist attack (Pickl et al. 2011; Brauner et al. 2013b).

$$R_s = T_s(A_s * M_s) * V_s * C_s$$

This is a modified approach of RAMCAPTM (2006), which also consists of threat, vulnerability, and consequences components. Cox (2008) examined the semi-qualitative RAMCAPTM approach and found several limitations (e.g., the use of arithmetic averages on logarithmic scales leads to distortions). He found that the approach was limited by aggregation with no weighting of values and did not react to intelligent adversaries that responded to the situation. He demanded new approaches such as the decision-tree analysis, probabilistic activity, AND-OR networks, and hierarchical optimization to depict the behavior of an intelligent attacker. The RiKoV project used new methodologies such as process modeling to estimate vulnerability. The process modeling for vulnerability estimation includes an expert-based indicator approach for assessing the effectiveness of security measures. The author and other researchers of CUAS developed this vulnerability methodology. It provides data of the *technical performance* of security measures and is called the *objective effectiveness* of security measures reducing risks or vulnerability. This is the first criterion according to the end-user requirements for a decision-tool such as “Determination of the objective effects of security measures” (see Section 3.1).

1st Decision Criterion: Technical/Objective Effectiveness of the Security Measures

Moreover, security experts of public transportation systems require a means to consider the costs of security measures in the context of their effectiveness. This cost-benefit structure can be called the *efficiency* of security measures. With Comes et al. (2011) stating that the criteria have to be independent, and the effectiveness already fulfilled by the first criterion, the author chose the *costs* of security measures as a second criterion. The Network for the Economic Analysis of Terrorism (NEAT) provides data of costs for security measures that have been used for this criterion (Pickl et al. 2009).

2nd Decision Criterion: The Costs of Security Measures

A special feature of public transportation is the role of the customer. “A lack of customer confidence in the security of the service encourages more people to use less safe systems” (Dunmore 2010:10) such as private cars. The satisfaction of customers has to be considered in decision processes of security measure implementation by public transportation providers; otherwise, customers may refuse to use public transportation.

The negative effects of security measures causing acceptance problems have been researched by the author in Chapter 4 and implemented in the decision process in form of a third criterion.

3rd Decision Criterion: Acceptance of Security Measures

In context of risk management and terrorist threats, the quantification of terrorist *threats* and *consequences* is often discussed. Both factors are relevant in assessing terrorist risks from a scientific point of view, but might be neglected in decision-making processes from a public transportation provider’s point of view. A public transportation provider is unable to influence terrorist threats. This is the responsibility of the authorities (such as the Federal Ministry of the Interior, Federal Office for the Protection of the Constitution, Federal Criminal Police Office, Federal Intelligence Service, etc.). The provider receives recommendations e.g. German Federal Ministry of the Interior (Bundesministerium des Innern 2005) that include possible threat scenarios. The decision-making process is sce-

nario-based; as a result, *threat* is not a part of the decision analysis, and depends on the scenario selection.

The *consequences* of terror acts are manifold. The assessment of casualties is a highly ethical problem for providers (Hess 2011), not considering the loss of image; thus, the consequences are not suitable as a decision criterion.

As a result, the author prioritized security measures according to the three criteria required by the expert (see Section 3.1):

1. Effectiveness of the security measure (Criterion 1)
2. Costs of the security measure (Criterion 2)
3. Acceptance of security measures (Criterion 3)

These three criteria represent the objective tricolon of *effectiveness*, *efficiency*, and *customer satisfaction* mentioned by Carnegie et al. (2010), which they recommended to public transportation providers. Figure 52 shows the decision-making process with the three criteria of finding the most suitable security measure which reduces the risk of terrorist attacks (objective effectiveness), on the one hand, and is cost-efficient and accepted by customers, on the other hand.

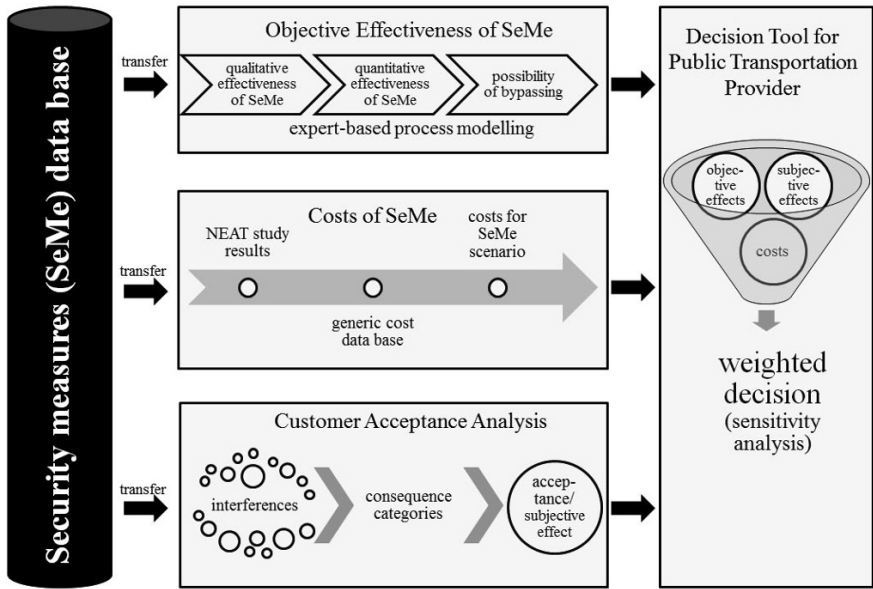


Figure 52: Model for decision-making—Effects of Security Measures (Source: author)

The database of security measures provides limited alternatives. The author, therefore, used multi-attribute decision-making (MADM) for analysis. The multi-objective decision making (MODM) was not used in this case. MADM employs an attribute tree like the one shown in Figure 53.

In Figure 53, the different alternatives a_i represent the different security measures. The different ICs are also called attributes and are weighted by the acceptance answers of surveyed KVB customers (Section 4.5). Aggregation revealed a criterion of respondents' acceptance, which is an indicator of acceptance problems related to security measures in comparison to each other.

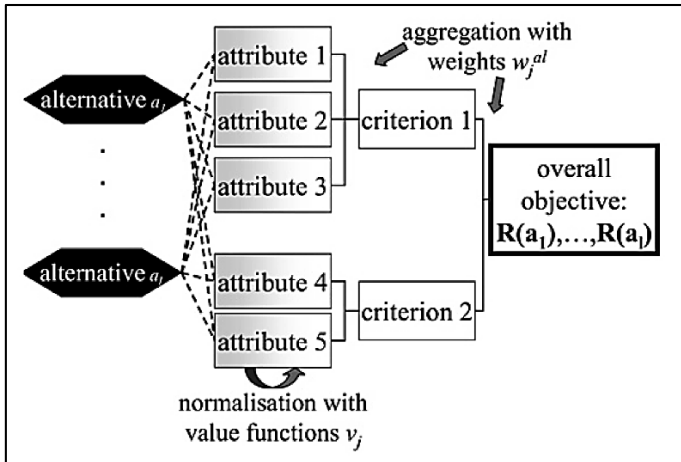


Figure 53: Attribute tree of measurable attributes in gradient boxes, criteria, and overall measurable goal in white boxes. Dependence of attributes on the alternatives (represented as diamonds) is shown by dashed lines. (Source: Comes et al. 2011)

Other criteria are the preventive effectiveness of security measures and the costs of the measures. Decision-makers have the opportunity to weigh the different criteria, based on their preferences to reach objectives according to the organization's values.

To ensure comparability of criteria, the values assigned must be normalized. The preferences of decision-makers for attributes and criteria can be expressed in terms of weights (Lin et al. 2014). Analysis allows assessment of already implemented security measures as well as future developments (proof of concepts).

The following sections explain the three criteria of MADM and their approaches in detail.

5.1.1 Criterion 1: Technical/Objective Effectiveness of Preventive Security Measures

“Vulnerability is the strength or weakness of potentially targeted asset and their protective systems to a specific threat. This involves the analyzing the existing capabilities and countermeasures at the asset or facility and their effectiveness in reducing those vulnerabilities”

(RAMCAP 2006:9).

Security Measures are countermeasures and their effectiveness part of vulnerability (cp. RAMCAP 2006). Criterion 1 represents the *objective level of security*. Krell defined *objective level of security* as the state of absence of certain hazards or hazardous elements, e.g. a terrorist attacker or a weapon (Krell 1980). This statement assumes that objective security is measurable and, in many cases, it is (e.g., crime statistics). In the field of terrorism, recorded prevented terrorist attacks are insignificant, so other methodologies have to be used to measure the effectiveness of *type 2* preventive security measures (Kersten and Klett 2008). Therefore, the definition of criterion 1 is adapted to an index of the effectiveness of preventive security measures.

The author used a new scenario-based approach to estimate the preventive efficiency of security measures that considers the scenario, the target object, and the behavior of an *intelligent adversary* as Cox (2008) described. To estimate the effectiveness of security measures, decision-makers carry out a two-stage, semi-quantitative analysis consisting of an expert interview in combination with a process model of the attacker that describes the *modus operandi* of the chosen scenario (see Figure 54). Both steps lead to an overall performance category (Brauner et al. 2014b, 2014f).

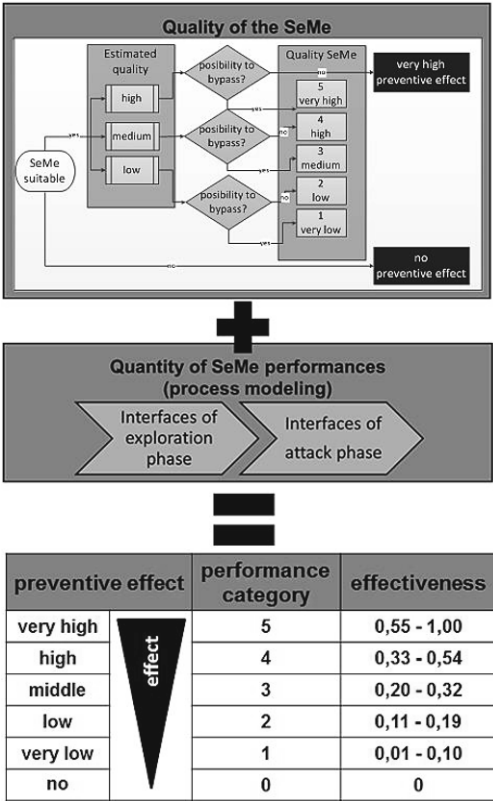


Figure 54: Estimation of security measure performance (Source: Brauner et al. 2014f, adapted by author)

For the first stage, the quality of effectiveness is estimated by a structural questionnaire as the first step. The decision-maker first determines whether a security measure is suitable in a given scenario. If not, no further investigation of the security measure is necessary because there is no performance (i.e., the performance category is zero). In the second step, the decision-maker roughly estimates the quality of every suitable security measure as *low*, *medium*, or *high*. In the third step, the decision-maker determines the possibility of bypassing the security measure in the scenario. If analysis reveals a suitable security measure that has a high estimated quality and cannot be bypassed by an attacker, the performance category is automatically listed as category five (very high). All other security measures receive a value of quality Q_s , which must be combined with a statement of where and how often the security measure may have an effect on an

attacker. This analysis is done in the second step. (Brauner et al. 2015; Brauner et al. 2014b)

The second step consists of a process analysis of the *modus operandi* of the attacker and seeks to quantify the effectiveness of the security measures. To accomplish this, the author his research team developed a generic process model of an attack applicable to every scenario except cyber-attacks (Brauner et al. 2014a). This process model allows decision-makers to identify interfaces where security measures can have an effect in the form of (a) physically detecting an attacker, (b) physically detecting a weapon, or (c) physically detecting both, considering the behavior of the attacker and the environment (e.g., station concourse, platform, or tunnel). In this analysis, two phases are examined—the exploration phase and the terroristic attack phase. Depending on the scenario, the process model contains six, eight, or 10 interfaces where preventive security measures might have an effect. Using a questionnaire and a software tool, the decision-maker reviews the interfaces and determines the physical detection of possibility (a), (b), or (c) and obtains a number of positive interfaces I_s . To determine the effectiveness of the security measure eff_s , the estimated values are set in relation to the maximum achievable values (Brauner et al. 2015; Brauner et al. 2014c). The idea of this efficiency factor comes from a technical model called the Carnot process. The process is named after Nicolas Léonard Sadi Carnot who used a similar formula to determine the efficiency of cyclic thermodynamic idealized processes (Carnot 1872).

$$eff_s = \frac{Q_s * I_s}{Q_{max} * I_{max}}$$

The completion of this analysis, leaves the decision-maker with a decimal value between 0 and 1 for each security measure, presenting a value for its effectiveness (for a, b, or c) in the examined scenario and can be transferred into a qualitative statement or performance category (see Figure 54) (Brauner et al. 2014c). For the MCDA, the performance categories of each security measure can be used as a criterion in the decision tree.

If the combination of different security measures is part of the investigation, an approach comparable with the calculation of stochastic independence is used to ensure that the effectiveness of a combination is equal to or higher than the highest effectiveness of every implemented security measure. Therefore, the different eff_s are transferred in the index $\bar{S}_s$ by subtraction $\bar{S}_s = 1 - eff_s$. The overall preventive effectiveness eff_{total} can be calculated by the following formula (Brauner et al. 2015):

$$eff_{total} = 1 - (\bar{S}_1 * \bar{S}_2 * ... * \bar{S}_n)$$

In the last step eff_{total} , the performance category has to be revised by the decision-maker because some combinations of security measures affect each other negatively or positively (reinforcing or degrading their effectiveness). The software tool displays the results and provides guidelines to correct the performance category.

In further research, Brauner et al. provided an additional framework to estimate the vulnerability of a potentially targeted asset by combining the performance category of security measures with analysis of structural weaknesses.

5.1.2 Criterion 2: Costs of Security Measures

Showing the effectiveness of security measures in the form of a criterion is insufficient if the *costs* are not considered as well. In an analysis, both values represent a kind of cost-benefit analysis. The determination of costs is challenging and depends on different factors (e.g., the definition of a system, structural requirements, technical implementation, amount, coverage, and daily operating time). Further costs can be split into different categories such as non-recurring costs (NRC) like investment costs and recurring costs (RC) that are incurred for services, maintenance, and personnel. Decision-makers have to take into account all relevant costs in their assessment. Different methodologies are available to capture the costs. For example, the Network for the Economic Analysis of Terrorism (NEAT) did an analysis called “An Economic Impact Analysis on Terrorist Attacks against Public Transport Networks” in 2009. In this analysis, Pickl et al. (2009) developed a generic model of a public transportation system that provided the basis for an economic analysis of costs for securing a system and the damages caused by terrorist attacks. The different calculations are set out in Pick et al. 2009. An example overview of the generated costs is displayed in Table 18.

Table 18: Example overview of costs of security measures (Source: Pickl et al. 2009, adapted by author)

Description	Investment costs		Annual recurring costs	
	min	max	min	max
Technology-based improvements				
Video surveillance infrastructure				
-On trains/coaches		100,000,000 €	1,000,000 €	5,000,000 €
-On station tracks		50,000,000 €	500,000 €	2,500,000 €
-On entrance areas of stations		25,000,000 €	250,000 €	1,250,000 €
-In tunnel systems		150,000,000 €	1,500,000 €	7,500,000 €
-Maintenance and depot areas		5,000,000 €	50,000 €	250,000 €
-Perimeter fencing (embankment and vicinity)		500,000,000 €	5,000,000 €	25,000,000 €
Recording of video surveillance			10,000 €	10,000 €
Monitoring of video surveillance				4,300,000 €
Detection systems (static or portable/handheld)				
-Weapons	150,000 €	4,000,000 €	50,000 €	1,000,000 €
-Chemicals or gas	50,000 €	2,000,000 €	20,000 €	1,000,000 €
-Biological detection	50,000 €	50,000 €	10,000 €	10,000 €
-Contamination meter	25,000 €	100,000 €	10,000 €	10,000 €
Luggage control		115,000,000 €		8,000,000 €
Vehicle location system		2,000,000 €	100,000 €	100,000 €
Emergency call devices in coaches				
Enhanced cyber security techniques			500,000 €	2,000,000 €
Additional personnel				
Patrols of security forces in trains and stations				36,000,000 €
K9 units		8,000,000 €		1,250,000 €

Infrastructure or facility modification				
Installing fixed blast-resistance barriers in trains		130,000,000 €	1,300,000 €	6,500,000 €
Installing fixed blast-resistance barriers at station entrances and rapid closure of station access doors		10,000,000 €	100,000 €	500,000 €
Installing glass barriers to separate station track from rail track		26,000,000 €	260,000 €	1,300,000 €
Intrusion detection system on tunnel network		25,000,000 €	250,000 €	1,250,000 €
Perimeter fencing at surface rail tracks		500,000,000 €	5,000,000 €	25,000,000 €
Retractable bollards in front of station entries		20,000,000 €	200,000 €	1,000,000 €
Pillars around elevated infrastructure		50,000,000 €	500,000 €	2,500,000 €
Training and educational upgrades				
Reinforcement of public awareness			1,000,000 €	25,000,000 €
Trainings on emergency response			500,000 €	2,000,000 €
First aid refurbishment			250,000 €	500,000 €
Combined emergency trainings with local public security (police, firefighters)			1,000,000 €	5,000,000 €
Organizational improvements				
Redundancy of tracks/ tunnels on main axis	50,000,000 €	200,000,000 €	1,000,000 €	5,000,000 €
Redundancy of control centers				15,000,000 €
Variable routes for dangerous transports				
Process-based improvements				
Emergency response planning				1,000,000 €

Computer Emergency Response Team (CERT)				1,000,000 €
Sum	50,275,000 €	1,922,150,000 €	20,360,000 €	187,730,000 €
“Costs of security measures: [...] • Investment costs from €50 million up to €1,922 million • Annual recurring costs from €20 million up to €188 million This means that 3%-30% of the annual turnover must be spent for the annual recurring costs.” (Pickl et al. 2009)				

The listed costs incurred directly depend on the nature coverage of the security measures, in this case 230 stations (an entire public transportation system). The MCDA is scenario-based and assesses a defined structure with a proximate environment, limiting the number of security measures. All estimated costs should be checked if they are life cycle costs (LCC), including those for purchases, training, usage, support, maintenance, and recycling (Norris 2001). A partial reduced view of the total costs of ownership (TCO) can lead to incorrect assumptions in the MCDA. Different frameworks are available to support the process of assessing LCC such as VDI 2884:2005 and IEC 60300-3-3:2004. In this illustrative application, the NEAT study of Pickl et al. (2009) provides a good orientation for estimation of costs, although the study does not consider all parts of LCC.

5.1.3 Criterion 3: Acceptance of Security Measures

The third criterion, acceptance, is part of Chapter 4 and consists of the translation matrix of security measures and interference criteria (IC) presented in Section 4.5. The Criterion 3 represents the subjective security level in public transportation and depends highly on the individual perception of the social environment (Wurtzbacher 2003). This also includes the objective security, but even more so the assessment of people’s perceptions in relation to individual experiences and social values. This includes media, communication, and security stability. The acceptance of security measures is a major factor of subjective security, because a lack of acceptance leads to mistrust, increasing insecurity perception, and customer loss in public transportation systems.

The author uses the *non-acceptance* in this criterion to show decision-makers the security measures that have serious acceptance problems and need, if implemented, further communication strategies or customer sensitizing.

5.2 Example Scenario for Application

According to the author (Brauner et al. 2015, 2014b), the assessment of the preventive effectiveness of security measures requires a terrorist attack scenario. For demonstration purposes, the following example is used to apply the methodology.

Target: A fictive subway station of a generic public transportation system in an urban area. The station has four entrances and two elevators to enter or exit the station. Entering the station via stairs or escalator leads passengers to one of two intermediate levels (north or south), where travel information is displayed and shops are located. A second stairway/escalator allows passengers to enter the railway, with two tracks located in the station basement (see Figure 55).

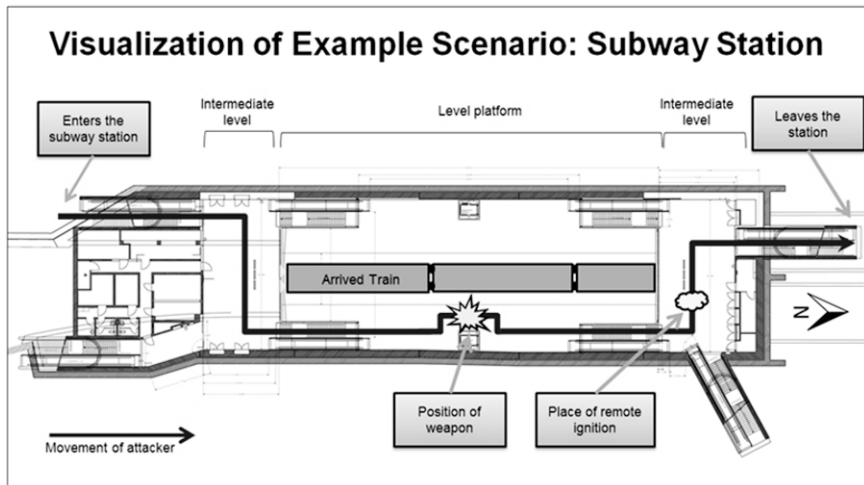


Figure 55: Plan of fictive subway station (Source: author, Brauner et al. 2014d)

Attacker: In this imagined scenario, one offender (without suicidal intention) enters the station carrying a bomb in a suitcase with the purpose of causing an explosion and harming as many passengers as possible. The suitcase with the bomb is placed next to the railway track among waiting passengers. On seeing a train arriving, the attacker remotely initiates the explosion while standing at a safe distance on one of the intermediate levels. Finally, the attacker leaves the station using one of the adjacent stairways.

Weapon: In the MCDA, the consequences were not considered because the author did not wish to assess or quantify passenger losses. Nevertheless, a fictive bomb in a suitcase is the equivalent of 1.5 kg TNT.

Security Measures: In this example, the following security measures are investigated:

1. Video surveillance (live mode + recording)
2. Intelligent video surveillance (behavior recognition: lost luggage)
3. Security personnel
4. Police officers + sniffer dogs (K9)
5. Access control (manual ticket inspection)
6. Detectors (metal/explosives/drugs)

5.3 Data Aggregation for Decision Criteria

Data can be expressed in various forms such as nominal, ordinal, or cardinal. While nominal and ordinal scales express qualitative values, cardinal scale displays quantitative values (Gallopín 1997). The methodology to estimate the *effectiveness* of security measures presents results in cardinal as well as ordinal scales. A cardinal scale is used in the MCDA for further analysis. The data for *Criterion 2 costs of security measures* are expressed in the form of a cardinal scale and can easily be transferred to the MCDA. The data for *Criterion 3 (non-) acceptance of security measures* is also expressed in a cardinal scale.

To compare different security measures, the different values must be normalized to a defined range (Kirkwood 1997) or, in other words, a close range from zero to one (Bertsch 2008). To perform this normalization a *value of use* function is required.

$$v_i: \begin{cases} \mathbb{R} \rightarrow [0,1] \\ x_i \mapsto v_i(x_i) \end{cases}$$

The author employed the function v_i by Bertsch (2008), which uses the range of possible values x_i of each indicator (i). The lowest value $x_{i,min}$ of an indicator represents the lowest value in the function (zero), while the highest value $x_{i,max}$ should represent the highest function value (one). If there is a linear relationship between x_i and the function value $v_i(x_i)$, the $v_i(x_i) = \frac{x_i - x_{i,min}}{x_{i,max} - x_{i,min}}$ operation can be used (Bertsch 2008).

Criterion 1—Technical/Objective Effectiveness of Preventive Security Measures

On 25th November 2014, a tabletop exercise with experts of the KVB, Berliner Verkehrsgesellschaft AöR, and Münchener Verkehrsgesellschaft mbH was carried out to analyze the *effectiveness of security measures* in the above-described scenario within a vulnerability analysis. The author displayed the results in this context and used the estimations of expert-based process modeling for the MCDA.

Results of Effectiveness Analysis:

The security experts of the three public transportation systems chose six security measures from the security measurement database to assess their effectiveness in the above-described scenario. Using the methodology of the author (Brauner et al. 2014b), the experts determined the performance categories for each security measure in the described scenario.

In a first step, the overall qualities of each security measures were estimated in the categories *low*, *medium*, and *high* (see Table 19) and the possibility of bypassing the security measure. In a second step, the quantitative analyses were executed. Therefore, the operation of the attacker was clustered in process steps according to a generic process model (1-7 and 10), several sub-processes were cancelled if not in the scenario existing (8+9) (Brauner et al. 2014d). The sub-process steps were pictured in Figure 56.

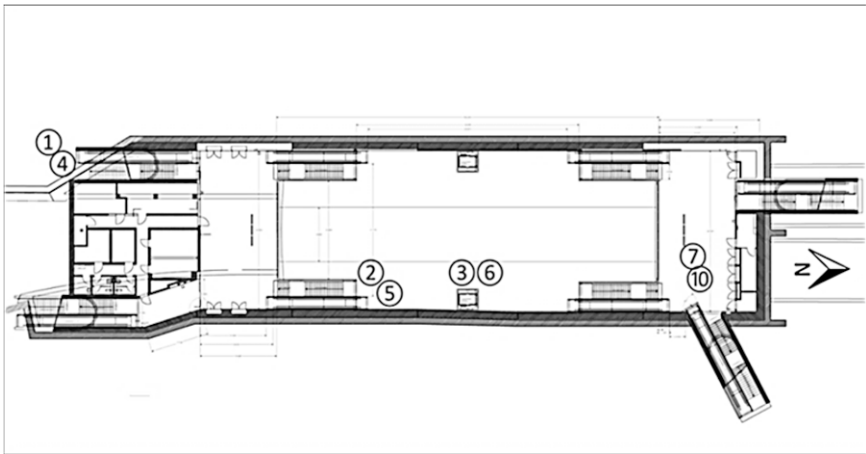


Figure 56: Process steps of attack mode according generic process model (Source: Brauner et al. 2014d)

For better visualization and discussion with experts, a model of the subway station was manufactured. The process steps described above were visualized on the model board and discussed. For each sub-process, the experts discussed in principle whether the pre-defined security measures can “*physically identify the attacker as perpetrators*” or “*the weapon (in this case a bomb)*” or “*cannot operate*”. As a result of the discussion, a quantitative value of “*effective processes steps*” for each security measure was documented in the software demonstrator for the quantification analysis (Brauner et al. 2014b).

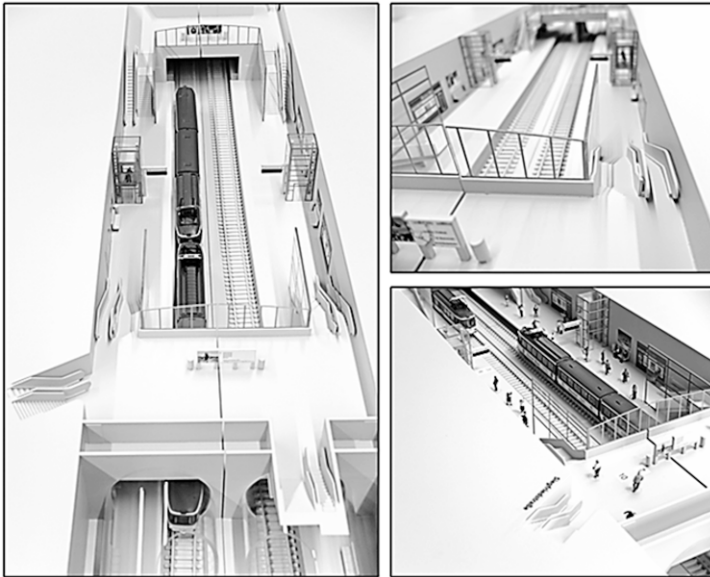


Figure 57: Model of subway station (Source: author)

1. Video surveillance (live mode and recording)

Four cameras (1-4) for recording of train operations are located at the two platforms at the end of the platforms. Two additional cameras are located on the two intermediate levels (5-6). The exact arrangement is shown in Figure 58. The individual cameras record over a period of 48 hours and can be switched in live mode to a control center, but without any specific work order of monitoring by control center personnel (Brauner et al. 2014d).

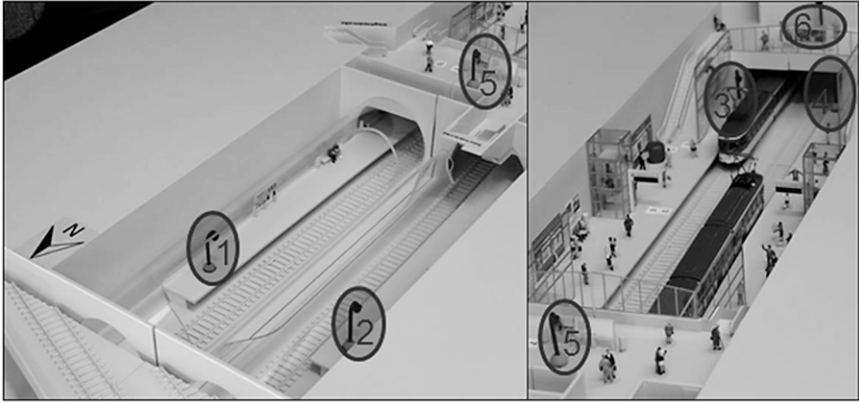


Figure 58: Positions of cameras for video surveillance (Source: Brauner et al. 2014d)

2. Intelligent video surveillance

The experts decided to implement intelligent video surveillance with the features of recording and software analysis for “tracking” customers as well as “detecting of lost luggage”. In addition, the analysis software can identify misplaced persons such as persons moving on the train tracks or in tunnels. The cameras were arranged as shown in Figure 59 to cover the whole subway station. In addition, two cameras cover the carrying-on-platform in the tunnels (11-12) (Brauner et al. 2014d).

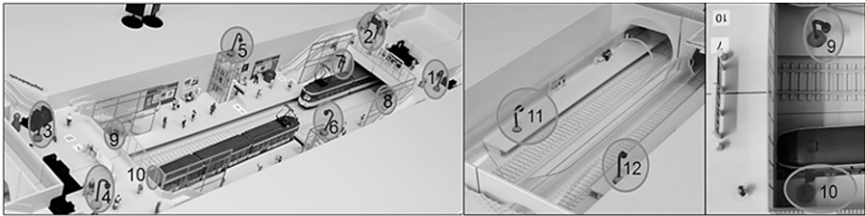


Figure 59: Positions of intelligent video surveillance (Source: Brauner et al. 2014d)

3. Security personnel

The security personnel move throughout the sub-station and can control travelers/passengers. They provide a point of contact for customers in case of questions and security issues (Brauner et al. 2014d).

4. Police officers with K9

Next to the entrances, the experts chose *police officers with K9* as an additional security measure for assessment. The police patrols can inspect suspicious persons, further the dogs are trained to identify explosives of potential offenders (Brauner et al. 2014d).

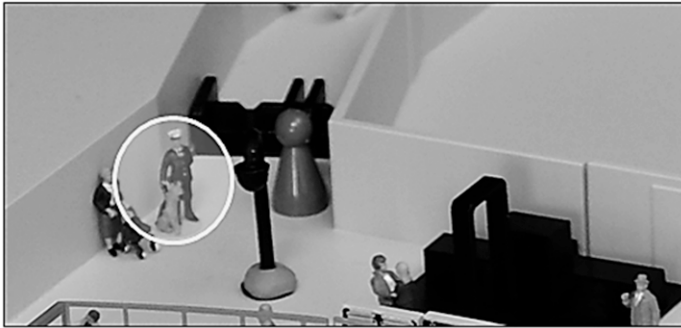


Figure 60: Positions of police officers with K9 (Source: Brauner et al. 2014d)

5. Access control with ticket control

At every entrance to the subway station *access controls* were implemented by the experts. These *access controls* consist of a manual ticket inspection by personnel (Brauner et al. 2014d).

6. Detectors

On two intermediate levels, the experts implemented a detector solution that allows passenger and luggage inspections. It contains the features to detect metal, various explosives devices, and various drugs. The luggage is examined through an X-ray device, the passengers by a gateway and hand scanners. This measure takes time, so only a random sample of passengers can be searched (Brauner et al. 2014d).

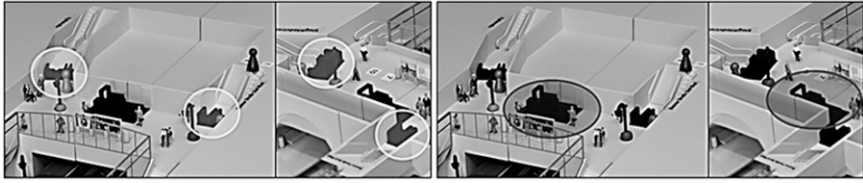


Figure 61: Position of access control (left) and detectors (right)
(Source: Brauner et al. 2014d)

The experts assessed the preventive effect of *video surveillance* and *access control* (*manual ticket inspection*) as being ineffective in identifying the terrorist in this scenario (see Table 19). Therefore, additional features are necessary such as *intelligent video surveillance* that recognize lost luggage in public areas. Currently, this technology sets off troublesome alarms in public transportation systems, depending on the settings. Hence, the experts assessed a very low preventive effect (performance category 1). *Security personnel* and *detectors* join the same performance category because, on one hand, *security personnel* are not explicitly trained to recognize possible attackers but still can recognize lost luggage (in this case the bomb in the luggage), and, on the other hand, *detectors* have high accuracy, but can only search a limited number of passengers. Among all six security measures in this scenario, *police officers with K9* (*sniffer dogs*) has the highest effectiveness, although its preventive effect is estimated as low (performance category 2). The exact values of the software demonstrator according to the positive effect interfaces in the process model were transferred to the MCDA and normalized. In order not to miss out any security measure in the decision process, the performance values of *video surveillance* and *access control* were set on the lowest possible value 0.001 and normalized too. The result is presented in Figure 62. The bar chart shows the normalized results of the tabletop exercise for this scenario. In this scenario, *police officers with K9* have the highest preventive effectiveness, followed by the *intelligent video surveillance* and *security personnel* and *detectors*. *Access control* and *video surveillance* appear marginally and are ineffective in preventing the scenario and reducing vulnerability (Brauner et al. 2014d).

Table 19: Criterion 1—Estimation of the preventive effectiveness of SeMe
(Source: author, according to Brauner et al. 2014d)

Security Measures	Quality	Preventive effect (scenario-based)	Performance cat. (exact value)	Reason of experts	Normalized Sum
	Number of interfaces with effect				
	Bypass possibility				
Video surveillance (live mode + recording)	low	no preventive effect	0 (0.001)	Operating range of camera currently about 25m; mostly effective in crime investigation (after event); intelligent and inconspicuous attackers cannot be recognized through cameras	0.004 *
	0 of 8				
	-				
Intelligent video surveillance (behavior recognition: lost luggage)	low	very low preventive effect	1 (0.05)	Intelligent camera systems can detect lost luggage after 30 sec.; most systems are set up for 1 min. detection to minimize troublesome alarms. In this scenario, the timeframe might be too short to interact with the attacker or prohibit the attack.	0.198
	1 of 8				
	no possibility of bypass				
Security personnel	low	very low preventive effect	1 (0.025)	No explicit training and education to recognize attacker, but chance to recognize lost luggage; attacker can easily bypasses service personnel.	0.099
	1 of 8				
	possibility of bypass				
Police officers + sniffer dogs (K9)	medium	low preventive effect	2 (0.15)	K9 sniffer dogs can only perform detection in short time periods and quiet circumstances; detection only at entrance and intermediate level possible; attacker can easily bypass the measure.	0.595
	2 of 8				
	possibility of bypass				
Access control (manual ticket inspection)	medium	no preventive effect	0 (0.001)	Attacker can purchase a valid ticket.	0.004 *
	0 of 8				
	-				
Detectors (metal/ explosives/ drugs)	low	very low preventive effect	1 (0.025)	Currently, detectors can technically search a limited number of passengers; therefore, just a sample of passengers can be searched.	0.099
	1 of 8				
	possibility of bypass				

* Normalized (SUM) for MCDA; 0.004 represents no preventive effect.

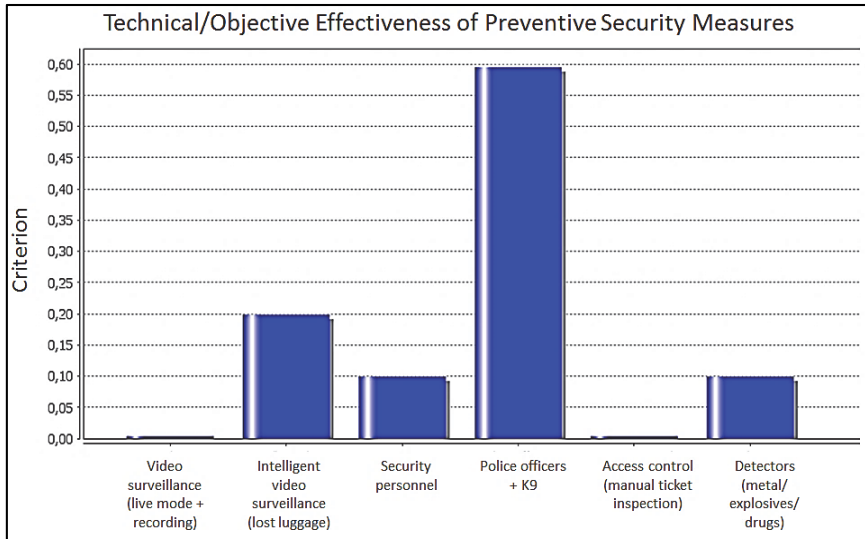


Figure 62: Bar chart of the criterion technical/objective effectiveness of preventive security measures (Source: author, KIT software 2014)

Criterion 2—Costs of Security Measures

In the second step, the author investigated the costs for the six chosen security measure combinations. Using the conclusions of the NEAT study of Pickl et al. (2009), the costs for a public transportation system (390 stations) were calculated based on one subway station according to the above structure (see Figure 55). The costs were associated with the investigation and annual recurring costs for a two-year period. The observation period can easily be changed according to user requirements.

Table 20: Criterion 2—Costs for SeMe in one subway station (Source: author, according to Pickl et al. 2009)

SeMe	Investment costs	Annual recurring costs		Normalized (SUM)*
		min	max	
Technology-based improvements				
-Video surveillance				0.079
On station tracks (6)	90,000 €	375 €	450 €	
At entrance areas of stations (4)	60,000 €	300 €	300 €	
In tunnel systems (2)	30,000 €	150 €	300 €	
Recording of video surveillance	incl.	500 €	500 €	
Monitoring of video surveillance			26,000 €	
-Intelligent video surveillance	see above	see above	see above	0.081
I-cam software	+5,000 €			
-Detection systems for weapons (metal/explosives/drugs) + patrol of security forces (7/24: 2 persons 8h and 3 work shifts)	10,256 € +208,000 €	500 €	2,564 € +208,000 €	0.163
Personnel				
-Patrols of security forces in trains and stations (7/24: 2 persons 8h and 3 work shifts)	208,200 €		208,200 €	0.158
-K9 units (2)	102,000 €		16,550 €	0.203
+ Police officer (2)	+208,200 €		+208,200 €	
-Access control (manual ticket inspection) (7/24: 4 persons 8h and 3 work shifts)	416,400 €		416,400 €	0.316

* The values are normalized according to the sum of the costs.

The costs were normalized according to the sum of all costs and transferred to the MCDA tool. The bar chart in Figure 63 reveals a ranking of the costs and

shows high costs for all security measures, which include personnel. The highest costs are imposed by the *access control* that needs four persons (one at each entrance, seven days a week and 24 hours) to check all passengers, followed by *police officers with K9, detectors* and, *security personnel* (patrols). Technical security measures such as *video surveillance* or more advanced *intelligent video surveillance* systems have the lowest costs in this scenario.

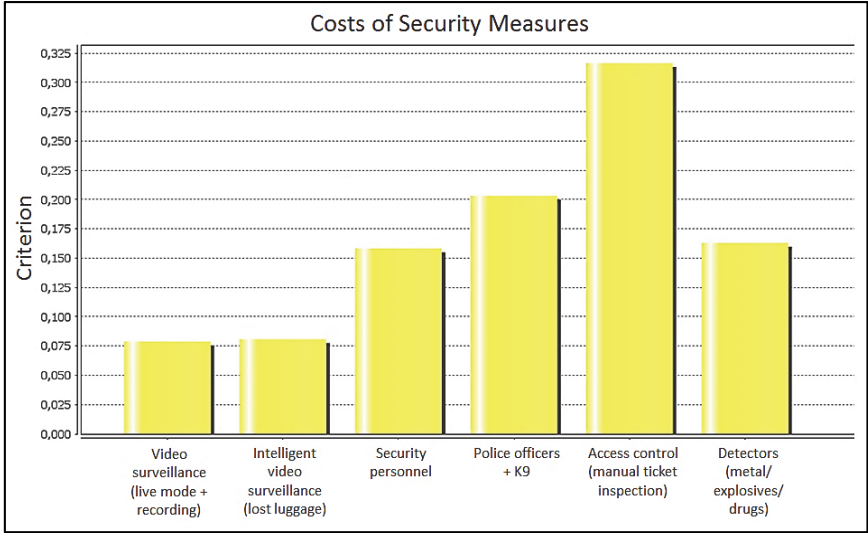


Figure 63: Bar chart of the criterion costs of security measures (Source: author, KIT software 2014)

Criterion 3—Acceptance of Security Measures

The interferences of security measures are expressed in the MCDA as sub-criteria of the criterion *acceptance of security measures*. Overall, 24 sub-criteria (different types of interference) are included in the acceptance criterion. Therefore, the results of the acceptance analysis (see Section 4.5) were transferred and applied to the scenario and choice of security measures. The author used the negative values of acceptance, representing *non-acceptance* or, specifically, the *acceptance problems* of each type of interference. The higher the degree of the overall *non-acceptance* of each security measure, the higher the future problems arising from customers’ lack of acceptance. The non-acceptance values were not normalized because the amplitude of the stacked bars represents the degree of problems customers had in accepting the consequences of the specific security measure. A normalization of all interferences would delete this effect. Hence, the

author chose to sum the relative values of non-acceptance of the interferences to get an impression of the overall non-acceptance. Figure 64 shows the overall non-acceptance of each security measures according to the customer survey feedback. It shows a higher non-acceptance towards security measures that are visible and communicate with the customer. Both variations of *video surveillance* that perform without any interaction with the customer have lower acceptance problems. Security measures with personnel have higher acceptance problems, especially *police officers with K9* has the highest acceptance problems, followed by *detectors (metal/explosives/drugs)*, which involve specific security checking process. *Security personnel* and *access control* are in the middle sector of the non-acceptance and almost equal.

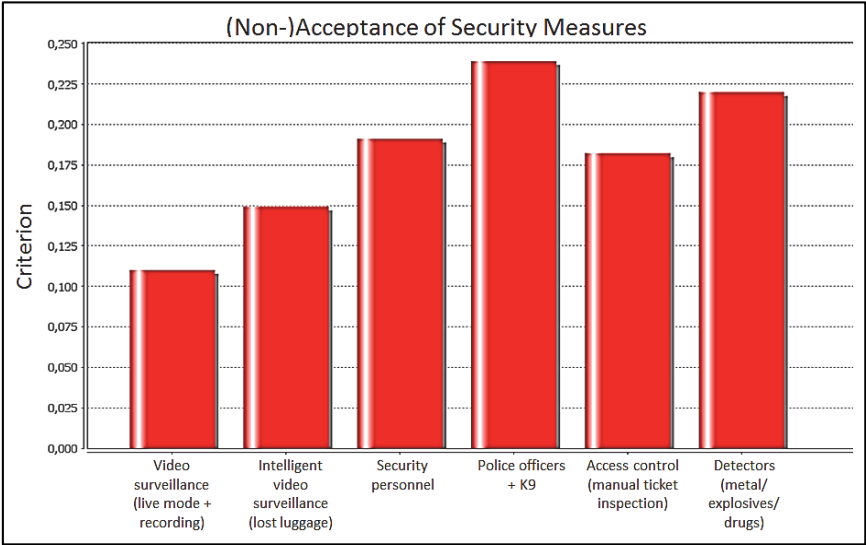


Figure 64: Bar chart of the criterion non-acceptance of security measures (Source: author, KIT software 2014)

The resolution of the bar chart can be increased up to tier two to show the non-acceptances of the *interferences* for each security measure. Figure 65 displays the acceptance problems of the interferences, offering a close view on each security measure. Each interference criteria is displayed, and it can be observed that not all IC affect all security measures. The stacked bar chart sums up the IC, while the amplitude of the IC represents the relative number of customers who had problems accepting the consequences of the IC. A detailed overview of the values are provided in Annex D—Data Sheet and Report MCDA Software.

The bar chart reveals that technical security measures such as *video surveillance* cause acceptance problems in the *anonymity* category (e.g. face detection, storage of data, etc.), whereas security measures having a “security check” character have high acceptance problems in the *integrity* (e.g. “customer is searched” and “customer luggage is scanned”) as well as *flexibility* (e.g. “luggage limitation” and “registration,” etc.). Obviously, the interferences in the category *personal rights* (e.g. “ticket is checked” and “a security guard is present,” etc.) do not face high acceptance problems as assumed in Figure 64. The non-technical security measures have high acceptance problems in by causing interferences in the flexibility of the customers (marked in different green colors).

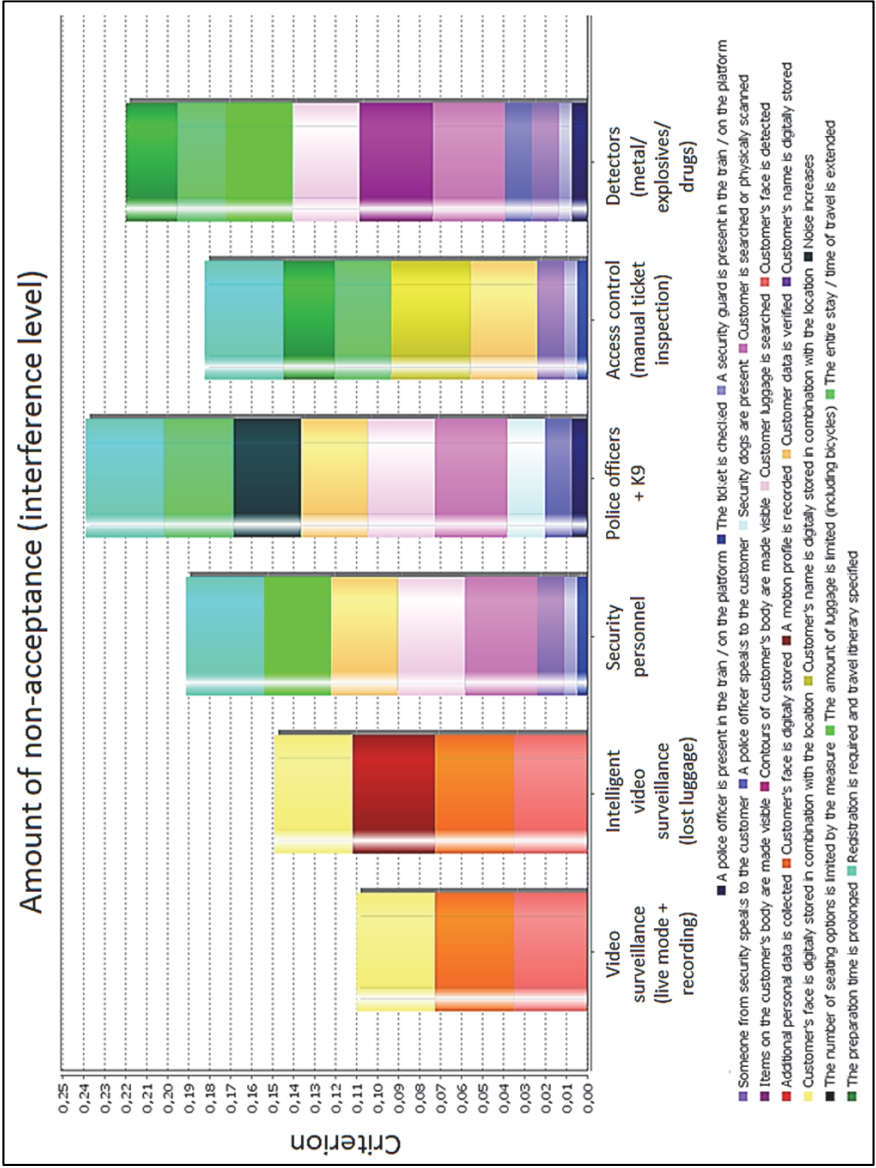


Figure 65: Bar chart of interference criteria for six example security measures (Source: author, KIT software 2014)

5.4 Decision Making Process and Sensitivity Analysis

In the last step, the three criteria were implemented in the MCDA to allow assessment by decision-makers. In the MCDA, the efficiency of the security measures in this scenario was operationalized by the attributes *technical/objective effectiveness* to reduce vulnerability, *costs for security measures*, and *subjective effectiveness* (public acceptance). The *objective effectiveness* was derived from an expert workshop with security experts of public transportation systems who determined the effectiveness by a structural questionnaire considering process modeling of a terrorist attack. The *cost of security measures* were derived from the NEAT study and applied to the given scenario. The costs and the effectiveness of the security measures represent the cost-benefit of the security measures (efficiency). Finally, the *subjective effectiveness* was added. It comprises the assessment of the interference criteria by KVB customers (in the *personal rights, integrity, anonymity, comfort, and flexibility* consequence categories).

Using an even weighting of all three criteria (33.3%), the MCDA leads to a bar chart to display the results of the entered data in a report or bar chart. Figure 66 displays the result of the six alternatives (security measures) and their overall quality. The quality integrates the three weightings criteria, although *subjective effectiveness* considers 24 sub criteria. In the chosen scenario (see Section 5.2), a bomb attack in a subway station, the security measure ***police officers with K9 is the best alternative***. It has a clear margin and no criterion dominates this alternative, although some criteria dominate others (e.g. objective effectiveness).

The security measure, *access control*, requires a large number of personnel, making this measure very expensive compared to others. It has no *objective effectiveness*, which is why it should not be implemented to reduce the vulnerability of the example scenario. The security measure, *intelligent video surveillance*, dominates *security personnel, detectors*, and *conventional video surveillance* in the criterion *objective effectiveness*. Although *objective effectiveness* is much lower than *police officers with K9*, this measure might be attractive as well because it entails lower costs (because personnel costs are minimized through automatic software assessment) and lower acceptance problems (mostly invisible to customers in the station) than *police officers with K9* does.

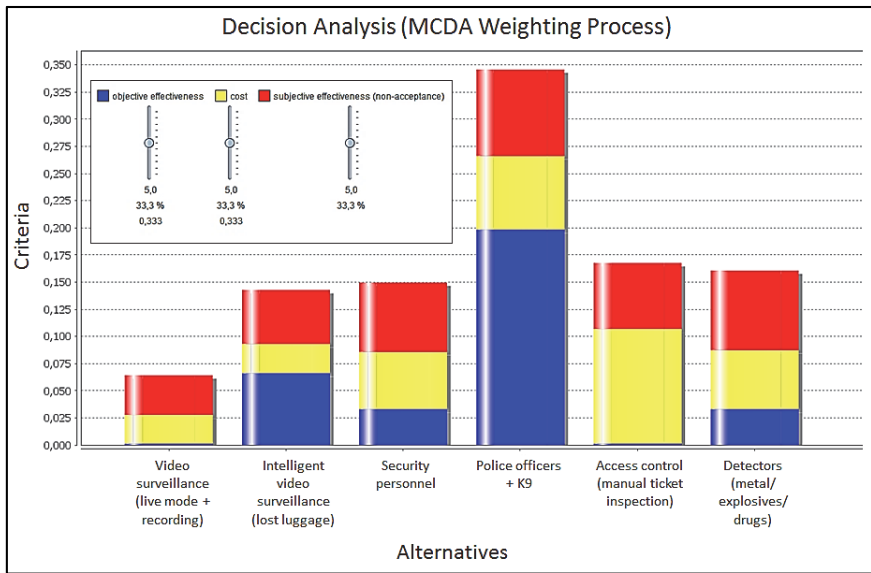


Figure 66: Stacked bar chart of MCDA of all three criteria (Source: author, software KIT 2014)

The criteria operate independently of each other enabling decision-makers to weigh the different criteria according to their own preferences or company requirements. This procedure changes the amplitude of the bars in the MCDA. In Figure 66, the weighting is even (33.3% of each criterion) by adjusting the controller of importance; this leads to the questions: *How is the stability of this decision according different weights of importance? When does the decision result (in this example “police officers with K9”) change?* A stability analysis was done to answer this question. Decision-makers can run a sensitivity analysis of different weightings that show at which weighting point the prioritization of security measures changes.

Figure 67 shows this analysis for the criterion *objective effectiveness*. The vertical line represents the “actual importance” setup (33.3% or 5.0 in MCDA). For example, if the importance of *objective effectiveness* is reduced to less than 0.5, the overall stack of *access control* will dominate that of *police officers with K9*. The best alternative would change to *access control*. Otherwise, if the importance is increased to more than 6.1, *detectors* will beat *access control*. If the importance is increased more than 6.9, *intelligent video surveillance* will beat *access control*, while at an increase of more than 7.8, *intelligent video surveil-*

lance will also beat *detectors*. The alternative *police officers with K9* will still be the best alternative and has a clear margin.

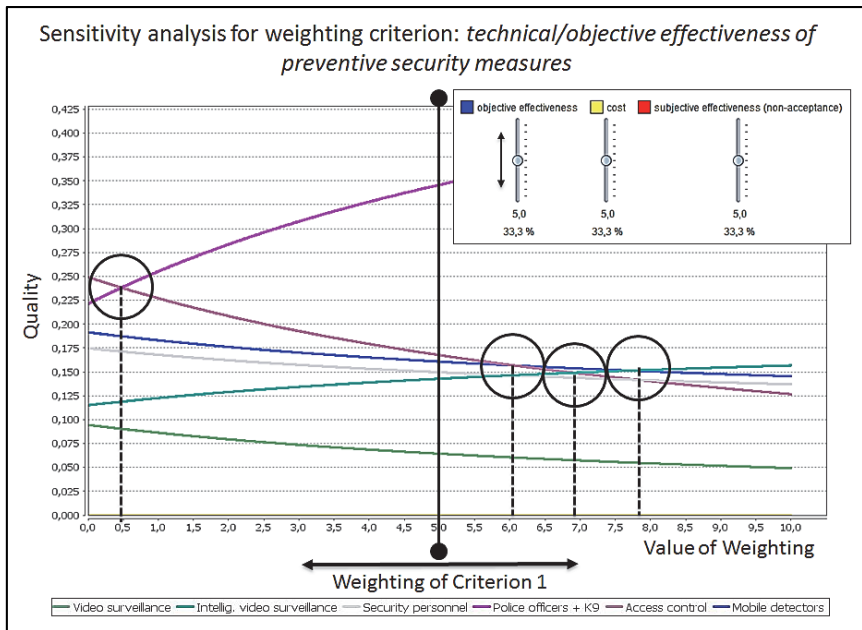


Figure 67: Results of sensitivity analysis for objective effectiveness (Source: author, software KIT 2014)

A similar analysis was done for the second criterion, *costs of security measures*. Figure 68 displays the results and reveals no change in the best alternative, *police officer with K9* by increasing or decreasing the weights of costs. This alternative will still dominate the decision process. The second best alternative, *access control*, loses by decreasing the weighting. If the importance is decreased to less than 4.4, *detectors* will dominate *access control* and if the importance is decreased to less than 3.4, *intelligent video surveillance* will beat *access control* as well. If the importance is below 1.7, *intelligent video surveillance* will dominate even *detectors*.

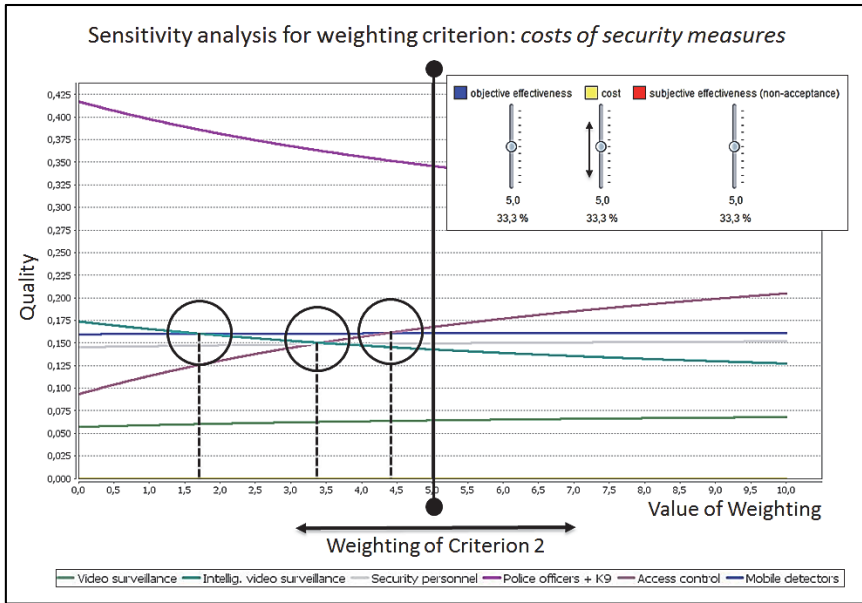


Figure 68: Results of sensitivity analysis for costs of security measures (Source: author, software KIT 2014)

A sensitivity analysis of the different sub-criteria of acceptance is not necessary, because the different sub-criteria are weighted by the acceptance analysis of the customers. A weighting by the decision-makers leads to bias in the criterion, *subjective effectiveness (acceptance)*. Nevertheless, decision-makers can weigh the importance of the overalls *acceptance* in their decision process by adjusting (increasing/decreasing) the importance of the other two criteria *objective/technical effectiveness* and *costs of security measures*.

5.5 Summary and Results of the MCDA for End-users' Risk Management

In an illustrative scenario of a terrorist bomb attack in a subway station, the process of decision making in risk management was carried out. Therefore, the following point of view was chosen:

Decision-maker is a public transportation provider, who decides according three decision criteria (see experts' requirements Section 3.1):

- Criterion 1: Technical/objective effectiveness of the security measure
- Criterion 2: Costs of the security measure
- Criterion 3: Acceptance of security measure

To support this decision process, security experts of three German public transportation systems joined a tabletop exercise and chose six of 81 security measures in a database, representing the alternatives in the decision process.

Criterion 1: To evaluate the *technical/objective effectiveness of security measures* in the scenario, the author used a vulnerability methodology that used an advanced questionnaire for expert interviews based on process modeling of the *modus operandi*. In the tabletop exercise, the same experts who determined the security measures also determined the *technical/objective effectiveness of security measures*. The results of the semi-quantitative analysis were normalized and implemented in the MCDA software as Criterion 1.

Criterion 2: For the estimation of *security measure costs*, the author adapted data of the Network for the Economic Analysis of Terrorism (NEAT) who did an analysis called “An Economic Impact Analysis on Terrorist Attacks against Public Transport Networks” in 2009 (Pickl et al. 2009). The costs of the generic model of a public transportation system were adapted to the scenario description, specifically, the structural conditions of the imagined subway station. In a first step, the chosen security measures were operationalized and linked to the NEAT data. In the second step, the costs of the generic public transportation system were transferred to the numbers of security measures and devices (estimated by the experts). In the last step, the costs were normalized and included in the MCDA software as Criterion 2.

Criterion 3: The author did a study consisting of online and field survey questioning of 1,937 customers of the Kölner Verkehrs-Betriebe AG about their views on 24 type of interference are caused by the 81 security measures in the security measure database. The 24 hindrances cover the effects of security measures at customer level in the consequences categories of personal rights, integrity, anonymity, comfort, and flexibility. In the survey, the customers had to decide whether they accepted such interference. The relative values of non-acceptance were applied to the MCDA software as Criterion 3, called the *subjective effects of security measures* or *acceptance of security measures*.

In case of independent criteria, the MCDA allows the weighting of criteria according to importance. In the example, all three criteria were equally weighted without preferences. The MCDA revealed that the alternative, *police officers with K9*, was the best security measure in this scenario with a clear margin in quality according the setting of importance. No other criterion dominated this alternative. In an additional sensitivity analysis, the author proved the stability of

this decision by analyzing different importance weightings. *Police officers with K9* were stable until the importance of the Criterion 1, *objective effectiveness*, was reduced to less than 0.5 (almost none).

Advantages and disadvantages of MCDA in risk management

The MCDA software, on one hand, provides a good tool to execute a structural decision process. The visualizations (e.g. bar charts) help to understand the results and realize the changes in the weighting of importance in form of a direct feedback in the charts. A report documents the changes. Furthermore, the stability of the decision can be analyzed by performing sensitivity analysis.

On the other hand, MCDA is a model of decision-making and is, therefore, limited in its settings and the implemented criteria data. The results are true as long as the validity of the software and the input is valid and known. The author cannot disregard that the empirically collected data consist uncertainty (Comes et al. 2011). Further, measurement errors cannot be excluded completely either as well as missing attributes (see Chapter 6). Although the decision process is easy to handle with the help of the MCDA software, the process of setting up the required data takes time/efforts, once collected the data can be used for different decision-analysis processes (like security measure database including description of effects of security measures, costs and acceptance).

In every decision process, decision-makers should be aware of the pros and cons of the MCDA that are summarized in Table 21.

Table 21: Pros and cons of MCDA for decision-makers (Source: author)

Pros	Cons
Easy access to decision process (structural process of decision making, end-user friendly)	Validity of the software (KIT 2014) and previous work sources (e.g. NEAT Pickl et al. 2009) are not completely known.
Good visualization of criteria (diagrams, e.g. bar charts)	Empirically collected data might involve uncertainty due to possible subjective perception or incomplete knowledge (Comes et al. 2011)
Easy implementation of preferences into decision process (weighting of importance)	The author cannot exclude measurement errors completely
Sensitivity analysis can be executed to see the stability of the decision	Decision-makers must first set up a database with their own structural requirements
Documentation of decision process (bar charts, sensitivity analysis, tables, report)	Lack of attributes possible

Overall, the decision process using MCDA is a contribution to risk management processes and includes the *technical/objective effectiveness of security measure*, *subjective effect of security measures* and the *costs of security measures* in the decision process. The second research question: “***What are appropriate decision criteria for the implementation of security measures in a public transportation system to prevent terrorist attacks?***” is adequately answered. The comparison of *objective effectiveness* (scenario-based preventive effect), the *costs of security measures*, and *customer acceptance* allows decision-makers to assess the consequences of an implement. It allows weighting depending on their preferences and priorities. The tool allows recommendations for decisions in the form of sensitivity analysis and provides a starting point for further action, e.g., implementation of security measures or public relations concerning security measures with problematic interference. The multi-criteria decision analysis structures and supports the decision process, and answers the question: “***How can a decision process be structured to find the most appropriate security measure based on the criteria in a holistic risk management system?***”

Finally, the author endeavored to consider all end-user requirements of Section 3.3 that could be accomplished in the study.

Requirements for a decision tool for risk management of terrorist attacks:

- Easy to use, applicable, and uncomplicated (user-orientated)
 - ➔ The MCDA tool is easy to use, applicable, and uncomplicated; methodology for objective effectiveness considers more efforts but is applicable due to demonstrator (Brauner et al. 2014a).
- Universally applicable to all security measures
 - ➔ System currently limited for preventive security measures (risk management).
- Determination of the objective effects of security measures
 - ➔ Scenario-based approach using experts’ interview and process modeling available.
- Includes the possibility to display the costs of security measures
 - ➔ Economic costs for chosen security measures can be extracted for scenario-based evaluation.
- Assessment of subjective effects of security measures
 - ➔ Security measure database contains universal values of interference acceptances by customers (consider time-bound, regular evaluations necessary).

- Weighting by the end-user according to company preferences
 - ➔ Importance weighting according company preferences possible in MCDA software.
- Documentation of decision-making processes
 - ➔ Documentation is possible through reports and charts.

6 Synthesis

“Not everything that can be counted counts, and not everything that counts can be counted”

Albert Einstein (1879-1955).

This section discusses the results of this study. It provides a quality assessment considering the further application of the results in risk management processes and discusses the reliability and feasibility of the methodology including data collection and processing. The “*assessment of the effects of security measures*” using the example of terrorist attacks in public transportation systems—as the book title promises—is discussed according to the results and implications for research.

“Quality assessment is an integral part of any systematic review. If the results of individual studies are biased and these are synthesized without any consideration of quality then the results of the review will also be biased” (Whiting et al. 2003:1-2).

The conceptual assumptions are justified by assessment of customer acceptance through the development of the decision tool (MCDA) for various security measures. The feasibility of the conceptual framework and the developed triangulation methods were combined in a constructive way and contribute new dimension to risk management systems.

The validation and verification of the data is a major challenge since no second independent data source is available. While there is the possibility of comparing isolated parts to other research results, validation of the entire triangulation methodology derives no definite conclusion. It should be noted that this study is a modest attempt at integrating technical, economic, and social-scientific (public acceptance of security measures) into a risk management system. Therefore, its reliability (especially the acceptance values) depends more on the definition of resolution and tendencies of results than exact values.

The quantification of social values is an ongoing process in the scientific community and a rarely discussed topic. While the understanding of human behavior is part of qualitative research, every attempt at quantification is a subject of assumptions. These assumptions are restrictions to limit to a manageable extent the influencing factors in a complex system. The model is a simplification of

reality and so study results depend on the kind of simplification employed as well as the point of investigation. As a result, the outcomes of these studies always have limited validity; in other words, the outcome is just as true or false as the described model itself. Therefore, derived conclusions must be discussed critically.

Although three criteria had been integrated into MCDA for risk management, the main focus of this study was the development of a methodology and execution of the *acceptance analysis* (Chapter 4) and the application of the results into a composite indicator for MCDA. In the following discussion about the methodology, the author will also mainly focus on this part. Firstly, the methodology is discussed critically by considering the developed framework of the acceptance study in Section 6.1. Although a direct validation of the results is not possible, the author compares the results with similar studies and underlines the statements and results, as far as possible, in Section 6.2. Finally, the author reflects on the theory in Section 6.3.

6.1 Discussion of the Methodology

Different facets and classifications of sciences are known in the literature. The process of scientific research is a systematic method of investigation or experimentation aimed at the discovery or interpretation of facts, the revision of theories and laws, or their practical application (Webster 2015). This interdisciplinary study is applied research, which is mainly an engineering discipline. The systematic quantification of subjective effects of security measures, guided by a conceptual framework, is an experiment to implement social science research into risk management. Many technical specifications have affected this analysis. In Section 6.1.1, the assets and drawbacks are discussed by taking into account the conceptual framework and the specifications. The pros and cons of criteria that are, in fact, composite indicators are discussed in Section 6.1.2.

6.1.1 *Verification of Results*

To assess the conceptual framework and the results of this study, the author used the guidelines of the United Nations Secretariat of the International Strategy for Disaster Reduction (UN/ISDR) (2008) and did a critical review of the research process. In their guidelines, the UN/ISDR (2008) published eleven requirements, which the author adapted and used for the verification analysis (see Table 22). The answers to this requirement include limitations of questionnaires/interviews as well as weighting problems by experts.

Table 22: Requirements of indicators (Source: UN/ISDR 2008 adapted by author)

Attainability	The measurement of the indicators should be achievable by the policy or project and thus should be sensitive to the improvements the project/policy wishes to achieve.
Clarity/Validity	Indicators should effectively target the factor they are measuring and should avoid ambiguity and arbitrariness in measurement.
Comparability	The indicator measurement should enable comparison over the different life-cycle stages of the policy or project as well as between different policies or projects.
Comprehensibility	The definition and expression of the indicator should be intuitively and easily comprehensible to users.
Measurability	Indicators should be defined so that their measurement and interpretation are as unambiguous as possible, preferably using data that is readily available, relevant, reliable, and meaningful.
Redundancy	While each input variable should measure a discrete phenomenon, separate indicators that measure the same phenomenon may be necessary and desirable.
Relevance	Indicators should be directly relevant to the issue being monitored or assessed and should be based on clearly understood linkages between the indicator and the phenomena under consideration.
Reliability	The results from an indicator should be replicable by different researchers using standard methods. The methods should be stable over time and as valid in the widest circumstances possible.
Sensitivity	Indicators should be able to reflect small changes in the things that the actions intend to change.
Time-bound	The time of an indicator's measurement, or the interval to which it applies, should be appropriate and clearly stated.
Completeness	The data should be complete and free of missing values.

Attainability: The objective of achieving a methodology to assess objective and subjective values in an integrated manner using a risk management process for events with manifold consequences is realistic to a limited extent. Since a new methodology has been developed and the data acquisition/analysis required great effort, the validation process is still problematic due to missing comparable data. Measuring the acceptance of security measures directly has not been possible; it can only be measured indirectly by other survey data by taking recourse to operationalization (Lucke 1995; Winzer et al. 2009). The author chose operationalization to measure interference (a new approach), which is a complex field. Inventing a conceptual framework to measure the IC, different assumptions were made to create a model that allows analysis and makes the objective attainable (cp. Section 3.1). On the opposite side, assumptions have a negative effect on the validity and comparability of the study.

Clarity/Validity: The experts of the KVB and the author attempted to draw statements in the questionnaires that were free of interpretation. The author could not exclude any misinterpretation of the interference criteria by the respondents, but the probability is very low because statements were kept short and understandable. The interference criteria considering time issues posed challenges because no specific timeframe existed. The re-translation of these criteria back to security measures was executed via weighting by experts (interviews with security experts of the Association of German Transport Companies). The acceptance of the IC considering timeframes allowed no reference to security measures without the weighting of the experts. In addition, the allocation of IC and security measures was based on the statements of the KVB experts and the author's assumptions; the ambiguity of the allocations is both a problem and an opportunity for interpretation.

Comparability: The comparability of the project to other life-cycle stages must be assessed critically. The results of the questionnaires depended highly on the current state of security in the city of Cologne and the situation within the Cologne public transportation system. Policy changes and future terrorist attacks (or their warnings) influence the perception of security and the acceptance of interferences by security measures. Therefore, the current security perception of customers was investigated as well. Comparability with other cities and future effects must be assessed critically to avoid bias. The approach of analyzing the interference of security measures in open public transportation systems in an overall manner is new and has not been previously described in the literature. Analysis of the overall acceptance of certain security measures such as body scanning screening equipment has been done (Turley and Stone 2006), but these studies do not provide reliable data for transfer to other security measures or do not focus on a decision tool to determine acceptance problems.

Comprehensibility: The definitions of the interference criteria are comprehensible and easy to understand. The methodology used these definitions to overcome comprehension problems by the customers in understanding the mechanism of different security measures. The author took particular care to use understandable interference criteria. In the field survey, most respondents had no doubts about the IC definitions. Nevertheless, the probability that respondents of the online survey misunderstood the IC because of comprehension problems cannot be eliminated. The author estimates this probability to be very low. One drawback of combining the IC into an overall indicator "*Criterion 3: subjective effects (acceptance)*" in the MCDA is a visual "loss of information" on single IC (in the form of one common stack). This can be overcome by setting the tier up to level two (visualization of IC) or

weighting the IC, using different approaches such as the analytical hierarchy process (cp. Saaty 1990) that is already implemented in the MCDA tool (KIT 2014). However, every weighting is subjective (Simpson and Katirai 2006) and complex analysis tools might reduce comprehensibility for decision-makers.

Measurability: IC (non-) acceptance responses are quantitative indicators because the answer possibilities for the IC are *binary*, defined by either *yes* or *no*. The author did not use an ordinal scale to avoid ranking problems in the different scales. Overall, (non-) acceptance of the IC is measured by the relative numbers of respondents. The results should be unambiguous, reliable, and meaningful, as long as the provided definitions of IC lead to no misunderstanding. The author estimates this probability as low but could not exclude it.

Redundancy: Redundancy is desirable but, at the IC level, is not applicable. More challenging is the fact that, at the level of security measures, some measures are not operable on their own. The operation of certain security measures requires a combination with others (*security concept*) such as *K9 sniffer dogs* that are supported and guided by e.g. *police officers* or other *security personnel*. As a result, these combinations affect multiple IC, leading to a higher level of non-acceptance. Additional indicators to evaluate the combinations of such measures would be desirable but were not available. Therefore, the assumed statistical independence of measured IC cannot be guaranteed.

Relevance: The author found the data to be relevant to the issue assessed, and considered the problem of subjective effects of security measures at the customer level, but the results were highly dependent on the current state of security. The acceptance or non-acceptance of interferences caused by security measures is always a balance of the perception of security and the willingness to accept measures with an understandable benefit to security. The MCDA decision tool cannot sufficiently display this mechanism. Therefore, the data represent only a *snapshot of the current situation*, with respondents considering the side effects. This might change after the next terrorist attack as behavioral reactions to terrorist attacks are manifold and can even cause additional, indirect damages (Gigerenzer 2006).

Reliability: Proving reliability was a challenging part of this study. Firstly, the framework of methodologies used in this study is a new approach not tried out by other researchers. Direct comparison of data would be preferable but is not possible. The methodologies used are standard procedures and allow other researchers to replicate the results. Secondly, the data should be stable over time, but that cannot be guaranteed, as social values are influenced by

many factors (Da Palma et al. 2012). This could lead to different results under other circumstances (e.g., time, location, and inspection group). According to the UN/ISDR (2008) definition, this study does not clearly fulfill the standards of reliability; however, this does not imply incorrect results.

Sensitivity: Saltelli et al. (1998) differentiated between stochastic (or aleatory) and subjective (or epistemic) uncertainties in decision-making tools. Sensitivity can be understood as the ability “[...] to reflect small changes in those things that the actions intend to change” (UN/ISDR 2008:7), or as the possibility to face both types of uncertainties. Analysis of the stochastic uncertainty of IC (non-) acceptance is not essential because the high dependency of the data caused extensive fluctuations. The objective of the data was not to achieve an exact description (exact values) for the (non-) acceptance of each IC (in terms of high resolution) because the re-translation to security measures also includes stochastic uncertainty. Furthermore, the data present an indicator of acceptance problems with the interferences of certain security measures (in terms of comparison). High resolution was not required for this study. The subjective (or epistemic) uncertainty (according to Saltelli et al. 1998) is included in the MCDA by the implementation of weighting coefficients by decision-makers. The weighting allows adjustments based on their own preferences and requirements. The possibility of running sensitivity analysis and analyzing at what point weighting changes the current decision to another (see Figure 67) implies the ability to react to changes.

Time-bound: The author considers the data to be a “snapshot” at the time of data acquisition. Subjective values such as IC acceptance are subject to different influences (see Section 2.5). Therefore, the data are limited to the time of indicator measurement and are valid until fluctuations occur in the state of security. These fluctuations might be a terrorist attacks or other events affecting security perception.

Completeness: The selection process of the different interference criteria was completed at the beginning of the study in cooperation with experts of the Kölner Verkehrs-Betriebe AG and was mainly based on the opinions of the security experts and their experience in public transportation systems. Nevertheless, the selection of the IC was, to a certain extent, subjective and influenced by the assumptions of the author. It cannot be ensured that there was no additional interference that was not captured in this analysis.

6.1.2 *Pros and Cons of an Acceptance Indicator Based on Interference Criteria*

Discussions about every kind of indicator are controversial. On one hand, indicators help summarize data and make them useful for decision-makers or policy-makers; on the other hand, the aggregation process is criticized for the arbitrary nature of its weighting (Saltelli et al. 2005). There is still no sight of an “end to the discussion”; therefore, it is even more important to be aware of the assets and drawbacks when using indicators in decision processes. The author noted many pros and cons that should be considered.

Table 23: List of pros and cons of a combined (non-) acceptance indicator for security measures (Source: Birkmann 2013; Fekete 2010; Saisana and Tarantola 2002, adapted by author)

PROS
▪ Summarizes complex or multi-dimensional issues, in view of supporting decision-makers (Saisana and Tarantola 2002) ▪ Easier to interpret than trying to find a trend in many separate indicators (Saisana and Tarantola 2002) ▪ Indicators can be easily visualized (e.g. MCDA) ▪ Possible transfer to SeMe database (objective) ▪ Sensitivity analysis of decision process can be implemented (e.g. MCDA) ▪ Easy documentation of the decision process ▪ Size of a list of indicators can be reduced (Saisana and Tarantola 2002) ▪ Complementary value (subjective effects) to the objective effects of security measures ▪ Easy to interpret and based on available data (Birkmann 2013) ▪ Cost effective—only measures important elements instead of trying to indicate all aspects (Birkmann 2013)

CONS
▪ Possibility of sending a misleading signal (Saisana and Tarantola 2002) ▪ Simplification and generalization (Fekete 2010) ▪ Subjective judgment in construction (Fekete 2010) ▪ Misjudgment of experts in determining the objective effectiveness ▪ Subject to misuse and at the disposal of politics (Fekete 2010) ▪ Increases the quantity of data needed because data are required for all the sub-indicators (IC in this case) (Saisana and Tarantola 2002) ▪ Problems with measurement: absence of data, different methods of statistical compilation, and errors in measurement (Fekete 2010) ▪ Problems with the averaging procedure: composite indices and averaging may conceal divergences, and some variables may cancel out the effect of another variable (Fekete 2010) ▪ Trade-off between simple averaging and weighting (Fekete 2010) ▪ Limited to time, location, observed population, and security situation

It is important to balance the benefits and limitations of criteria/indicators before using them. In combination with an MCDA, it simplifies complex decision processes, shows trends, displays results, and analyzes decision processes using stability (sensitivity) analysis (KIT 2014).

6.2 Comparison to Other Social/Technical Studies

In the different fields of science, many studies deal with social-technical issues in various sectors (see Section 2.6). In the sector of public transportation system, a few studies have investigated the *acceptance of security measures* and set in relation to objective and economic effects of security measures, mostly focusing on a specific measure and not developing a methodology to determine the effects of different security measures (like captured in the security measure database in Section 4.2). In the following section, different studies about the social-technical investigation of security measures are compared to the results of the study.

In the MuViT research project, Apelt and Möllers (2011) determined constant acceptance of video surveillance in Germany between 50% and 90%. They also evaluated European studies and revealed a trend toward increasing acceptance. This study revealed high acceptance (see the red non-acceptance bar in Figure 66). Although, both results have similarities, they are still not comparable because different groups were investigated. For the objective effectiveness criterion, Apelt and Möllers (2011) stated that Closed Circuit Television (CCTV) is

helpful in attacker identification or crime prosecution after an event but questioned a preventive effect, referring to other studies. The same result was revealed by the expert-based methodology using a process model (see Section 5.1.1). The blue bar in Figure 66 represents the experts' evaluation of the preventive effectiveness of video surveillance.

Turley and Stone (2006) executed a study for the Department of Transport of the British Market Research Bureau (BMRB) called 'Public Attitudes toward Transport Security Measures', which investigated body scanners and their public acceptance on the Heathrow Express platforms at Paddington Station in London. In different trials, four to five passengers were chosen randomly to be scanned in a body scanner as well as their baggage in an x-ray machine. The main objective of this study was to find qualitative answers regarding the acceptance or unacceptance of security screening. To accomplish this, 20 interviews were carried out. The results were expressed in qualitative answers about the topics of privacy, selection process, practicalities, role of police, and specific health issues. The author compared the statements with the quantitative results of the acceptance study (see Section 4.5).

Table 24: Comparison of qualitative results and quantitative results from the BMRB acceptance study (Source: Turley and Stone 2006, author)

Turley and Stone (2006) (n=20)	Brauner (n>1,500) acceptance in [%]	
Privacy: “Respondents considered the role of BTP [British Transport Police] officers to be to protect the public by dealing with potentially dangerous situations if they arose, such as if someone was found to be carrying explosives. There were respondents who <u>felt reassured by the police presence</u> at the screening equipment, especially those in the <u>older age groups</u> as it was <u>felt that the officers’ presence acted as a deterrent from terrorist activity</u>. However, there were respondents who felt <u>BTP presence to be intimidating</u>. <u>Young black male respondents</u>, who had experienced what they considered to be humiliating police stop and searches in the past, were especially <u>concerned</u>” (Turley and Stone 2006:48). “<u>Male respondents and also older respondents</u> generally felt that the image posed very <u>little invasion to their privacy</u>. However, <u>female respondents</u>, particularly in the younger age groups, were <u>more likely to voice their concern</u> over the nature of the screened image and queried whether the equipment would be able to scan beneath their underwear” (Turley and Stone 2006:47).	A security guard is present in the train/on the platform	85.1%
	A police officer is present in the train/on the platform	82.1%
	Someone from security speaks to the customer	69.1%
	A police officer speaks to the customer	69.4%
	Customer is searched or physically scanned	17.3%
	Items on the customer's body are made visible	16.2%
	Contours of customer's body are made visible	11.2%
	Additional personal data is collected	7.2%
Selection process: “[...] They were <u>generally suspicious of the concept of random selection</u> described to them by screening staff as they felt that such a process allowed those staffing the equipment to act on their own <u>prejudices when selecting people</u>” (Turley and Stone 2006:47).	Not captured because the random selection process is not intended in actual implementation (loss of security)	-
Health issues: “[...]There were respondents who accepted that the scanning equipment did not use x-rays and as such assumed it was safe and that the equipment would have been tested to ensure its safety prior to the trial” (Turley and Stone 2006:5).	Not captured because author assumed that there is no health interference of body scanners or otherwise no permission	-
Practicalities: “Whilst respondents ideally saw everyone being screened, it was widely felt that, if used by all commuters of a particular train service, the scanner would cause <u>large delays due to the perceived waiting times</u> involved. This was a key concern for both those who were screened and those who were not; <u>delays were generally seen to be frustrating and ultimately unacceptable</u>” (Turley and Stone 2006:47).	The entire stay/time of travel is extended (automatic luggage control and body scanning)	32.5%
	The preparation time is prolonged (automatic luggage control and body scanning)	43.7%
	The amount of luggage is limited (including bicycles)	23.9%

Although, the qualitative answers are not directly comparable to the values of the acceptance study, some similarities and differences can be identified. Firstly, Turley and Stone (2006) received widely varying answers about the presence of police on platforms. From the list of interviewed customers, the number of “young black male respondents” could not clearly been identified so an assessment of this statement is difficult. In this acceptance study, the presence of police or other security personnel was highly accepted.

Privacy of body screening was a major acceptance issue in the study, and a closer look at the IC revealed acceptance values between 7.2% and 17.2%, which can be interpreted as unacceptance. Turley and Stone determined “little invasion to privacy” for male and older respondents, but female respondents were more concerned about screening. This result differs from the acceptance study.

The topic of practicalities was represented in the acceptance study by the travel time, preparation time, and amount of luggage IC. Turley and Stone (2006) investigated their high unacceptance, and the author found similar results for a prolonged travel time (32.5%) and limitations of luggage amounts (23.9%). Prolonged preparation time was accepted by 43.7% and not explicitly captured by Turley and Stone (2006). Overall, the studies are not comparable due to different research approaches (see Table 1), scope, and limitations (e.g., groups of respondents), but both provide discussion about the complexity of acceptance.

To demonstrate another perception of acceptance, Mitchener-Nissen et al. (2011) investigated the acceptance of body scanners in airports, which are closed transportation systems (see Section 2.1). They published additional quantitative acceptance values in an empirical study of the Manchester airport. They questioned 225 passengers about their preference if they had the choice between automatic screening by a backscatter whole body scanner (WBS) or pat-down checks by security personnel. In this direct comparison, 88.0% of the respondents preferred the body scanner, 9.8% the pat-down security check, and 2.2% refused an answer. In a catalog of provided statements, 30.2% said WBS is less intrusive, and 23.6% endorsed the speed of WBS compared to conventional pat-down checks. Reasons such as “provides better security” and “more thorough than a pat-down” were selected by 18.2% and 7.1% of the respondents.

Table 25: Comparison of body scanner acceptance in open and closed (public) transportation systems (Source: Mitchener-Nissen et al. 2011, author)

Mitchener-Nissen et al. (2011) (n=225 divided into %)		Brauner (n>1,500) acceptance in [%]	
<i>Respondents who chose the WBS option:</i>	88.0%	A security guard is present in the train/on the platform	85.1%
- Less intrusive/personal than pat-downs	30.2%	A police officer is present in the train/on the platform	82.1%
- Speed; quicker than a pat-down	23.6%	Someone from security speaks to the customer	69.1%
- Provides better security than a pat-down	18.2%	A police officer speaks to the customer	69.4%
- More thorough than a pat-down	7.1%	Customer is searched or physically scanned	17.3%
- Easy to use	3.6%	Items on the customer's body are made visible	16.2%
- Do not know	0.4%	Contours of customer's body are made visible	11.2%
- Other	4.9%	Additional personal data is collected	7.2%
<i>Respondents who chose the pat-down option:</i>	9.8%	The entire stay/time of travel is extended	32.5%
- Familiarity; it's what I am used to	3.1%	The preparation time is prolonged	43.7%
- Health concerns regarding the scanners	2.7%	The amount of luggage is limited (including bicycles)	23.9%
- Do not like the scanner images	1.8%		
- Whole body scans are too intrusive	0.9%		
- Other	1.3%		
<i>Respondents with no preference for either option:</i>	2.2%		

The recommendations and restrictions³ in aviation services lead to other expectations and acceptances on the customer level (e.g., habituation effects and conscious decision for travel, including advanced security check). Treating acceptance of security measures such as body scanners the same in open and closed transportation systems is a false assumption. Therefore, the author cannot compare the results. Furthermore, Mitchener-Nissen et al. (2011) missed an important point in their study; every technical security measure—this includes body scanners—that raises an alarm has to be checked by personnel, in this case a pat-down control. This procedure is set and not considered in the questionnaire. Therefore, it is not a “this or that” choice; both choices are complementary. Nevertheless, it is important to keep aviation security systems in mind because, in many fields, they have a leading role in future developments in public transportation systems.

Not all research results can be discussed at this point. The discourse in these example studies displays the different approaches and kind of results in the field of security measure acceptance. It shows the difficulties researchers face when comparing acceptance levels captured with various methodologies. Often, a common understanding of “acceptance” is missing so a comparison or validation of research results with those of others is impossible.

6.3 Reflections on Theory/Future Research Needs

“A wonderful fact to reflect upon, that every human creature is constituted to be that profound secret and mystery to every other.”

-Charles Dickens (1812–1870), “A Tale of Two Cities”

Social science research increases the understanding of many mechanisms of socio-technological perception and acceptance, but these studies provide a rather rough understanding of all the background factors that influence people’s evaluation (Renn 1994). This is the challenge today’s scientists face in the discussion to justify composite indicators such as *objective*, *economic*, and *social effect criteria*. Reflecting on this study, a critical issue could not be solved in this study: measurement of acceptance or non-acceptance does not imply *acceptability* and further *certainty*. The different components are psychological and social in nature as Frongillo (1999) claimed in the context of validation of measures of food

³ Regulation EC No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security; also EC No 1138/2004; EC No 622/2003 and EC No 1486/2003; ICAO Aviation Security Manual (Doc 8973 – restricted)

security. Decision-makers must keep this in mind when evaluating the acceptance of interference. It is a model that simplifies a complex system of different influencing and interactive factors and, accordingly, should be understood as such. The results of the acceptance of interference represent more of an indicator of tendencies and rankings than resolute values.

In future, it would be helpful to have common conceptual frameworks that use the same definitions and understanding to make results comparable between social-technical studies. If indicators involving assumptions are used, the results have to be “assessed carefully to avoid resulting in a product of dubious analytic rigour” (OECD 2008:137). Addressing this and working on a common understanding will improve this interdisciplinary research approach. Integrated research considering technical, human, social, and ethical values is increasing but must be supported by all stakeholders (COM 2004). Research programs such as the German Civil Security Research Programme of the BMBF (2012) at the national level or the Horizon 2020 Work Programme—Secure Societies (2014) fund security research, including societal effects, as a mandatory condition for implicitness.

The author recommends continuous funding of social science research in this area and acceptance of results/recommendations in technology-based research disciplines. The author warns of the use of the indicators in policies to judge security measures in general. Therefore, the study is set up in a defined context (see Table 3) with predefined limitations (see Section 3.4). Policies play a major role and should be included in the process of security measure implementation. It is important to understand their role in influencing the security perception of the public through statements and media representation. Regarding tension about terrorist threats, the sensitization of certain issues and handling is important for dealing with perceived insecurity by society and security measure implementation and their side effects (Dunmore 2010, Leven et al. 2010, Spencer 2013). The results of this study can provide operators of critical infrastructure, in this case, public transportation systems, decision support and argumentation for implementation choices by considering customers’ opinions.

Finally, future research should be open-minded regarding new interdisciplinary research approaches that deal with relatively controversial topics such as integration of social-scientific aspects into risk management. The reduction of social complexity to a “black box” indicator is certainly a cause of disagreement for qualitatively oriented social scientists (Fekete 2010:86) but provides new opportunities. Decision-tools combining different criteria such as costs, (objective) effectiveness, and (subjective) acceptance can support integration of ideas and allow investigation into content. Debates on such topics are enriching as long they improve models and results at the professional level and do not lead to de-

motivation. A broad analysis of all influencing factors of social acceptance (according to Section 2.5) of security measures in the context of development trends such as the security perception (e.g. R+V Insurance 2011) helps to understand the mechanisms and is highly desirable.

To increase the security level in a socially accepted manner, a common communication strategy is needed at the levels of research, industry, operator, and policy as well as a management process for continuous evaluation. “A review of technical, economic, and political procedures to make prudent judgments about acceptability is therefore needed” (Renn 1994:90).

In future, the author will focus research more sharply on the customer and consider the point of view of resilience strategies. According to the European Security Research & Innovation Forum (ESRIF), “human beings are at the core of security processes. [...] Certain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and have the ability to recover” (ESRIF 2009:243). The objective of further research should be to analyze the different facets of vulnerability and resilience of critical infrastructure (CI) using the example of public transportation. Based on the character of the CI themselves and their high impacts on society, research can determine how the customers of the CI can be part of a resilience strategy to enhance the efforts of the CI providers and authorities. The results of this doctoral study can be implemented as part of the perception of security and security measures (Brauner 2015).

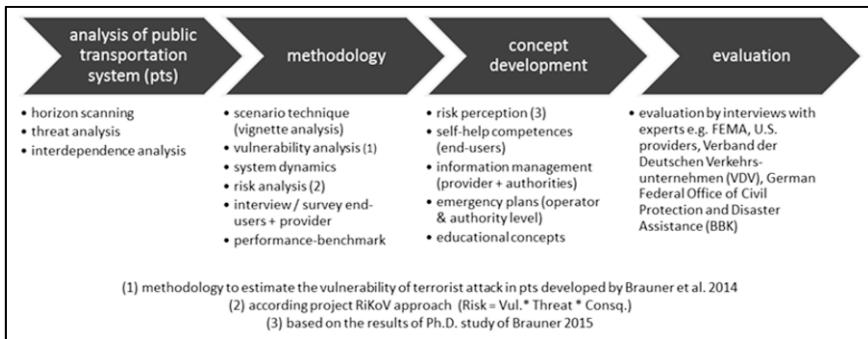


Figure 69: Critical infrastructure resilience (CIR) study (Source: Brauner 2015)

7 Conclusion

“They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety”

Benjamin Franklin (1706-1790).

Today’s world is a complex system of social, technical, and business infrastructures. On one hand, the interdependencies of these structures make this system stable and allow manifold opportunities of development; on the other hand, these intertwined structures cause vulnerabilities in the case of disturbances. The anxiety of our society has increased in recent years (R+V Insurance 2011), causing increased demand for security and safety; as a result, “security” has become a product/service that is ensured by policies, authorities, and providers of infrastructure, among others. A branch of industry grew up quickly to provide security products/services (technical or personnel) to satisfy the security demand. Events with high impacts such as terrorist attacks heighten public discussions about greater security, demanding better and/or more products/service, while providers complain about limited budgets and new costs for the new security standard. Another view, almost hidden, is increasingly getting into the realm of public awareness: Consequently, following the trend of “securitization”, the newly implemented security measures have caused *social interference* and curtailed the *freedom of the individual*. This effect has been neglected by decision-makers so far, but becomes more importance since public news investigate topics such as data acquisition and storage of the U.S. National Security Agency.

In Germany, discrimination regarding personal rights and the right to freedom play a major role, even in security measures intended to have a social benefit. Referring to historical developments, this discussion should involve all stakeholders. Looking closely at the development of, for example, terrorist attacks, the discussion leads to increasing numbers and types of security measures without any regard for backward trends (reduction of measures). This inevitably leads to the implementation of security measures with different levels of acceptance or rejection and neglects customers, who submit to the interferences because they want or need to travel. (Fischer et al. 2014)

The Commission of European Communities encourages all stakeholders of security research to consider human factors and social and ethical values, includ-

ing public perception related to threats and security measures (COM 2004), to achieve a balanced state of security in the socio-technical system. Further, Renn claimed: “The present situation that large-scale-technologies meet public opposition and potential substitutes not vigorously pursued by consumers and policy-makers alike demands a reflection on the normative implications of social science investigations for public preferences and policy evaluation” (Renn 1994:86).

Therefore, the question arises of how the security and safety of an individual as well as society as a community can be ensured while respecting individual freedom and taking privacy seriously. “Privacy protection requires continuous reassessment of criteria” (ESIF 2009:240). To answer this question, criteria that are good indicators must be determined. One possible approach to this question is to involve individuals in the discussion of what kind of drawbacks (interferences) are acceptable.

This research proves that an integrated decision analysis for the implementation of security measures is feasible in public transportation systems. For the first time, a decision framework has been developed, which considers *subjective effects of security measures* (customers’ acceptance of drawbacks/interferences) in risk management processes to break the vicious circle of “securitization” by considering the negative societal effects as well. Using the multi-criteria decision analysis (MCDA) allows consideration of both the socio-economic and socio-technical aspects in the context of a complex system of decision processing and securing critical infrastructure such as public transportation systems. It allows analysis of different scenarios with various security measures in a database and provides decision-makers the possibility to weigh the importance of *objective effects*, *subjective effects*, and *costs of security measures* according to company preferences. The decision process is transparent, can be evaluated according the decision stability and documented in reports with all data. Therefore, this framework of integrated decision analysis is a major contribution to the overall service of public transportation systems toward total quality management, including customer satisfaction (Degenhart and Fiedrich 2004).

Studies such as this are an example of interdisciplinary research combining engineering disciplines with social science disciplines to achieve an application with additional benefits for decision-makers. The conceptual framework fosters the integration of social scientific aspects with technical and economic approaches by taking into account end-user needs right from the beginning. Although the combination of different indicators (i.e., social, economic, and technical) still remains a challenge for research and reflects assumptions and model restrictions, the understanding of complex systems and their integration into decision pro-

cesses will be crucial for future prioritization of security measures in critical infrastructure.

References

- American Heritage Dictionary of the English Language (4th Ed.). (2000).** Houghton Mifflin Company. Accessed at <http://www.thefreedictionary.com/>; 31.05.2012.
- American Public Transit Association. (2004, April).** *Survey of United States Transit System Security Needs and Funding Priorities: Summary of Findings*. Washington D.C.
- Apelt, M. and Möllers, N. (2011).** *Wie intelligente Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung*. Z Außen Sicherheitspolitik, 4, pp. 587-589. Research results of MuViT, BMBF research project about pattern recognition and video tracking (in German: soziologische Perspektiven auf Mustererkennung und Video Tracking), www.bmbf.de/pubRD/Projektumriss_MuViT.pdf
- Barclay, P., Buckley, J., Brantingham, P.J., Brantingham, P.L., and Whinn-Yates, T. (1996).** Preventing auto theft in suburban Vancouver commuter lots: effects of a bike patrol. In Clarke, R.V. (Ed.), *Preventing Mass Transit Crime. Crime Prevention Studies* (Vol. 6). Monsey, NY: Criminal Justice Press.
- Beck, U. (1986).** *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Berlin: Suhrkamp Verlag. p. 43.
- Belyová, L. and Schulze-Bramey, U. (2009).** Der Mensch, das Maß aller Dinge? – sicherheitskulturelle Aspekte auf dem Prüfstand. In: Winzer, P. (Ed.) *Weiterentwicklung des Wuppertaler Generic-Management-Konzeptes. Berichte zum Generic-Management*. Ed. 1/2009. Wuppertal: Bergische Universität Wuppertal. pp. 107–114. ISBN 978-3-8322-7997-4.
- Berliner Morgenpost. (2009, June 24).** Article about Vandalismus. Accessed at <http://www.morgenpost.de/berlin/article1119319/Graffiti-kosten-Bahn-und-BVG-15-4-Millionen-Euro.html>; 31.05.2012
- Bertsch, V. (2008).** *Uncertainty handling in multi-attribute decision support for industrial risk management*. Karlsruhe: Universitätsverlag Karlsruhe. pp. 18.
- Birkmann, J. (2013).** Data, indicators and criteria for measuring vulnerability: theoretical bases and requirements. In: *Measuring vulnerability to natural hazards: Towards disaster resilient societies* (2nd Ed.). Birkmann, J. (Ed.). Tokyo: United Nations University Press. p. 96.
- Booth, W.C, Colomb, G.G., and Williams J.M (2003).** *The Craft of Research* (2nd Ed.). Chicago: University Of Chicago Press. p. 8.
- Brauner, F. (2015).** *CIR - Critical Infrastructure Resilience: Strategies for societal resilience to face the vulnerability of critical infrastructures such as public transportation systems*. Research Proposal, unpublished, Jan. 31, 2015.
- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer T., and Maertens, J. (2013a).** *RiKoV Project Report L1.4 – Security Measures*, TH Köln, Cologne.

- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer T., and Maertens, J. (2014a).** *RiKoV Project Report Process modeling L2.1*, TH Köln, Cologne.
- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer T., and Maertens, J. (2014b).** *RiKoV Project Report L4.2 – Vulnerability Analysis*, TH Köln, Cologne.
- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer T., and Maertens, J. (2014c).** *RiKoV Internal Project Report AP5.2 Method for estimation of security measure effectiveness*, TH Köln, Cologne.
- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer T., and Maertens, J. (2014d).** *RiKoV Internal Project Report, Tabletop Exercise*, TH Köln, Cologne.
- Brauner, F., Baumgarten, C., Bentler, C., Kornmayer, T., Mudimu, O.A., and Lechleuthner, A. (2014e, August 24-28).** *Vulnerability analysis for terrorist attacks on public transportation systems based on process modelling*. Extended abstract published in Ammann, W. J. (Eds.) *Global Risk Forum GRF Davos, 5th International Disaster and Risk Conference - IDRC Davos 2014: Integrative Risk Management*. Davos. pp.48-52.
- Brauner, F., Baumgarten, C., Kornmayer, T., Bentler, C., Mudimu, O.A., and Lechleuthner, A. (2014f, September 16-18).** *A Methodology for a vulnerability analysis of public transportation systems in context of terrorist attacks*. In: Thoma, K., Häring, I., and Leismann, T. (Eds.) *9th Future Security, Security Research Conference* in Berlin. Stuttgart: Fraunhofer Verlag. pp. 271-277.
- Brauner, F., Baumgarten, C., Schmitz, W., Neubecker, K.A., Mudimu, O.A., and Lechleuthner, A. (2013b, November 13).** *RiKoV Risk analysis of terrorist threats to rail-bound public transportation: development of an integrated planning solution for efficient economic and organisational measures*. In: Conference Proceedings of *10th World Congress on Railway Research 2013*. Sydney.
- Brauner, F., Fiedrich, F., Lechleuthner, A., and Mudimu, O.A. (2013d, November 25-28).** *Terror threats in public transportation - A study about customers' perception of security measures*. In: Conference Proceedings of *10th World Congress on Railway Research 2013*. Sydney.
- Brauner, F., Maertens, J., Bracker, H., Mudimu, O.A., and Lechleuthner, A. (2015, May 24-27).** *Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts*. *IS-CRAM 2015 - Information Systems for Crisis Response and Management*. Kristiansand.
- Brosius, F. (2014).** *SPSS 22 für Dummies* (1.Aufl.). Weinheim: Wiley-VCH Verlag. p. 202, 231.
- Bühl, A. (2014).** *SPSS 22 Einführung in die moderne Datenanalyse* (14. Aufl.). Hallbergmoos: Pearson, pp. 153-164, 171, 596, 633-682.
- Bundesministerium des Innern. (2005).** *Rahmenkonzeption Umsetzung der Handlungsempfehlungen zur Aufklärung und Beratung von Betreibern des Öffentlichen Personenverkehrs zur Früherkennung geplanter Anschläge* (Verschlussache).
- Bundesministerium für Bildung und Forschung. (2012).** Programm Forschung für zivile Sicherheit; http://www.bmbf.de/pub/Rahmenprogramm_Sicherheitsforschung_2012.pdf; Accessed at 16.03.2015
- Bundesministerium für Bildung und Forschung. (2013a).** Gesellschaftliche Dimensionen der Forschung: vier Säulen; Accessed at <http://www.bmbf.de/de/12654.php>; 16.03.2015

- Bundesministerium für Bildung und Forschung. (2013b).** Gesellschaftlicher Dialog im Sicherheitsforschungsprogramm; Accessed at <http://www.bmbf.de/en/12655.php>; 16.03.2015
- Burkhard, A., Cohrs, R., Ludewig, K., Malyska, A., Reichel, F., Ross, D., and Weber, U. (2008).** Verband Deutscher Verkehrsunternehmen (VDV). *VDV Mitteilung Nr. 7018, Sicherheitsleitfaden für ÖPNV-Unternehmen – Safety and Security*. Köln: VDV.
- Carnegie, J., Deka, D., and Voorhees, A. M. (2010).** *Customer Perceptions of Transit Security*. New Jersey Department of Transportation Bureau of Research and U.S. Department of Transportation Federal Highway Administration Final Report. pp. 6-15.
- Carnot, S. (1872).** *Réflexions sur la puissance motrice du feu et sur les machines propres à développer cette puissance*. Annales scientifiques de l'École Normale Supérieure 2(1), pp. 393-457.
- CNN. (2013).** Mumbai Attacks. Accessed at <http://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/>; 25.03.2015
- Cömertpay, S., Korkusuz, S., and Alay, H. (2007).** *Motivationstheorie nach Maslow*. München: GRIN Verlag.
- Comes, T., Hiete, M., Wijngaards, N., and Schultmann, F. (2011).** Decision maps: a framework for multi-criteria decision support under severe uncertainty. *J Decision Support Systems*, 52, pp. 108-118.
- Commission communication (COM). (2004).** *Commission communication on the implementation of the preparatory action on the enhancement of the European industrial potential in the field of security research, towards a programme to advance European security through research and technology*. COM/2004/0072. Brussels.
- Cox, L.A. Jr. (2008).** Some Limitations of “Risk = Threat × Vulnerability × Consequence” for Risk Analysis of Terrorist Attacks. *J Risk Analysis*, 28(6), pp. 1749-1761.
- Da Palma, P.J., Lopes, M.P., and Monteiro, A.S. (2012).** The impact of objective and subjective measures of security on subjective well-being: evidence from Portugal. In Webb, D. and Wills-Herrera, E. (Eds.) *Subjective Well-Being and Security*. Heidelberg: Springer, pp. 70-71.
- Daase, C. and Kessler, O. (2007).** Knowns and Unknowns in the War on Terror. Uncertainty and the Political Construction of Danger. *J Security Dialogue*, 38(4), pp. 414-415.
- Degenhart, T. and Fiedrich, S. (2004).** *Die Kundenstimme explizit erfassen – Theorie und Praxis. Durchdachte Modifikation als Grundlage einer individuellen All-In-One-Lösung; Wissensbasierte Unternehmensorganisation – Inhalte, Instrumente, Szenarien*; Aachen: Shaker Verlag. pp. 93-109.
- Denzin, N.K. (1970).** Strategies of multiple triangulation. In: Denzin, N.K. (Ed.) *The Research Act: A Theoretical Introduction to Sociological Methods*. London: Butterworth, pp. 297-313.
- Department of Homeland Security. (2006).** *National Infrastructure Protection Plan 2006*. p. 105.
- Department of Homeland Security. (2009).** *National Infrastructure Protection Plan 2009*. pp. 105, 109, 111.
- Department of Homeland Security. (2013).** What is Critical Infrastructure?. Accessed at <http://www.dhs.gov/what-critical-infrastructure/>; 08.03.2015

- Deutsches Institut für Normung e.V. (DIN). (2014).** *IEC 60300-3-3:2004 Dependability management - Part 3-3: Application guide - Life cycle costing*; German version EN 60300-3-3:2004, Berlin: BEUTH Verlag.
- Dungan, J. L., Gao D., and Pang, A. T. (2002).** *Definitions of Uncertainty*. NASA Ames Research Center, Computer Science Department, University of California Santa Cruz. Accessed at <ftp://ftp.cse.ucsc.edu/pub/reinas/papers/white.pdf>; 18.06.2012
- Dunmore, G. (2010).** Achieving the Right Balance. *Public Transport International Magazine*, Jan/Feb 2010. Accessed at <http://www.uitp.org/publications/public-transport-magazine-details.cfm?lg=en&iddoc=237>; 31.05.2012
- European Security Research & Innovation Forum (ESRIF). (2009, December).** *European Security Research & Innovation Forum Final Report*. p. 243.
- Falkenrath, R.A. (2000, October).** *Analytic models and policy prescription: understanding recent innovation in U.S. counterterrorism*. BCSIA Discussion Paper 2000-31, ESDP Discussion Paper ESDP-2000-03, John F. Kennedy School of Government, Harvard University. p. 28.
- Federal Transit Administration (FTA) - U.S. Department of Transportation. (2003, January).** *The Public Transportation System Security and Emergency Preparedness Planning Guide*. Final Report DOT-FTA-MA-26-5019-03-01/DOT-VNTSC-FTA-03-01. Washington D.C.
- Fekete, A. (2010).** *Assessment of social vulnerability to river floods in Germany*. Graduate Research Series PhD Dissertation, Publication Series of UNU-EHS, Bonn. Vol. 4. p. 20, 78.
- Fischer, S., Klüfers, P., Masala, C., and Wagner, K. (2014).** (Un-)Sicherheitswahrnehmung und Sicherheitsmaßnahmen im internationalen Vergleich. In *Forschungsforum Öffentliche Sicherheit*. Schiller, J., Gerhold, L., Steiger, S., and Jäckel, H. (Eds.) *Schriftenreihe Sicherheit Nr. 14*, p. 36.
- Frongillo, E.A. (1999).** Validation of Measures of Food Insecurity and Hunger. *J Nutrition*, 129(2). pp. 506-509.
- Gallopín, G.C. (1997).** Indicators and Their Use. Information for Decision-making. Part One – Introduction. In: Moldan, B., Billharz, S., and Matravers, R. (Eds.). *Sustainability Indicators. A Report on the Project on Indicators of Sustainable Development*. (Scientific Committee on Problems of the Environment Series-SCOPE Series, Edition 58). Chichester: Wiley, pp. 13–27.
- Gigerenzer, G. (2006).** Out of the frying pan into the fire: behavioral reactions to terrorist attacks. *J Risk Analysis*, 26(2), pp. 347–351. DOI: 10.1111/j.1539-6924.2006.00753.x.
- Guerrero, P. (2002).** *Mass Transit: Challenges in Securing Transit Systems*. Government Accounting Office (GAO), GAO-02-1075T; Washington D.C.
- Hempel, L., Meier, J., Rau, H., Steltner, C., and Vedder, D. (2011).** *Subjektive Sicherheit im Öffentlichen Personenverkehr*: Gemeinsamer Abschlussbericht. pp. 11, 66.
- Hess, J.T. (2011).** *Schutzziele im Umgang mit Naturrisiken in der Schweiz* (Doctoral dissertation). ETH No. 17956. vdf Hochschulverlag AG ETH Zürich. pp. 96-98.
- Hesseling, R. (1995).** Theft from cars: Reduced or displaced? *European Journal on Criminal Policy and Research*, 3(3), pp. 79-92.

- International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). (2009).** *IEC/ISO 31010: Risk management – Risk assessment techniques*. Geneva.
- International Programme on Chemical Safety (IPCS). (2001).** Framework for the Integration of Health and Ecological Risk Assessment Included. In: *Integrated Risk Assessment – Report Prepared for the WHO/UNEP/ILO*. Definitions.
- International Risk Governance Council (IRGC). (2005).** *White Paper on Risk Governance – Towards an integrated approach*. Geneva. p. 150.
- Jonkman, S.N., van Gelder, P.H.A.J.M., and Vrijling, J.K. (2003).** An overview of quantitative risk measures for loss of life and economic damage. *J Hazardous Materials*. A99, pp. 1-30.
- Karlsruhe Institute of Technology (KIT) - Institute for Nuclear and Energy Technologies (IKET). (2014).** Tim Müller, MCDA Multi Criteria Decision Analysis, Software V 4.0 build (4224), (Permission to use software by Dr. Tim Müller).
- Kenney, D.J. (1986).** Crime on the subways: measuring the effectiveness of the Guardian Angels. *J Justice Quarterly*, 3 (4), pp. 481-496.
- Kersten, H. and Klett, G. (2008).** *Der IT Security Manager* (Aufl. 2). Wiesbaden: Vieweg+Teubner Verlag. pp. 101-103. ISBN 978-3-8348-0429-7.
- Kersten, H., Reuter, J., and Schröder, K.-W. (2013).** *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*, Wiesbaden: Springer Verlag, p. 279. ISBN 978-3-658-01723-1.
- Kirkwood, C.W. (1997).** *Strategic decision making: multiobjective decision analysis with spreadsheets*. Belmont: Duxbury Press.
- Köhn, A. and Bornewasser, M. (2012).** *Subjektives Sicherheitsempfinden – Working Paper Nr. 9*. In: Frevel, B. (Ed). *Kooperative Sicherheitspolitik in der Stadt*. Münster. pp 1-8.
- Kölner Verkehrs-Betriebe AG (KVB), Groskopf Rescue Engineering Consulting (2014, April 31).** *Bericht Kundenbefragung zur Akzeptanz von Sicherheitsmaßnahmen*, V1.0, Köln.
- Kölner Verkehrs-Betriebe AG (KVB). (2015).** Ausschnitt Liniennetzplan. Figure 1 & Figure 28 are pictures under copyright, authorized by Wolfgang Brandenburg i+d Verkehrsplanungs- und Design GmbH, Leverkusen. Accessed at <http://www.kvb-koeln.de/german/fahrplan/linienplan.html>; 04.04.2016.
- Krasmann, S., Kreissl, R., Kühne, S., Paul, B., and Schlepper, C. (2014).** *Die gesellschaftliche Konstruktion von Sicherheit - Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung*. In: Schiller, J., Gerhold, L., Steiger, S, and Jäckel, H. (Eds.). *Schriftenreihe Sicherheit Nr. 13*. Berlin: Forschungsforum Öffentliche Sicherheit. p. 91.
- Krell, G. (1980).** Die Entwicklung des Sicherheitsbegriffs. *J Beiträge zur Konfliktforschung*, 10 (3), pp. 33–57.
- Laycock, G. and Austin, C. (1992).** *Crime prevention in parking facilities*. *Security Journal*, 3(3), pp. 154-160.
- Lechleuthner, A., Mudimu, O.A., and Brauner, F. (2012, May 31).** *Vorhabensbeschreibung Projekt RiKoV - Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen öffentlichen Personenverkehrs*. Technische Hochschule Köln. Köln. pp. 3, 21.
- Leven, J., Langenscheid, T., and Gerlach, J. (2010).** Sicherheitskonzepte im ÖPNV. *Der Nahverkehr*. Vol. 4, pp. 14-19.

- Lin, L., Moehle, S., Muenzberg, T., and Raskob, W. (2014, September 16-18).** *A Decision Support Approach: Evaluating The Effectiveness of Security Measures by Scenario-based Multi-Criteria Analysis*. In: Thoma, K.; Häring, I.; Leismann, T. (Eds.), *9th Future Security, Security Research Conference* in Berlin. Stuttgart: Fraunhofer Verlag. pp. 263-270.
- Lucke, D. (1995).** *Akzeptanz. Legitimität in der „Abstimmungsgesellschaft“*. Wiesbaden: Springer Fachmedien Wiesbaden GmbH. <http://dx.doi.org/10.1007/978-3-663-09234-6>.
- Maslow, A. (1942).** The Dynamics of Psychological Security-Insecurity. *J Personality*, 10 (4), pp. 331-344.
- Maslow, A. (1943).** A theory of human motivation. *J Psychological Review*, 50(4), pp. 370-396.
- Meng, S. and Vollbracht, M. (2014).** *Akzeptanz von Sicherheitsmaßnahmen*, Karlsruhe Institute of Technology, RiKoV Report L5.3, pp. 24-26.
- Merriam-Webster's Dictionary. (2014).** Accessed at <http://www.merriam-webster.com/dictionary/acceptance>; 01.02.2015.
- Mitchener-Nissen, T., Bowers, K., and Chetty, K. (2011).** Public attitude to airport security: The case of whole body scanners. *J Security Journal*, 25, pp. 229-243. doi: 10.1057/sj.2011.20.
- Nagenborg, M. (2011, September 11-15).** *Zum Verhältnis von 'Sicherheit' und '(negativer) Freiheit' am Beispiel von Isaiah Berlin's Two Concepts of Liberty (1969). XXII. Deutscher Kongress für Philosophie*, Ludwig-Maximilians-Universität München. p. 3. Accessed at http://epub.ub.uni-muenchen.de/12561/1/Nagenborg2011_Sicherheit_und_negative_Freiheit.pdf; 01.02.2015
- Norris, G.A. (2001).** Integrating Life Cycle Cost Analysis and LCA. *J Life Cycle Assessment*, 6(2), pp. 118-120. doi 10.1007/BF02977849.
- Organisation for Economic Co-Operation and Development (OECD). (2008).** *Handbook on Constructing Composite Indicators: Methodology and User Guide*, p. 137. ISBN 978-92-64-04345-9.
- Pennell, S., Curtis, C., and Henderson, J. (1986).** *Guardian Angels: An Assessment of Citizen Response to Crime*. Washington, DC: National Institute of Justice, U.S. Department of Justice.
- Pennell, S., Curtis, C., Henderson, J., and Tayman, J. (1989).** Guardian Angels: A unique approach to crime prevention. *J Crime and Delinquency*, 35, pp. 378-400.
- Pickl, S., Loechel, A., Neubecker, K.A., and Schmitz, W. (2009).** *An Economic Impact Analysis on Terrorist Attacks against Public Transport Networks*. Network for the Economic Analysis of Terrorism (NEAT). Universität der Bundeswehr München.
- Pickl, S., Raskob, W., Lechleuthner, A., Laible, W., Schmitz, W. et al. (2011).** Common Proposal for joint research project: RiKoV Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen ÖPV: Eine Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen, BMBF Projekt Förderlinie - Sicherheitsökonomie und Sicherheitsarchitektur, München.
- R+V Insurance. (2011).** *Studie–Die Ängste der Deutschen 2011*. Accessed at http://www.ruv.de/de/presse/r_v_infocenter/studien/aengste-der-deutschen.jsp; 31.05.2012
- RAMCAP™ - Risk Analysis and Management for Critical Asset Protection. (2006).** *A Framework*. Washington: ASME Innovative Technologies Institute, LL. pp. 12-54, 61, 67. Accessed at www.asme-iti.org/RAMCAP/RAMCAP_Framework_2.cfm; 01.02.2015

- Renn, O. (1980).** *Wahrnehmung und Akzeptanz technischer Risiken* (Doctoral dissertation). (Band1) University of Cologne, Vol I, pp. 8-10, 43, 61.
- Renn, O. (1994, Nov 18-20).** Public Acceptance of Energy Technologies. In: *European Strategy for Energy Research and Technological Development*. Seminar proceedings, Fondazione Giorgio Cini, Venezia, November 18-20, 1993. Luxemburg: Office for Official Publications of the European Community. ISBN 92-825-9199-9. pp. 77-93.
- Rhode, J. (2012, April 17).** Ergebnisse des Projektes ‘Sicherheit in offenen Verkehrssystemen Eisenbahn’ – SinoVE. Presentation. *BMBF Innovationsforum Zivile Sicherheit Berlin*. Accessed at www.bmbf.de/pub/innovationsforum_zivile_sicherheit_2012.pdf; 01.02.2015
- Saaty, T.L. (1990).** *Multicriteria Decision Making: The Analytic Hierarchy Process. Planning, Priority Setting, Resource Allocation* (2nd Ed.). Pittsburgh: RWS Publishing. ISBN 0-9620317-2-0.
- Saisana, M. and Tarantola, S. (2002).** *State-of-the-art Report on Current Methodologies and Practices for Composite Indicator Development*. EUR 20408 EN. JRC – Joint Research Centre, European Commission, Institute for the Protection and Security of the Citizen Technological and Economic Risk Management. Ispra. pp. 5-6, 8, 9-10.
- Saltelli, A, Nardo, M., Saisana, M., and Tarantola, S. (2005).** Composite Indicators – The Controversy and the Way Forward. In: *Organisation for Economic Co-operation and Development Statistics, Knowledge and Policy Key Indicators to Inform Decision Making*. Paris. pp. 360-361.
- Saltelli, A., Tarantola, S., and Chan, K. (1998).** Presenting results from model based studies to decision-makers: Can sensitivity analysis be a defogging agent? *J Risk Analysis*, 18(6). pp. 799-803. ISSN 0272-4332.
- Schlüter, N., Schulze-Bramey, U., and Winzer, P. (2010).** Sicherheitsbefragungen – Die sozialwissenschaftliche Dimension beim Schutz von Verkehrsinfrastrukturen. In Fähnrich, K. and Franczyk, B. (Eds.). *INFORMATIK 2010*. Bonn: Köllen Druck + Verlag GmbH. pp. 801–806. Accessed at http://www.versiert.info/projektvorstellung/pdf/LNI_GI_FGProQ_Sicherheitsbefragung_v2.pdf; 01.02.2015
- Schneekener, U. (2013).** Bedingt abwehrbereit: Politische und administrative Reaktionsmuster für das Terrorrisiko. In Daase, C.; Engert, S., and Junk, J. (Eds.) *Verunsicherte Gesellschaft - überforderter Staat: Zum Wandel der Sicherheitskultur*. Frankfurt: Campus Verlag. p. 36.
- Schulze-Bramey, U. (2012).** *Methodik zur permanenten Erfassung und Auswertung des individuellen subjektiven Sicherheitsempfinden, dargestellt am Beispiel von Fahrgästen des ÖPNV bei Großveranstaltungen (Doctoral dissertation)*. Bergische Universität Wuppertal. Aachen: Shaker-Verlag. pp. 26-30. ISBN 978-3-8440-1120-3.
- Shields, P.M. and Rangarajan, N. (2013).** *A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management*. Stillwater: New Forums Press. p. 24.
- Simpson, D.M. and Katirai, M. (2006).** *Indicator Issues and Proposed Framework for a Disaster Preparedness Index (DPi)*. Working Paper 06-03, Center for Hazards Research and Policy Development, University of Louisville. pp. 1-8.
- Slovic, P. (2000).** *The Perception of Risk*. Earthscan Risk in Society (Series). London: Routledge. pp. 1, 220-231. ISBN 978-1-8538-3528-5.

- Slovic, P., Lichtenstein, S., and Fischhoff, B. (1984).** Modeling the societal impact of fatal accidents. *J Management Science*, 30(4), pp. 464-474.
- Spencer, A. (2013).** Probleme und Schwierigkeiten bei der Messung objektiver Sicherheit. In Daase, C., Engert, S. and Junk, J. (Eds.) *Verunsicherte Gesellschaft - überforderter Staat: Zum Wandel der Sicherheitskultur*. Frankfurt: Campus Verlag, pp. 64-72.
- Staes, L., Reep, A., Chaudhary, R., Tucci, J., Sapper, D., Borum, R., and Kelly III, A.J. (2006, July).** *Identification of Cost-Effective Methods to Improve Security at Transit Operating/Maintenance Facilities and Passenger Stations*. U.S. Department of Transportation, Federal Transit Administration, FTA-FL-26-71054-03, Washington, D.C. pp. 8-10, 12-13, 85-90.
- Turley, C. and Stone, V. (2006).** *Public Attitudes towards Transport Security Measures*. Report of British Market Research Bureau (BMRB) Social Research. BMRB/CT/45104-644. Department for Transportation. London. pp. 3-5, 7, 13-14.
- Tversky, A. and Kahneman, D. (1974, September 27).** Judgment under Uncertainty: Heuristics and Biases. Biases in Judgments reveal some heuristics of thinking under uncertainty. *J Science*, New Series, 185(4157), pp. 1124-1131.
- Tversky, A. and Kahneman, D. (1992).** Advances in Prospect Theory: Cumulative Representation of Uncertainty. *J Risk and Uncertainty*, 5, pp. 297-323.
- U.S. Coast Guard (USCG) – Department of Homeland Security. (2006).** *Incident Management Handbook. Chapter 25 – Glossary*.
- UITP - International Association of Public Transport. (2010, November).** Position Paper. *Secure Public Transport in a Changeable World*. Accessed at http://www.uitp.org/sites/default/files/cck-focus-papers-files/focus_security_en_OK.pdf; 01.02.2015.
- UITP - International Association of Public Transport. (2012).** *What is public transportation?*. Accessed at <http://www.uitp.org/Public-Transport/why-public-transport/index.cfm>; 31.05.2014.
- UN/ISDR - United Nations Secretariat of the International Strategy for Disaster Reduction. (2008).** *Indicators of Progress. Guidance on Measuring the Reduction of Disaster Risks and the Implementation of the Hyogo Framework for Action*. Genf. p. 7.
- United Nations. (2004).** *Living with Risk – A global review of disaster reduction initiatives* (1+2 Vol.). New York and Geneva: United Nations ISDR.
- Verband Deutscher Ingenieure (VDI). (2005).** *VDI 2884 "Beschaffung, Betrieb und Instandhaltung von Produktionsmitteln unter Anwendung von Life Cycle Costing (LCC)"*. Berlin: Beuth Verlag.
- Verband Deutscher Verkehrsunternehmen e.V. (VDV) (no date).** *Leitfaden für die Durchführung von Kundenzufriedenheitsbefragungen im ÖPNV, Bundesministerium für Verkehr, Bau und Stadtentwicklung*.
- Wagner, D. and Lehnigk, N. (2010).** *Sicherheit im Öffentlichen Personennahverkehr des Landes Brandenburg*. Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) Studie. pp. 11-13, 36.
- Welsh, B.C., Farrington, D.P., and O'Dell, S.J. (2010).** *Effectiveness of Public Area Surveillance for Crime Prevention. Security Guards, Place Managers and Defensible Space*. Swedish Na-

- tional Council for Crime Prevention. Stockholm: Fritzes Kundservice. pp. 22-27. ISBN 978-91-86027-49-0.
- Westland, J. (2006).** *The Project Management Life Cycle*. London/Philadelphia: Kogan Page/Cambridge University Press. p. 84. ISBN 0-7494-4555-6.
- Whiting, P., Rutjes, A.W.S., Reitsma, J.B., Bossuyt, P.M.M., and Kleijnen, J. (2003).** The development of QUADAS: a tool for the quality assessment of studies of diagnostic accuracy included in systematic reviews. *J BMC Medical Research Methodology*, 3(25). doi:10.1186/1471-2288-3-25.
- Wills-Herrera, E., Orozco, L. E., Forero-Pineda, C., Pardo, O., and Andonova, V. (2012).** The Relation Between Perceptions of Insecurity, Social Capital, and Subjective Well-Being: Empirical Evidence from Areas of Rural Conflict in Columbia. In: Webb, D. and Wills-Herrera, E. (Eds.) *Subjective Well-Being and Security*. Heidelberg, London, New York: Springer Dordrecht. pp. 177-181.
- Wilson, J.M., Jackson, B.A., Eisman, M., Steinberg, P., and Riley, K.J. (2007).** *Securing America's Passenger-Rail Systems, Homeland Security*. Pittsburgh: RAND Corporation. ISBN 978-0-8330-4117-3.
- Winzer, P., Schlüter, N., and Schulze-Bramey, U. (2009, August 27-29).** *Indicators for security and safety* in public transportation platforms – a case study. Paper presented at 12th International QMOD and Toulon-Verona Conference on Quality and Service Sciences (ICQSS). Verona.
- Wurtzbacher, J. (2003).** *Sicherheit als gemeinschaftliches Gut*. In: J Leviathan 31(1), DOI: 10.1007/s11578-003-0005-1. pp. 92-116

Annex A—List of Security Measures in Public Transportation System

Measures	Short/ Brief description	Application area	Result	
			Cate-gory	Time
Technical measures				
Video surveillance				
Live mode	Analog or digital surveillance cameras transmit video signals to one or more monitors immediately. Depending on the equipment, operators can vary perspective or zoom. Live mode surveillance is used for active surveillance by security staff.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs, surveillance of technical facilities etc.	passive	P/O
Videotap-ing	See above, combined with storage media used for image evaluation afterwards. Authorities use videotaping for the investigation after accidents, incidents or crimes.	See above.	passive	P
Light intensifier	Using light intensification in the IR spectrum leads to a good visible image even under low-light situations.	See above.	passive	P

IR thermography (IRT)	IRT can determine temperatures via infrared radiation.	IRT enables the detection of persons even in dark environment. Operators use it mainly for the surveillance of technical facilities (e.g. to report overheating or fire).	passive	P
Face recognition	Computer software systems used to identify faces by database matching.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs, surveillance of technical facilities etc.	passive	P
License plate recognition and recording	See above, using the technology to identify license plates.	See above.	passive	P
Behavior recognition	With the help of a computer system the following analysis can be performed: ▪ Left items (ownerless suitcases) ▪ Taken items (car park surveillance, picture alarms) ▪ Facade surveillance of specific items or persons ▪ Movements and directions of groups (crowd management) ▪ Tracking of persons in a two-dimensional space (using one camera) ▪ Loitering ▪ Counting people	Surveillance of public areas such as airports, stations and public transport, sensitive hubs, surveillance of technical facilities etc. The behavior recognition possibility detects predefined conspicuous behavior of people.	passive	P
Detection of explosives or chemical and biological weapons (IR camera)	IR cameras can display non-visible gases.	Detection and surveillance of sensitive areas in specific gases.	passive	O

Voice re- cording + analyzing	Video surveillance combined with voice recording allows gaining a better overview of current events.	Limited radius, stations.	passive	P
...addition al trans- mission to authorities	Authorities directly receive information/videos about surveillance of neuralgic points.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs, surveillance of technical facilities etc.	passive	P/O
Access controls (AC), luggage screening (LS)				
AC manu- al ticket inspection	Before entering train platforms, passengers have to show a valid ticket to staff, which is controlling the validation of the tickets. Persons without a valid ticket may not enter the platforms. It is possible to register the amount of passengers precisely.	Surveillance of passenger flows; counting persons within the system	active	P
AC auto- matically ticket in- spection	It is similar to description above, but a machine validates the ticket.	See above.	passive	P
AC with biometric detection (face recogni- tion, fin- gerprint, iris recog- nition, etc.)	AC with biometric detection compares individual measurable characteristics of persons via detectors with a database. The characteristics are unique, constantly measurable and universal. E.g.: ▪ face recognition, ▪ fingerprint, ▪ iris recognition	Determine the entry admission in control centers, information interfaces and other sensible technical facilities	passive	P
AC with body scanner (terahertz radiation)	Full-body scanners use terahertz radiation to display the body of persons or objects hidden underneath the clothes. Thus, body scanners can display weapons or explosives using different technologies.	People screening at airports, security areas etc.	passive	P
LS manual luggage screening	Before entering security areas, the carry-on luggage is checked on predetermined items or materials. This procedure is executed by staff of an authority or a private security company.	Luggage screening at sensible institutions	passive	P

LS automatic luggage screening	Like the description above. An automatic luggage scanner supports the staff.	See above.	active	P
AC with RFID/credit-card or smartphone identification	Access control to closed areas, e.g. hotels. RFID keys are used in locking systems.	Access control to closed areas	active	P
Detectors				
Identification of smell/odor	Detectors identify and measure specific smells, e.g. drug and other chemical compounds. Thus, detectors can identify specific weapons/explosives.	People screening at airports, security areas etc.	active	P
Increase in sweating	Detectors identify and measure specific smells. Assuming that aggressors are tensed and therefore sweating more than an average person, identification within a crowd possible.	See above.	active	P
Pyrometer/Increase in body temperature	Pyrometers identify persons having temperature, e.g. at the airport: persons suspected of carrying SARS can be detected.	See above.	active	P
Mobile detectors of explosives	Mobile detectors using terahertz- or IR-technology can detect explosives.	See above.	passive	O
Metal detectors	Metal detectors identify metal items acoustically using an artificial magnetic field. Depending on the functionality, a distinction of different metals is possible. There are handsets as well as walk-through metal detectors.	See above.	passive	P
Technical detectors of explosives	Ion mobility spectrometers (IMS) run chemical analyses. First known as “plasma chromatograph” it is characterized by achieving detection limits in the lower ppb range short detection, a short response time and the detection of different chemical substance classes under atmospheric pressure.	Screening of people and general cargo at airports, security areas etc.	passive	P

Explosives (K9)	Different substances e.g. explosives or drugs are often detected by special trained animals (mostly dogs).	See above.	passive	P
Fluid detectors	Detection of fluids in luggage, identifying liquid explosives	See above.	passive	P
Light sensors (differences in brightness)	Light sensors detect People or items crossing light barriers.	Detecting people in unapproved areas.	passive	P
Sound recognition + hook-up	Sensible microphones using noise level measurements alert, if a noise level is over a certain predefined threshold.	See above.	passive	P
Movement sensors	Movement sensors detect changes in thermal radiation. Because of this, detectors can detect movements of objects.	See above.	passive	P
Detection of CBRN (HAM-LeT)	Sensors can detect the presence, the amount and the spreading of chemical, biological, radioactive or nuclear hazards.	Surveillance of buildings, technical facilities	passive	P
Hazard detection systems				
Fire and smoke detectors	Fire and smoke detectors use the measurement of heat or the solids content in the air to detect heat development and smoke. Those detectors can also be battery-operated and therefore be independent of power grid.	Surveillance of buildings, technical facilities	active	O
Intrusion detectors	There are different types of intrusion detectors. Some detect breaks in the circuit, others are motion detectors. After detection, detectors alert acoustically or optically or send a signal to the control center.	See above.	active	P
Flooding warning device	Several sensors alert if there is unintentional threshold in technical facilities.	Surveillance of buildings, technical facilities	active	P

Vehicle equipment (bus/train)				
Emergency brakes	Emergency brakes, used in the passenger compartment, stop the vehicle spontaneously and without intervention of the driver.	Trains, subways, trams	active	P/O
Voice contact with driver/ operator	The voice contact connects the passenger compartment to the cab.	See above.	passive	P/O
Inflammable material	Inflammable materials are used in passenger compartments to reduce the risk of a fire inside the compartment after an accident.	See above.	active	O
GPS location monitoring vehicles	GPS submitters are located in the vehicles. In the case of an emergency (e.g. use of an emergency break, derailment) the control center receives the position automatically.	See above.	passive	P/O
Alarm button, listening device for driver	The alarm button or listening device for driver is connected to the control center	See above.	active	O
Train manipulation systems (ETCS and FFB)	Mechanical and magnetic bans, inductive train protection as well as safety dead man's switch circuits can manipulate the train.	Trains, subways, trams	active	P

Communication equipment				
Systems for transferring the data (e.g. radio, telephone, GSM)	Site monitoring via GPS, use of private mobile radio, data exchange systems, emergency-systems with priority switching.	Trains, subways, trams	passive	P/O
Emergency call stations	Emergency call stations, permanently installed on platforms, connect the accident victim to authorities.	See above.	passive	P/O
Barrier systems against the spread of hazards				
Inflatable barriers for interruption of airflow	If biological, chemical hazards or smoke is released spread, barriers being inflated in rail tunnels can interrupt the airflow.	Rail tunnels	active	O
Self-closing doors	Self-closing doors are connected to fire and smoke detectors.	Constructional fire protection	active	P/O
Fire-resistant cloths, roller shutters	Fire-resistant cloths and roller shutters are basic elements of constructional fire prevention in modern stations.	See above.	active	O
Platform edge doors (PED)	Platform edge doors separate the tracks and platforms with glass facades. The doors open automatically to help people boarding.	Stations	active	P/O
Drones				
Unmanned aerial vehicles (UAV)	Drones supervise track systems or depots. They can detect thieves taking wires, people applying graffiti or terrorists via video surveillance in predefined areas.	Surveillance of buildings, technical facilities	passive	P/O

Constructional measures				
Reduction of alcoves/recesses	If a station is renovated, niches and hard visible areas are changed to be better visible or better exposed.	Stations	active	P
Friendly painting of station	Areas within the station painted in bright or warm colors.	See above.	active	P
Transparency of stations	Within the planning of new stations, planners focus on creating good visibilities and using transparent materials (e.g. glass).	See above.	active	P
Vandalism-resistant materials	Stations are provided with scratch-proof foils on surfaces (e.g. glass) and surface materials, which are easy to clean (paints).	Stations	active	P
Bomb-proof shelters	Solid constructed areas (e.g. made of concrete) can shelter passengers in case of explosions.	See above.	passive	O
Emergency escape routes	Designated entrances and exits combined with emergency escape routes provide an organized evacuation. Normally the routes are well marked, so passengers can see those routes even when filled with smoke or there is no light. The markings are plates combined with persistent paints, or special flooring.	Stations	active	O
Perimeter protection setting				
Protective fences	Protective fences prevent unauthorized people from entering sensible areas or facilities.	Access control to buildings, technical facilities	passive	P
Access restrictions for cars, trucks, and other vehicles	Access restrictions prevent cars, trucks and other vehicles from entering sensible areas or facilities.	See above.	passive	P

Structural fire protection measures				
Ventilation systems	Ventilation systems connected with fire or smoke detectors can exchange a huge volume of air.	Stations, rail tunnels	active	O
Hydrants and supply of fire-extinguishing agents	In some buildings, the authorities predefine a volume of extinguishing agents. Either the type or volume of agents is defined.	See above.	passive	O
Automatic extinguishing systems	Automatic extinguishing systems are connected with fire or smoke detectors. The type of the systems and of the extinguishing agents depend on the type of building or facilities they are installed in.	Stations, shopping facilities	active	O
Emergency lighting	Emergency lightings ensure the possibility to evacuate buildings, even if there are blackouts or smoked areas.	Stations, rail tunnels	active	O
Fire-resistant and fire-retardant materials	Fire-resistant and fire-retardant materials prevent the fast spreading of fire. To separate fire compartments from each other, those materials are used as well.	See above.	active	O
Personnel				
Security service	There are external (service provider) or internal security personnel. Security services exercise the domiciliary right of the owner, the tenant, or the facility.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs,	active	P/O
Inspector/ticket collector	Inspectors and ticket collectors check the validity of tickets. Inspectors in long-distance traffic have several duties. They communicate with drivers and announce anomalies within the service. They also report emergency situations and support rescue services.	See above.	active	P/O

Operation service	Operation services ensure a running transport for passengers and goods. They maintain and shunt trains and wagons (e.g. testing brakes).	See above.	active	P/O
Regular service	Regular service personnel have different duties depending on their operation in long-distance or local traffic. Their duties are informing passengers (also in case of incidents). In case of emergencies service personnel alert rescue teams introduce them in the locations. They are trained in first aid as well coordinate evacuations.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs,	active	P/O
Police officers	Security personnel and police officers patrol together to combine their competencies. Security personnel can only exercise domiciliary whereas police officers can check identities.	See above.	active	P/O
Plain-clothes officers	Plain-clothes offices have the same competencies as police officers. The advantage of using plain-clothes officers is that they operate undercover, as offenders will not recognize them as police officers. Thus, the plain-clothes officer can hardly been bypassed by aggressors.	See above.	active	P/O
Patrol with dog	Dogs have a highly subjective security effect. Depending on the type of dog, patrols with dog are used for protection or detection of explosives, drugs etc.	Surveillance of public areas such as airports, stations and public transport, sensitive hubs.	active	P/O
Security screening of personnel	Security staff screens personnel for previous convictions. This is very important especially if the personnel work in critical sectors, e.g. control centers.	-	active	P/O
Education and training	Educating and training staff ensures effectiveness.	-	passive	P/O
Equipment of personnel	Some equipment supports the personnel fulfill their duties (see communication).	-	passive	P/O

Organizational measures				
Company organizational structure for emergencies	A part of preliminary planning is to predefine competencies and the distribution of goods in a separate organizational structure.	Preliminary planning, management	passive	O
Emergency and evacuation plans	Emergency plans and evacuation concepts for predefined scenarios are instruction for incidents or emergencies. Those plans help to handle critical situations.	See above.	passive	O
Emergency exercises and training	Emergency exercises involving every organization and participant of critical situations have synergetic effects. Within the exercise, the participants get to know each other and learn about the procedures of the other organizations. Furthermore, the participants can test emergency concepts and equipment for their suitability.	See above.	passive	O
Provision of emergency equipment	Emergency equipment (e.g. AED, stretchers) used to rescue people from the track area may be difficult to transport within the station. Therefore it is necessary to provide those materials next to platforms. It may be useful to equip the local fire department with special vehicles as well (e.g. vehicles riding on tracks).	See above.	passive	O
Connection to authorities	Videos of camera surveillance are connected to authorities and are used to plan in advance (e.g. develop operational plans), to exercise together, etc.	See above.	passive	P/O
Public relations work/ sensitization of customers	Media campaigns and recurrent announcements can rise passengers' attention e.g. to watch for ownerless luggage.	Preliminary planning, management	passive	P/O
Control and coordination center	Integration of control and coordination center in incident planning.	See above.	passive	P/O

Construction of travel routes				
Rail track surveillance (energy switches)	Low current flows through tracks. The flow is measured in determined time intervals. If the track is destroyed because of sabotage or an accident, breaks in the circuit can be registered. This helps to telemonitor the integrity of the track bed.	Tracks	passive	P
Possible emergency stops	Emergency stops provide a possibility to stop safely in emergency situations and prevent the spread of fire or contamination.	See above.	passive	O
Roadway monitoring systems (e.g., SKADA)	Roadway monitoring systems are computer-aided systems for the surveillance of other systems.	Rail network	passive	P/O
Other measures				
Measures within the travel operation	If there is an incident within the travel operation, it is necessary to keep up other travel operations in the system. Therefore, exercises involving control centers, diversions and replacement services are important measure in the prevention.	Preliminary planning, management	passive	P/O
IT-Security	Cyber-attacks mostly occur on linked computer systems. Therefore, firewalls, undocking systems from public networks increase the IT security.	IT-control; rail networks, control center	passive	P/O
UWB effector systems	UWB (Ultra-Wide-Band) generate radio-frequency radiation covering a wide frequency spectrum. This damages or inhibits electronic devices, e.g. electric detonators in bags.	Deactivation of suspicious weapons	active	O
Protection against HPM effector systems	HPM radiation can destroy important electric components, which may be important to secure the travel operation. Shielding those electronics is an effective protection against HPM radiation.	Protection of important electric facilities	passive	P

Annex B—Questionnaires of Survey

Source: Kölner Verkehrs-Betriebe AG (KVB), Groskopf Rescue Engineering Consulting (2014, April 31). *Bericht Kundenbefragung zur Akzeptanz von Sicherheitsmaßnahmen*, V1.0, Köln according to the author's specifications and research design.

RIKOV-Fragebogen »Online-Befragung«

Wir führen im Rahmen des Forschungsprojektes RIKOV eine Befragung zur Akzeptanz von Sicherheitsmaßnahmen durch. Hierzu haben wir ein paar Fragen an Sie.

Der folgende Fragebogen ist anonym. Es können keine Rückschlüsse zwischen Ihnen und den Antworten gezogen werden.

Wie beurteilen Sie Ihr derzeitiges Sicherheitsgefühl bei der Nutzung des Schienenverkehrs?

sehr schlecht, schlecht, akzeptabel, gut, sehr gut

Sie werden einer Sicherheitsmaßnahme unterzogen, ihre Mitreisenden dagegen nicht. Akzeptieren Sie dies aufgrund...

eines bestimmten Merkmals z.B. Ihr Aussehen?

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

eines Zufallsprinzips

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

Welche der folgenden Situationen akzeptieren Sie als Sicherheitsmaßnahme (ja/nein)?

- Ihre Fahrkarte wird kontrolliert. ₁
- Ein Sicherheitsmitarbeiter ist in der Bahn/am Bahnsteig anwesend. ₁
- Hunde sind anwesend. ₁
- Ein Polizist ist in der Bahn/am Bahnsteig anwesend. ₁
- Ein Sicherheitsmitarbeiter spricht Sie an. ₁
- Ein Polizist spricht Sie an. ₁

- Ihr Gepäck wird durchsucht. ₂
- Sie werden durchsucht oder abgetastet. ₂
- Gegenstände an Ihrem Körper werden sichtbar gemacht. ₂
- Umrisse Ihres Körpers werden sichtbar gemacht. ₂

- Ihr Gesicht wird erfasst. ₃
- Ihr Name wird erfasst. ₃
- Ihr Gesicht wird gespeichert. ₃
- Ihr Name wird gespeichert. ₃
- Ihr Gesicht wird in Verbindung mit dem Ort gespeichert. ₃
- Ihr Name wird in Verbindung mit dem Ort gespeichert. ₃
- Zusätzliche persönliche Daten werden von Ihnen erfasst. ₃
- Ein Bewegungsprofil wird von Ihnen erstellt. ₃

Akzeptieren Sie die folgenden möglichen Auswirkungen von Sicherheitsmaßnahmen?

- Die Sauberkeit in den Bahnen/in der Haltestelle wird verschlechtert. ₄
- Eine Geruchsbelästigung wird erzeugt. ₄
- Eine Lärmbelästigung entsteht. ₄
- Die Lichtverhältnisse werden verschlechtert? ₄
- Die Helligkeit wird erhöht? ₄
- Wird die Anzahl der Sitzplatzmöglichkeiten durch die Maßnahme begrenzt. ₄
- Wird die Bequemlichkeit der Sitzplätze durch die Maßnahmen beschränkt. ₄
- Wird die Umgebungstemperatur durch die Sicherheitsmaßnahme erhöht. ₄
- Wird die Umgebungstemperatur durch die Sicherheitsmaßnahme verringert. ₄

- Die Nutzung des Systems ist nicht barrierefrei. ₅
- Die Mitnahme von Gepäck (auch Fahrrad) wird beschränkt. ₅
- Sie müssen sich vor der Fahrt registrieren und den Fahrweg angeben. ₅
- Es wird schwieriger in eine andere Bahn umzusteigen. ₅
- Die Betriebszeiten der Bahnen werden verkürzt. ₅
- Die Taktung der Bahnen wird vergrößert. ₅

- Die gesamte Aufenthaltsdauer wird verlängert. ₆
- Die Vorbereitungszeit wird verlängert. ₆
- Wartezeiten werden verlängert. ₆
- Die Umsteigedauer wird verlängert. ₆

In welchem Maß dürfen Sicherheitsmaßnahmen den Fahrpreis pro Fahrt steigen lassen?

kleiner 0,50 €, zwischen 0,50 € und 1,50 €, größer 1,50 €

Akzeptieren Sie eine aufwandsbezogene Erhebung einer Sicherheitsgebühr (z.B. für Koffer)?

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

Beeinflusst Sie die Sichtbarkeit einer Sicherheitsmaßnahme in Ihrem Sicherheitsgefühl?

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

Fühlen Sie sich ausreichend über Sicherheitsmaßnahmen informiert/aufgeklärt?

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

Verändert sich Ihre Akzeptanz, wenn Sie Wirkung, Mechanismus oder Erfolge einer Sicherheitsmaßnahme kennen?

ja, nein

Haben Sie Wünsche an Sicherheitsmaßnahmen?**Freitext**

Eine Sicherheitsmaßnahme deckt konsequent z.B. das Schwarzfahren, das Rauchen am Bahnsteig oder den Alkoholgenuss in der Bahn auf. Würden Sie eine solche Sicherheitsmaßnahme dann akzeptieren?

trifft nicht zu, trifft kaum zu, trifft zu, trifft stark zu, trifft sehr stark zu

Was möchten Sie uns gerne im Rahmen dieser Umfrage noch mitteilen?**Freitext*****Statistische Angaben******Ihr Geschlecht***

weiblich, männlich

Ihr Alter

bis 20 Jahre, 20-60 Jahre, über 60 Jahre

Wie häufig nutzen Sie den Schienenverkehr in der Woche?

nie, 1x-2x, 2x-5x, 6x-8x, über 8x

Haben Sie die Möglichkeit ein alternatives Verkehrsmittel zu nutzen?

ja, nein

Wie häufig nutzen Sie das alternative Verkehrsmittel im Vergleich zum ÖPV?

sehr selten, selten, ausgeglichen, oft, sehr oft

RIKOV-Fragebogen »Feldbefragung«

Auswahl 1

Wir führen im Rahmen des Forschungsprojektes RIKOV eine Befragung zur Akzeptanz von Sicherheitsmaßnahmen durch. Hierzu haben wir ein paar Fragen an Sie. Der folgende Fragebogen ist anonym. Es können keine Rückschlüsse zwischen Ihnen und den Antworten gezogen werden.

Wie beurteilen Sie Ihr derzeitiges Sicherheitsgefühl bei der Nutzung des Schienenverkehrs?

(v_1)

sehr schlecht ☐ (1) schlecht ☐ (2) akzeptabel ☐ (3) gut ☐ (4) sehr gut ☐ (5)

Sie werden einer Sicherheitsmaßnahme unterzogen, Ihre Mitreisenden dagegen nicht. Akzeptieren Sie dies aufgrund... eines bestimmten Merkmals z.B. Ihr Aussehen?

(v_2)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

eines Zufallsprinzips

(v_3)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Welche der folgenden Situationen akzeptieren Sie als Sicherheitsmaßnahme?

Auswahl 1 (Persönlichkeitsrechte):

- | | | | |
|---|---------------------------------|-----------------------------------|--------|
| ▪ Ein Sicherheitsmitarbeiter ist in der Bahn/am Bahnsteig anwesend. | Ja ☐ (1) | Nein ☐ (0) | (v_19) |
| ▪ Hunde sind anwesend. | Ja ☐ (1) | Nein ☐ (0) | (v_20) |
| ▪ Ein Sicherheitsmitarbeiter spricht Sie an. | Ja ☐ (1) | Nein ☐ (0) | (v_22) |
| ▪ Ein Polizist ist in der Bahn/am Bahnsteig anwesend. | Ja ☐ (1) | Nein ☐ (0) | (v_21) |
| ▪ Ein Polizist spricht Sie an. | Ja ☐ (1) | Nein ☐ (0) | (v_23) |
| ▪ Ihre Fahrkarte wird kontrolliert. | Ja ☐ (1) | Nein ☐ (0) | (v_18) |

Akzeptieren Sie die folgenden möglichen Auswirkungen von Sicherheitsmaßnahmen?

Auswahl 1 (Kornfort):

- | | | | |
|--|---------------------------------|-----------------------------------|--------|
| ▪ Die Sauberkeit in den Bahnen/in der Haltestelle wird verschlechtert. | Ja ☐ (1) | Nein ☐ (0) | (v_44) |
| ▪ Eine Geruchsbelästigung wird erzeugt. | Ja ☐ (1) | Nein ☐ (0) | (v_45) |
| ▪ Eine Lärmbelästigung entsteht. | Ja ☐ (1) | Nein ☐ (0) | (v_46) |
| ▪ Die Lichtverhältnisse werden verschlechtert | Ja ☐ (1) | Nein ☐ (0) | (v_47) |
| ▪ Die Helligkeit wird erhöht. | Ja ☐ (1) | Nein ☐ (0) | (v_48) |
| ▪ Die Anzahl der Sitzplatzmöglichkeiten durch die Maßnahme begrenzt. | Ja ☐ (1) | Nein ☐ (0) | (v_49) |
| ▪ Die Bequemlichkeit der Sitzplatzmöglichkeiten durch die Maßnahme begrenzt. | Ja ☐ (1) | Nein ☐ (0) | (v_50) |
| ▪ Die Umgebungstemperatur durch die Sicherheitsmaßnahme erhöht. | Ja ☐ (1) | Nein ☐ (0) | (v_51) |
| ▪ Die Umgebungstemperatur durch die Sicherheitsmaßnahme verringert. | Ja ☐ (1) | Nein ☐ (0) | (v_52) |

In welchem Maße dürfen Sicherheitsmaßnahmen den Fahrpreis pro Fahrt steigen lassen?

(v_66)

gar nicht ☐ (1) kleiner 0,50 € ☐ (2) zwischen 0,50 € und 1,50 € ☐ (3) größer 1,50 € ☐ (4)

Akzeptieren Sie eine aufwandsbezogene Erhebung einer Sicherheitsgebühr (z.B. für Koffer)?

(v_67)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Beeinflusst Sie die Sichtbarkeit einer Sicherheitsmaßnahme in Ihrem Sicherheitsgefühl?

(v_77)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Fühlen Sie sich ausreichend über Sicherheitsmaßnahmen informiert/aufgeklärt?

(v_83)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Verändert sich Ihre Akzeptanz, wenn Sie Wirkung, Mechanismus oder Erfolge einer Sicherheitsmaßnahme kennen? (v_84)
 Ja ☐ [1] Nein ☐ [2]

Haben Sie Wünsche an Sicherheitsmaßnahmen? (v_85)

Eine Sicherheitsmaßnahme deckt konsequent z.B. das Schwarzfahren, das Rauchen am Bahnsteig oder den Alkoholgenuss in der Bahn auf. Würden Sie eine solche Sicherheitsmaßnahme dann akzeptieren? (v_91)
 trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Was möchten Sie uns gerne im Rahmen dieser Umfrage noch mitteilen? (v_92)

Statistische Angaben

Zur wissenschaftlichen Verwertbarkeit benötigen wir noch ein paar anonyme statistische Angaben.

Befragungsort (v_101)	Ihr Geschlecht (v_93)	Ihr Alter (v_94)
Rathaus/Heumarkt ☐ (1)	weiblich ☐ (1)	bis 20 Jahre ☐ (1)
Plusstraße ☐ (2)	männlich ☐ (2)	20-60 Jahre ☐ (2)
Appellhofplatz ☐ (3)		über 60 Jahre ☐ (3)

Zeit (v_102)	Lichtverhältnisse (v_103)	Geräuschkulisse (v_104)
Mo-Fr 06:00-10:00 Uhr ☐ (1)	dunkel ☐ (1)	leise ☐ (1)
Mo-Fr 14:00-18:00 Uhr ☐ (2)	normal ☐ (2)	normal ☐ (2)
Mo-Do 20:00-02:00 Uhr ☐ (3)	hell ☐ (3)	laut ☐ (3)
Fr-Sa 00:00-04:00 Uhr ☐ (4)		
Sa 14:00-18:00 Uhr ☐ (5)		
So 14:00-18:00 Uhr ☐ (6)		

Wie häufig nutzen Sie den Schienenverkehr in der Woche? (v_95)
 nie ☐ (1) 1-2 mal ☐ (2) 2-5 mal ☐ (3) 6-8 mal ☐ (4) über 8 mal ☐ (5)

Haben Sie die Möglichkeit ein alternatives Verkehrsmittel zu nutzen? (v_96)
 Ja ☐ [1] Nein ☐ [2]

Wie häufig nutzen Sie das alternative Verkehrsmittel im Vergleich zum ÖPV? (v_97)
 sehr selten ☐ (1) selten ☐ (2) ausgeglichen ☐ (3) oft ☐ (4) sehr oft ☐ (5)

Besonderheiten zu Befragungszeitpunkt, -ort, aktuelle Umgebungseinflüsse (v_105)

RIKOV-Fragebogen »Feldbefragung«

Auswahl 2

Wir führen im Rahmen des Forschungsprojektes RIKOV eine Befragung zur Akzeptanz von Sicherheitsmaßnahmen durch. Hierzu haben wir ein paar Fragen an Sie. Der folgende Fragebogen ist anonym. Es können keine Rückschlüsse zwischen Ihnen und den Antworten gezogen werden.

Wie beurteilen Sie Ihr derzeitiges Sicherheitsgefühl bei der Nutzung des Schienenverkehrs?

(v_1)

sehr schlecht ☐ (1) schlecht ☐ (2) akzeptabel ☐ (3) gut ☐ (4) sehr gut ☐ (5)

Sie werden einer Sicherheitsmaßnahme unterzogen, Ihre Mitreisenden dagegen nicht. Akzeptieren Sie dies aufgrund...

eines bestimmten Merkmals z.B. Ihr Aussehen?

(v_2)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

eines Zufallsprinzips

(v_3)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Welche der folgenden Situationen akzeptieren Sie als Sicherheitsmaßnahme?

Auswahl 2 (Körperliche Integrität):

- | | | | |
|--|---------------------------------|-----------------------------------|--------|
| ▪ Ihr Gepäck wird durchsucht. | Ja ☐ (1) | Nein ☐ (0) | (v_24) |
| ▪ Sie werden durchsucht oder abgetastet. | Ja ☐ (1) | Nein ☐ (0) | (v_25) |
| ▪ Gegenstände an Ihrem Körper werden sichtbar gemacht. | Ja ☐ (1) | Nein ☐ (0) | (v_26) |
| ▪ Umrisse Ihres Körpers werden sichtbar gemacht. | Ja ☐ (1) | Nein ☐ (0) | (v_27) |

Akzeptieren Sie die folgenden möglichen Auswirkungen von Sicherheitsmaßnahmen?

Auswahl 2 (Flexibilität):

- | | | | |
|---|---------------------------------|-----------------------------------|--------|
| ▪ Die Nutzung des Systems ist nicht barrierefrei. | Ja ☐ (1) | Nein ☐ (0) | (v_53) |
| ▪ Die Mitnahme von Gepäck (auch Fahrrad) wird beschränkt. | Ja ☐ (1) | Nein ☐ (0) | (v_54) |
| ▪ Sie müssen sich vor der Fahrt registrieren und den Fahrweg angeben. | Ja ☐ (1) | Nein ☐ (0) | (v_55) |
| ▪ Es wird schwieriger in eine andere Bahn umzusteigen. | Ja ☐ (1) | Nein ☐ (0) | (v_56) |
| ▪ Die Betriebszeiten der Bahnen werden verkürzt. | Ja ☐ (1) | Nein ☐ (0) | (v_57) |
| ▪ Die Taktung der Bahnen wird vergrößert. | Ja ☐ (1) | Nein ☐ (0) | (v_58) |

In welchem Maße dürfen Sicherheitsmaßnahmen den Fahrpreis pro Fahrt steigen lassen?

(v_66)

gar nicht ☐ (1) kleiner 0,50 € ☐ (2) zwischen 0,50 € und 1,50 € ☐ (3) größer 1,50 € ☐ (4)

Akzeptieren Sie eine aufwandsbezogene Erhebung einer Sicherheitsgebühr (z.B. für Koffer)?

(v_67)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Beeinflusst Sie die Sichtbarkeit einer Sicherheitsmaßnahme in Ihrem Sicherheitsgefühl?

(v_77)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Fühlen Sie sich ausreichend über Sicherheitsmaßnahmen informiert/aufgeklärt?

(v_83)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Verändert sich Ihre Akzeptanz, wenn Sie Wirkung, Mechanismus oder Erfolge einer Sicherheitsmaßnahme kennen?

(v_84)

Ja ☐ (1) Nein ☐ (2)

Haben Sie Wünsche an Sicherheitsmaßnahmen?

(v_85)

Eine Sicherheitsmaßnahme deckt konsequent z.B. das Schwarzfahren, das Rauchen am Bahnsteig oder den Alkoholgenuss in der Bahn auf. Würden Sie eine solche Sicherheitsmaßnahme dann akzeptieren?

(v_91)

trifft nicht zu ☐ (1)

trifft kaum zu ☐ (2)

trifft zu ☐ (3)

trifft stark zu ☐ (4)

trifft sehr stark zu ☐ (5)

Was möchten Sie uns gerne im Rahmen dieser Umfrage noch mitteilen?

(v_92)

Statistische Angaben

Zur wissenschaftlichen Verwertbarkeit benötigen wir noch ein paar anonyme statistische Angaben.

Befragungsort

(v_101)

Rathaus/Heumarkt ☐ (1)

Piusstraße ☐ (2)

Appellhofplatz ☐ (3)

Ihr Geschlecht

(v_93)

weiblich ☐ (1)

männlich ☐ (2)

Ihr Alter

(v_94)

bis 20 Jahre ☐ (1)

20-60 Jahre ☐ (2)

über 60 Jahre ☐ (3)

Zeit

(v_102)

Mo-Fr 06:00-10:00 Uhr ☐ (1)

Mo-Fr 14:00-18:00 Uhr ☐ (2)

Mo-Do 20:00-02:00 Uhr ☐ (3)

Fr-Sa 00:00-04:00 Uhr ☐ (4)

Sa 14:00-18:00 Uhr ☐ (5)

So 14:00-18:00 Uhr ☐ (6)

Lichtverhältnisse

(v_103)

dunkel ☐ (1)

normal ☐ (2)

hell ☐ (3)

Geräuschkulis

(v_104)

leise ☐ (1)

normal ☐ (2)

laut ☐ (3)

Wie häufig nutzen Sie den Schienenverkehr in der Woche?

(v_95)

nie ☐ (1)

1-2 mal ☐ (2)

2-5 mal ☐ (3)

6-8 mal ☐ (4)

über 8 mal ☐ (5)

Haben Sie die Möglichkeit ein alternatives Verkehrsmittel zu nutzen?

(v_96)

Ja ☐ [1]

Nein ☐ [2]

Wie häufig nutzen Sie das alternative Verkehrsmittel im Vergleich zum ÖPV?

(v_97)

sehr selten ☐ (1)

selten ☐ (2)

ausgeglichen ☐ (3)

oft ☐ (4)

sehr oft ☐ (5)

Besonderheiten zu Befragungszeitpunkt, -ort, aktuelle Umgebungseinflüsse

(v_105)

RIKOV-Fragebogen »Feldbefragung«

Auswahl 3

Wir führen im Rahmen des Forschungsprojektes RIKOV eine Befragung zur Akzeptanz von Sicherheitsmaßnahmen durch. Hierzu haben wir ein paar Fragen an Sie. Der folgende Fragebogen ist anonym. Es können keine Rückschlüsse zwischen Ihnen und den Antworten gezogen werden.

Wie beurteilen Sie Ihr derzeitiges Sicherheitsgefühl bei der Nutzung des Schienenverkehrs?

(v_1)

sehr schlecht ☐ (1) schlecht ☐ (2) akzeptabel ☐ (3) gut ☐ (4) sehr gut ☐ (5)

Sie werden einer Sicherheitsmaßnahme unterzogen, Ihre Mitreisenden dagegen nicht. Akzeptieren Sie dies aufgrund... eines bestimmten Merkmals z.B. Ihr Aussehen?

(v_2)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

eines Zufallsprinzips

(v_3)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Welche der folgenden Situationen akzeptieren Sie als Sicherheitsmaßnahme?

Auswahl 3 (Anonymität):

- | | | | |
|---|---------------------------------|-----------------------------------|--------|
| ▪ Ihr Gesicht wird erfasst. | Ja ☐ [1] | Nein ☐ [0] | (v_28) |
| ▪ Ihr Name wird erfasst. | Ja ☐ [1] | Nein ☐ [0] | (v_29) |
| ▪ Ihr Gesicht wird gespeichert. | Ja ☐ [1] | Nein ☐ [0] | (v_30) |
| ▪ Ihr Name wird gespeichert. | Ja ☐ [1] | Nein ☐ [0] | (v_31) |
| ▪ Ihr Gesicht wird in Verbindung mit dem Ort gespeichert. | Ja ☐ [1] | Nein ☐ [0] | (v_32) |
| ▪ Ihr Name wird in Verbindung mit dem Ort gespeichert. | Ja ☐ [1] | Nein ☐ [0] | (v_33) |
| ▪ Zusätzliche persönliche Daten werden von Ihnen erfasst. | Ja ☐ [1] | Nein ☐ [0] | (v_34) |
| ▪ Ein Bewegungsprofil wird von Ihnen erstellt. | Ja ☐ [1] | Nein ☐ [0] | (v_35) |

Akzeptieren Sie die folgenden möglichen Auswirkungen von Sicherheitsmaßnahmen?

Auswahl 3 (Wartezeit):

- | | | | |
|---|---------------------------------|-----------------------------------|--------|
| ▪ Die gesamte Aufenthaltsdauer wird verlängert. | Ja ☐ [1] | Nein ☐ [0] | (v_59) |
| ▪ Die Vorbereitungszeit wird verlängert. | Ja ☐ [1] | Nein ☐ [0] | (v_60) |
| ▪ Wartezeiten werden verlängert. | Ja ☐ [1] | Nein ☐ [0] | (v_61) |
| ▪ Die Umsteigedauer wird verlängert. | Ja ☐ [1] | Nein ☐ [0] | (v_62) |

In welchem Maße dürfen Sicherheitsmaßnahmen den Fahrpreis pro Fahrt steigen lassen?

(v_66)

gar nicht ☐ (1) kleiner 0,50 € ☐ (2) zwischen 0,50 € und 1,50 € ☐ (3) größer 1,50 € ☐ (4)

Akzeptieren Sie eine aufwandsbezogene Erhebung einer Sicherheitsgebühr (z.B. für Koffer)?

(v_67)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Beeinflusst Sie die Sichtbarkeit einer Sicherheitsmaßnahme in Ihrem Sicherheitsgefühl?

(v_77)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Fühlen Sie sich ausreichend über Sicherheitsmaßnahmen informiert/aufgeklärt?

(v_83)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Verändert sich Ihre Akzeptanz, wenn Sie Wirkung, Mechanismus oder Erfolge einer Sicherheitsmaßnahme kennen?

(v_84)

Ja ☐ [1] Nein ☐ [2]

Haben Sie Wünsche an Sicherheitsmaßnahmen?

(v_85)

Eine Sicherheitsmaßnahme deckt konsequent z.B. das Schwarzfahren, das Rauchen am Bahnsteig oder den Alkoholgenuss in der Bahn auf. Würden Sie eine solche Sicherheitsmaßnahme dann akzeptieren?

(v_91)

trifft nicht zu ☐ (1) trifft kaum zu ☐ (2) trifft zu ☐ (3) trifft stark zu ☐ (4) trifft sehr stark zu ☐ (5)

Was möchten Sie uns gerne im Rahmen dieser Umfrage noch mitteilen?

(v_92)

Statistische Angaben

Zur wissenschaftlichen Verwertbarkeit benötigen wir noch ein paar anonyme statistische Angaben.

Befragungsort	(v_101)	Ihr Geschlecht	(v_93)	Ihr Alter	(v_94)
Rathaus-/Heumarkt	☐ (1)	weiblich	☐ (1)	bis 20 Jahre	☐ (1)
Piusstraße	☐ (2)	männlich	☐ (2)	20-60 Jahre	☐ (2)
Appellhofplatz	☐ (3)			über 60 Jahre	☐ (3)
Zeit	(v_102)	Lichtverhältnisse	(v_103)	Geräuschkulisse	(v_104)
Mo-Fr 06:00-10:00 Uhr	☐ (1)	dunkel	☐ (1)	leise	☐ (1)
Mo-Fr 14:00-18:00 Uhr	☐ (2)	normal	☐ (2)	normal	☐ (2)
Mo-Do 20:00-02:00 Uhr	☐ (3)	hell	☐ (3)	laut	☐ (3)
Fr-Sa 00:00-04:00 Uhr	☐ (4)				
Sa 14:00-18:00 Uhr	☐ (5)				
So 14:00-18:00 Uhr	☐ (6)				

Wie häufig nutzen Sie den Schienenverkehr in der Woche?

(v_95)

nie ☐ (1) 1-2 mal ☐ (2) 2-5 mal ☐ (3) 6-8 mal ☐ (4) über 8 mal ☐ (5)

Haben Sie die Möglichkeit ein alternatives Verkehrsmittel zu nutzen?

(v_96)

Ja ☐ (1) Nein ☐ (2)

Wie häufig nutzen Sie das alternative Verkehrsmittel im Vergleich zum ÖPV?

(v_97)

sehr selten ☐ (1) selten ☐ (2) ausgeglichen ☐ (3) oft ☐ (4) sehr oft ☐ (5)

Besonderheiten zu Befragungszeitpunkt, -ort, aktuelle Umgebungseinflüsse

(v_105)

Annex C—Process Modeling—Results Expert Workshop

Source: Brauner et al. (2014d) RiKoV Internal Project Report, TH Köln, Tabletop Exercise, Cologne.

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienengebunden ÖPV-System		
Video - mit Aufzeichnungen	Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	0	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	niedrig	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwort-möglichkeiten:	Informationen finden Sie hier:
Sicherheitsmaßnahme wirkt an keiner Stelle im Prozessmodell!		
Präventive Wirkung der Sicherheitsmaßnahme:	0	
	Keine Wirkung	
Exakter Wert	0	

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienenengebunden ÖPV-System

Video - mit Erkennung von Verhalten	Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	1	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	niedrig	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwort- möglichkeiten:	Informationen finden Sie hier:
Kann die Sicherheitsmaßnahmen vom Täter aktiv umgangen werden?	Nein	Datentabelle Sicherheits- maßnahmen
Sind alle Voraussetzungen für die Sicherheitsmaßnahmen erfüllt?	Ja	
Sind alle notwendigen Maßnahmen in dem Maßnahmenbündel vorhanden?	Ja	
Präventive Wirkung der Sicherheitsmaßnahme:	1	
	Sehr geringe Wirkung	
Exakter Wert	0,05	

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienengebunden ÖPV-System

<i>Zugang - mit manueller Ticketkontrolle</i>	<i>Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän</i>	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	0	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	mittel	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwort-möglichkeiten:	Informationen finden Sie hier:
Sicherheitsmaßnahme wirkt an keiner Stelle im Prozessmodell!		
Präventive Wirkung der Sicherheitsmaßnahme:	0	
	Keine Wirkung	
Exakter Wert	0	

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienengebunden ÖPV-System

<i>Detektor - mobile Sprengstoffdetektoren</i>	<i>Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän</i>	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	1	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	niedrig	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwort- möglichkeiten:	Informationen finden Sie hier:
Kann die Sicherheitsmaßnahmen vom Täter aktiv umgangen werden?	Ja	Datentabelle Sicherheits- maßnahmen
Sind alle Voraussetzungen für die Sicherheitsmaßnahmen erfüllt?	Ja	
Sind alle notwendigen Maßnahmen in dem Maßnahmenbündel vorhanden?	Ja	
Präventive Wirkung der Sicherheitsmaßnahme:	1	
	Sehr geringe Wirkung	
Exakter Wert	0,025	

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienenengebunden ÖPV-System

Personal - Servicepersonal	Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	1	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	niedrig	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwort- möglichkeiten:	Informationen finden Sie hier:
Kann die Sicherheitsmaßnahmen vom Täter aktiv umgangen werden?	Ja	Datentabelle Sicherheits- maßnahmen
Sind alle Voraussetzungen für die Sicherheitsmaßnahmen erfüllt?	Ja	
Sind alle notwendigen Maßnahmen in dem Maßnahmenbündel vorhanden?	Ja	
Präventive Wirkung der Sicherheitsmaßnahme:	1	
	Sehr geringe Wirkung	
Exakter Wert	0.025	

Bestimmung der Wirkung einer Sicherheitsmaßnahmen bezogen auf ein Szenario (inkl. Zielobjekt) im schienengebunden ÖPV-System

<i>Personal - Streife mit Hunden</i>	<i>Einzeltäter - Bombe - Bahnhof Bahnsteig subterrän</i>	
Ermittlung der präventiven Wirkung der Sicherheitsmaßnahme		
An wie vielen Stellen im Prozessmodell kann die Sicherheitsmaßnahme wirken?	2	Prozessmodell AP 2.1 FHK
Wie viele Stellen existieren in dem Prozesspfad dieser Vignette?	8	
Wie groß würden Sie die Wirkung dieser Sicherheitsmaßnahme grob abschätzen?	mittel	Interner Bericht FHK zum AP 5.2
Entscheidungsfragen:	Antwortmöglichkeiten:	Informationen finden Sie hier:
Kann die Sicherheitsmaßnahmen vom Täter aktiv umgangen werden?	Ja	Datentabelle Sicherheitsmaßnahmen
Sind alle Voraussetzungen für die Sicherheitsmaßnahmen erfüllt?	Ja	
Sind alle notwendigen Maßnahmen in dem Maßnahmenbündel vorhanden?	Ja	
Präventive Wirkung der Sicherheitsmaßnahme:	2	
	Geringe Wirkung	
Exakter Wert	0.15	

Annex D—Data Sheet and Report MCDA Software

Source: Author, MCDA - Multi Criteria Decision Analysis Software developed by Karlsruhe Institute of Technology (KIT) - Institute for Nuclear and Energy Technologies (IKET). (2014). Tim Müller, Software V4.0 build (4224).

Engage and earn										
Kriterien	Video surv.	Video surv.	Intelling. v.	Intelling. v.	Security pe.	Security pe.	Police offic.	Police offic.	Access cont.	Mobile detector.
	0,054	0,143	0,149	0,160	0,167	0,179	0,179	0,179	0,167	0,160
☐ subjective effectiveness (poor-)										
☐ A police officer is present.	0,000	0,000	0,000	0,000	0,000	0,179	0,179	0,000	0,000	0,179
☐ The ticket is checked	0,000	0,000	0,000	0,116	0,116	0,000	0,000	0,116	0,116	0,000
☐ A security guard is present.	0,000	0,000	0,000	0,149	0,149	0,000	0,000	0,149	0,149	0,149
☐ Someone from security sp.	0,000	0,000	0,000	0,309	0,309	0,000	0,000	0,309	0,309	0,309
☐ A police officer speaks to th.	0,000	0,000	0,000	0,000	0,000	0,306	0,306	0,000	0,000	0,306
☐ Security dogs are present	0,000	0,000	0,000	0,000	0,000	0,433	0,433	0,000	0,000	0,000
☐ Customer is searched or p.	0,000	0,000	0,000	0,827	0,827	0,000	0,000	0,000	0,000	0,827
☐ Items on the customer's bo.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,838
☐ Contours of customer's bo.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ Customer luggage is sear.	0,000	0,000	0,000	0,768	0,768	0,768	0,768	0,000	0,000	0,768
☐ Customer's face is detected	0,843	0,843	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ Additional personal data is	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ Customer's face is digitally.	0,901	0,901	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ A motion profile is recorded	0,000	0,941	0,941	0,000	0,000	0,767	0,767	0,767	0,767	0,000
☐ Customer data is verified	0,000	0,000	0,000	0,767	0,767	0,767	0,767	0,767	0,767	0,000
☐ Customer's name is digital.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ Customer's face is digitally.	0,899	0,899	0,899	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ Customer's name is digital.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,908	0,000	0,000
☐ Noise increases	0,000	0,000	0,000	0,000	0,000	0,771	0,771	0,000	0,000	0,000
☐ The number of seating opt.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
☐ The amount of luggage is li.	0,000	0,000	0,000	0,761	0,761	0,000	0,000	0,000	0,000	0,761
☐ Registration is required an.	0,000	0,000	0,000	0,895	0,895	0,895	0,895	0,895	0,895	0,000
☐ The entire stay / time of trav.	0,000	0,000	0,000	0,000	0,000	0,794	0,794	0,643	0,643	0,556
☐ The preparation time is pro.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,589	0,589	0,589
☐ Objective effectiveness	0,004	0,001	0,188	0,050	0,025	0,595	0,150	0,004	0,001	0,025
☐ cost	0,079	207550,000	0,081	212550,000	0,158	416400,000	0,203	534950,000	832800,000	428820,000

Report MCDA Software

Overview

This report considers the task: To find the most suitable security measure, which reduce the risk of terrorist attacks (objective effectiveness), on the one hand, and is cost-efficient and accepted by customers, on the other hand.

MCDA: decision finding

The task proposes a number of six alternatives:

Police officers + K9 detection of explosive devices possible

Quality: 0.345857

Access control manual ticket inspection (service personnel)

Quality: 0.167529

Detectors metal/explosives /drugs

Quality: 0.160716

Security personnel moving around the station, ticket inspection possible, manual luggage control

Quality: 0.149561

Intelligent video surveillance behavior recognition = lost luggage alarm

Quality: 0.142823

Video surveillance live mode + recording

Quality 0.0643059

A number of **26** criteria are considered for evaluation.

1. **Technical/Objective Effectiveness of Security Measures** according to the chosen scenario - Importance: 0.333333
2. **Cost of the security measure** - Importance: 0.333333
3. **Non-Acceptance of Interference** Importance: 0.333333 **split into:**
 - Noise increases - Importance: 0.0138889
 - Customer's face is detected - Importance: 0.0138889
 - The number of seating options is limited by the measure - Importance: 0.0138889
 - Additional personal data is collected - Importance: 0.0138889

- A police officer speaks to the customer - Importance: 0.0138889
- Contours of customer's body are made visible - Importance: 0.0138889
- Items on the customer's body are made visible - Importance: 0.0138889
- Customer's face is digitally stored - Importance: 0.0138889
- Security dogs are present - Importance: 0.0138889
- A motion profile is recorded - Importance: 0.0138889
- Customer data is verified - Importance: 0.0138889
- A police officer is present in the train/on the platform - Importance: 0.0138889
- The ticket is checked - Importance: 0.0138889
- A security guard is present in the train/on the platform - Importance: 0.0138889
- Customer is searched or physically scanned – Importance: 0.0138889
- Someone from security speaks to the customer - Importance: 0.0138889
- Customer luggage is searched - Importance: 0.0138889
- Customer's name is digitally stored - Importance: 0.0138889
- Customer's face is digitally stored in combination with the location - Importance: 0.0138889
- Customer's name is digitally stored in combination with the location - Importance: 0.0138889
- The amount of luggage is limited (including bicycles) - Importance: 0.0138889
- Registration is required and travel itinerary specified - Importance: 0.0138889
- The entire stay / time of travel is extended - Importance: 0.0138889
- The preparation time is prolonged - Importance: 0.0138889

Summary

"*Police officers + K9*" is the best alternative. It has a clear margin. There are big differences between the alternatives. No criterion is dominating the solution. Some criteria dominate others.

Stability

The following criteria cause alternatives to change order:

- Objective effectiveness
- Cost
- Acceptance:
 - Items on the customer's body are made visible
 - Customer data is verified
 - Customer is searched or physically scanned
 - Customer luggage is searched
 - Customer's name is digitally stored in combination with the location
 - The amount of luggage is limited (including bicycles)
 - Registration is required and travel itinerary specified

The following criteria **do not** cause alternatives to change order:

- Noise increases
- Customer's face is detected
- The number of seating options is limited by the measure
- Additional personal data is collected
- A police officer speaks to the customer
- Contours of customer's body are made visible
- Customer's face is digitally stored
- Security dogs are present
- A motion profile is recorded
- A police officer is present in the train / on the platform
- The ticket is checked
- A security guard is present in the train / on the platform
- Someone from security speaks to the customer
- Customer's name is digitally stored
- Customer's face is digitally stored in combination with the location
- The entire stay / time of travel is extended
- The preparation time is prolonged